
AWS Direct Connect

User Guide



Table of Contents

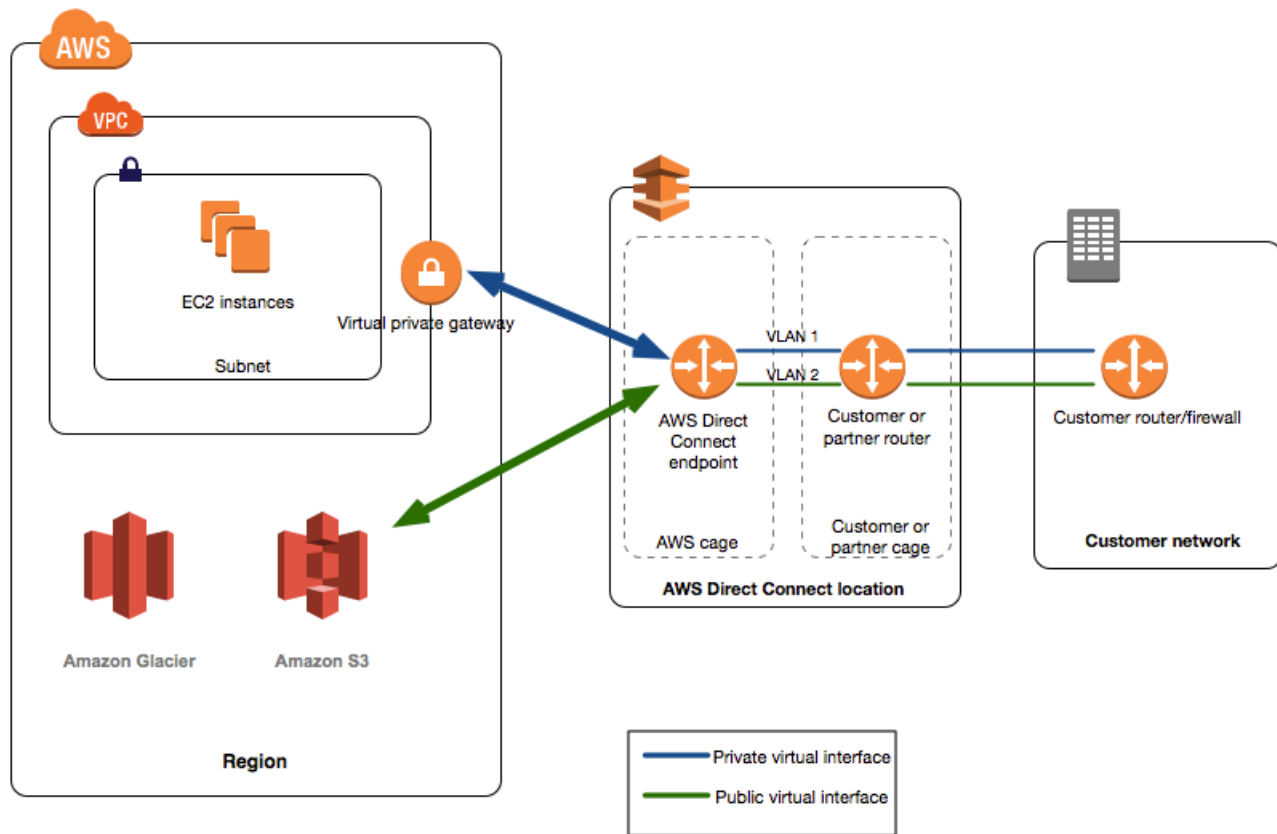
What is AWS Direct Connect?	1
AWS Direct Connect Components	2
Network Requirements	2
AWS Direct Connect Limits	3
Resources	3
Accessing a Remote AWS Region	3
Getting Started	5
Step 1: Sign Up for Amazon Web Services	5
Step 2: Submit AWS Direct Connect Connection Request	6
Accept Your Hosted Connection	7
Step 3: Download the LOA-CFA	7
Step 4: (Optional) Configure Redundant Connections	8
Step 5: Create a Virtual Interface	9
Step 6: Download Router Configuration	12
Step 7: Verify Your Virtual Interface	13
Connections	14
Creating a Connection	15
Downloading the LOA-CFA	16
Viewing Connection Details	16
Deleting a Connection	17
Accepting a Hosted Connection	17
Requesting Cross Connects	19
Virtual Interfaces	25
Prerequisites for Virtual Interfaces	25
Creating a Virtual Interface	26
Downloading the Router Configuration File	29
Viewing Virtual Interface Details	31
Deleting a Virtual Interface	32
Creating a Hosted Virtual Interface	32
Accepting a Hosted Virtual Interface	33
Adding or Removing a BGP Peer	34
Associating a Virtual Interface	36
LAGs	38
Creating a LAG	39
Updating a LAG	41
Associating a Connection with a LAG	41
Disassociating a Connection From a LAG	42
Deleting a LAG	42
Using IAM	44
AWS Direct Connect Actions	44
AWS Direct Connect Resources	44
AWS Direct Connect Keys	45
Example Policy for AWS Direct Connect	45
Using Tags	46
Tag Restrictions	46
Working with Tags	47
Using the AWS CLI	48
Step 1: Create a Connection	48
Step 2: Download the LOA-CFA	49
Step 3: Create a Virtual Interface and get the Router Configuration	49
Logging API Calls	54
AWS Direct Connect Information in CloudTrail	54
Understanding AWS Direct Connect Log File Entries	55
Troubleshooting	58

Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect	58
Troubleshooting a Cross Connection to AWS Direct Connect	60
Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect	60
Troubleshooting a Remote Connection to AWS Direct Connect	62
Document History	63
AWS Glossary	66

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 public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing Internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the region with which it is associated. You can provision a single connection to any AWS Direct Connect location in North America and use it to access public AWS services in all North America regions and AWS GovCloud (US).

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



Contents

- [AWS Direct Connect Components \(p. 2\)](#)
- [Network Requirements \(p. 2\)](#)
- [AWS Direct Connect Limits \(p. 3\)](#)
- [Resources \(p. 3\)](#)
- [Accessing a Remote AWS Region in North America \(p. 3\)](#)

AWS Direct Connect Components

The following are the key components that you'll use for AWS Direct Connect.

Connection	Create a <i>connection</i> in an AWS Direct Connect location to establish a network connection from your premises to an AWS region. For more information, see Connections (p. 14) .
Virtual Interface	Create a <i>virtual interface</i> to enable access to AWS services. A public virtual interface enables access to public-facing services, such as Amazon S3. A private virtual interface enables access to your VPC. For more information, see Virtual Interfaces (p. 25) and Prerequisites for Virtual Interfaces (p. 25) .

