AWS Direct Connect

User Guide

API Version 2013-10-22

AWS Direct Connect: User Guide

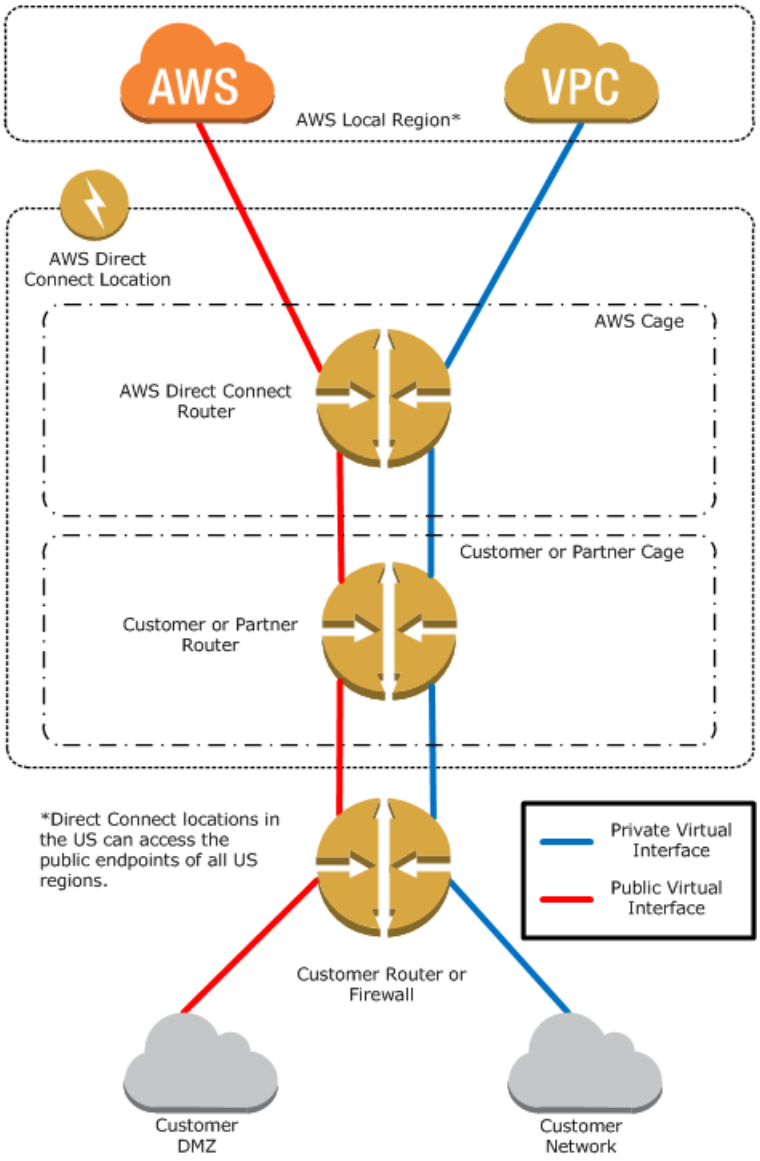
Table of Contents

What is AWS Direct Connect?

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to the AWS cloud (for example, to Amazon EC2 and Amazon S3) and to Amazon VPC, bypassing Internet service providers in your network path. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US).

AWS Direct Connect supports both the IPv4 and IPv6 communication protocols. You can configure your virtual interface for an IPv4 BGP peering session, an IPv6 BGP peering session, or both. However, not all AWS services support IPv6; check the service documentation to verify that IPv6 addressing is supported.

The following diagram shows how AWS Direct Connect interfaces with your network.



Requirements

To use AWS Direct Connect, your network must meet one of the following conditions:

- Your network is colocated with an existing AWS Direct Connect location. For more information about available AWS Direct Connect locations, see http://aws.amazon.com/directconnect/.
- You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). For a list of AWS Direct Connect partners who can help you connect, see http://aws.amazon.com/directconnect.
- You are working with an independent service provider to connect to AWS Direct Connect.

In addition, your network must meet the following conditions:

- Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet. Auto Negotiation for the port must be disabled. You must support 802.1Q VLANs across these connections.
- Your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication.
- Optionally, you can configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but will not take effect until you configure it on your router.

To connect to Amazon VPC, you must first do the following:

- Provide a private Autonomous System Number (ASN). Amazon allocates a private IPv4 address in the 169.x.x.x range to you.
- Create a virtual private gateway and attach it to your VPC. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the *Amazon VPC User Guide*.

To connect to public AWS products such as Amazon EC2 and Amazon S3, you need to provide the following:

- A public ASN that you own (preferred) or a private ASN. If you're adding a BGP peer to an existing virtual interface, the ASN must be private or already whitelisted for that virtual interface.
- For an IPv4 BGP session, public IPv4 addresses (/31 for each end of the BPG session). If you do not have public IPv4 addresses to assign to this connection, log on to AWS and then open a ticket with AWS Support.
- The public IPv4 routes or IPv6 routes that you will advertise over BGP. For IPv6 routes, you can specify a prefix length of /64 or shorter.

AWS Direct Connect Limits

The following table lists the limits related to AWS Direct Connect. Unless indicated otherwise, you can request an increase for any of these limits by using the AWS Direct Connect Limits form.

Component	Limit	Comments
Virtual interfaces per AWS Direct Connect connection	50	This limit can be increased upon request.
Active AWS Direct Connect connections per region per account	10	This limit can be increased upon request.
Routes per Border Gateway Protocol (BGP) session	100	This limit cannot be increased.

How Do I...?

How Do I...	Relevant Topics
Get a general product overview and information about pricing	AWS Direct Connect product information
Sign up for AWS Direct Connect and configure a connection	Getting Started at an AWS Direct Connect Location (p. 5)

How Do I...	Relevant Topics
Work with AWS Direct Connect connections	Working With AWS Direct Connect Connections (p. 35)
Calculate monthly costs	Pricing
Troubleshoot issues with AWS Direct Connect	Troubleshooting AWS Direct Connect (p. 58)

Getting Started with AWS Direct Connect

You can get started using AWS Direct Connect by choosing the scenario below that is appropriate for your environment.

Topics

Getting Started at an AWS Direct Connect Location

You can get started using AWS Direct Connect by completing the steps shown in the following table.

Step 1: Sign Up for Amazon Web Services

To use AWS Direct Connect, you need an AWS account if you don't already have one.

To sign up for an Amazon Web Services account

1. Open http://aws.amazon.com/, and then choose **Create an AWS Account**.

2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Step 2: Submit AWS Direct Connect Connection Request

You can submit a connection request using the AWS Direct Connect console. Provide the following information:

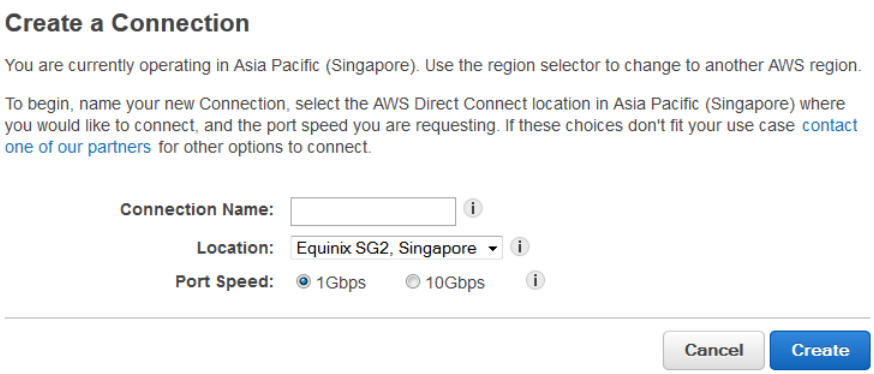
- Your contact information.
- The AWS Direct Connect location to which to connect.

  Work with a partner in the AWS Partner Network (APN) to help you establish network circuits between an AWS Direct Connect location and your data center, office, or colocation environment, or to provide colocation space within the same facility as the AWS Direct Connect location. APN partners supporting AWS Direct Connect also provide connections for less than 1G. For the list of AWS Direct Connect partners who belong to the AWS Partner Network (APN), go to http://aws.amazon.com/directconnect/partners.
- Whether you need the services of an AWS Direct Connect partner who is a member of the AWS Partner Network (APN).
- The port speed you require, either 1 Gbps or 10 Gbps. You cannot change the port speed after you've created the connection request. If you need to change the port speed, you must create and configure a new connection. For port speeds less than 1G, contact an APN partner who supports AWS Direct Connect.

  AWS Direct Connect supports two port speeds: 1 Gbps: 1000BASE-LX (1310nm) over single-mode fiber and 10 Gbps: 10GBASE-LR (1310nm) over single-mode fiber. Select a port speed compatible with your existing network.

To create a new AWS Direct Connect connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. Select the region that you would like to connect to AWS Direct Connect. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. On the **Welcome to AWS Direct Connect** screen, choose **Get Started with Direct Connect**.
4. In the **Create a Connection** dialog box, do the following:



   a. For **Connection Name**, enter a name for the connection.

b. For **Location**, select the appropriate AWS Direct Connect location.

Note
If you don't have equipment at an AWS Direct Connect location, choose **contact one of our partners**.

c. Select the appropriate port speed, and then choose **Create**.

Your connection is listed on the **Connections** pane of the AWS Direct Connect console.

Step 3: Download the LOA-CFA and Complete the Cross Connect

AWS will make a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) available to you to download, or email you with a request for more information after you've created the connection request. If you receive a request for more information, you must respond within 7 days or the connection will be deleted. The LOA-CFA is the authorization to connect to AWS, and is required by the colocation provider to establish the connection.

To download the LOA-CFA

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the navigation pane, choose **Connections**.
3. Choose the arrow next to your connection to expand its details.
4. Choose **Download LOA-CFA**.

   Note
   If the link is not enabled, the LOA-CFA is not yet available for you to download. Check your email for a request for more information. If it's still unavailable, or you haven't received an email after 72 hours, contact AWS Support.
5. In the dialog box, optionally enter the name of your provider if you want it to appear with your company name as the requester in the LOA-CFA. Choose **Download**. The LOA-CFA is downloaded to your computer as a PDF file.

After you download the LOA-CFA, follow these steps to establish the dedicated connection:

1. Contact the colocation provider to request a cross-network connection. This is frequently referred to as a *cross connect*.
   - You must be a customer of the colocation provider, and you must present them with the LOA-CFA that authorizes the connection to the AWS router.
   - The contact process can vary for each colocation provider. For more information about each AWS Direct Connect location, see Requesting Cross Connects at AWS Direct Connect Locations (p. 44).
2. Give the colocation provider the necessary information to connect to your network. The diagram in What is AWS Direct Connect? (p. 1) shows various placement options. You should verify that your equipment meets the specifications set out in Requirements (p. 2).

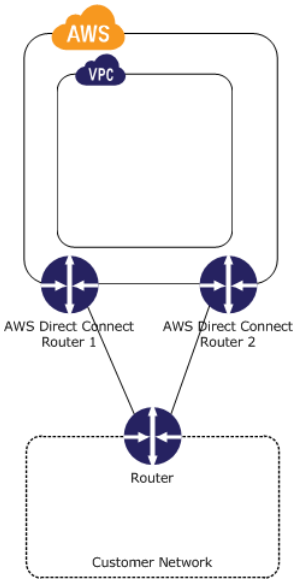
The LOA-CFA expires after 90 days. If your connection is not up after 90 days, we'll send you an email alerting you that the LOA-CFA has expired. To refresh the LOA-CFA with a new issue date, you can download it again from the AWS Direct Connect console. If you do not take any action, we will delete the connection.

Note
Port-hour billing starts 90 days after you created the connection, or after the connection between your router and the AWS router is established, whichever comes first. For more

information, see AWS Direct Connect Pricing. If you no longer want the connection after you've reissued the LOA-CFA, you must delete the connection yourself. For more information, see Delete a Connection (p. 35).

(Optional) Step 4: Configure Redundant Connections with AWS Direct Connect

To provide for failover, we recommend that you request and configure two dedicated connections to AWS as shown in the following figure. These connections can terminate on one or two routers in your network.



There are different configuration choices available when you provision two dedicated connections:

- Active/Active (BGP multipath). Both connections are active to handle traffic. If one connection becomes unavailable, all traffic is routed through the other connection. This multipath arrangement does not load balance traffic between the AWS router and the customer's router. This is the default configuration.
- Active/Passive (failover). One connection is handling traffic, and the other is on standby. If the active connection becomes unavailable, all traffic is routed through the passive connection. You will need to AS path prepend the routes on one of your links for it to be the passive link.

How you configure the connections doesn't affect redundancy, but it does affect the policies that determine how your data is routed over both connections. We recommend that you configure both connections as active. You'll configure your BGP information in "Step 5: Create a Virtual Interface", below.

Step 5: Create a Virtual Interface

The next step is to provision your virtual interfaces. Each virtual interface must be tagged with a customer-provided tag that complies with the Ethernet 802.1Q standard. This tag is required for any traffic traversing the AWS Direct Connect connection. You can provision virtual interface (VLAN) connections to the AWS Cloud, Amazon VPC, or both. To begin using your virtual interface, you need to advertise at least one prefix using BGP, up to a maximum of 100 prefixes.

We advertise appropriate Amazon prefixes to you so you can reach either your VPCs or other AWS products. You can access all Amazon Web Services prefixes in your region through this connection; for example, Amazon EC2, Amazon S3, and Amazon.com. You do not have access to non-Amazon prefixes or prefixes outside of your region. For the current list of IP prefixes advertised on AWS Direct Connect public connections, see the list in the AWS Direct Connect Discussion Forum.

