
AWS Direct Connect

User Guide

API Version 2013-10-22



AWS Direct Connect: User Guide

Table of Contents

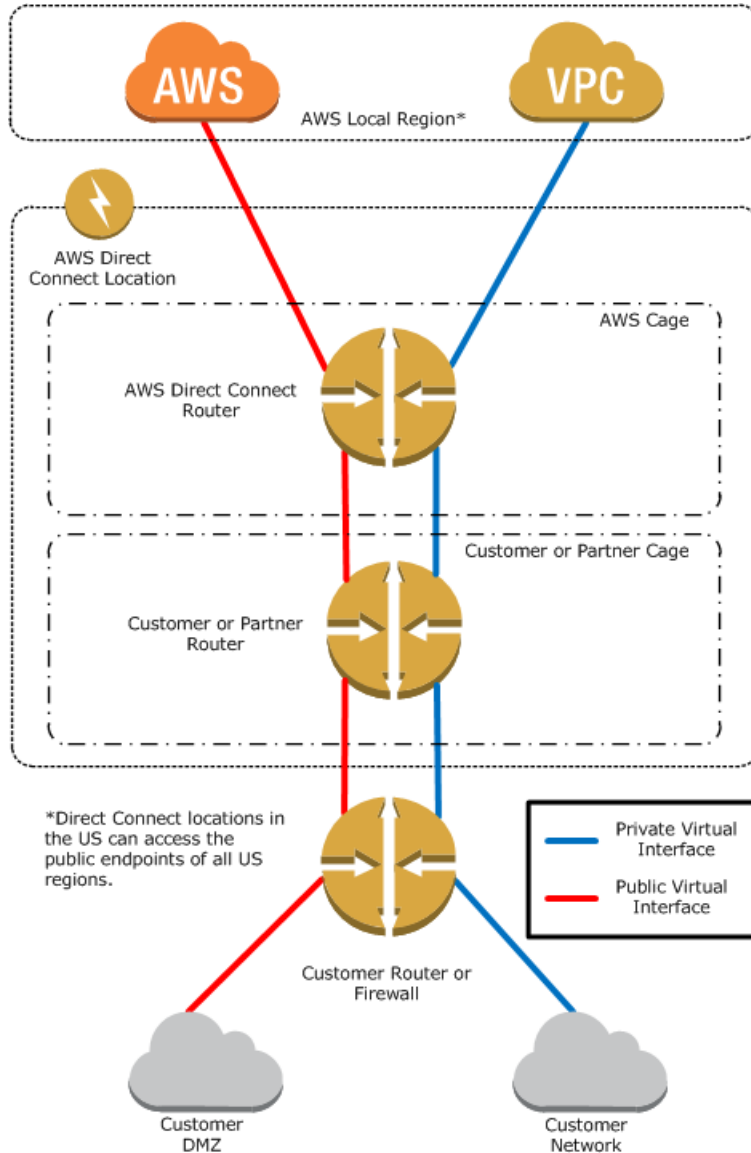
What is AWS Direct Connect?	1
Requirements	2
AWS Direct Connect Limits	3
How Do I...?	3
Getting Started	5
Getting Started at an AWS Direct Connect Location	5
Step 1: Sign Up for Amazon Web Services	5
Step 2: Submit AWS Direct Connect Connection Request	6
Step 3: Download the LOA-CFA and Complete the Cross Connect	7
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect	8
Step 5: Create a Virtual Interface	9
Step 6: Download Router Configuration	12
Step 7: Verify Your Virtual Interface	13
Getting Started with a Partner or Network Carrier	14
Step 1: Sign Up for Amazon Web Services	14
Step 2: Submit AWS Direct Connect Connection Request	14
Step 3: Download the LOA-CFA and Request a Cross Connect from Your Network Provider	16
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect	16
Step 5: Create a Virtual Interface	17
Step 6: Download Router Configuration	21
Step 7: Verify Your Virtual Interface	22
Getting Started with a Sub-1G AWS Direct Connect Partner	22
Step 1: Sign Up for Amazon Web Services	23
Step 2: Request a sub-1G connection from an APN Partner supporting AWS Direct Connect	23
Step 3: Accept Your Hosted Connection	23
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect	24
Step 5: Create a Virtual Interface	25
Step 6: Download Router Configuration	28
Step 7: Verify Your Virtual Interface	29
Working With Connections	31
View Connection Details	31
Delete a Connection	31
Accept a Hosted Connection	32
Working With Virtual Interfaces	33
View Virtual Interface Details	33
Delete a Virtual Interface	34
Create a Hosted Virtual Interface	34
Accept a Hosted Virtual Interface	35
Accessing a Remote AWS Region	37
Requesting Cross Connects	38
Using IAM	41
No AWS Direct Connect ARNs	41
AWS Direct Connect Actions	41
AWS Direct Connect Keys	42
Example Policy for AWS Direct Connect	42
Logging API Calls	43
AWS Direct Connect Information in CloudTrail	43
Understanding AWS Direct Connect Log File Entries	44
Troubleshooting	48
Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect	48
Troubleshooting a Cross Connection to AWS Direct Connect	50
Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect	50
Troubleshooting a Remote Connection to AWS Direct Connect	52

Resources	53
Document History	54
AWS Glossary	57

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 Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3)) and to Amazon Virtual Private Cloud (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).