Network Requirements

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

- Your network is colocated with an existing AWS Direct Connect location. For more information about available AWS Direct Connect locations, see [AWS Direct Connect Product Details](#).
- You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). For information, see [APN Partners Supporting AWS Direct Connect](#).
- 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.

You can optionally configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but will not take effect until you configure it on your router.

AWS Direct Connect supports both the IPv4 and IPv6 communication protocols. IPv6 addresses provided by public AWS services are accessible through AWS Direct Connect public virtual interfaces.

AWS Direct Connect supports a maximum transmission unit (MTU) of up to 1522 bytes at the physical connection layer (14 bytes ethernet header + 4 bytes VLAN tag + 1500 bytes IP datagram + 4 bytes FCS).

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 on a private virtual interface	100	This limit cannot be increased.
Routes per Border Gateway Protocol (BGP) session on a public virtual interface	1,000	This limit cannot be increased.
Number of connections per link aggregation group (LAG)	4	This limit can be increased upon request.
Number of link aggregation groups (LAGs) per region	10	This limit can be increased upon request.

Resources

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

Resource	Description
AWS Direct Connect product information	General product overview.
Pricing	Calculate monthly costs.
AWS Developer Tools	Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
AWS Direct Connect FAQ	The top questions asked about this product.
AWS Direct Connect Forum	A community-based forum for discussing technical questions related to AWS Direct Connect.
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.
Contact Us	A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.

Accessing a Remote AWS Region in North America

AWS Direct Connect locations in North America can access public resources in any North America 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, see [Virtual Interfaces \(p. 25\)](#).

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 North America. 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.

Getting Started with AWS Direct Connect

You can set up an AWS Direct Connect connection in one of the following ways:

- At an AWS Direct Connect location.
- Through a member of the AWS Partner Network (APN) or a network carrier.
- Through a hosted connection provided by a member of the APN.

A partner in the APN can help you establish network circuits between an AWS Direct Connect location and your data center, office, or colocation environment, or provide colocation space within the same facility as the AWS Direct Connect location. For more information, see <http://aws.amazon.com/directconnect/partners>. 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 APN to connect you.

Before you begin, verify that your equipment meets the specifications set out in [Network Requirements \(p. 2\)](#).

Topics

- [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 \(p. 7\)](#)
- [Step 4: \(Optional\) Configure Redundant Connections \(p. 8\)](#)
- [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 <https://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. Before you begin, ensure that you have the following information:

- The port speed that you require: 1 Gbps or 10 Gbps. You cannot change the port speed after you've created the connection request.
- The AWS Direct Connect location to which to connect.

If you require a port speed less than 1 Gbps, you cannot request a connection using the console. Instead, contact an APN partner, who will create a hosted connection for you. The hosted connection appears in your AWS Direct Connect console, and must be accepted before use. Skip the following procedure and go to [Accept Your Hosted Connection \(p. 7\)](#).

To create a new AWS Direct Connect connection

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation bar, select the region in which to connect to AWS Direct Connect. 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 US East (N. Virginia). Use the region selector to change to another AWS region.

To begin, name your new Connection, select the AWS Direct Connect location in this region where you would like to connect, and the port speed. For more information, see [Regions and Endpoints](#). For other options to connect you can [contact one of our partners](#).

This connection will have access to AWS public services in all North American regions. For more information, [see the user guide](#).

Please note that port-hours are billed once the connection between the AWS router and your router is established, or 90 days after you create the connection. For more information, please [see our FAQ](#).

Connection Name ⓘ

LAG Association None (Stand-alone Connection) Associate with LAG ⓘ

Location ⓘ

Port Speed 1Gbps 10Gbps ⓘ

- a. For **Connection Name**, enter a name for the connection.
- b. For **LAG Association**, specify whether the connection is standalone, or if it should be associated with a link aggregation group (LAG) in your account. If you associate the connection with a LAG, select the LAG ID. The connection is created with the same port speed and location as specified in the LAG. For more information, see [Link Aggregation Groups \(p. 38\)](#).

- c. 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**.

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

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

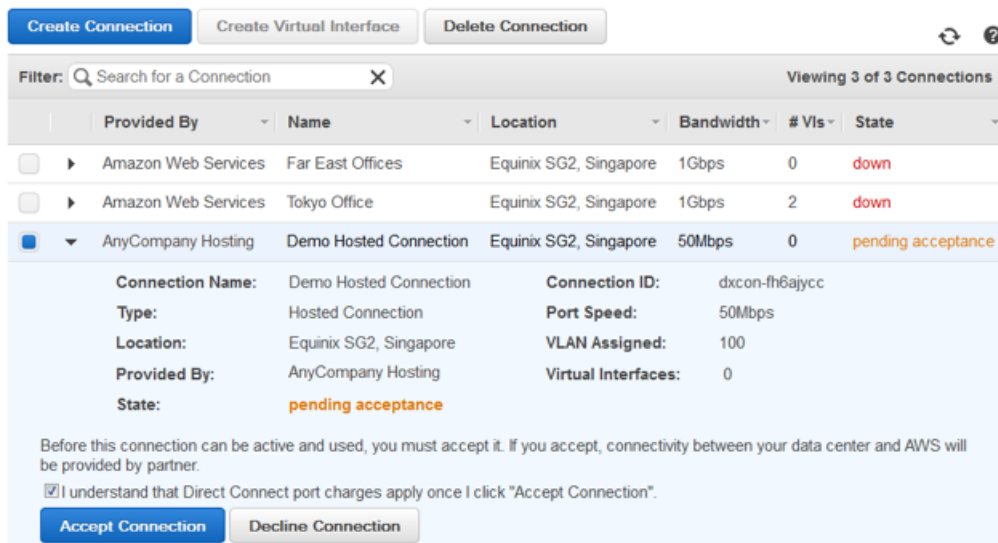
For more information about creating and working with AWS Direct Connect connections, see [Connections](#) (p. 14).

Accept Your Hosted Connection

If you requested a sub-1G connection from your selected partner, they create a hosted connection for you. You must 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, select the region in which the hosted connection resides. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select a connection, and then choose the arrow to expand details about the connection.



5. Select **I understand that Direct Connect port charges apply once I click "Accept This Connection"**, and then choose **Accept Connection**.
6. Go to [Step 4](#) (p. 8) to continue setting up your AWS Direct Connect connection.