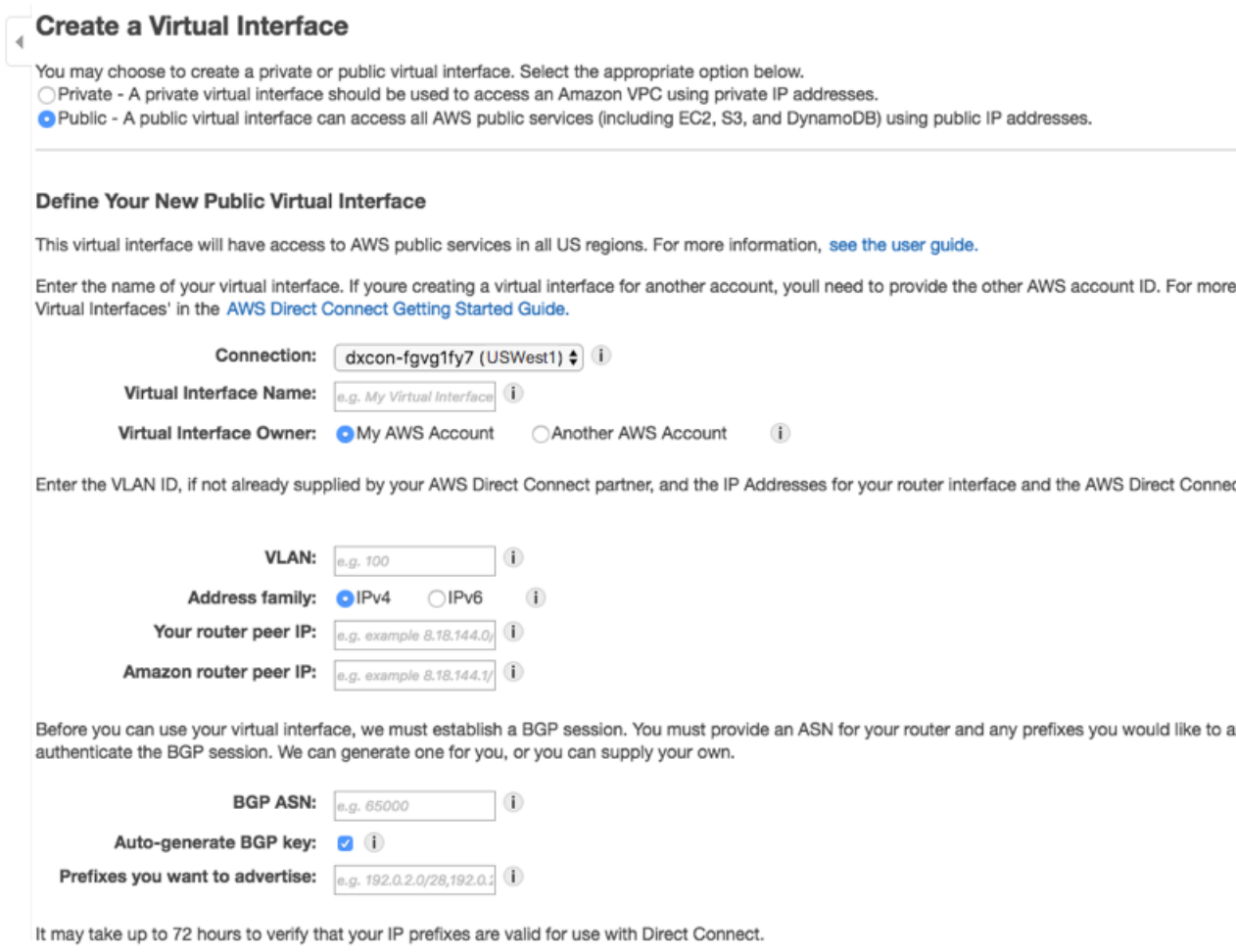
To connect to other AWS services using IPv6 addresses, you can configure the BGP session for your virtual interface to use IPv6. However, not all AWS services support IPv6; check the service documentation to verify that IPv6 addressing is supported. You cannot specify your own peer IPv6 addresses for the BGP peering session. Amazon automatically allocates you a /125 IPv6 CIDR.

To provision a virtual interface connection to non-VPC services

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to connect to AWS Direct Connect. Public virtual interfaces are used by services such as Amazon S3 and Amazon Glacier that aren't in a VPC. Before you begin, you need the following information:

- A new, unused VLAN tag that you select.
- A public or private Border Gateway Protocol (BGP) Autonomous System Number (ASN). If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range. Autonomous System (AS) prepending will not work if you use a private ASN.
- For IPv4, a unique IPv4 CIDR for your interface IP addresses that does not overlap another IPv4 CIDR announced via AWS Direct Connect.
- For IPv4, a unique IPv4 CIDR range to announce via AWS Direct Connect that does not overlap another IPv4 CIDR announced via AWS Direct Connect.

1. Verify that the VLAN is not already in use on this AWS Direct Connect connection for another virtual interface.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use, and then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, choose **Public**.



5. In the **Define Your New Public Virtual Interface** dialog box, do the following:

   a. For **Connection**, select an existing physical connection on which to create the virtual interface.

   b. For **Virtual Interface Name**, enter a name for the virtual interface.

   c. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.

   d. For **VLAN** , enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - For **Your router peer IP**, enter the IPv4 CIDR destination address where traffic should be sent.
      - For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select the **Auto-generate BGP key** check box to have AWS generate a BGP key.

      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then for **BGP Authentication Key**, enter your BGP MD5 key.

   i. For **Prefixes you want to advertise**, enter the IPv4 CIDR destination addresses (separated by commas) where traffic should be routed to you over the virtual interface.

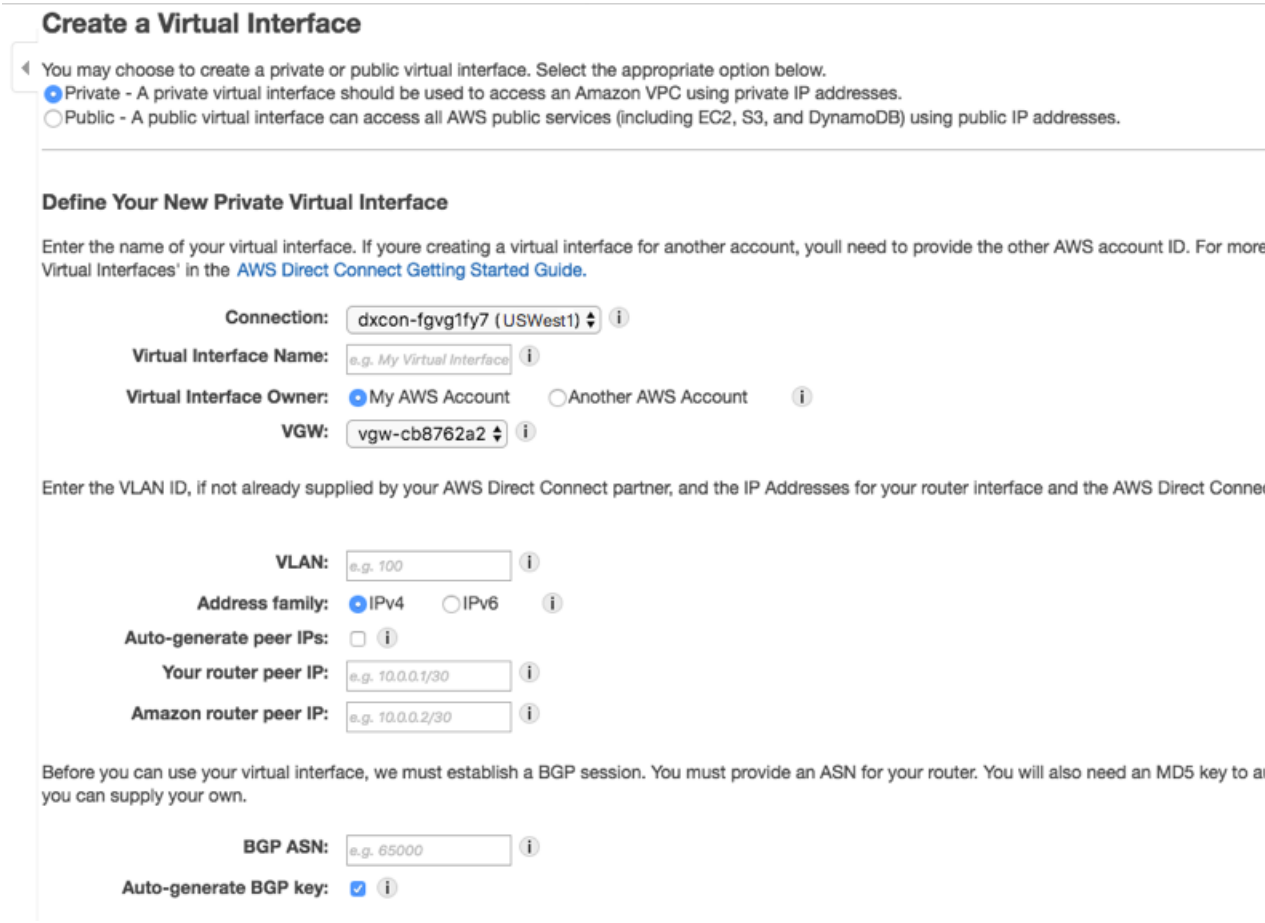
6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 13).

To provision a private virtual interface to a VPC

After you have placed an order for an AWS Direct Connect connection, you can create a virtual interface to use to connect to AWS Direct Connect. When you create a private virtual interface to a VPC, you'll need a private virtual interface for each VPC you want to connect to (e.g., You'll need three private virtual interfaces to connect to three VPCs). Before you begin, you need the following additional information:

- A new, unused VLAN tag that you select.
- A public or private BGP ASN. If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range.
- The network prefixes to advertise. Any advertised prefix must include only your ASN in the BGP AS-PATH.
- The virtual private gateway to which to connect. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the *Amazon VPC User Guide*.

1. Verify that the VLAN is not already in use on this connection.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use and choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, select **Private**.



5. Under **Define Your New Private Virtual Interface**, do the following:

   a. For **Virtual Interface Name**, enter a name for the virtual interface.

   b. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.

   c. For **VGW**, select the virtual gateway to which to connect.

   d. For **VLAN**, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
      - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box, and then for **Your router peer IP**, enter the destination IPv4 CIDR address that Amazon should send traffic to. In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select the **Auto-generate BGP key** check box to have AWS generate a BGP key.

      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then for **BGP Authentication Key**, enter your BGP MD5 key.

6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 13).

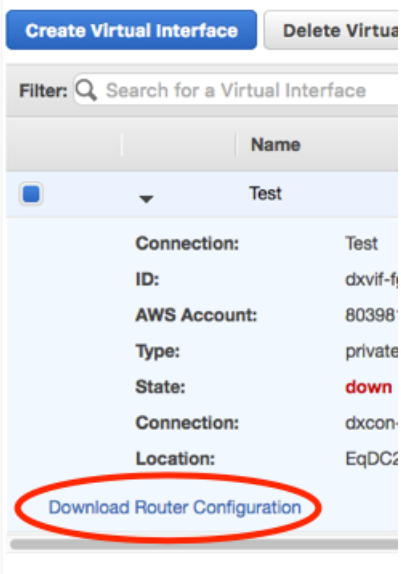
   Note
   If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation. For more information, see Enable Route Propagation in Your Route Table in the *Amazon VPC User Guide*.

Step 6: Download Router Configuration

After you have created a virtual interface for your AWS Direct Connect connection, you can download the router configuration file.

To download router configuration

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the **Virtual Interfaces** pane, select a virtual interface, choose the arrow to show more details, and then choose **Download Router Configuration**.



3. In the **Download Router Configuration** dialog box, do the following:
   a. For **Vendor**, select the manufacturer of your router.
   b. For **Platform**, select the model of your router.
   c. For **Software**, select the software version for your router.
4. Choose **Download**, and then use the appropriate configuration for your router to ensure that you can connect to AWS Direct Connect:

   Cisco IOS

```
interface GigabitEthernet0/1
no ip address

interface GigabitEthernet0/1.VLAN_NUMBER
description "Direct Connect to your Amazon VPC or AWS Cloud"
encapsulation dot1Q VLAN_NUMBER
ip address YOUR_PEER_IP
```

```
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
neighbor AWS_PEER_IP password MD5_key
network 0.0.0.0
exit

! Optionally configure Bidirectional Forwarding Detection (BFD).

interface GigabitEthernet0/1.VLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP fall-over bfd
```

Cisco NX-OS

```
feature interface-vlan
vlan VLAN_NUMBER
name "Direct Connect to your Amazon VPC or AWS Cloud"

interface VlanVLAN_NUMBER
  ip address YOUR_PEER_IP/30
  no shutdown

interface Ethernet0/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan VLAN_NUMBER
  no shutdown

router bgp CUSTOMER_BGP_ASN
  address-family ipv4 unicast
    network 0.0.0.0
  neighbor AWS_PEER_IP remote-as 7224
    password 0 MD5_key
    address-family ipv4 unicast

! Optionally configure Bidirectional Forwarding Detection (BFD).

feature bfd
interface VlanVLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
bfd
```

Juniper JunOS

```
configure exclusive
edit interfaces ge-0/0/1
set description "Direct Connect to your Amazon VPC or AWS Cloud"
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_NUMBER
set family inet mtu 1500
set family inet address YOUR_PEER_IP
```

```
top

edit policy-options policy-statement EXPORT-DEFAULT
edit term DEFAULT
set from route-filter 0.0.0.0/0 exact
set then accept
up
edit term REJECT
set then reject
top

set routing-options autonomous-system CUSTOMER_BGP_ASN

edit protocols bgp group EBGP
set type external
set peer-as 7224

edit neighbor AWS_PEER_IP
set local-address YOUR_PEER_IP
set export EXPORT-DEFAULT
set authentication-key "MD5_key"
top
commit check
commit and-quit

# Optionally configure Bidirectional Forwarding Detection (BFD).

set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 minimum-interval 300
set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 multiplier 3
```

Step 7: Verify Your Virtual Interface

After you have established virtual interfaces to the AWS cloud or to Amazon VPC, you can verify your AWS Direct Connect connections using the following procedures.

To verify your virtual interface connection to the AWS cloud

- Run `traceroute` and verify that the AWS Direct Connect identifier is in the network trace.

To verify your virtual interface connection to Amazon VPC

1. Using a pingable AMI, such as one of the Amazon Linux AMIs, launch an EC2 instance into the VPC that is attached to your virtual private gateway. The Amazon Linux AMIs are available in the **Quick Start** tab when you use the instance launch wizard in the Amazon EC2 console. For more information, see Launch an Amazon EC2 Instance in the *Amazon EC2 User Guide for Linux Instances*. Ensure that the security group that's associated with the instance includes a rule permitting inbound ICMP traffic (for the ping request).
2. After the instance is running, get its private IP address (for example, 10.0.0.4). The Amazon EC2 console displays the address as part of the instance details.
3. Ping the private IP address and get a response.

Getting Started with a Partner or Network Carrier

If you don't have equipment hosted in the same facility as AWS Direct Connect, you can use a network provider to connect to AWS Direct Connect. The provider does not have to be a member of the Amazon Partner Network (APN) partner to connect you. You can get started using a network provider to connect to AWS Direct Connect by completing the steps shown in the following table.

Step 1: Sign Up for Amazon Web Services

To use AWS Direct Connect, you need an AWS account if you don't already have one.

To sign up for an Amazon Web Services account

1. Open http://aws.amazon.com/, and then choose **Create an AWS Account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Step 2: Submit AWS Direct Connect Connection Request

You can submit a connection request using the AWS Direct Connect console. You need to provide the following information:

- Your contact information.
- The AWS Direct Connect location to which to connect.