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 on available AWS Direct Connect locations, go to <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, go to <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 may configure Bidirectional Forwarding Detection (BFD).

To connect to Amazon Virtual Private Cloud (Amazon VPC), you must first do the following:

- Provide a private Autonomous System Number (ASN). Amazon allocates a private IP 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.
- Public IP addresses (/31) (that is, one for each end of the BGP session) for each BGP session. If you do not have public IP addresses to assign to this connection, log on to AWS and then [open a ticket with AWS Support](#).
- The public routes that you will advertise over BGP.

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)
Work with AWS Direct Connect connections	Working With AWS Direct Connect Connections (p. 31)

AWS Direct Connect User Guide
How Do I...?

How Do I...	Relevant Topics
Calculate monthly costs	Pricing
Troubleshoot issues with AWS Direct Connect	Troubleshooting AWS Direct Connect (p. 48)

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 \(p. 5\)](#)
- [Getting Started with a Partner or Network Carrier \(p. 14\)](#)
- [Getting Started with a Sub-1G AWS Direct Connect Partner \(p. 22\)](#)

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 (p. 5)
Step 2: Submit AWS Direct Connect Connection Request (p. 6)
Step 3: Download the LOA-CFA and Complete the Cross Connect (p. 7)
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect (p. 8)
Step 5: Create a Virtual Interface (p. 9)
Step 6: Download Router Configuration (p. 12)
Step 7: Verify Your Virtual Interface (p. 13)

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:

AWS Direct Connect User Guide

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

Create a Connection

You are currently operating in Asia Pacific (Singapore). Use the region selector to change to another AWS region.

To begin, name your new Connection, select the AWS Direct Connect location in Asia Pacific (Singapore) where you would like to connect, and the port speed you are requesting. If these choices don't fit your use case [contact one of our partners](#) for other options to connect.

Connection Name: ⓘ

Location: Equinix SG2, Singapore ⓘ

Port Speed: 1Gbps 10Gbps ⓘ

- 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*.

AWS Direct Connect User Guide (optional) Step 4: Configure Redundant Connections with AWS Direct 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 \(p. 38\)](#).
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 \(p. 2\)](#).

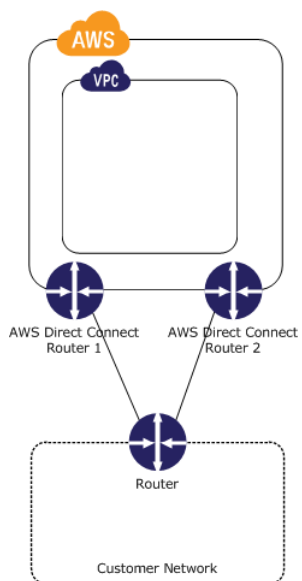
The LOA-CFA expires after 90 days. If your connection is not up after 90 days, we'll send you an email alerting you that the LOA-CFA has expired. To refresh the LOA-CFA with a new issue date, you can download it again from the AWS Direct Connect console. If you do not take any action, we will delete 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 \(p. 31\)](#).

(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 Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), and Amazon.com. You do not have access to non-A 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 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.
 - 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.
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**.

AWS Direct Connect User Guide

Step 5: Create a Virtual Interface

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Public Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Your router peer IP: ⓘ

Amazon router peer IP: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router, and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

Prefixes you want to advertise: ⓘ

It may take up to 72 hours to verify that your IP prefixes are valid for use with Direct Connect.

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 **Interface Name**, enter a name for the virtual interface.
 - c. For **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. For **Your router peer IP**, enter the IPv4 CIDR destination address where traffic should be sent.
 - f. For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.
 - g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.
 - 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 Authorization 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. 12).

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 then choose **Create Virtual Interface**.
4. In the **Create a Virtual Interface** pane, select **Private**.

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

VGW: ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Auto-generate peer IPs: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

5. Under **Define Your New Private Virtual Interface**, do the following:
 - a. For **Interface Name**, enter a name for the virtual interface.

- b. For **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. 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. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.
- g. 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 Authorization Key**, enter your BGP MD5 key.

6. Choose **Continue**, and then download your router configuration. For more information, see [Step 6: Download Router Configuration \(p. 12\)](#).