Step 3: Download the LOA-CFA

AWS makes a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) available to you to download, or emails 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

is deleted. The LOA-CFA is the authorization to connect to AWS, and is required by the colocation provider or your network provider to establish the cross-network connection (cross-connect).

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 to have 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, do one of the following:

- If you're working with a network provider, send the LOA-CFA to your network provider so that they can order a cross connect for you. You cannot order a cross connect for yourself in the AWS Direct Connect location if you do not have equipment there. Your network provider does this for you.
- If you have equipment at the AWS Direct Connect location, contact the colocation provider to request a cross-network connection. For more information, see [Requesting Cross Connects at AWS Direct Connect Locations](#) (p. 19). 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, as well as the necessary information to connect to your network.

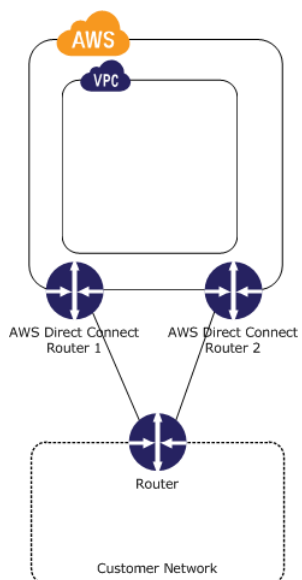
The LOA-CFA expires after 90 days. To refresh the LOA-CFA with a new issue date, you can download it again from the AWS Direct Connect console. If you do not take any action, we delete the connection.

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](#).

Step 4: (Optional) Configure Redundant Connections

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).** This is the default configuration, where both connections are active. AWS Direct Connect supports multipathing to multiple virtual interfaces within the same location, and traffic is load-shared between interfaces based on flow. If one connection becomes unavailable, all traffic is routed through the other connection.
- **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 need to prepend the AS path to the routes on one of your links for that 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.

Step 5: Create a Virtual Interface

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to begin using it. You can create a private virtual interface to connect to your VPC, or you can create a public virtual interface to connect to AWS services that aren't in a VPC.

Before you begin, ensure that you have the following information:

- A unique virtual local area network (VLAN) tag that's not in use on the AWS Direct Connect connection for another virtual interface. The number must be between 1 and 4094.
- 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.
- (Public virtual interface): For an IPv4 BGP peering session, unique public IPv4 addresses (/30) that you own for each side of the BGP peering connection, and a unique IPv4 CIDR range to announce via AWS Direct Connect.
- (Private virtual interface): The virtual private gateway to connect to. For more information, see [Adding a Hardware Virtual Private Gateway to Your VPC](#) in the *Amazon VPC User Guide*.

For more information, see [Prerequisites for Virtual Interfaces \(p. 25\)](#).

Note

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

To provision a public virtual interface to non-VPC services

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the **Connections** pane, select the connection to use, and then choose **Actions, Create Virtual Interface**.
3. 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

This virtual interface will have access to AWS public services in all US regions. For more information, [see the user guide](#).

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 interfaces, see the [AWS Direct Connect Getting Started Guide](#).

Connection: dxcon-fgvg1fy7 (USWest1) ⓘ

Virtual Interface Name: e.g. My Virtual Interface ⓘ

Virtual 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: e.g. 100 ⓘ

Address family: IPv4 IPv6 ⓘ

Your router peer IP: e.g. example 8.18.144.0 ⓘ

Amazon router peer IP: e.g. example 8.18.144.1 ⓘ

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 to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: e.g. 65000 ⓘ

Auto-generate BGP key: ⓘ

Prefixes you want to advertise: e.g. 192.0.2.0/28,192.0.2.1/28 ⓘ

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

4. In the **Define Your New Public Virtual Interface** dialog box, do the following:
 - a. For **Connection**, select an existing physical connection on which to create the virtual interface.
 - b. For **Virtual Interface Name**, enter a name for the virtual interface.
 - c. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account ID.
 - d. For **VLAN**, enter the VLAN number.
 - e. If you're configuring an IPv4 BGP peer, choose **IPv4** and do the following:
 - For **Your router peer IP**, enter the IPv4 CIDR destination address to which Amazon should send traffic.
 - For **Amazon router peer IP**, enter the IPv4 CIDR address to use to send traffic to Amazon.
 - f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
 - g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway.
 - h. Select the **Auto-generate BGP key** check box to have Amazon generate a BGP key.

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

- i. For **Prefixes you want to advertise**, enter the IPv4 CIDR destination addresses (separated by commas) to which traffic should be routed over the virtual interface.
5. Choose **Continue**, and then download your router configuration. For more information, see [Step 6: Download Router Configuration \(p. 12\)](#).

When you create a private virtual interface to a VPC, you need a private virtual interface for each VPC to which to connect. For example, you need three private virtual interfaces to connect to three VPCs.

To provision a private virtual interface to a VPC

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the **Connections** pane, select the connection to use, and then choose **Actions, Create Virtual Interface**.
3. In the **Create a Virtual Interface** pane, choose **Private**.

The screenshot shows the 'Create a Virtual Interface' page in the AWS Direct Connect console. At the top, there are two radio buttons: 'Private' (selected) and 'Public'. Below this is the 'Define Your New Private Virtual Interface' section. It includes a 'Connection' dropdown menu, a 'Virtual Interface Name' text input, a 'Virtual Interface Owner' radio button selection (selected 'My AWS Account'), and a 'VGW' dropdown menu. Below these are fields for 'VLAN', 'Address family' (selected 'IPv4'), 'Auto-generate peer IPs' (checkbox), 'Your router peer IP', and 'Amazon router peer IP'. At the bottom, there is a 'BGP ASN' text input and an 'Auto-generate BGP key' checkbox (checked).

4. Under **Define Your New Private Virtual Interface**, do the following:
 1. For **Virtual Interface Name**, enter a name for the virtual interface.
 2. For **Virtual Interface Owner**, choose the **My AWS Account** option if the virtual interface is for your AWS account ID.
 3. For **VGW**, select the virtual gateway to which to connect.
 4. For **VLAN #**, enter the VLAN number.
 5. If you're configuring an IPv4 BGP peer, choose **IPv4** and do the following:
 - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.

- To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box. For **Your router peer IP**, enter the destination IPv4 CIDR address to which Amazon should send traffic. For **Amazon router peer IP**, enter the IPv4 CIDR address to use to send traffic to Amazon.
6. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
 7. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway.
 8. To have Amazon generate a BGP key, select the **Auto-generate BGP key** check box.