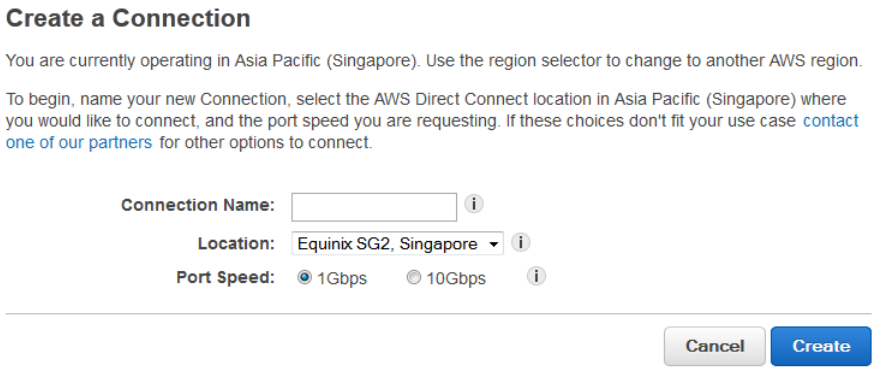
  Work with a partner in the AWS Partner Network (APN) to help you establish network circuits between an AWS Direct Connect location and your data center, office, or colocation environment, or to provide colocation space within the same facility as the AWS Direct Connect location. APN partners supporting AWS Direct Connect also provide connections for less than 1G. For the list of AWS Direct Connect partners who belong to the AWS Partner Network (APN), go to http://aws.amazon.com/directconnect/partners.
- Whether you need the services of an AWS Direct Connect partner who is a member of the AWS Partner Network (APN).
- The port speed you require, either 1 Gbps or 10 Gbps. You cannot change the port speed after you've created the connection request. If you need to change the port speed, you must create and

configure a new connection. For port speeds less than 1G, contact an APN partner who supports AWS Direct Connect.

AWS Direct Connect supports two port speeds: 1 Gbps: 1000BASE-LX (1310nm) over single-mode fiber and 10 Gbps: 10GBASE-LR (1310nm) over single-mode fiber. Select a port speed compatible with your existing network.

To create a new AWS Direct Connect connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. Select the region that you would like to connect to AWS Direct Connect. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. On the **Welcome to AWS Direct Connect** screen, choose **Get Started with Direct Connect**.
4. In the **Create a Connection** dialog box, do the following:



   a. For **Connection Name**, enter a name for the connection.
   b. For **Location**, select the appropriate AWS Direct Connect location.

      Note
      If you don't have equipment at an AWS Direct Connect location, choose **contact one of our partners**.

   c. Select the appropriate port speed, and then choose **Create**.

   Your connection is listed on the **Connections** pane of the AWS Direct Connect console.

Step 3: Download the LOA-CFA and Request a Cross Connect from Your Network Provider

AWS will make a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) available to you to download, or email you with a request for more information after you've created the connection request. If you receive a request for more information, you must respond within 7 days or the connection will be deleted. The LOA-CFA is the authorization to connect to AWS, and is required by your network provider to establish the connection.

To download the LOA-CFA

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the navigation pane, choose **Connections**.
3. Choose the arrow next to your connection to expand its details.
4. Choose **Download LOA-CFA**.

Note
If the link is not enabled, the LOA-CFA is not yet available for you to download. Check your email for a request for more information. If it's still unavailable, or you haven't received an email after 72 hours, contact AWS Support.

5. In the dialog box, optionally enter the name of your provider if you want it to appear with your company name as the requester in the LOA-CFA. Choose **Download**. The LOA-CFA is downloaded to your computer as a PDF file.

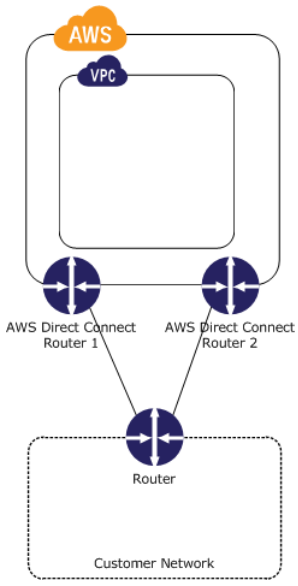
After you've downloaded the LOA-CFA, send it to your network provider so they can order a cross connect for you. You will not be able to order a cross connect for yourself in the AWS Direct Connect location if you do not have equipment there. Your network provider will have to do this for you.

The LOA-CFA expires after 90 days. If your connection is not up after 90 days, we'll send you an email alerting you that the LOA-CFA has expired. To refresh the LOA-CFA with a new issue date, you can download it again from the AWS Direct Connect console. If you do not take any action, we will delete the connection.

Note
Port-hour billing starts 90 days after you created the connection, or after the connection between your router and the AWS router is established, whichever comes first. For more information, see AWS Direct Connect Pricing. If you no longer want the connection after you've reissued the LOA-CFA, you must delete the connection yourself. For more information, see Delete a Connection (p. 35).

(optional) Step 4: Configure Redundant Connections with AWS Direct Connect

To provide for failover, we recommend that you request and configure two dedicated connections to AWS as shown in the following figure. These connections can terminate on one or two routers in your network.



There are different configuration choices available when you provision two dedicated connections:

- Active/Active (BGP multipath). Both connections are active to handle traffic. If one connection becomes unavailable, all traffic is routed through the other connection. This multipath arrangement

does not load balance traffic between the AWS router and the customer's router. This is the default configuration.

- Active/Passive (failover). One connection is handling traffic, and the other is on standby. If the active connection becomes unavailable, all traffic is routed through the passive connection.

How you configure the connections doesn't affect redundancy, but it does affect the policies that determine how your data is routed over both connections. We recommend that you configure both connections as active.

Step 5: Create a Virtual Interface

The next step is to provision your virtual interfaces. Each virtual interface must be tagged with a customer-provided tag that complies with the Ethernet 802.1Q standard. This tag is required for any traffic traversing the AWS Direct Connect connection. You can provision virtual interface (VLAN) connections to the AWS Cloud, Amazon VPC, or both. To begin using your virtual interface, you need to advertise at least one prefix using BGP, up to a maximum of 100 prefixes.

We advertise appropriate Amazon prefixes to you so you can reach either your VPCs or other AWS products. You can access all Amazon Web Services prefixes in your region through this connection; for example, Amazon EC2, Amazon S3, and Amazon.com. You do not have access to non-Amazon prefixes or prefixes outside of your region. For the current list of IP prefixes advertised on AWS Direct Connect public connections, see the list in the AWS Direct Connect Discussion Forum.

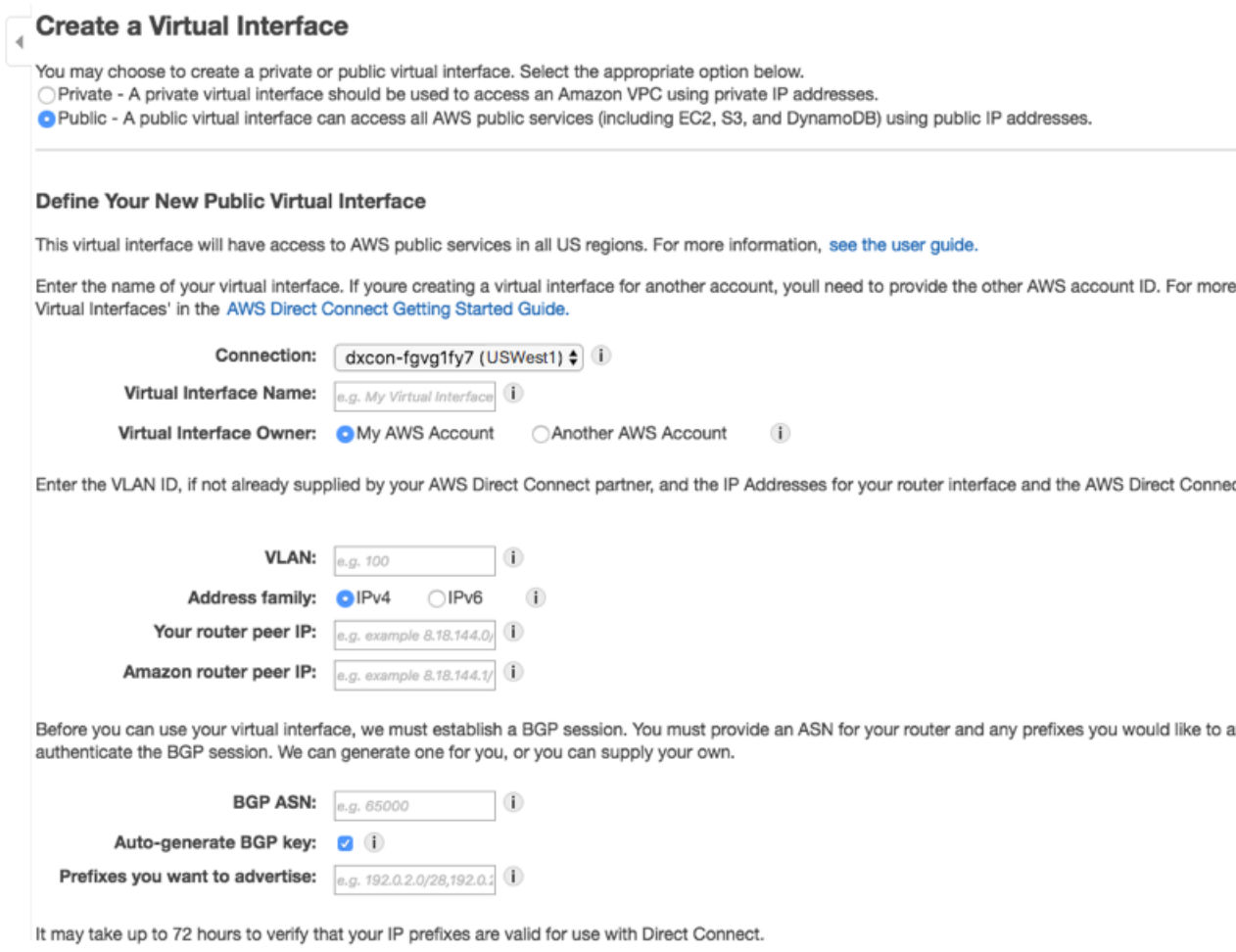
To connect to other AWS services using IPv6 addresses, you can configure the BGP session for your virtual interface to use IPv6. However, not all AWS services support IPv6; check the service documentation to verify that IPv6 addressing is supported. You cannot specify your own peer IPv6 addresses for the BGP peering session. Amazon automatically allocates you a /125 IPv6 CIDR.

To provision a virtual interface connection to non-VPC services

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to connect to AWS Direct Connect. Public virtual interfaces are used by services such as Amazon S3 and Amazon Glacier that aren't in a VPC. Before you begin, you need the following information:

- A new, unused VLAN tag that you select.
- A public or private Border Gateway Protocol (BGP) Autonomous System Number (ASN). If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range. Autonomous System (AS) prepending will not work if you use a private ASN.
- For IPv4, a unique IPv4 CIDR for your interface IP addresses that does not overlap another IPv4 CIDR announced via AWS Direct Connect.
- For IPv4, a unique IPv4 CIDR range to announce via AWS Direct Connect that does not overlap another IPv4 CIDR announced via AWS Direct Connect.

1. Verify that the VLAN is not already in use on this AWS Direct Connect connection for another virtual interface.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use, and then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, choose **Public**.



5. In the **Define Your New Public Virtual Interface** dialog box, do the following:

   a. For **Connection**, select an existing physical connection on which to create the virtual interface.

   b. For **Virtual Interface Name**, enter a name for the virtual interface.

   c. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.

   d. For **VLAN**, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - For **Your router peer IP**, enter the IPv4 CIDR destination address where traffic should be sent.
      - For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select the **Auto-generate BGP key** check box to have AWS generate a BGP key.

      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then for **BGP Authentication Key**, enter your BGP MD5 key.

   i. For **Prefixes you want to advertise**, enter the IPv4 CIDR destination addresses (separated by commas) where traffic should be routed to you over the virtual interface.

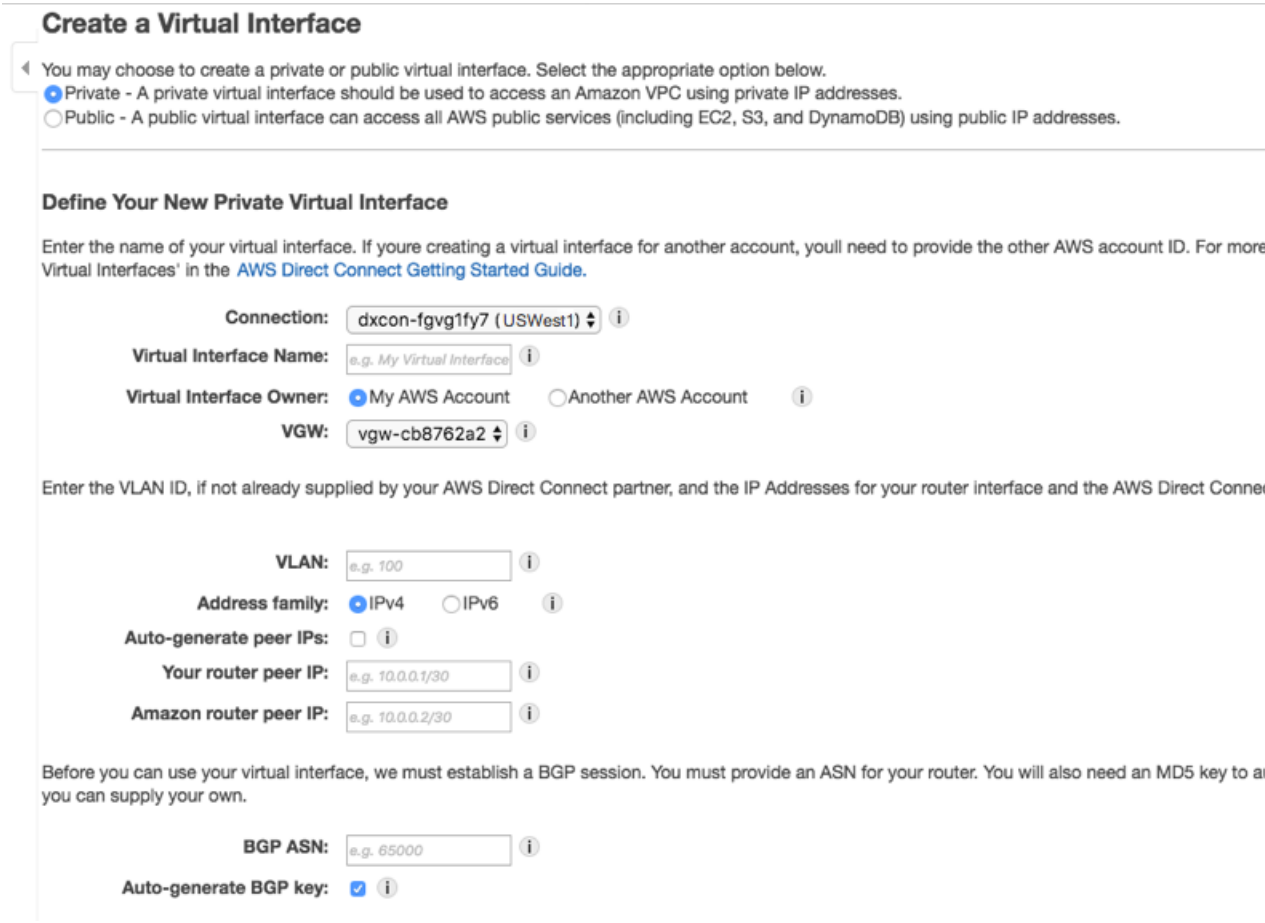
6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 23).