Note

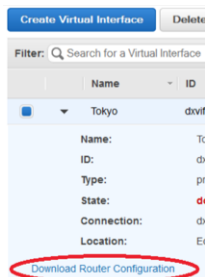
If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation. For more information, see [Enable Route Propagation in Your Route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

```
interface GigabitEthernet0/1
no ip address
speed 1000
full-duplex

interface GigabitEthernet0/1.VLAN_NUMBER
description direct connect to aws
encapsulation dot1Q VLAN_NUMBER
ip address IP_ADDRESS

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

Juniper

```
edit interfaces ge-0/0/1
set description " AWS Direct Connect "
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_ID
set family inet mtu 1500
set family inet address IP_ADDRESS
exit
exit

edit protocols bgp group ebgp
set type external
set authentication-key "MD5_KEY"
set peer-as 7224
set neighbor NEIGHBOR IP ADDRESS
```

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 (p. 14)
Step 2: Submit AWS Direct Connect Connection Request (p. 14)
Step 3: Download the LOA-CFA and Request a Cross Connect from Your Network Provider (p. 16)
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect (p. 16)
Step 5: Create a Virtual Interface (p. 17)
Step 6: Download Router Configuration (p. 21)
Step 7: Verify Your Virtual Interface (p. 22)

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:

Create a Connection

You are currently operating in Asia Pacific (Singapore). Use the region selector to change to another AWS region.

To begin, name your new Connection, select the AWS Direct Connect location in Asia Pacific (Singapore) where you would like to connect, and the port speed you are requesting. If these choices don't fit your use case [contact one of our partners](#) for other options to connect.

Connection Name: ⓘ

Location: Equinix SG2, Singapore ⓘ

Port Speed: 1Gbps 10Gbps ⓘ

- 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.

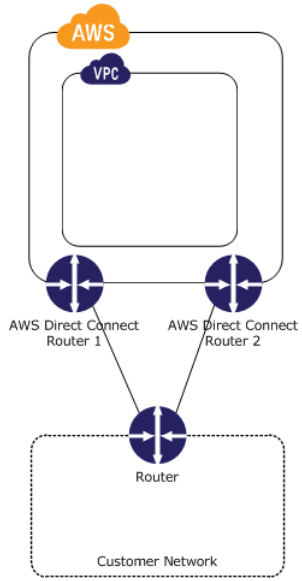
The LOA-CFA expires after 90 days. If your connection is not up after 90 days, we'll send you an email alerting you that the LOA-CFA has expired. To refresh the LOA-CFA with a new issue date, you can download it again from the AWS Direct Connect console. If you do not take any action, we will delete 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. 31).

(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 Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), and Amazon.com. You do not have access to non-AWS 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 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.

AWS Direct Connect User Guide

Step 5: Create a Virtual Interface

- 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.
 - 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.
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**.

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Public Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Your router peer IP: ⓘ

Amazon router peer IP: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router, and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

Prefixes you want to advertise: ⓘ

It may take up to 72 hours to verify that your IP prefixes are valid for use with Direct Connect.

Cancel

Continue

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 **Interface Name**, enter a name for the virtual interface.
 - c. For **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. For **Your router peer IP**, enter the IPv4 CIDR destination address where traffic should be sent.

- f. For **Amazon router peer IP**, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.
- g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.
- 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 Authorization 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 \(p. 21\)](#).

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**.

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

VGW: ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Auto-generate peer IPs: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

5. Under **Define Your New Private Virtual Interface**, do the following:
 - a. For **Interface Name**, enter a name for the virtual interface.
 - b. For **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. 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. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.
 - g. 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 Authorization Key**, enter your BGP MD5 key.
6. Choose **Continue**, and then download your router configuration. For more information, see [Step 6: Download Router Configuration \(p. 21\)](#).

Note

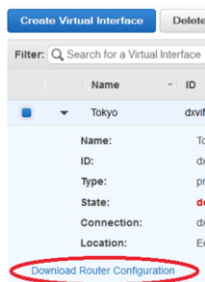
If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation. For more information, see [Enable Route Propagation in Your Route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

```
interface GigabitEthernet0/1
no ip address
speed 1000
full-duplex

interface GigabitEthernet0/1.VLAN_NUMBER
description direct connect to aws
encapsulation dot1Q VLAN_NUMBER
ip address IP_ADDRESS

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

Juniper

```
edit interfaces ge-0/0/1
set description " AWS Direct Connect "
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_ID
set family inet mtu 1500
set family inet address IP_ADDRESS
exit
exit

edit protocols bgp group ebgp
set type external
set authentication-key "MD5_KEY"
set peer-as 7224
set neighbor NEIGHBOR IP ADDRESS
```

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 \(p. 23\)](#)

[Step 2: Request a sub-1G connection from an APN Partner supporting AWS Direct Connect \(p. 23\)](#)

Step 3: Accept Your Hosted Connection (p. 23)
(optional) Step 4: Configure Redundant Connections with AWS Direct Connect (p. 24)
Step 5: Create a Virtual Interface (p. 25)
Step 6: Download Router Configuration (p. 28)
Step 7: Verify Your Virtual Interface (p. 29)

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.