To provide your own BGP key, clear the **Auto-generate BGP key** check box. For **BGP Authentication Key**, enter your BGP MD5 key.
5. Choose **Continue**, and then download your router configuration. For more information, see [Step 6: Download Router Configuration \(p. 12\)](#).

Note

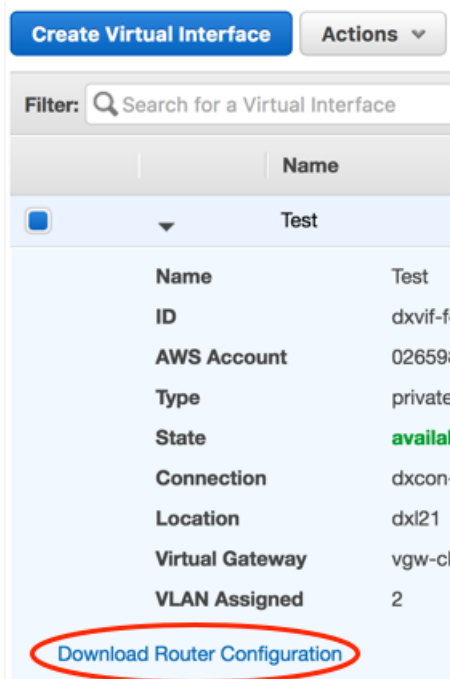
If you use the VPC wizard to create a VPC, route propagation is automatically enabled for you. With route propagation, routes are automatically populated to the route tables in your VPC. If you choose, you can disable route propagation. For more information, see [Enable Route Propagation in Your Route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

For example configuration files, see [Example Router Configuration Files \(p. 30\)](#).

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 connection using the following procedures.

To verify your virtual interface connection to the AWS Cloud

- Run `tracert` 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 an Amazon Linux AMI, 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 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 IPv4 address (for example, 10.0.0.4). The Amazon EC2 console displays the address as part of the instance details.
3. Ping the private IPv4 address and get a response.

Connections

To create an AWS Direct Connect connection, you need the following information:

- **AWS Direct Connect location**

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. For the list of AWS Direct Connect partners who belong to the APN, see [APN Partners Supporting AWS Direct Connect](#).

- **Port speed**

AWS Direct Connect supports two port speeds: 1 Gbps: 100BASE-LX (1310nm) over single-mode fiber and 10 Gbps: 10GBASE-LR (1310nm) over single-mode fiber. 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 1 Gbps, you cannot request a connection using the console. Instead, you can contact an APN partner who supports AWS Direct Connect and who can provision a hosted connection for you.

After you've requested the connection, AWS makes a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) available to you to download, or emails you with a request for more information. If you receive a request for more information, you must respond within 7 days or the connection is deleted. The LOA-CFA is the authorization to connect to AWS, and is required by your network provider to order a cross connect for you. You cannot order a cross connect for yourself in the AWS Direct Connect location if you do not have equipment there; your network provider does this for you.

For information about associating a connection with a link aggregation group (LAG), see [Associating a Connection with a LAG \(p. 41\)](#).

After you've created a connection, create a virtual interface to connect to public and private AWS resources. For more information, see [Virtual Interfaces \(p. 25\)](#).

Topics

- [Creating a Connection \(p. 15\)](#)

- [Viewing Connection Details](#) (p. 16)
- [Deleting a Connection](#) (p. 17)
- [Accepting a Hosted Connection](#) (p. 17)

Creating a Connection

You can create a standalone connection, or you can create a connection to associate with a LAG in your account. If you associate a connection with a LAG, it's created with the same port speed and location as specified in the LAG.

To create a new connection

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation bar, select the region in which to connect to AWS Direct Connect. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, choose **Connections, Create Connection**.
4. In the **Create a Connection** dialog box, enter the following values, and then choose **Create**:

Create a Connection

You are currently operating in US East (N. Virginia). Use the region selector to change to another AWS region.

To begin, name your new Connection, select the AWS Direct Connect location in this region where you would like to connect, and the port speed for your use case, for other options to connect you can [contact one of our partners](#).

This connection will have access to AWS public services in all North American regions. For more information, [see the user guide](#).

Please note that port-hours are billed once the connection between the AWS router and your router is established, or 90 days after you establish the connection. For more information, please [see our FAQ](#).

Connection Name ⓘ

LAG Association None (Stand-alone Connection) Associate with LAG ⓘ

Location ⌵ ⓘ

Port Speed 1Gbps 10Gbps ⓘ

- a. For **Connection Name**, enter a name for the connection.
- b. For **LAG Association**, specify whether the connection is standalone, or if it should be associated with a LAG. If you associate the connection with a LAG, select the LAG ID.
- c. 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**.

- d. Select the appropriate port speed that is compatible with your existing network.

To create a connection using the command line or API

- [create-connection](#) (AWS CLI)
- [CreateConnection](#) (AWS Direct Connect API)

Downloading the LOA-CFA

After AWS has processed your connection request, you can download the Letter of Authorization and Connecting Facility Assignment (LOA-CFA).

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 to have it 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.
6. Send the LOA-CFA to your network provider or colocation provider so that they can order a cross connect for you. The contact process can vary for each colocation provider. For more information, see [Requesting Cross Connects at AWS Direct Connect Locations \(p. 19\)](#).

The LOA-CFA expires after 90 days. If your connection is not up after 90 days, we send you an email alerting you that the LOA-CFA has expired. To refresh the LOA-CFA with a new issue date, download it again from the AWS Direct Connect console. If you do not take any action, we 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 Direct Connect endpoint 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 [Deleting a Connection \(p. 17\)](#).

To download the LOA-CFA using the command line or API

- [describe-loa](#) (AWS CLI)
- [DescribeLoa](#) (AWS Direct Connect API)

Viewing Connection Details

You can view the current status of your connection. You can also view your connection ID (for example, `dxcon-12nikabc`) and verify that it matches the connection ID on the Letter of Authorization and Connecting Facility Assignment (LOA-CFA) that you received or downloaded.

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 in the navigation bar. 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.

To describe a connection using the command line or API

- [describe-connections](#) (AWS CLI)
- [DescribeConnections](#) (AWS Direct Connect API)

Deleting 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 [Deleting a Virtual Interface](#) (p. 32).

If the connection is part of a link aggregation group (LAG), you cannot delete the connection if doing so will cause the LAG to fall below its setting for minimum number of operational connections.

To delete a connection

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. If necessary, change the region in the navigation bar. 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 **Actions, Delete Connection**.
5. In the **Delete Connection** dialog box, choose **Delete**.