To provision a private virtual interface to a VPC

After you have placed an order for an AWS Direct Connect connection, you can create a virtual interface to use to connect to AWS Direct Connect. When you create a private virtual interface to a VPC, you'll need a private virtual interface for each VPC to which to connect to (e.g., you'll need three private virtual interfaces to connect to three VPCs). Before you begin, you need the following additional information:

- A new, unused VLAN tag that you select.
- A public or private BGP ASN. If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range.
- The network prefixes to advertise. Any advertised prefix must include only your ASN in the BGP AS-PATH.
- The virtual private gateway to which to connect. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the *Amazon VPC User Guide*.

1. Verify that the VLAN is not already in use on this connection.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use, and then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, choose **Private**.



5. Under **Define Your New Private Virtual Interface**, do the following:

   a. For **Virtual Interface Name**, enter a name for the virtual interface.

   b. For **Virtual Interface Owner**, choose the **My AWS Account** option if the virtual interface is for your AWS account ID.

   c. For **VGW**, select the virtual gateway to connect to.

   d. For **VLAN #**, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
      - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box, and then for **Your router peer IP**, enter the destination IPv4 CIDR address that Amazon should send traffic to. For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select the **Auto-generate BGP key** check box to have AWS generate a BGP key.

      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then for **BGP Authentication Key**, enter your BGP MD5 key.

6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 23).

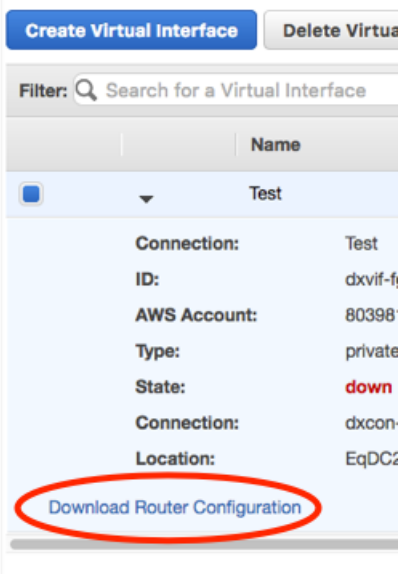
   Note
   If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation. For more information, see Enable Route Propagation in Your Route Table in the *Amazon VPC User Guide*.

Step 6: Download Router Configuration

After you have created a virtual interface for your AWS Direct Connect connection, you can download the router configuration file.

To download router configuration

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the **Virtual Interfaces** pane, select a virtual interface, choose the arrow to show more details, and then choose **Download Router Configuration**.



3. In the **Download Router Configuration** dialog box, do the following:
   a. For **Vendor**, select the manufacturer of your router.
   b. For **Platform**, select the model of your router.
   c. For **Software**, select the software version for your router.
4. Choose **Download**, and then use the appropriate configuration for your router to ensure that you can connect to AWS Direct Connect:

   Cisco IOS

```
interface GigabitEthernet0/1
no ip address

interface GigabitEthernet0/1.VLAN_NUMBER
description "Direct Connect to your Amazon VPC or AWS Cloud"
encapsulation dot1Q VLAN_NUMBER
ip address YOUR_PEER_IP
```

```
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
neighbor AWS_PEER_IP password MD5_key
network 0.0.0.0
exit

! Optionally configure Bidirectional Forwarding Detection (BFD).

interface GigabitEthernet0/1.VLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP fall-over bfd
```

Cisco NX-OS

```
feature interface-vlan
vlan VLAN_NUMBER
name "Direct Connect to your Amazon VPC or AWS Cloud"

interface VlanVLAN_NUMBER
  ip address YOUR_PEER_IP/30
  no shutdown

interface Ethernet0/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan VLAN_NUMBER
  no shutdown

router bgp CUSTOMER_BGP_ASN
  address-family ipv4 unicast
    network 0.0.0.0
  neighbor AWS_PEER_IP remote-as 7224
    password 0 MD5_key
    address-family ipv4 unicast

! Optionally configure Bidirectional Forwarding Detection (BFD).

feature bfd
interface VlanVLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
bfd
```

Juniper JunOS

```
configure exclusive
edit interfaces ge-0/0/1
set description "Direct Connect to your Amazon VPC or AWS Cloud"
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_NUMBER
set family inet mtu 1500
set family inet address YOUR_PEER_IP
```

```
top

edit policy-options policy-statement EXPORT-DEFAULT
edit term DEFAULT
set from route-filter 0.0.0.0/0 exact
set then accept
up
edit term REJECT
set then reject
top

set routing-options autonomous-system CUSTOMER_BGP_ASN

edit protocols bgp group EBGP
set type external
set peer-as 7224

edit neighbor AWS_PEER_IP
set local-address YOUR_PEER_IP
set export EXPORT-DEFAULT
set authentication-key "MD5_key"
top
commit check
commit and-quit

# Optionally configure Bidirectional Forwarding Detection (BFD).

set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 minimum-interval 300
set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 multiplier 3
```

Step 7: Verify Your Virtual Interface

After you have established virtual interfaces to the AWS cloud or to Amazon VPC, you can verify your AWS Direct Connect connections using the following procedures.

To verify your virtual interface connection to the AWS cloud

- Run `traceroute` and verify that the AWS Direct Connect identifier is in the network trace.

To verify your virtual interface connection to Amazon VPC

1. Using a pingable AMI, such as one of the Amazon Linux AMIs, launch an EC2 instance into the VPC that is attached to your virtual private gateway. The Amazon Linux AMIs are available in the **Quick Start** tab when you use the instance launch wizard in the Amazon EC2 console. For more information, see Launch an Amazon EC2 Instance in the *Amazon EC2 User Guide for Linux Instances*. Ensure that the security group that's associated with the instance includes a rule permitting inbound ICMP traffic (for the ping request).
2. After the instance is running, get its private IP address (for example, 10.0.0.4). The Amazon EC2 console displays the address as part of the instance details.
3. Ping the private IP address and get a response.

Getting Started with a Sub-1G AWS Direct Connect Partner

If you want to purchase a sub-1G connection through a partner, follow the steps listed in the table below.

Note
A sub-1G connection only supports one virtual interface.

Step 1: Sign Up for Amazon Web Services

To use AWS Direct Connect, you need an AWS account if you don't already have one.

To sign up for an Amazon Web Services account

1. Open http://aws.amazon.com/, and then choose **Create an AWS Account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Step 2: Request a sub-1G connection from an APN Partner supporting AWS Direct Connect

You must request a sub-1G connection from an APN partner. You cannot order Sub-1G services from the AWS Direct Connect console. For a list of APN partners that support AWS Direct Connect, see APN Partners supporting AWS Direct Connect.

Your partner will create a hosted connection for you, and it will appear in your AWS Direct Connect console.

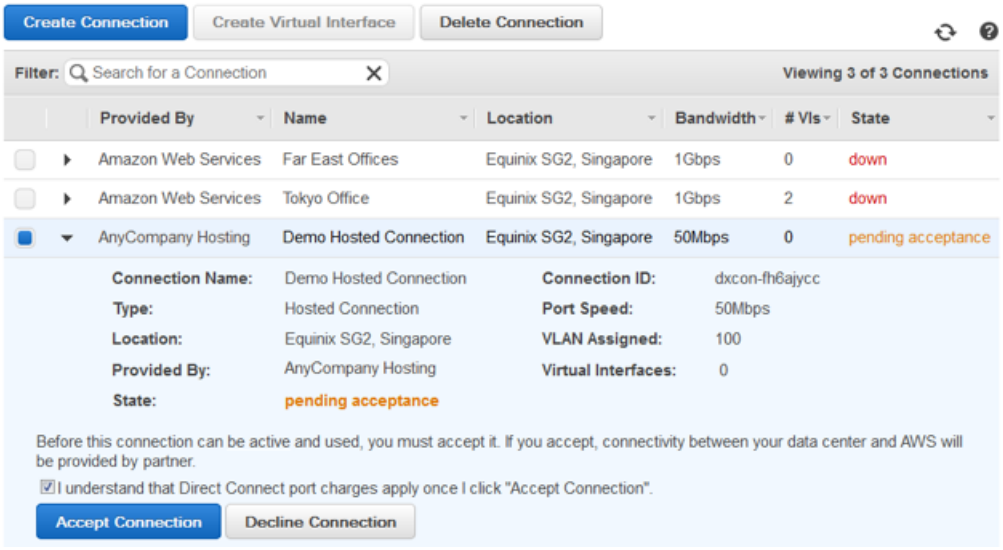
Step 3: Accept Your Hosted Connection

Your selected partner will create a hosted connection for you. You will need to accept it in the AWS Direct Connect console before you can create a virtual interface.

To accept a hosted connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.

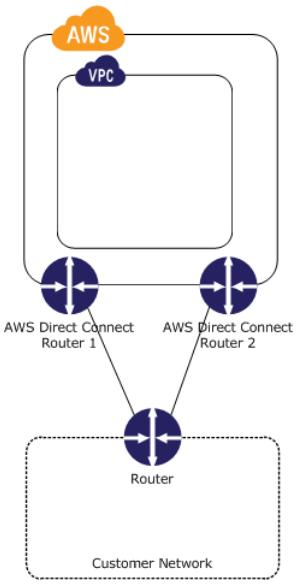
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select a connection, and then choose the arrow to expand details about the connection.



5. Select **I understand that Direct Connect port charges apply once I click "Accept This Connection"**, and then choose **Accept Connection**.

(optional) Step 4: Configure Redundant Connections with AWS Direct Connect

To provide for failover, we recommend that you request and configure two dedicated connections to AWS as shown in the following figure. These connections can terminate on one or two routers in your network.



There are different configuration choices available when you provision two dedicated connections:

- Active/Active (BGP multipath). Both connections are active to handle traffic. If one connection becomes unavailable, all traffic is routed through the other connection. This multipath arrangement does not load balance traffic between the AWS router and the customer's router. This is the default configuration.
- Active/Passive (failover). One connection is handling traffic, and the other is on standby. If the active connection becomes unavailable, all traffic is routed through the passive connection.

How you configure the connections doesn't affect redundancy, but it does affect the policies that determine how your data is routed over both connections. We recommend that you configure both connections as active. AWS will treat return traffic on those links as Active/Active.

Step 5: Create a Virtual Interface

The next step is to provision your virtual interface. You can only create a single virtual interface on a hosted connection. You can provision a virtual interface (VLAN) connection to the public AWS Cloud or to Amazon VPC. To begin using your virtual interface, you need to advertise at least one prefix using BGP, up to a maximum of 100 prefixes.

We advertise appropriate Amazon prefixes to you so you can reach either your VPCs or other AWS products. You can access all Amazon Web Services prefixes in your region through this connection; for example, Amazon EC2, Amazon S3, and Amazon.com. You do not have access to non-Amazon prefixes or prefixes outside of your region. For the current list of IP prefixes advertised on AWS Direct Connect public connections, see the list in the AWS Direct Connect Discussion Forum.

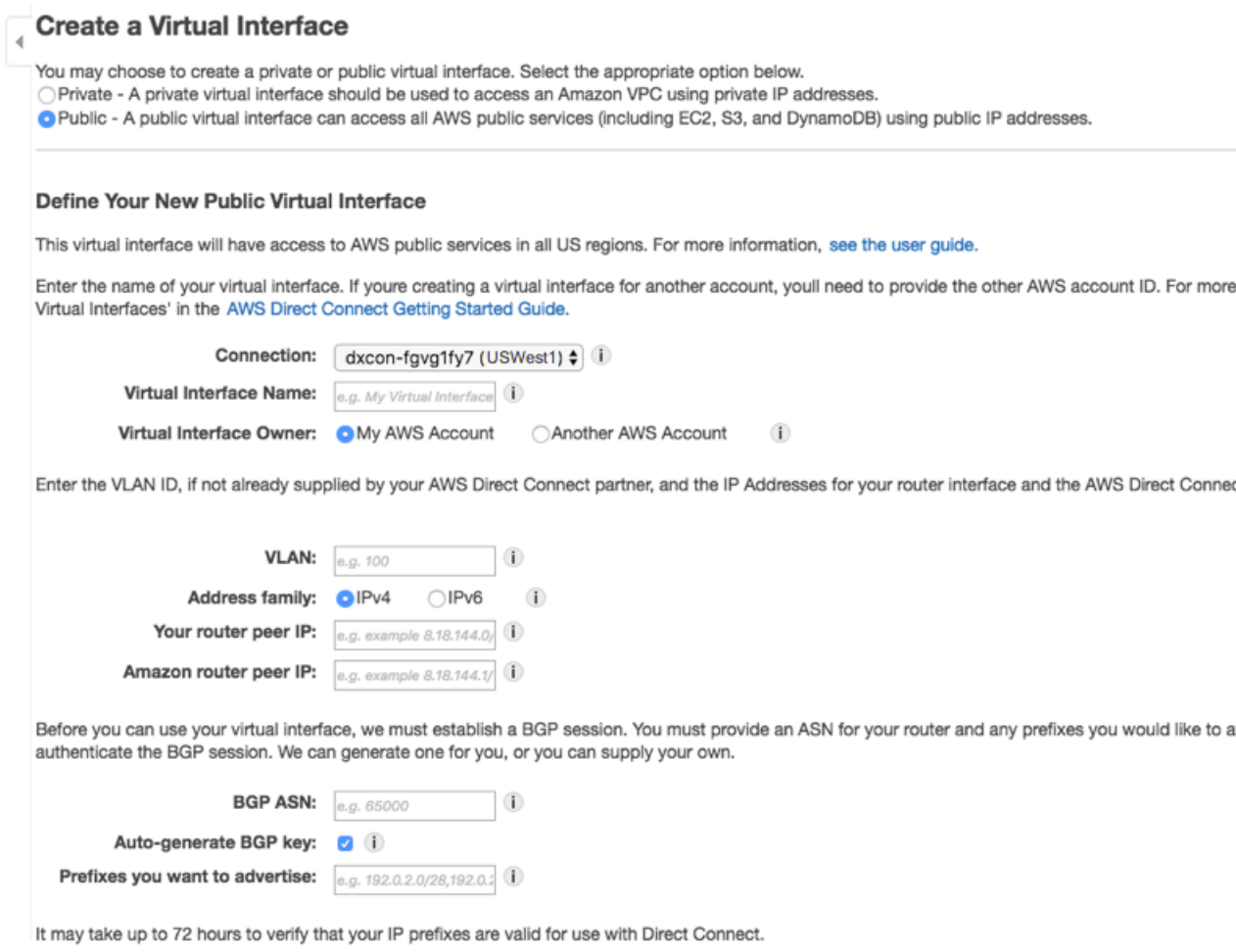
To connect to other AWS services using IPv6 addresses, you can configure the BGP session for your virtual interface to use IPv6. However, not all AWS services support IPv6; check the service documentation to verify that IPv6 addressing is supported. You cannot specify your own peer IPv6 addresses for the BGP peering session. Amazon automatically allocates you a /125 IPv6 CIDR.