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

The screenshot shows the AWS Direct Connect console interface. At the top, there are buttons for "Create Connection", "Create Virtual Interface", and "Delete Connection". Below these is a search filter and a refresh icon. The main area displays a table of connections:

	Provided By	Name	Location	Bandwidth	# VIs	State
<input type="checkbox"/>	Amazon Web Services	Far East Offices	Equinix SG2, Singapore	1Gbps	0	down
<input type="checkbox"/>	Amazon Web Services	Tokyo Office	Equinix SG2, Singapore	1Gbps	2	down
<input checked="" type="checkbox"/>	AnyCompany Hosting	Demo Hosted Connection	Equinix SG2, Singapore	50Mbps	0	pending acceptance

The selected connection details are shown below:

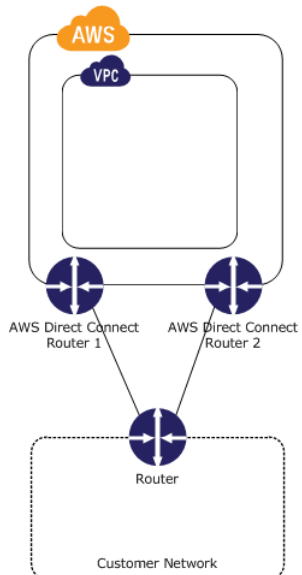
- Connection Name:** Demo Hosted Connection
- Connection ID:** dxcon-fh6ajycc
- Type:** Hosted Connection
- Port Speed:** 50Mbps
- Location:** Equinix SG2, Singapore
- VLAN Assigned:** 100
- Provided By:** AnyCompany Hosting
- Virtual Interfaces:** 0
- State:** pending acceptance

Below the details, there is a note: "Before this connection can be active and used, you must accept it. If you accept, connectivity between your data center and AWS will be provided by partner." and a checkbox: "I understand that Direct Connect port charges apply once I click 'Accept Connection'". At the bottom are buttons for "Accept Connection" and "Decline 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 Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), and Amazon.com. You do not have access to non-AWS 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 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.
 - 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.
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**.

AWS Direct Connect User Guide

Step 5: Create a Virtual Interface

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Public Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Your router peer IP: ⓘ

Amazon router peer IP: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router, and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

Prefixes you want to advertise: ⓘ

It may take up to 72 hours to verify that your IP prefixes are valid for use with Direct Connect.

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 **Interface Name** field, enter a name for the virtual interface.
 - c. In **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. In the **Your router peer IP** field, enter the IPv4 CIDR destination address where traffic should be sent.
 - f. In the **Amazon router peer IP** field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.
 - g. 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.
 - 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 Authorization 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 \(p. 28\)](#).

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**.

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Interface Name: ⓘ

Interface Owner: My AWS Account Another AWS Account ⓘ

VGW: ⓘ

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: ⓘ

Auto-generate peer IPs: ⓘ

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

5. Under **Define Your New Private Virtual Interface**, do the following:
 - a. In the **Interface Name** field, enter a name for the virtual interface.

- b. In **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. 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. 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.
- g. 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 Authorization 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 \(p. 28\)](#).

Note

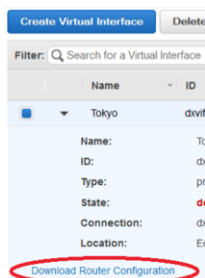
If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. For more information on enabling route propagation, see [Enable Route Propagation in Your Route Table](#) in the *Amazon VPC User Guide*. With route propagation, routes are automatically populated to the route 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

```
interface GigabitEthernet0/1
no ip address
speed 1000
full-duplex

interface GigabitEthernet0/1.VLAN_NUMBER
description direct connect to aws
encapsulation dot1Q VLAN_NUMBER
ip address IP_ADDRESS

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

Juniper

```
edit interfaces ge-0/0/1
set description " AWS Direct Connect "
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_ID
set family inet mtu 1500
set family inet address IP_ADDRESS
exit
exit