To delete a connection using the command line or API

- [delete-connection](#) (AWS CLI)
- [DeleteConnection](#) (AWS Direct Connect API)

Accepting 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 in the navigation bar. 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 buttons for 'Create Connection', 'Create Virtual Interface', and 'Delete Connection'. Below these is a search filter 'Filter: Search for a Connection' and a refresh icon. The main area displays a table of connections:

Provided By	Name	Location	Bandwidth	# VIs	State
Amazon Web Services	Far East Offices	Equinix SG2, Singapore	1Gbps	0	down
Amazon Web Services	Tokyo Office	Equinix SG2, Singapore	1Gbps	2	down
AnyCompany Hosting	Demo Hosted Connection	Equinix SG2, Singapore	50Mbps	0	pending acceptance

The 'Demo Hosted Connection' is expanded to show details:

- Connection Name:** Demo Hosted Connection
- Connection ID:** dxcon-fh8ajycc
- 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 warning: '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.' A checkbox is checked with the text 'I understand that Direct Connect port charges apply once I click "Accept Connection"'. At the bottom are 'Accept Connection' and 'Decline Connection' buttons.

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

To accept a hosted connection using the command line or API

- `confirm-connection` (AWS CLI)
- `ConfirmConnection` (AWS Direct Connect API)

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 [Downloading the LOA-CFA \(p. 16\)](#).

- [Asia Pacific \(Tokyo\) \(p. 20\)](#)
- [Asia Pacific \(Singapore\) \(p. 20\)](#)
- [Asia Pacific \(Sydney\) \(p. 20\)](#)
- [Asia Pacific \(Mumbai\) \(p. 20\)](#)
- [Canada \(Central\) \(p. 21\)](#)
- [China \(Beijing\) \(p. 21\)](#)
- [EU \(Frankfurt\) \(p. 21\)](#)
- [EU \(Ireland\) \(p. 21\)](#)
- [EU \(London\) \(p. 22\)](#)

- [South America \(São Paulo\)](#) (p. 22)
- [US East \(N. Virginia\)](#) (p. 22)
- [US East \(Ohio\)](#) (p. 23)
- [AWS GovCloud \(US\)](#) (p. 23)
- [US West \(N. California\)](#) (p. 23)
- [US West \(Oregon\)](#) (p. 23)

Asia Pacific (Tokyo)

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

Asia Pacific (Singapore)

Location	How to request a connection
Equinix Singapore (Equinix SG2)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Global Switch, Singapore	Requests for cross connects can be submitted by contacting Global Switch at salesingapore@globalswitch.com .
GPX Mumbai	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net .
iAdvantage MEGA-i, Hong Kong	Requests for cross connects can be submitted by contacting iAdvantage at cs@iadvantage.net or by placing an order at iAdvantage Cabling Order e-Form .

Asia Pacific (Sydney)

Location	How to request a connection
Equinix Sydney (Equinix SY3)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Global Switch (Global Switch SY6)	Requests for cross connects can be submitted by contacting Global Switch at salesydney@globalswitch.com .
NEXTDC Melbourne (NEXTDC M1)	Requests for cross connects can be submitted by contacting NEXTDC at nxtops@nextdc.com .

Asia Pacific (Mumbai)

Location	How to request a connection
GPX Mumbai	Requests for cross connects can be submitted by contacting GPX at nkankane@gpxglobal.net .

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

Canada (Central)

Location	How to request connection
Cologix Montreal	Requests for cross connects can be submitted by contacting Cologix at aws@cologix.com .
Netelligent Montreal	Requests for cross connects can be submitted by contacting Netelligent at directconnect@netelligent.ca .

China (Beijing)

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

EU (Frankfurt)

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

EU (Ireland)

Location	How to request a connection
Digital Realty (UK) (Sovereign House and London Meridian Gate)	Requests for cross connects can be submitted by contacting Digital Realty (UK) at amazon.orders@digitalrealty.com .

Location	How to request a connection
Eircom Clonshaugh	Requests for cross connects can be submitted by contacting Eircom at awsorders@eircom.ie .
Equinix London (Slough) (Equinix LD4-LD6)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Interxion Dublin	Requests for cross connects can be submitted by contacting Interxion at customer.services@interxion.com .

EU (London)

Location	How to request connection
Digital Realty (UK) (Sovereign House and London Meridian Gate)	Requests for cross connects can be submitted by contacting Digital Realty (UK) at amazon.orders@digitalrealty.com .
Equinix London (Slough) (Equinix LD4-LD6)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .

South America (São Paulo)

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

US East (N. Virginia)

Location	How to request a connection
CoreSite 32 Avenue of the Americas, New York	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal . After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.
CoreSite Northern Virginia (CoreSite VA1 and VA2)	Requests for cross connects can be submitted by placing an order at the CoreSite Customer Portal . After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.
Equinix Ashburn (Equinix DC1-DC6, and DC10-DC11)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .
Equinix Dallas (Equinix DA1-DA3, and DA6)	Requests for cross connects can be submitted by contacting Equinix at awsdealreg@equinix.com .

US East (Ohio)

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

AWS GovCloud (US)

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

US West (N. California)

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

US West (Oregon)

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

Location	How to request a connection
TierPoint Seattle	Requests for cross connects can be submitted by contacting TierPoint at sales@tierpoint.com .

Virtual Interfaces

You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a private virtual interface to connect to your VPC, or you can create a public virtual interface to connect to AWS services that aren't in a VPC, such as Amazon S3 and Amazon Glacier. You can configure multiple virtual interfaces on a single AWS Direct Connect connection. For private virtual interfaces, you need one private virtual interface for each VPC to connect to from the AWS Direct Connect connection.

To connect to other AWS services using IPv6 addresses, check the service documentation to verify that IPv6 addressing is supported.

We advertise appropriate Amazon prefixes to you so you can reach either your VPCs or other AWS services. You can access all AWS prefixes in your region through this connection; for example, Amazon EC2, 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 use your AWS Direct Connect connection with another AWS account, you can create a hosted virtual interface for that account. A hosted virtual interface works the same as a standard virtual interface and can connect to public resources or a VPC.