To provision a public virtual interface connection to non-VPC services

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to connect to AWS Direct Connect. Public virtual interfaces are used by services such as Amazon S3 and Amazon Glacier that aren't in a VPC. Before you begin, you need the following information:

- A new, unused VLAN tag that you select.
- A public or private Border Gateway Protocol (BGP) Autonomous System Number (ASN). If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range. Autonomous System (AS) prepending will not work if you use a private ASN.
- For IPv4, a unique IPv4 CIDR for your interface IP addresses that does not overlap another IPv4 CIDR announced via AWS Direct Connect.
- For IPv4, a unique CIDR range to announce via AWS Direct Connect that does not overlap another IPv4 CIDR announced via AWS Direct Connect.

1. Verify that the VLAN is not already in use on this AWS Direct Connect connection for another virtual interface.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use, and then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, select **Public**.



5. In the **Define Your New Public Virtual Interface** dialog box, do the following:

   a. In the **Connection** field, select an existing physical connection on which to create the virtual interface.

   b. In the **Virtual Interface Name** field, enter a name for the virtual interface.

   c. In **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.

   d. The **VLAN** field will already be filled in and grayed out.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - In the **Your router peer IP** field, enter the IPv4 CIDR destination address where traffic should be sent.
      - In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. In the **BGP ASN** field, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select **Auto-generate BGP key** check box to have AWS generate one.

To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then in the **BGP Authentication Key** field, enter your BGP MD5 key.

i. In the **Prefixes you want to advertise** field, enter the IPv4 CIDR destination addresses (separated by commas) where traffic should be routed to you over the virtual interface.

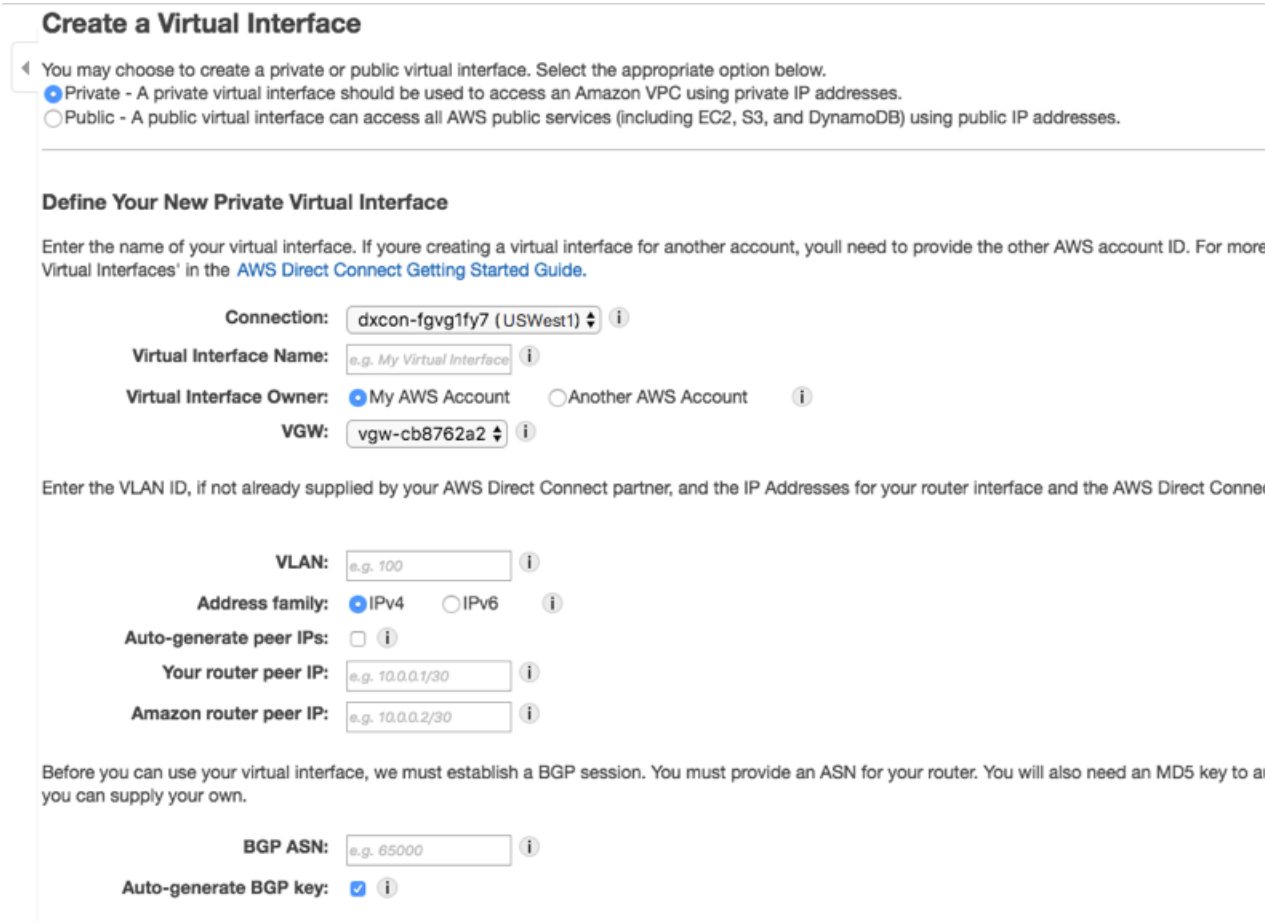
6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 32).

To provision a private virtual interface to a VPC

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to use to connect to AWS Direct Connect. When you create a private virtual interface to a VPC, you'll need a private virtual interface for each VPC you want to connect to (e.g., You'll need three private virtual interfaces to connect to three VPCs). Before you begin, you need the following additional information:

- A new, unused VLAN tag that you select.
- A public or private BGP ASN. If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range.
- The network prefixes to advertise. Any advertised prefix must include only your ASN in the BGP AS-PATH.
- The virtual private gateway to connect to. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the *Amazon VPC User Guide*.

1. Verify that the VLAN is not already in use on this connection.
2. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
3. In the **Connections** pane, select the connection to use, and then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, select **Private**.



5. Under **Define Your New Private Virtual Interface**, do the following:

   a. In the **Virtual Interface Name** field, enter a name for the virtual interface.

   b. In **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.

   c. In the **VGW** list, select the virtual gateway to connect to.

   d. The **VLAN** field will already be filled in and grayed out.

   e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
      - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box, and then in the **Your router peer IP** field, enter the destination IPv4 CIDR address that Amazon should send traffic to. In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   g. In the **BGP ASN** field, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   h. Select **Auto-generate BGP key** check box to have AWS generate one.

      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then in the **BGP Authentication Key** field, enter your BGP MD5 key.

6. Choose **Continue**, and then download your router configuration. For more information, see Step 6: Download Router Configuration (p. 32).

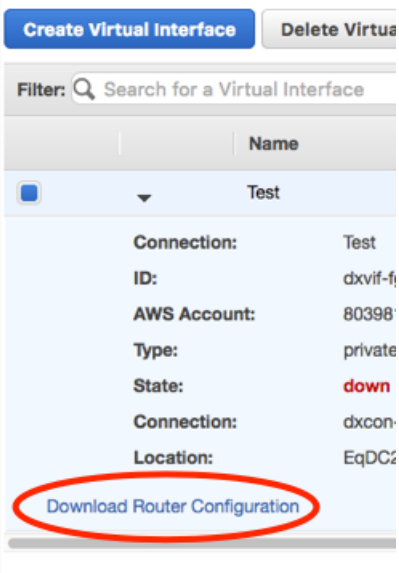
   Note
   If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. For more information on enabling route propagation, see Enable Route Propagation in Your Route Table in the *Amazon VPC User Guide*. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation.

Step 6: Download Router Configuration

After you have created a virtual interface for your AWS Direct Connect connection, you can download the router configuration file.

To download router configuration

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the **Virtual Interfaces** pane, select a virtual interface, choose the arrow to show more details, and then choose **Download Router Configuration**.



3. In the **Download Router Configuration** dialog box, do the following:
   a. In the **Vendor** list, select the manufacturer of your router.
   b. In the **Platform** list, select the model of your router.
   c. In the **Software** list, select the software version for your router.
4. Choose **Download**, and then use the appropriate configuration for your router to ensure that you can connect to AWS Direct Connect:

   Cisco IOS

```
interface GigabitEthernet0/1
no ip address

interface GigabitEthernet0/1.VLAN_NUMBER
description "Direct Connect to your Amazon VPC or AWS Cloud"
encapsulation dot1Q VLAN_NUMBER
```

```
ip address YOUR_PEER_IP

router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
neighbor AWS_PEER_IP password MD5_key
network 0.0.0.0
exit

! Optionally configure Bidirectional Forwarding Detection (BFD).

interface GigabitEthernet0/1.VLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP fall-over bfd
```

Cisco NX-OS

```
feature interface-vlan
vlan VLAN_NUMBER
name "Direct Connect to your Amazon VPC or AWS Cloud"

interface VlanVLAN_NUMBER
  ip address YOUR_PEER_IP/30
  no shutdown

interface Ethernet0/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan VLAN_NUMBER
  no shutdown

router bgp CUSTOMER_BGP_ASN
  address-family ipv4 unicast
    network 0.0.0.0
  neighbor AWS_PEER_IP remote-as 7224
    password 0 MD5_key
    address-family ipv4 unicast

! Optionally configure Bidirectional Forwarding Detection (BFD).

feature bfd
interface VlanVLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
bfd
```

Juniper JunOS

```
configure exclusive
edit interfaces ge-0/0/1
set description "Direct Connect to your Amazon VPC or AWS Cloud"
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_NUMBER
set family inet mtu 1500
```

```
set family inet address YOUR_PEER_IP
top

edit policy-options policy-statement EXPORT-DEFAULT
edit term DEFAULT
set from route-filter 0.0.0.0/0 exact
set then accept
up
edit term REJECT
set then reject
top

set routing-options autonomous-system CUSTOMER_BGP_ASN

edit protocols bgp group EBGP
set type external
set peer-as 7224

edit neighbor AWS_PEER_IP
set local-address YOUR_PEER_IP
set export EXPORT-DEFAULT
set authentication-key "MD5_key"
top
commit check
commit and-quit

# Optionally configure Bidirectional Forwarding Detection (BFD).

set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 minimum-interval 300
set protocols bgp group EBGP neighbor AWS_PEER_IP bfd-liveness-detection
 multiplier 3
```

Step 7: Verify Your Virtual Interface

After you have established virtual interfaces to the AWS cloud or to Amazon VPC, you can verify your AWS Direct Connect connections using the following procedures.

To verify your virtual interface connection to the AWS cloud

- Run `traceroute` and verify that the AWS Direct Connect identifier is in the network trace.

To verify your virtual interface connection to Amazon VPC

1. Using a pingable AMI, such as one of the Amazon Linux AMIs, launch an Amazon EC2 instance into the VPC that is attached to your virtual private gateway. The Amazon Linux AMIs are available in the **Quick Start** tab when you use the instance launch wizard in the Amazon EC2 console. For more information about launching an Amazon EC2 instance using an Amazon Linux AMI, see Launch an Amazon EC2 Instance in the *Amazon EC2 User Guide for Linux Instances*. Ensure that the security group that's associated with the instance includes a rule permitting inbound ICMP traffic (for the ping request).
2. After the instance is running, get its private IP address (for example, 10.0.0.4). The Amazon EC2 console displays the address as part of the instance details.
3. Ping the private IP address and get a response.

Working With AWS Direct Connect Connections

You can manage your AWS Direct Connect connections and view connection details, accept hosted connections, and delete connections. For information about how to create a new connection, see Step 2: Submit AWS Direct Connect Connection Request (p. 6).

Topics

View Connection Details

You can view the current status of your connection. You can also view your connection ID, which looks similar to this example dxcon-xxxx, and verify that it matches the connection ID on the Letter of Authorization (LOA) that you received from Amazon.

To view details about a connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select a connection, and then choose the arrow next to the connection to view its details.

   The service provider associated with the connection is listed in the **Provided By** column.

Delete a Connection

You can delete a connection as long as there are no virtual interfaces attached to it. Deleting your connection stops all port hour charges for this connection. AWS Direct Connect data transfer charges are associated with virtual interfaces. Any cross connect or network circuit charges are independent of

AWS Direct Connect and must be cancelled separately. For more information about how to delete a virtual interface, see Delete a Virtual Interface (p. 38).

To delete a connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select the connection to delete, and then choose **Delete Connection**.
5. In the **Delete Connection** dialog box, choose **Delete**.