edit protocols bgp group ebgp
set type external
set authentication-key "MD5_KEY"
set peer-as 7224
set neighbor NEIGHBOR IP ADDRESS
```

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 \(p. 31\)](#)
- [Delete a Connection \(p. 31\)](#)
- [Accept a Hosted Connection \(p. 32\)](#)

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 \(p. 34\)](#).

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.

The screenshot shows the AWS Direct Connect console interface. At the top, there are three buttons: 'Create Connection', 'Create Virtual Interface', and 'Delete Connection'. Below these is a search bar with the text 'Filter: Search for a Connection' and a close button. To the right, it says 'Viewing 3 of 3 Connections'. The main table has columns: 'Provided By', 'Name', 'Location', 'Bandwidth', '# VIs', and 'State'. There are three rows of connections. The first two are from 'Amazon Web Services' and are in a 'down' state. The third is from 'AnyCompany Hosting' and is in a 'pending acceptance' state. Below the table, the details for the 'Demo Hosted Connection' are shown. The details include: Connection Name: Demo Hosted Connection, Connection ID: dxcon-fh6ajycc, Type: Hosted Connection, Port Speed: 50Mbps, Location: Equinix SG2, Singapore, VLAN Assigned: 100, Provided By: AnyCompany Hosting, Virtual Interfaces: 0, and State: pending acceptance. At the bottom of the details, there is a note: 'Before this connection can be active and used, you must accept it. If you accept, connectivity between your data center and AWS will be provided by partner.' Below the note is a checked checkbox with the text 'I understand that Direct Connect port charges apply once I click "Accept Connection"'. At the bottom of the details are two buttons: 'Accept Connection' and 'Decline Connection'.

	Provided By	Name	Location	Bandwidth	# VIs	State
<input type="checkbox"/>	Amazon Web Services	Far East Offices	Equinix SG2, Singapore	1Gbps	0	down
<input type="checkbox"/>	Amazon Web Services	Tokyo Office	Equinix SG2, Singapore	1Gbps	2	down
<input checked="" type="checkbox"/>	AnyCompany Hosting	Demo Hosted Connection	Equinix SG2, Singapore	50Mbps	0	pending acceptance

Connection Name: Demo Hosted Connection **Connection ID:** dxcon-fh6ajycc
Type: Hosted Connection **Port Speed:** 50Mbps
Location: Equinix SG2, Singapore **VLAN Assigned:** 100
Provided By: AnyCompany Hosting **Virtual Interfaces:** 0
State: pending acceptance

Before this connection can be active and used, you must accept it. If you accept, connectivity between your data center and AWS will be provided by partner.

I understand that Direct Connect port charges apply once I click "Accept 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'll 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.

Topics

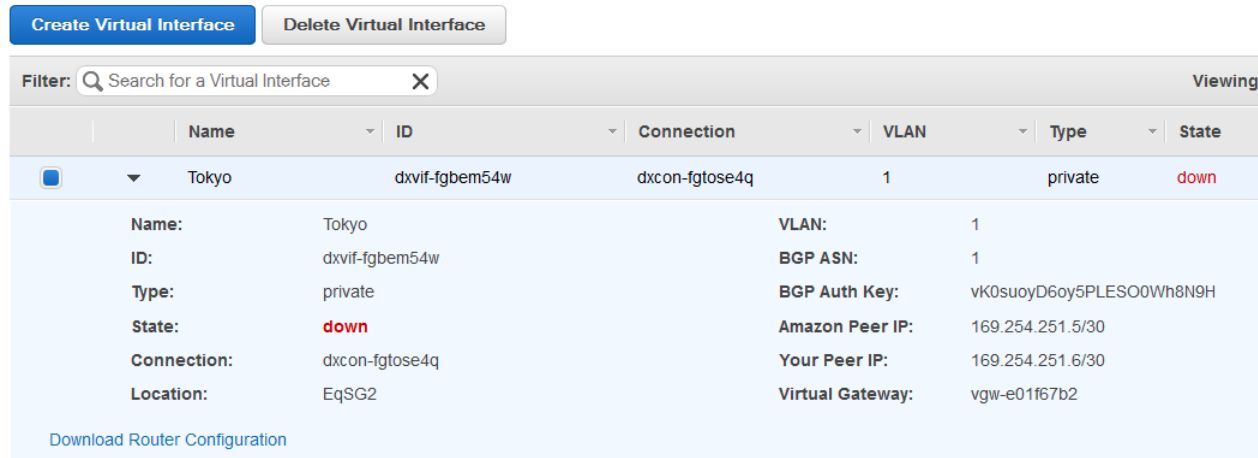
- [View Virtual Interface Details \(p. 33\)](#)
- [Delete a Virtual Interface \(p. 34\)](#)
- [Create a Hosted Virtual Interface \(p. 34\)](#)
- [Accept a Hosted Virtual Interface \(p. 35\)](#)

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 then 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 **Interface Name** field, enter a name for the virtual interface.
 - b. In **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. 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. 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.
 - f. 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 Authorization 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.

AWS Direct Connect User Guide

Accept a Hosted Virtual Interface

1 Virtual Interfaces Need to be Accepted
1 virtual interfaces have been created for you by another account, and will not be usable until you accept them.

Delete Virtual Interface

Filter: Search for a Virtual Interface X Viewing 1 of 1 Virtual Interfaces

Name	ID	Connection	VLAN	Type	State
test	dxvif-ftz4u8yv	dxcon-fgtxqsv2	101	private	pending acceptance

Connection: test VLAN Assigned: 101
ID: dxvif-ftz4u8yv BGP ASN: 65000
AWS Account: 966563127903 Your Peer IP:
Type: private Amazon Peer IP:
State: pending acceptance Virtual Gateway:
Connection: dxcon-fgtxqsv2
Location: EqSG2

Before this virtual interface can be active and used, you must accept it.
 I understand that I will be responsible for data transfer charges incurred for this interface.

Accept Virtual Interface Decline 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**.

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 \(p. 9\)](#).

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 \(p. 7\)](#).

Location	Region Served	How to Request Connection
CoreSite 32 Avenue of the Americas, New York	US East (N. Virginia)	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 Northern Virginia (CoreSite VA1 and VA2)	US East (N. Virginia)	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	Region Served	How to Request Connection