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

Contents

- [Prerequisites for Virtual Interfaces \(p. 25\)](#)
- [Creating a Virtual Interface \(p. 26\)](#)
- [Viewing Virtual Interface Details \(p. 31\)](#)
- [Deleting a Virtual Interface \(p. 32\)](#)
- [Creating a Hosted Virtual Interface \(p. 32\)](#)
- [Accepting a Hosted Virtual Interface \(p. 33\)](#)
- [Adding or Removing a BGP Peer \(p. 34\)](#)
- [Associating a Virtual Interface with a Connection or LAG \(p. 36\)](#)

Prerequisites for Virtual Interfaces

The following information is needed for a virtual interface:

- **VLAN:** Each virtual interface must be tagged with a new, unused customer-provided tag (VLAN ID) that complies with the Ethernet 802.1Q standard. This tag is required for any traffic traversing the AWS Direct Connect connection. The number must be between 1 and 4094.
- **Peer IP addresses:** The IP address ranges that are assigned to each end of the virtual interface for the BGP peering session. A virtual interface can support a BGP peering session for IPv4, IPv6, or one of each (dual-stack). You cannot create multiple BGP sessions for the same IP addressing family on the same virtual interface.
 - IPv4: For a public virtual interface, you must specify public IPv4 addresses (/30) that you own. For a private virtual interface, Amazon can generate private IPv4 addresses for you.
 - IPv6: Regardless of the type of virtual interface, Amazon automatically allocates you a /125 IPv6 CIDR. You cannot specify your own peer IPv6 addresses.
- **BGP information:** A virtual interface must have 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 does not work if you use a private ASN. You can provide your own MD5 BGP authentication key, or you can let Amazon generate one for you.
- (Private virtual interface only) The virtual private gateway for your VPC. For more information, see [Adding a Hardware Virtual Private Gateway to Your VPC](#) in the *Amazon VPC User Guide*.
- (Public virtual interface only) Public IPv4 routes or IPv6 routes that you will advertise over BGP. You must advertise at least one prefix using BGP, up to a maximum of 100 prefixes.
 - IPv4: The IPv4 CIDR must not overlap with another IPv4 CIDR announced via AWS Direct Connect. If you do not have public IPv4 addresses, [open a ticket with AWS Support](#).
 - IPv6: Specify a prefix length of /64 or shorter.

Creating a Virtual Interface

You can create a public virtual interface to connect to public resources (non-VPC services), or a private virtual interface to connect to your VPC.

Before you begin, ensure that you have read the information in [Prerequisites for Virtual Interfaces](#) (p. 25).

To provision a public virtual interface

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **Connections**, select the connection to use, and then choose **Actions**, **Create Virtual Interface**.
3. 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

This virtual interface will have access to AWS public services in all US regions. For more information, [see the user guide](#).

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 interfaces, see the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Virtual Interface Name: ⓘ

Virtual 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: ⓘ

Address family: IPv4 IPv6 ⓘ

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 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.

4. In the **Define Your New Public Virtual Interface** dialog box, do the following:
 - a. For **Connection**, select an existing physical connection on which to create the virtual interface.
 - b. For **Virtual Interface Name**, enter a name for the virtual interface.
 - c. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account.
 - d. For **VLAN**, enter the ID number for your virtual local area network (VLAN).
 - e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:
 - For **Your router peer IP**, enter the IPv4 CIDR destination address to which Amazon should send traffic.
 - For **Amazon router peer IP**, enter the IPv4 CIDR address to use to send traffic to Amazon.
 - f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
 - g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway.
 - h. To have AWS generate a BGP key, select the **Auto-generate BGP key** check box .

To provide your own BGP key, clear the **Auto-generate BGP key** check box. For **BGP Authentication Key**, enter your BGP MD5 key.
 - i. For **Prefixes you want to advertise**, enter the IPv4 CIDR destination addresses (separated by commas) to which traffic should be routed over the virtual interface.
5. Choose **Continue**.

After you've created the virtual interface, you can download the router configuration for your device. For more information, see [Downloading the Router Configuration File \(p. 29\)](#).

To provision a private virtual interface to a VPC

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **Connections**, select the connection to use, and choose **Create Virtual Interface**.
3. 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 interfaces, see the [AWS Direct Connect Getting Started Guide](#).

Connection: ⓘ

Virtual Interface Name: ⓘ

Virtual 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: ⓘ

Address family: IPv4 IPv6 ⓘ

Auto-generate peer IPs: ⓘ

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. You will also need an MD5 key to authenticate the BGP session. When you can supply your own.

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

4. Under **Define Your New Private Virtual Interface**, do the following:
 - a. For **Virtual Interface Name**, enter a name for the virtual interface.
 - b. For **Virtual Interface Owner**, select the **My AWS Account** option if the virtual interface is for your AWS account.
 - 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).
 - e. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:
 - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
 - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box. For **Your router peer IP**, enter the destination IPv4 CIDR address to which Amazon should send traffic. For **Amazon router peer IP**, enter the IPv4 CIDR address to use to send traffic to AWS.
 - f. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
 - g. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway.
 - h. To have AWS generate a BGP key, select the **Auto-generate BGP key** check box .

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

5. Choose **Continue**.

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*.

After you've created the virtual interface, you can download the router configuration for your device. For more information, see [Downloading the Router Configuration File \(p. 29\)](#).

To create a private virtual interface using the command line or API

- [create-private-virtual-interface](#) (AWS CLI)
- [CreatePrivateVirtualInterface](#) (AWS Direct Connect API)

To create a public virtual interface using the command line or API

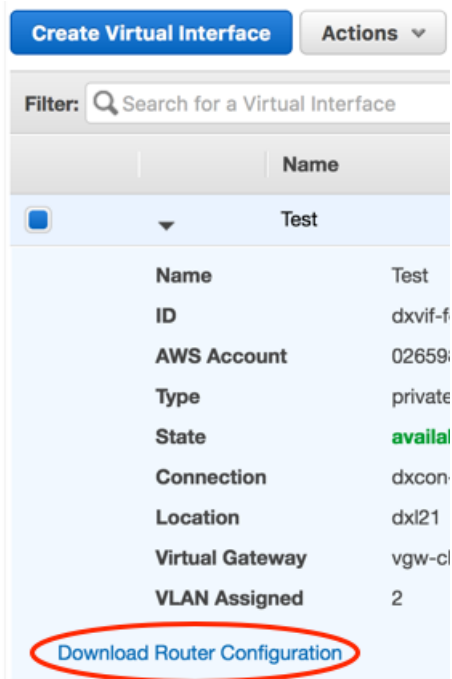
- [create-public-virtual-interface](#) (AWS CLI)
- [CreatePublicVirtualInterface](#) (AWS Direct Connect API)

Downloading the Router Configuration File

After you've created the virtual interface, you can download the router configuration file for your router, and then use the appropriate configuration to ensure that you can connect to AWS Direct Connect.