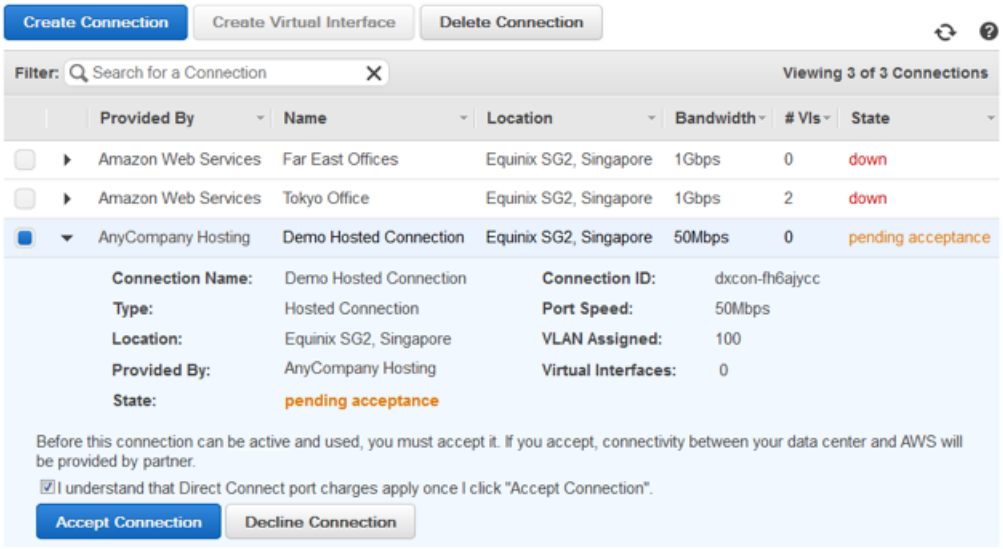
Accept a Hosted Connection

If you are interested in purchasing a hosted connection, you must contact a partner in the AWS Partner Network (APN). The partner provisions the connection for you. After the connection is configured, it appears in the **Connections** pane in the AWS Direct Connect console.

Before you can begin using a hosted connection, you must accept the connection.

To accept a hosted connection

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select a connection, and then choose the arrow to expand details about the connection.



5. Select **I understand that Direct Connect port charges apply once I click "Accept This Connection"**, and then choose **Accept Connection**.

Working With AWS Direct Connect Virtual Interfaces

You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a public virtual interface to connect to public resources, or a private virtual interface to connect to your VPC. You can configure multiple virtual interfaces on a single AWS Direct Connect connection, and you need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key.

To use your AWS Direct Connect connection with another AWS account, you can create a hosted virtual interface for that account. These hosted virtual interfaces work the same as standard virtual interfaces and can connect to public resources or a VPC.

A virtual interface can support a BGP peering session for IPv4, IPv6, or one of each (dual-stack). You cannot create multiple BGP sessions for the same IP addressing family on the same virtual interface.

Topics

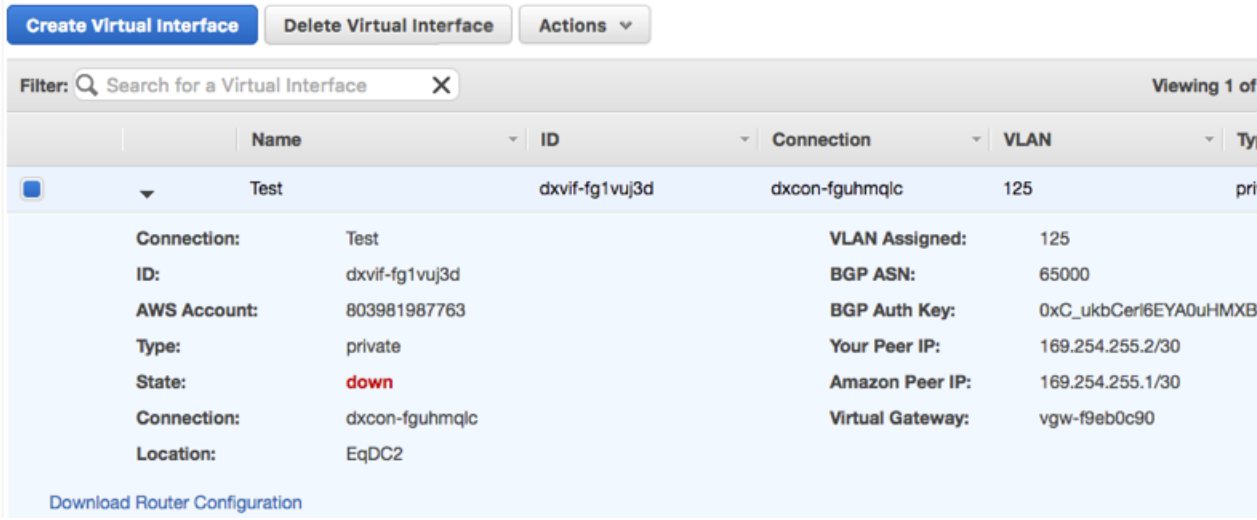
View Virtual Interface Details

You can view the current status of your virtual interface; the connection state, name, and location; VLAN and BGP details; and peer IP addresses.

To view details about a virtual interface

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.

2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Virtual Interfaces**.
4. In the **Virtual Interfaces** pane, select a virtual interface and choose the arrow next to the virtual interface to view its details.



Delete a Virtual Interface

Before you can delete a connection, you must delete its virtual interface. The number of virtual interfaces configured on a connection is listed in the **VIs** column in the **Connection** pane. Deleting a virtual interface stops AWS Direct Connect data transfer charges associated with the virtual interface.

To delete a virtual interface

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Virtual Interfaces**.
4. In the **Virtual Interfaces** pane, select a virtual interface, and then choose **Delete Virtual Interface**.
5. In the **Delete Virtual Interface** dialog box, choose **Delete**.

Create a Hosted Virtual Interface

You can create a public or private hosted virtual interface.

For any hosted Virtual Interface you will need a new, unused VLAN tag that you select.

For a public virtual interface you will need:

- A unique CIDR for your interface IP addresses that does not overlap another CIDR announced via AWS Direct Connect.
- A unique CIDR range to announce via AWS Direct Connect that does not overlap another CIDR announced via AWS Direct Connect.

To create a hosted virtual interface

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select the connection to add a virtual interface to, and then choose **Create Virtual Interface**.
5. On the **Create a Virtual Interface** screen, select the **Private** option.
6. Under **Define Your New Private Virtual Interface**, do the following:

   a. In the **Virtual Interface Name** field, enter a name for the virtual interface.

   b. In **Virtual Interface Owner**, select the **Another AWS Account** option, and then in the **Account ID** field, enter the ID number to associate as the owner of this virtual interface.

   c. In the **VLAN** field, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094 .

   d. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:

      - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
      - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box, and then in the **Your router peer IP** field, enter the destination IPv4 CIDR address that Amazon should send traffic to. In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

   e. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.

   f. In the **BGP ASN** field, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, an ASN you own or a private ASN between 64512 to 65535.

   g. Select the **Auto-generate BGP key** check box if you would like AWS to generate one for you.

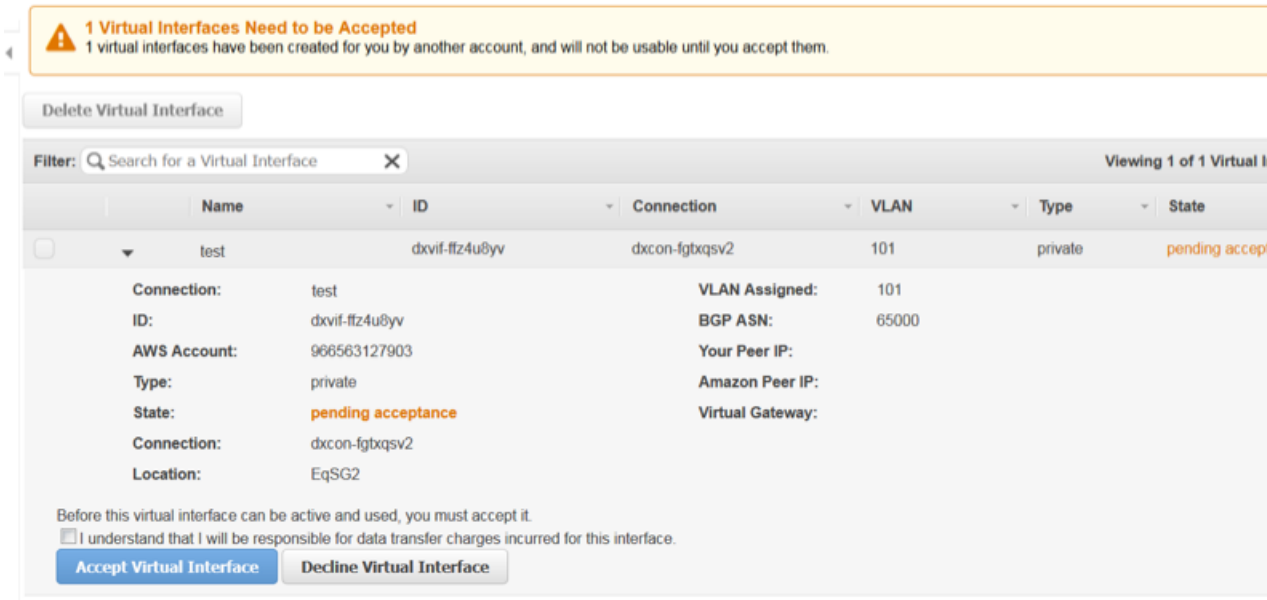
      To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then in the **BGP Authentication Key** field, enter your BGP MD5 key.
7. Choose **Continue**. The new interface is added to the list of virtual interfaces on the **Virtual Interfaces** pane.

Accept a Hosted Virtual Interface

Before you can begin using a hosted virtual interface, you must have an existing virtual gateway and you must accept the virtual interface.

To accept a hosted virtual interface

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints.
3. In the navigation pane, choose **Virtual Interfaces**.
4. In the **Virtual Interfaces** pane, select the check box next to the virtual interface you want to accept, and then choose the arrow to expand details about the virtual interface.



5. Select the **I understand that I will be responsible for data transfer charges incurred for this interface** check box, and then choose **Accept Virtual Interface**.
6. In the **Accept Virtual Interface** dialog box, select a virtual private gateway, and then choose **Accept**.

Add or Remove a BGP Peer

A virtual interface can support a single IPv4 BGP peering session and a single IPv6 BGP peering session. You can add an IPv6 BGP peering session to a virtual interface that has an existing IPv4 BGP peering session, or you can add an IPv4 BGP peering session to a virtual interface that has an existing IPv6 BGP peering session.

You cannot specify your own peer IPv6 addresses for an IPv6 BGP peering session. Amazon automatically allocates you a /125 IPv6 CIDR.

Multiprotocol BGP is not supported. IPv4 and IPv6 operate in dual-stack mode for the virtual interface.

To add a BGP peer

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the navigation pane, choose **Virtual Interfaces** and select the virtual interface.
3. Choose **Actions**, **Add Peering**.
4. (Private virtual interface) To add an IPv4 BGP peer, do the following:

   - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
   - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box, and then in the **Your router peer IP** field, enter the destination IPv4 CIDR address that Amazon should send traffic to. In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

5. (Public virtual interface) To add an IPv4 BGP peer, do the following:
   - For **Your router peer IP**, enter the IPv4 CIDR destination address where traffic should be sent.
   - For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.
6. (Private or public virtual interface) To add an IPv6 BGP peer, the **Auto-generate peer IPs** is selected by default. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses; you cannot specify custom IPv6 addresses.

7. In the **BGP ASN** field, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534. For a public virtual interface, the ASN must be private or already whitelisted for the virtual interface.
8. Select the **Auto-generate BGP key** check box if you want AWS to generate one for you.

   To provide your own BGP key, clear the **Auto-generate BGP key** check box, and then in the **BGP Authentication Key** field, enter your BGP MD5 key.
9. Choose **Continue**.

If your virtual interface has both an IPv4 and IPv6 BGP peering session, you can delete one of the BGP peering sessions (but not both).

To delete a BGP peer

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/.
2. In the navigation pane, choose **Virtual Interfaces** and select the virtual interface.

3. Choose **Actions**, **Delete Peering**.
4. To delete the IPv4 BGP peer, choose **IPv4**. To delete the IPv6 BGP peer, choose **IPv6**.
5. Choose **Delete**.

Accessing a Remote AWS Region in the US

AWS Direct Connect locations in the United States can access public resources in any US region. You can use a single AWS Direct Connect connection to build multi-region services. To connect to a VPC in a remote region, you can use a virtual private network (VPN) connection over your public virtual interface.

To access public resources in a remote region, you must set up a public virtual interface and establish a border gateway protocol (BGP) session. For more information about creating virtual interfaces see Step 5: Create a Virtual Interface (p. 8).

After you have created a public virtual interface and established a BGP session to it, your router learns the routes of the other AWS regions in the US. You can then also establish a VPN connection to your VPC in the remote region. To learn more about configuring VPN connectivity to a VPC, see Scenarios for Using Amazon Virtual Private Cloud in the *Amazon VPC User Guide*.

Any data transfer out of a remote region is billed at the remote region data transfer rate. For more information about data transfer pricing, see the Pricing section on the AWS Direct Connect detail page.

Requesting Cross Connects at AWS Direct Connect Locations

After you have downloaded your Letter of Authorization and Connecting Facility Assignment (LOA-CFA), you need to complete your cross-network connection, also known as a *cross connect*. If you already have equipment located in an AWS Direct Connect location, contact the appropriate provider to complete the cross connect. For specific instructions for each provider, see the table below. Contact your provider for cross connect pricing. After the cross connect is established, you can create the virtual interfaces using the AWS Direct Connect console.

If you do not already have equipment located in an AWS Direct Connect location, you can work with one of the partners in the AWS Partner Network (APN) to help you to connect to an AWS Direct Connect location. For a list of partners in the APN with experience connecting to AWS Direct Connect, see APN Partners supporting AWS Direct Connect. You need to share the LOA-CFA with your selected provider to facilitate your cross connect request.

An AWS Direct Connect location provides access to AWS in the region it is associated with. You can establish connections with AWS Direct Connect locations in multiple regions, but a connection in one region does not provide connectivity to other regions.

Note
If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires. To renew a LOA-CFA that has expired, you can download it again from the AWS Direct Connect console. For more information, see Step 3: Download the LOA-CFA and Complete the Cross Connect (p. 7).

Asia Pacific (Tokyo)

Location	How to request a connection
Equinix Osaka (Equinix OS1)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Equinix Tokyo (Equinix TY2)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.

Asia Pacific (Singapore)

Location	How to request a connection
Equinix Singapore (Equinix SG2)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Global Switch, Singapore	Requests for cross connects can be submitted by contacting Global Switch at salessingapore@globalswitch.com.
GPX Mumba	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net.

Asia Pacific (Sydney)

Location	How to request a connection
Equinix Sydney (Equinix SY3)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Global Switch (Global Switch SY6)	Requests for cross connects can be submitted by contacting Global Switch at salessydney@globalswitch.com.

Asia Pacific (Mumbai)

Location	How to request a connection
GPX Mumbai	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net.
Sify Rabale, Mumbai	Requests for cross connects can be submitted by contacting Sify at aws.directconnect@sifycorp.com.

China (Beijing)

Location	How to request connection
Sinnet Jiuxianqiao IDC	Requests for cross connects can be submitted by contacting Sinnet at dx-order@sinnet.com.cn.

EU (Frankfurt)

Location	How to request a connection
Equinix Amsterdam	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.