Equinix Ashburn (Equinix DC1-DC6, and DC10-DC11)	US East (N. Virginia)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Dallas (Equinix DA1-DA3, and DA6)	US East (N. Virginia)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
CoreSite One Wilshire and 900 North Alameda	US West (N. California)	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)	US West (N. California)	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)	US West (N. California)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Silicon Valley (Equinix SV1 and SV5)	US West (N. California)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
EdgeConneX, Portland, OR	US West (Oregon)	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)	US West (Oregon)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Switch SUPERNAP 8, Las Vegas, NV	US West (Oregon)	Requests for cross connects can be submitted by contacting Switch SUPERNAP at orders@super- nap.com .
Equinix Silicon Valley (Equinix SV1 and SV5)	AWS GovCloud (US)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Terremark NAP do Brasil, Sao Paulo	South America (São Paulo)	Requests for cross connects can be submitted by contacting Terremark at implementationbrasil@terremark.com .
Tivit	South America (São Paulo)	Requests for cross connects can be submitted by contacting Tivit at contact@tivit.com.br .
Eircom Clonshaugh	EU (Ireland)	Requests for cross connects can be submitted by contacting Eircom at awsorders@eircom.ie .
Equinix London (Slough) (Equinix LD4-LD6)	EU (Ireland)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .

Location	Region Served	How to Request Connection
TelecityGroup (Sovereign House, Harbor Exchange 6/7, Harbor Exchange 8/9, and London Meridian Gate)	EU (Ireland)	Requests for cross connects can be submitted by contacting the TelecityGroup Network Operations Center at amazon.orders@telecity.com .
Equinix Amsterdam (Equinix AM3)	EU (Frankfurt)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Frankfurt (Equinix FR5)	EU (Frankfurt)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Interxion Frankfurt	EU (Frankfurt)	Requests for cross connects can be submitted by emailing Customer.Services@interxion.com .
Telehouse Voltaire, Paris (TH2)	EU (Frankfurt)	Requests for cross connects can be submitted by creating a request at the Customer Portal . Request type: DFM/SFM Layout/Connectivity/MMR Circuit Commissioning
Sinnet Jiuxianqiao IDC	China (Beijing)	Requests for cross connects can be submitted by contacting Sinnet at dx-order@sinnnet.com.cn .
Equinix Osaka (Equinix OS1)	Asia Pacific (Tokyo)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Tokyo (Equinix TY2)	Asia Pacific (Tokyo)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Singapore (Equinix SG2)	Asia Pacific (Singapore)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Global Switch, Singapore	Asia Pacific (Singapore)	Requests for cross connects can be submitted by contacting Global Switch at salessingapore@glob-alswitch.com .
GPX Mumbai	Asia Pacific (Singapore)	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net .
Equinix Sydney (Equinix SY3)	Asia Pacific (Sydney)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Global Switch (Global Switch SY6)	Asia Pacific (Sydney)	Requests for cross connects can be submitted by contacting Global Switch at salessydney@glob-alswitch.com .
GPX Mumbai	Asia Pacific (Mumbai)	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net .
Sify Rabale, Mumbai	Asia Pacific (Mumbai)	Requests for cross connects can be submitted by contacting Sify at aws.directconnect@sifycorp.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 Amazon Web Services resources.

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 \(p. 42\)](#).

No AWS Direct Connect ARNs

AWS Direct Connect itself has no specific resources for you to control access to. Therefore, there are no AWS Direct Connect ARNs for you to use in an IAM policy. You use an asterisk (*) as the resource when writing a policy to control access to AWS Direct Connect actions. For more information about ARNs, see [ARNs](#) in *IAM User Guide*.

AWS Direct Connect Actions

In an IAM policy, you can specify any and 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 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 cloud resources.

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

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](#) (p. 43)
- [Understanding AWS Direct Connect Log File Entries](#) (p. 44)

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-fhajolly",
      "connectionName": "MyExampleConnection"
    }
  },
  ...additional entries
  ]
}
```