To download a router configuration

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the **Virtual Interfaces** pane, select the 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 Router Configuration**.

Example Router Configuration Files

The following are examples of router configuration files.

Cisco IOS

```
interface GigabitEthernet0/1
no ip address

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

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

! Optionally configure Bidirectional Forwarding Detection (BFD).

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

Cisco NX-OS

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

interface VlanVLAN_NUMBER
ip address YOUR_PEER_IP/30
no shutdown

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

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

! Optionally configure Bidirectional Forwarding Detection (BFD).

feature bfd
interface VlanVLAN_NUMBER
bfd interval 300 min_rx 300 multiplier 3
```

```
router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as 7224
bfd
```

Juniper JunOS

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

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

set routing-options autonomous-system CUSTOMER_BGP_ASN

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

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

# Optionally configure Bidirectional Forwarding Detection (BFD).

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

Viewing 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 in the navigation bar. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, choose **Virtual Interfaces**.
4. In the **Virtual Interfaces** pane, select a virtual interface and choose the arrow next to the virtual interface to view its details.

The screenshot shows the AWS Direct Connect console interface. At the top, there is a 'Create Virtual Interface' button and an 'Actions' dropdown menu. Below this is a search filter: 'Filter: Search for a Virtual Interface'. The main content area displays a table with one virtual interface listed:

Name	ID	Connection	VLAN	Type
Test	dxvif-fg1vuj3d	dxcon-fguhmqlc	125	private

Below the table, there is a detailed view of the selected virtual interface 'Test':

Name	Test	BGP Status	down
ID	dxvif-fg1vuj3d	BGP ASN	65000
AWS Account	803981987763	BGP Auth Key	0xC_ukbCerl6EYA0uHMXBlmN
Type	private	Your Peer IP	169.254.255.2/30
State	available	Amazon Peer IP	169.254.255.1/30
Connection	dxcon-fguhmqlc		
Location	EqDC2		
Virtual Gateway	vgw-f9eb0c90		
VLAN Assigned	125		

At the bottom of the details view, there is a link: 'Download Router Configuration'.

To describe virtual interfaces using the command line or API

- [describe-virtual-interfaces](#) (AWS CLI)
- [DescribeVirtualInterfaces](#) (AWS Direct Connect API)

Deleting 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 in the navigation bar. 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 **Actions, Delete Virtual Interface**.
5. In the **Delete Virtual Interface** dialog box, choose **Delete**.

To delete a virtual interface using the command line or API

- [delete-virtual-interface](#) (AWS CLI)
- [DeleteVirtualInterface](#) (AWS Direct Connect API)

Creating a Hosted Virtual Interface

You can create a public or private hosted virtual interface. Before you begin, ensure that you have read the information in [Prerequisites for Virtual Interfaces](#) (p. 25).

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 in the navigation bar. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, choose **Connections**.
4. In the **Connections** pane, select the connection to which to add a virtual interface and 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. For **Virtual Interface Name**, enter a name for the virtual interface.
 - b. For **Virtual Interface Owner**, choose **Another AWS Account**. For **Account ID**, enter the AWS account ID number to associate as the owner of this virtual interface.
 - c. For **VLAN #**, enter the ID number for your virtual local area network (VLAN).
 - d. If you're configuring an IPv4 BGP peer, choose **IPv4**, and do the following:
 - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
 - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box. For **Your router peer IP**, enter the destination IPv4 CIDR address to which Amazon should send traffic. For **Amazon router peer IP**, enter the IPv4 CIDR address to use to send traffic to AWS.
 - e. If you're configuring an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
 - f. For **BGP ASN**, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway.
 - g. Select the **Auto-generate BGP key** check box if you would like AWS to generate one for you.

To provide your own BGP key, clear the **Auto-generate BGP key** check box. For **BGP Authentication Key**, enter your BGP MD5 key.
7. Choose **Continue**. The new interface is added to the list of virtual interfaces on the **Virtual Interfaces** pane.
8. After the hosted virtual interface is accepted by the owner of the other AWS account, you can [download the router configuration file \(p. 29\)](#).

To create a hosted private virtual interface using the command line or API

- [allocate-private-virtual-interface](#) (AWS CLI)
- [AllocatePrivateVirtualInterface](#) (AWS Direct Connect API)

To create a hosted public virtual interface using the command line or API

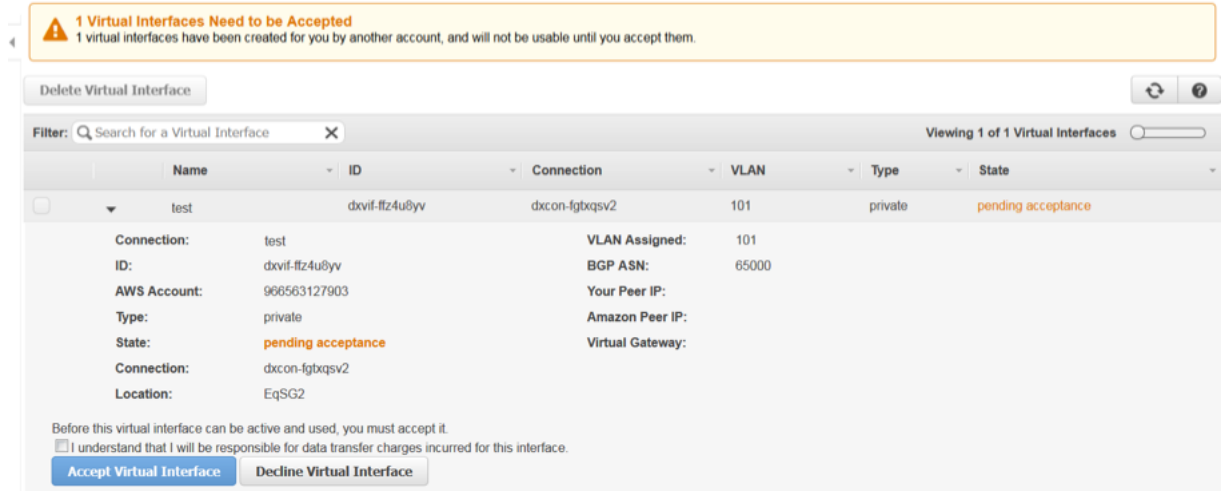
- [allocate-public-virtual-interface](#) (AWS CLI)
- [AllocatePublicVirtualInterface](#) (AWS Direct Connect API)

Accepting 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 in the navigation bar. 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 and choose the arrow to expand details about the virtual interface.