Location	How to request a connection
(Equinix AM3)	
Equinix Frankfurt (Equinix FR5)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Interxion Frankfurt	Requests for cross connects can be submitted by contacting Interxion at customer.services@interxion.com.
Interxion Madrid	Requests for cross connects can be submitted by contacting Interxion at customer.services@interxion.com.
Interxion Stockholm	Requests for cross connects can be submitted by contacting Interxion at customer.services@interxion.com.
Telehouse Voltaire, Paris (TH2)	Requests for cross connects can be submitted by creating a request at the Customer Portal. Request type: DFM/SFM Layout/Connectivity/MMR Circuit Commissioning

EU (Ireland)

Location	How to request a connection
Digital Realty (UK) (Sovereign House and London Meridian Gate)	Requests for cross connects can be submitted by contacting Digital Realty (UK) at amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Requests for cross connects can be submitted by contacting Eircom at awsorders@eircom.ie.
Equinix London (Slough) (Equinix LD4-LD6)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Interxion Dublin	Requests for cross connects can be submitted by contacting Interxion at customer.services@interxion.com.

South America (São Paulo)

Location	How to request a connection
Terremark NAP do Brasil, Sao Paulo	Requests for cross connects can be submitted by contacting Terremark at implementationbrasil@terremark.com.
Tivit	Requests for cross connects can be submitted by contacting Tivit at contact@tivit.com.br.

US East (N. Virginia)

Location	How to request a connection
CoreSite 32 Avenue of the Americas, New York	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.

Location	How to request a connection
CoreSite Northern Virginia (CoreSite VA1 and VA2)	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.
Equinix Ashburn (Equinix DC1-DC6, and DC10-DC11)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Equinix Dallas (Equinix DA1-DA3, and DA6)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.

US East (Ohio)

Location	How to request a connection
Equinix Chicago (Equinix CH1-CH2, and CH4)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
QTS Chicago	Requests for cross connects can be submitted by contacting QTS at AConnect@qtsdatacenters.com.

AWS GovCloud (US)

Location	How to request a connection
Equinix Silicon Valley (Equinix SV1 and SV5)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.

US West (N. California)

Location	How to request a connection
CoreSite One Wilshire and 900 North Alameda	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.
CoreSite Silicon Valley (CoreSite SV3 – SV7)	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.
Equinix Los Angeles (LA3 and LA4)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Equinix Silicon Valley (Equinix SV1 and SV5)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.

US West (Oregon)

Location	How to request a connection
EdgeConneX, Portland, OR	Requests for cross connects can be submitted by placing an order on the EdgeOS Customer Portal. After you have submitted the form, EdgeConneX will provide a service order form for approval. You can send questions to cloudaccess@edgeconnex.com.
Equinix Seattle (Equinix SE2 and SE3)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com.
Pittock Block, Portland, OR	Requests for cross connects can be submitted by email at crossconnect@pittock.com, or by phone at +1 503 226 6777.
Switch SUPERNAP 8, Las Vegas, NV	Requests for cross connects can be submitted by contacting Switch SUPERNAP at orders@supernap.com.
TierPoint Seattle	Requests for cross connects can be submitted by contacting TierPoint at sales@tierpoint.com.

Using AWS Identity and Access Management with AWS Direct Connect

You can use AWS Identity and Access Management with AWS Direct Connect to specify which AWS Direct Connect actions a user under your Amazon Web Services account can perform. For example, you could create an IAM policy that gives only certain users in your organization permission to use the `DescribeConnections` action to retrieve data about your AWS Direct Connect connections.

Permissions granted using IAM cover all the Amazon Web Services resources you use with AWS Direct Connect, so you cannot use IAM to control access to AWS Direct Connect data for specific resources. For example, you cannot give a user access to AWS Direct Connect data for only a specific virtual interface.

> **Important**
> Using AWS Direct Connect with IAM doesn't change how you use AWS Direct Connect. There are no changes to AWS Direct Connect actions, and no new AWS Direct Connect actions related to users and access control. For an example of a policy that covers AWS Direct Connect actions, see Example Policy for AWS Direct Connect (p. 50).

AWS Direct Connect Actions

In an IAM policy, you can specify any or all actions that AWS Direct Connect offers. The action name must include the lowercase prefix `directconnect:`. For example: `directconnect:DescribeConnections`, `directconnect:CreateConnection`, or `directconnect:*` (for all AWS Direct Connect actions). For a list of the actions, see the *AWS Direct Connect API Reference*.

AWS Direct Connect Resources

AWS Direct Connect does not support resource-level permissions; therefore, you cannot control access to specific AWS Direct Connect resources. You must use an asterisk (*) to specify the resource when writing a policy to control access to AWS Direct Connect actions.

AWS Direct Connect Keys

AWS Direct Connect implements the following policy keys:

- `aws:CurrentTime` (for date/time conditions)
- `aws:EpochTime` (the date in epoch or UNIX time, for use with date/time conditions)
- `aws:SecureTransport` (Boolean representing whether the request was sent using SSL)
- `aws:SourceIp` (the requester's IP address, for use with IP address conditions)
- `aws:UserAgent` (information about the requester's client application, for use with string conditions)

If you use `aws:SourceIp`, and the request comes from an Amazon EC2 instance, the instance's public IP address is used to determine if access is allowed.

> **Note**
> For services that use only SSL, such as Amazon Relational Database Service and Amazon Route 53, the `aws:SecureTransport` key has no meaning.

Key names are case-insensitive. For example, `aws:CurrentTime` is equivalent to `AWS:currenttime`.

For more information about policy keys, see Condition in *IAM User Guide*.

Example Policy for AWS Direct Connect

This section shows a simple policy for controlling user access to AWS Direct Connect.

> **Note**
> In the future, AWS Direct Connect might add new actions that should logically be included in the following policy, based on the policy's stated goals.

Example

The following sample policy allows a group to retrieve any AWS Direct Connect data, but not create or delete any resources.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "directconnect:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information about writing IAM policies, see Overview of IAM Policies in the *IAM User Guide*.

Using Tags with AWS Direct Connect

You can optionally assign tags to your AWS Direct Connect resources to categorize or manage them. A tag consists of a key and an optional value, both of which you define.

You can tag the following AWS Direct Connect resources.

Resource	Amazon Resource Name (ARN)
Connections	arn:aws:directconnect:*region*:*account-id*:dxcon/*connection-id*
Virtual interfaces	arn:aws:directconnect:*region*:*account-id*:dxvif/*virtual-interface-id*

For example, you have two AWS Direct Connect connections in a region, each in different locations. Connection `dxcon-11aa22bb` is a connection serving production traffic, and is associated with virtual interface `dxvif-33cc44dd`. Connection `dxcon-abcabcab` is a redundant (backup) connection, and is associated with virtual interface `dxvif-12312312`. You might choose to tag your connections and virtual interfaces as follows, to help distinguish them:

Resource ID	Tag key	Tag value
`dxcon-11aa22bb`	Purpose	Production
	Location	Amsterdam
`dxvif-33cc44dd`	Purpose	Production
`dxcon-abcabcab`	Purpose	Backup
	Location	Frankfurt
`dxvif-12312312`	Purpose	Backup

Tag Restrictions

The following rules and restrictions apply to tags:

- Maximum number of tags per resource: 50
- Maximum key length: 128 Unicode characters
- Maximum value length: 265 Unicode characters
- Tag keys and values are case sensitive.
- The `aws:` prefix is reserved for AWS use — you can't create or delete tag keys or values with this prefix. Tags with this prefix do not count against your tags per resource limit.
- Allowed characters are letters, spaces, and numbers representable in UTF-8, plus the following special characters: + - = . _ : / @

Working with Tags

Currently, you can work with tags using the AWS Direct Connect API, the AWS CLI, the AWS Tools for Windows PowerShell, or an AWS SDK only. To apply or remove tags, you must specify the Amazon Resource Name (ARN) for the resource. For more information, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *Amazon Web Services General Reference*.

To add a tag using the AWS CLI

Use the tag-resource command:

```
aws directconnect tag-resource --resource-arn
 arn:aws:directconnect:region:account-id:resource-type/resource-id --tags
 "key=key,value=value"
```

To describe your tags using the AWS CLI

Use the describe-tags command:

```
aws directconnect describe-tags --resource-arns
 arn:aws:directconnect:region:account-id:resource-type/resource-id
```

To delete a tag using the AWS CLI

Use the untag-resource command:

```
aws directconnect untag-resource --resource-arn
 arn:aws:directconnect:region:account-id:resource-type/resource-id --tag-
keys key
```

Logging AWS Direct Connect API Calls in AWS CloudTrail

AWS Direct Connect is integrated with AWS CloudTrail, a service that captures API calls made by or on behalf of your AWS account. This information is collected and written to log files that are stored in an Amazon Simple Storage Service (S3) bucket that you specify. API calls are logged when you use the AWS Direct Connect API, the AWS Direct Connect console, a back-end console, or the AWS CLI. Using the information collected by CloudTrail, you can determine what request was made to AWS Direct Connect, the source IP address the request was made from, who made the request, when it was made, and so on.

To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

Topics

AWS Direct Connect Information in CloudTrail

If CloudTrail logging is turned on, calls made to all AWS Direct Connect actions are captured in log files. All of the AWS Direct Connect actions are documented in the AWS Direct Connect API Reference. For example, calls to the **CreateConnection**, **CreatePrivateVirtualInterface**, and **DescribeConnections** actions generate entries in CloudTrail log files.

Every log entry contains information about who generated the request. For example, if a request is made to create a new connection to AWS Direct Connect (**CreateConnection**), CloudTrail logs the user identity of the person or service that made the request. The user identity information helps you determine whether the request was made with root credentials or AWS Identity and Access Management (IAM) user credentials, with temporary security credentials for a role or federated user, or by another service in AWS. For more information about CloudTrail fields, see CloudTrail Event Reference in the AWS CloudTrail User Guide.

You can store your log files in your bucket for as long as you want, but you can also define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted by using Amazon S3 server-side encryption (SSE).

Understanding AWS Direct Connect Log File Entries

CloudTrail log files can contain one or more log entries composed of multiple JSON-formatted events. A log entry represents a single request from any source and includes information about the requested action, any input parameters, the date and time of the action, and so on. The log entries do not appear in any particular order. That is, they do not represent an ordered stack trace of the public API calls.

The following log file record shows that a user called the **CreateConnection** action.

```
{
    "Records": [{
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...additional entries
  ]
}
```

The following log file record shows that a user called the **CreatePrivateVirtualInterface** action.

```
{
```

```
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...additional entries
  ]
}
```


The following log file record shows that a user called the **DescribeConnections** action.

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...additional entries
  ]
}
```

The following log file record shows that a user called the **DescribeVirtualInterfaces** action.

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
```

```
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...additional entries
  ]
}
```

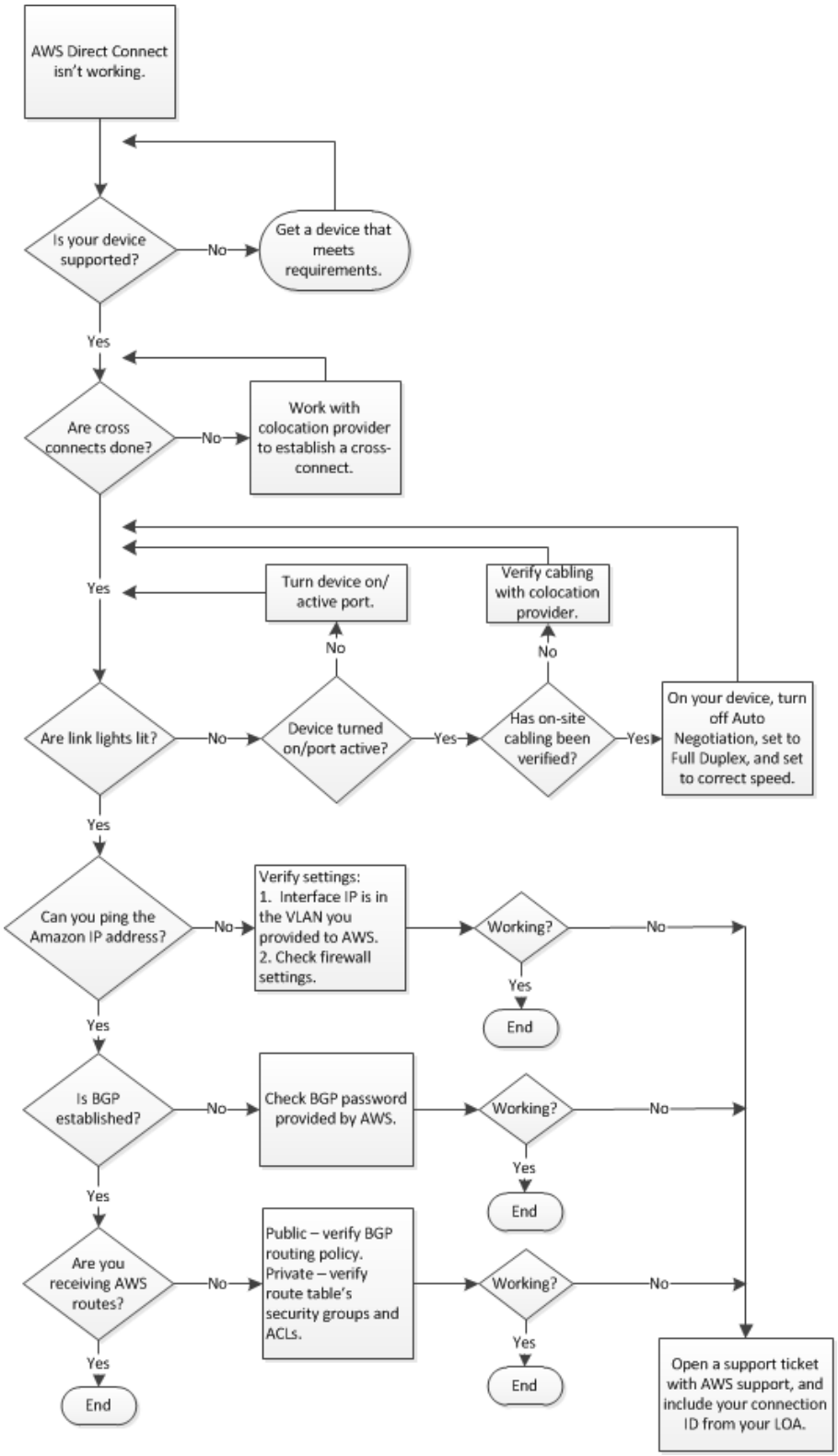
Troubleshooting AWS Direct Connect

The following table lists troubleshooting resources that you'll find useful as you work with AWS Direct Connect.