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

AWS Direct Connect User Guide
Understanding AWS Direct Connect Log File Entries

```
{
  "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-fhajoly",
        "newPrivateVirtualInterface": {
          "virtualInterfaceName": "MyVirtualInterface",
          "customerAddress": "[PROTECTED]",
          "authKey": "[PROTECTED]",
          "asn": -1,
          "virtualGatewayId": "vgw-bb09d4a5",
          "amazonAddress": "[PROTECTED]",
          "vlan": 123
        }
      },
      "responseElements": {
        "virtualInterfaceId": "dxvif-fgq6lm6w",
        "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-fhajoly",
        "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",
    }
  ]
}
```

AWS Direct Connect User Guide
Understanding AWS Direct Connect Log File Entries

```
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "Coral/Jakarta",
    "requestParameters": {
      "connectionId": "dxcon-fhajolly"
    },
    "responseElements": null
  },
  ...additional entries
]
}
```

Troubleshooting AWS Direct Connect

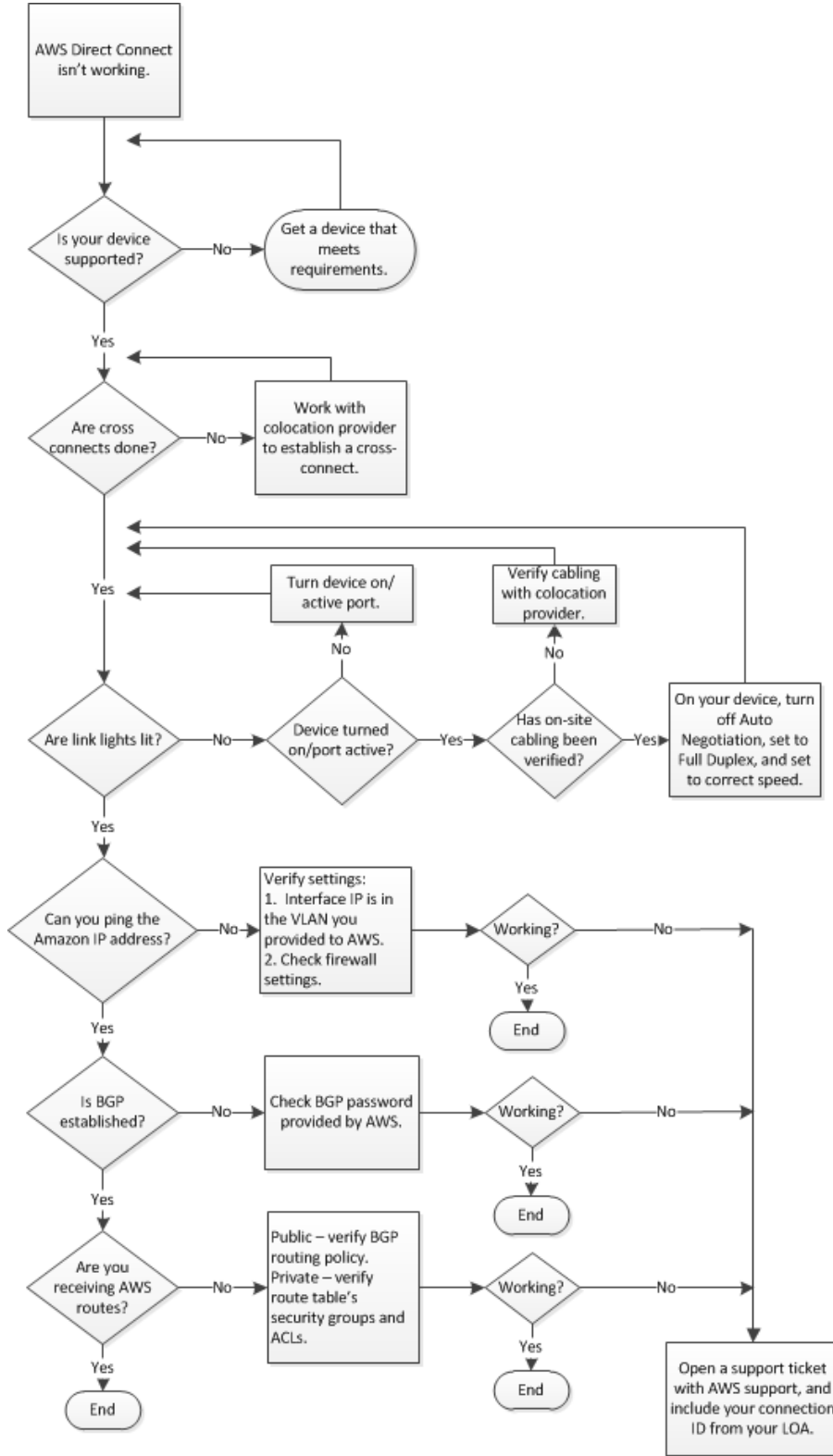
The following table lists troubleshooting resources that you'll find useful as you work with AWS Direct Connect.