Resource	Description
Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect (p. 58)	Flow chart that provides the steps necessary to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility.
Troubleshooting a Cross Connection to AWS Direct Connect (p. 60)	Task list that provides the steps necessary to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility.
Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect (p. 60)	Flow chart that provides the steps necessary to diagnose, troubleshoot, and repair a faulty connection to AWS Direct Connect when connecting remotely through a service provider.
Troubleshooting a Remote Connection to AWS Direct Connect (p. 62)	Task list that provides the steps necessary to diagnose, troubleshoot, and repair a faulty connection to AWS Direct Connect when connecting remotely through a service provider.

Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect

You can use the following flow chart to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility. For a text-based version of this flow chart, see Troubleshooting a Cross Connection to AWS Direct Connect (p. 60).


AWS Direct Connect isn't working.
Is your device supported?
No
Get a device that meets requirements.
Yes
Are cross connects done?
No
Work with colocation provider to establish a cross-connect.
Yes
Are link lights lit?
No
Turn device on/ active port.
No
Device turned on/port active?
Yes
Verify cabling with colocation provider.
No
Has on-site cabling been verified?
Yes
On your device, turn off Auto Negotiation, set to Full Duplex, and set to correct speed.
Yes
Can you ping the Amazon IP address?
No
Verify settings:
1. Interface IP is in the VLAN you provided to AWS.
2. Check firewall settings.
Working?
No
Yes
End
Yes
Is BGP established?
No
Check BGP password provided by AWS.
Working?
No
Yes
End
Yes
Are you receiving AWS routes?
No
Public – verify BGP routing policy.
Private – verify route table's security groups and ACLs.
Working?
No
Yes
End
Yes
End
Open a support ticket with AWS support, and include your connection ID from your LOA.

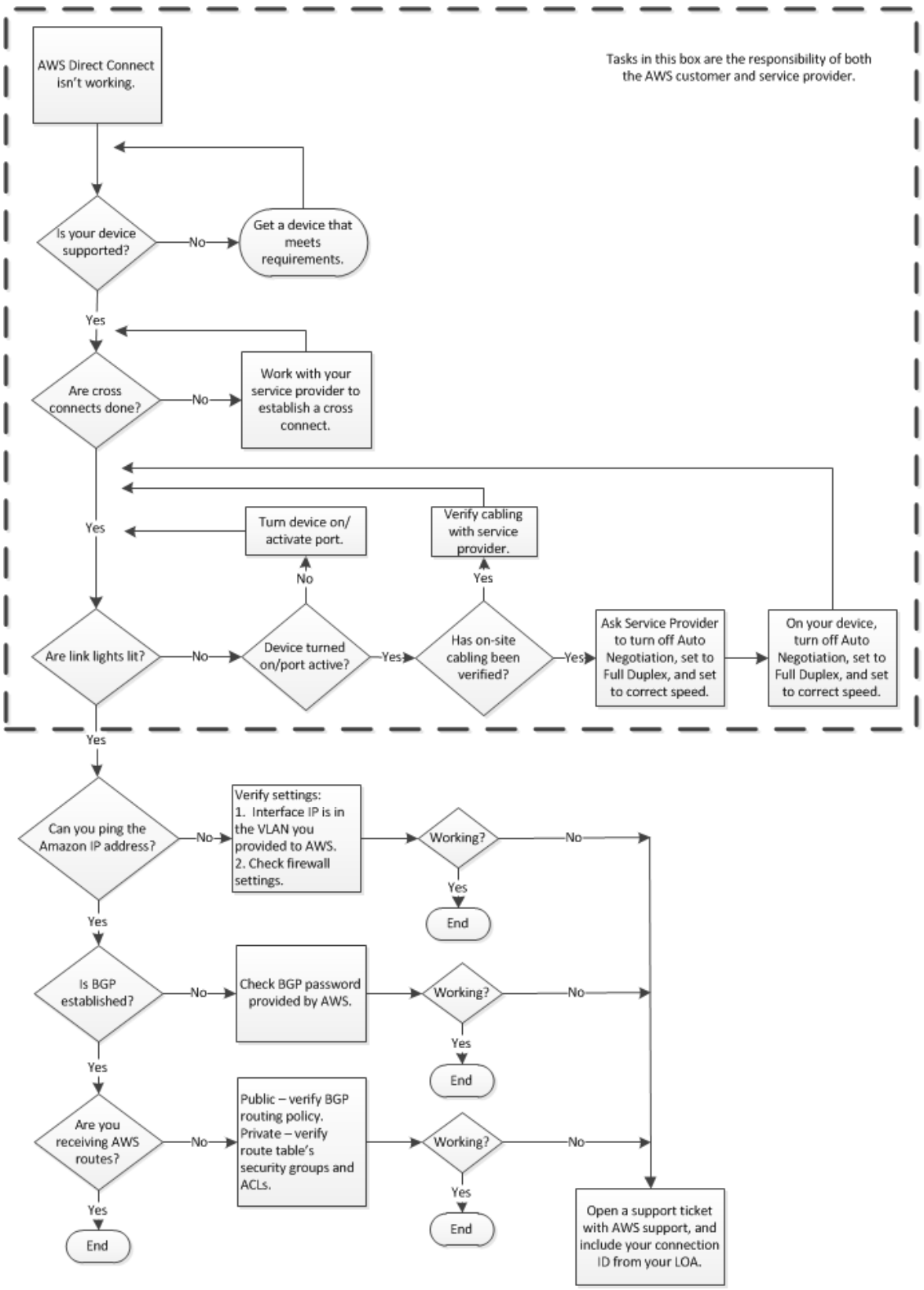
Troubleshooting a Cross Connection to AWS Direct Connect

You can use the following tasks to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility. To see these tasks in a flow chart, see Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect (p. 58).

1. Verify that your device is supported by AWS Direct Connect. If not, get a device that meets the AWS Direct Connect requirements. For more information, see What is AWS Direct Connect? (p. 1).
2. Verify that your AWS Direct Connect cross connects are established. If they are not, work with your colocation provider to establish them.
3. Verify that your router's link lights are working. If they are not, turn on your device and activate the ports.
4. Verify with your colocation provider that there are no cabling problems. If necessary, on your device, turn off Auto Negotiation, set the device to Full Duplex, and set the device to the correct speed.
5. If you cannot ping the Amazon IP address, verify that the interface IP address is in the VLAN you provided to Amazon Web Services and then verify your firewall settings. If you still cannot connect to AWS Direct Connect, open a support ticket with AWS support for assistance and include the original ticket number from your letter of authorization (LOA).
6. If you cannot establish Border Gateway Protocol (BGP) after verifying the password provided by Amazon, open a support ticket with AWS support for assistance and include the original ticket number from your LOA.
7. If you are not receiving Amazon routes and you cannot verify public BGP routing policy, private route table security groups, or access control lists (ACLs), open a support ticket with AWS support and include your connection ID from your LOA.

Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect

You can use the following flow chart to diagnose, troubleshoot, and repair a faulty connection to AWS Direct Connect when connecting remotely through a service provider. For a text-based version of this flow chart, see Troubleshooting a Remote Connection to AWS Direct Connect (p. 62).


AWS Direct Connect isn't working.
Tasks in this box are the responsibility of both the AWS customer and service provider.
Is your device supported?
No
Get a device that meets requirements.
Yes
Are cross connects done?
No
Work with your service provider to establish a cross connect.
Yes
Turn device on/ activate port.
Verify cabling with service provider.
No
Yes
Are link lights lit?
No
Device turned on/port active?
Yes
Has on-site cabling been verified?
Yes
Ask Service Provider to turn off Auto Negotiation, set to Full Duplex, and set to correct speed.
On your device, turn off Auto Negotiation, set to Full Duplex, and set to correct speed.
Yes
Can you ping the Amazon IP address?
No
Verify settings:
1. Interface IP is in the VLAN you provided to AWS.
2. Check firewall settings.
Working?
No
Yes
End
Yes
Is BGP established?
No
Check BGP password provided by AWS.
Working?
No
Yes
End
Yes
Are you receiving AWS routes?
No
Public – verify BGP routing policy.
Private – verify route table's security groups and ACLs.
Working?
No
Yes
End
Yes
End
Open a support ticket with AWS support, and include your connection ID from your LOA.

Troubleshooting a Remote Connection to AWS Direct Connect

You can use the following tasks to diagnose, troubleshoot, and repair a faulty connection to AWS Direct Connect when connecting remotely through a service provider. To see these tasks in a flow chart, see Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect (p. 60).

1. Verify that your device is supported by AWS Direct Connect. If not, get a device that meets the AWS Direct Connect requirements. For more information, see What is AWS Direct Connect? (p. 1).
2. Verify that your AWS Direct Connect cross connects are established. If they are not, work with your service provider to establish them.
3. Verify that your router's link lights are working. If they are not, turn on your device and activate the ports.
4. Verify with your service provider that there are no cabling problems.
5. Ask your service provider to turn off Auto Negotiation on their device, to set their device to Full Duplex, and to set their device to the correct speed.
6. On your device, turn off Auto Negotiation, set the device to Full Duplex, and set the device to the correct speed.
7. If you cannot ping the Amazon IP address, verify that the interface IP address is in the VLAN that you provided to Amazon Web Services, and then verify your firewall settings. If you still cannot connect to AWS Direct Connect, open a support ticket with AWS support for assistance and include the original ticket number from your letter of authorization (LOA).
8. If you cannot establish Border Gateway Protocol (BGP) after verifying the password provided by Amazon, open a support ticket with AWS support for assistance and include the original ticket number from your LOA.
9. If you are not receiving Amazon routes and you cannot verify public BGP routing policy, private route table security groups, or access control lists (ACLs), open a support ticket with AWS support and include your connection ID from your LOA.

AWS Direct Connect Resources

The following related resources can help you as you work with this service.

- **AWS Direct Connect Technical FAQ** – The top questions developers have asked about this product.
- **AWS Direct Connect Release Notes** – A high-level overview of the current release, as well as notes about any new features, corrections, and known issues.
- **Discussion Forums** – A community-based forum for developers to discuss technical questions related to Amazon Web Services.
- **AWS Direct Connect Product Information**– The primary web page for information about AWS Direct Connect.

- **Classes & Workshops** – Links to role-based and specialty courses as well as self-paced labs to help sharpen your AWS skills and gain practical experience.
- **AWS Developer Tools** – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- **AWS Whitepapers** – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- **AWS Support Center** – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- **AWS Support** – The primary web page for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- **Contact Us** – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- **AWS Site Terms** – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

Document History

- **API version:** 2012-10-25

The following table describes the important changes since the last release of the *AWS Direct Connect User Guide*.

Change	Description	Release Date
IPv6 support	Your virtual interface can now support an IPv6 BGP peering session. For more information, see Add or Remove a BGP Peer (p. 40).	2016-12-01
Tagging support	You can now tag your AWS Direct Connect resources. For more information, see Using Tags with AWS Direct Connect (p. 51).	2016-11-04
Self-service LOA-CFA	You can now download your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) using the AWS Direct Connect console or API.	2016-06-22
New location in Silicon Valley	Updated topic to include the addition of the new Silicon Valley location in the US West (N. California) region.	2016-06-03
New location in Amsterdam	Updated topic to include the addition of the new Amsterdam location in the EU (Frankfurt) region.	2016-05-19
New locations in Portland, Oregon and Singapore	Updated topic to include the addition of the new Portland, Oregon and Singapore locations in the US West (Oregon) and Asia Pacific (Singapore) regions.	2016-04-27
New location in Sao Paulo, Brasil	Updated topic to include the addition of the new Sao Paulo location in the South America (São Paulo) region.	2015-12-09
New locations in Dallas, London, Silicon Valley, and Mumbai	Updated topics to include the addition of the new locations in Dallas (US East (N. Virginia) region), London (EU (Ireland) region), Silicon Valley (AWS GovCloud (US) region), and Mumbai (Asia Pacific (Singapore) region).	2015-11-27

Change	Description	Release Date
New location in the China (Beijing) region	Updated topics to include the addition of the new Beijing location in the China (Beijing) region.	2015-04-14
New Las Vegas location in the US West (Oregon) region	Updated topics to include the addition of the new AWS Direct Connect Las Vegas location in the US West (Oregon) region.	2014-11-10
New EU (Frankfurt) region	Updated topics to include the addition of the new AWS Direct Connect locations serving the EU (Frankfurt) region.	2014-10-23
New Getting Started Topics	Added two new getting started topics to cover AWS Direct Connect partners, network carriers, and sub-1G partners. For more information, see Getting Started with a Partner or Network Carrier (p. 16) and Getting Started with a Sub-1G AWS Direct Connect Partner (p. 26).	2014-10-23
New locations in the Asia Pacific (Sydney) region	Updated topics to include the addition of the new AWS Direct Connect locations serving the Asia Pacific (Sydney) region.	2014-07-14
Support for AWS CloudTrail	Added a new topic to explain how you can use CloudTrail to log activity in AWS Direct Connect. For more information, see Logging AWS Direct Connect API Calls in AWS CloudTrail (p. 53).	2014-04-04
Support for accessing remote AWS regions	Added a new topic to explain how you can access public resources in a remote region. For more information, see Accessing a Remote AWS Region in the US (p. 43).	2013-12-19
Support for hosted connections	Updated topics to include support for hosted connections.	2013-10-22
New location in the EU (Ireland) region	Updated topics to include the addition of the new AWS Direct Connect location serving the EU (Ireland) region.	2013-06-24
New Seattle location in the US West (Oregon) region	Updated topics to include the addition of the new AWS Direct Connect location in Seattle serving the US West (Oregon) region.	2013-05-08
Support for using IAM with AWS Direct Connect	Added a topic about using AWS Identity and Access Management with AWS Direct Connect. For more information, see Using AWS Identity and Access Management with AWS Direct Connect (p. 49).	2012-12-21

Change	Description	Release Date
New Asia Pacific (Sydney) region	Updated topics to include the addition of the new AWS Direct Connect location serving the Asia Pacific (Sydney) region.	2012-12-14
New AWS Direct Connect console, and the US East (N. Virginia) and South America (Sao Paulo) regions	Replaced the AWS Direct Connect Getting Started Guide with the AWS Direct Connect User Guide. Added new topics to cover the new AWS Direct Connect console, added a billing topic, added router configuration information, and updated topics to include the addition of two new AWS Direct Connect locations serving the US East (N. Virginia) and South America (Sao Paulo) regions.	2012-08-13
Support for the EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo) regions	Added a new troubleshooting section and updated topics to include the addition of four new AWS Direct Connect locations serving the US West (Northern California), EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo) regions.	2012-01-10
Support for the US West (Northern California) region	Updated topics to include the addition of the US West (Northern California) region.	2011-09-08
Public release	The first release of AWS Direct Connect.	2011-08-03

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the *AWS General Reference*.