Resource	Description
Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect (p. 48)	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. 50)	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. 50)	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. 52)	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 \(p. 50\)](#).

AWS Direct Connect User Guide
Flow Chart: Troubleshooting a Cross Connection to
AWS Direct Connect



Troubleshooting a Cross Connection to AWS Direct Connect

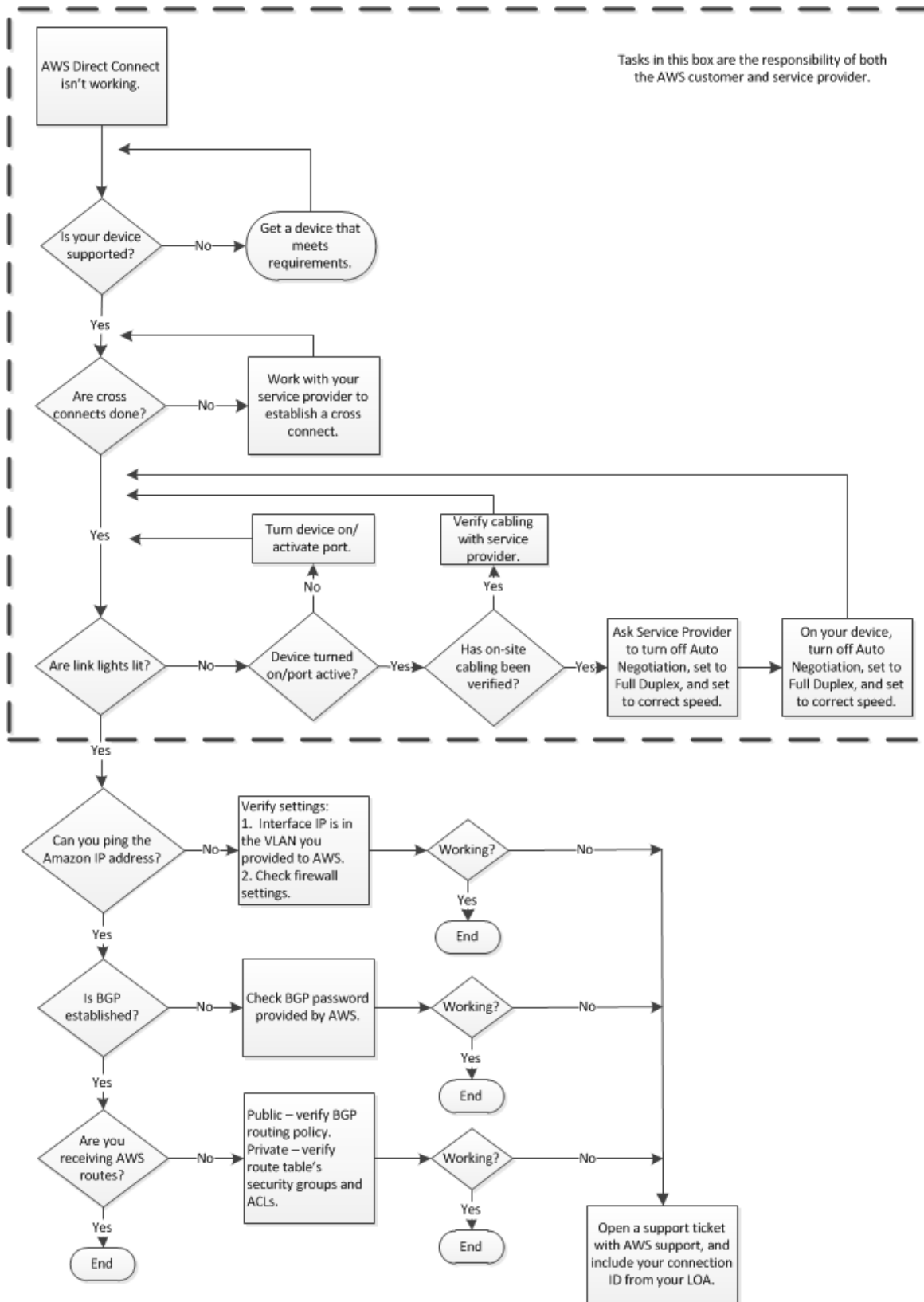
You can use the following tasks to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility. To see these tasks in a flow chart, see [Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect](#) (p. 48).

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. 52).

AWS Direct Connect User Guide
Flow Chart: Troubleshooting a Remote Connection to
AWS Direct Connect



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 \(p. 50\)](#).

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.

- [AWS Training and Courses](#) – 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 and resources that provide documentation, code samples, release notes, and other information to help you build innovative applications with AWS.
- [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
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
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

Change	Description	Release Date
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. 14) and Getting Started with a Sub-1G AWS Direct Connect Partner (p. 22) .	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. 43) .	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. 37) .	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. 41) .	2012-12-21
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

Change	Description	Release Date
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*.