5. Select the **I understand that I will be responsible for data transfer charges incurred for this interface** check box and choose **Accept Virtual Interface**.
6. In the **Accept Virtual Interface** dialog box, select a virtual private gateway, and choose **Accept**.
7. After you've accepted the hosted virtual interface, the owner of the AWS Direct Connect connection can download the router configuration file. The **Download Router Configuration** option is not available for the account that accepts the hosted virtual interface.

To accept a hosted private virtual interface using the command line or API

- [confirm-private-virtual-interface](#) (AWS CLI)
- [ConfirmPrivateVirtualInterface](#) (AWS Direct Connect API)

To accept a hosted public virtual interface using the command line or API

- [confirm-public-virtual-interface](#) (AWS CLI)
- [ConfirmPublicVirtualInterface](#) (AWS Direct Connect API)

Adding or Removing a BGP Peer

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

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

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

To add a BGP peer

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **Virtual Interfaces** and select the virtual interface.
3. Choose **Actions, Add Peering**.
4. (Private virtual interface) To add an IPv4 BGP peer, do the following:
 - To have AWS generate your router IP address and Amazon IP address, select **Auto-generate peer IPs**.
 - To specify these IP addresses yourself, clear the **Auto-generate peer IPs** check box. For **Your router peer IP**, enter the destination IPv4 CIDR address to which Amazon should send traffic. In the **Amazon router peer IP** field, enter the IPv4 CIDR address to use to send traffic to AWS.

Add a BGP Peering to Your Virtual Interface
Enter the peer addresses and BGP session information for the new BGP peering.

Address family: IPv4 IPv6 ⓘ

Auto-generate peer IPs: ⓘ

Your router peer IP: ⓘ

Amazon router peer IP: ⓘ

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

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

Add a BGP Peering to Your Virtual Interface
Enter the peer addresses and BGP session information for the new BGP peering.

Address family: IPv4 IPv6 ⓘ

Auto-generate peer IPs: ⓘ

BGP ASN: ⓘ

Auto-generate BGP key: ⓘ

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

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

9. Choose **Continue**.

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

To delete a BGP peer

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **Virtual Interfaces** and select the virtual interface.
3. Choose **Actions, Delete Peering**.
4. To delete the IPv4 BGP peer, choose **IPv4**. To delete the IPv6 BGP peer, choose **IPv6**.
5. Choose **Delete**.

To create a BGP peer using the command line or API

- [create-bgp-peer](#) (AWS CLI)
- [CreateBGPPeer](#) (AWS Direct Connect API)

To delete a BGP peer using the command line or API

- [delete-bgp-peer](#) (AWS CLI)
- [DeleteBGPPeer](#) (AWS Direct Connect API)

Associating a Virtual Interface with a Connection or LAG

You can associate a virtual interface with a link aggregation group (LAG), or another connection.

You cannot associate a virtual interface if the target connection or LAG has an existing associated virtual interface with the following matching attributes:

- A conflicting VLAN number
- (Public virtual interfaces) The same IP address range for the Amazon router, or for the customer router
- (Private virtual interfaces) The same virtual private gateway and the same IP address range for the Amazon router, or for the customer router

You cannot disassociate a virtual interface from a connection or LAG, but you can re-associate it or delete it. For more information, see [Deleting a Virtual Interface \(p. 32\)](#).

Important

Connectivity to AWS is temporarily interrupted during the association process.

To associate a virtual interface with a connection

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **Virtual Interfaces**, and select the virtual interface.
3. Choose **Actions, Associate Connection or LAG**.

4. Choose the required connection, select the confirmation check box, and choose **Continue**.

You can use the same procedure above to associate a virtual interface with a LAG. Alternatively, you can use the **LAGs** screen.

To associate a virtual interface with a LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.
3. Choose **Actions, Associate Virtual Interface**.
4. Choose the required virtual interface, select the confirmation check box, and choose **Continue**.

To associate a virtual interface using the command line or API

- [associate-virtual-interface](#) (AWS CLI)
- [AssociateVirtualInterface](#) (AWS Direct Connect API)

Link Aggregation Groups

A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

You can create a LAG from existing connections, or you can provision new connections. After you've created the LAG, you can associate existing connections (whether standalone or part of another LAG) with the LAG.

The following rules apply:

- All connections in the LAG must use the same bandwidth. The following bandwidths are supported: 1 Gbps and 10 Gbps.
- You can have a maximum of 4 connections in a LAG. Each connection in the LAG counts towards your overall connection limit for the region.
- All connections in the LAG must terminate at the same AWS Direct Connect endpoint.

When you create a LAG, you can download the Letter of Authorization and Connecting Facility Assignment (LOA-CFA) for each new physical connection individually from the AWS Direct Connect console. For more information, see [Downloading the LOA-CFA \(p. 16\)](#).

All LAGs have an attribute that determines the minimum number of connections in the LAG that must be operational for the LAG itself to be operational. By default, new LAGs have this attribute set to 0. You can update your LAG to specify a different value—doing so means that your entire LAG becomes non-operational if the number of operational connections falls below this threshold. This attribute can be used to prevent over-utilization of the remaining connections.

All connections in a LAG operate in Active/Active mode.

Note

When you create a LAG or associate more connections with the LAG, we may not be able to guarantee enough available ports on a given AWS Direct Connect endpoint.

Topics

- [Creating a LAG \(p. 39\)](#)

- [Updating a LAG \(p. 41\)](#)
- [Associating a Connection with a LAG \(p. 41\)](#)
- [Disassociating a Connection From a LAG \(p. 42\)](#)
- [Deleting a LAG \(p. 42\)](#)

Creating a LAG

You can create a LAG by provisioning new connections, or aggregating existing connections.

You cannot create a LAG with new connections if this results in you exceeding the overall connections limit for the region.

To create a LAG with new connections

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, **Create LAG**.
3. Choose **Request new Connections**, and provide the following information.
 - **Location:** Select the location for the LAG.
 - **LAG Name:** Specify a name for the LAG.
 - **Connection Bandwidth:** Select the port speed for the connections.
 - **Number of new Connections:** Specify the number of connections that must be provisioned in the LAG.

Create a LAG

You are currently operating in US East (N. Virginia). Use the region selector to change to another AWS region.

This connection will have access to AWS public services in all North American regions. For more information, [see the user guide](#).

To begin, specify whether to create a LAG from one or more of your existing Connections, or by ordering new Connections.

Use existing Connections Request new Connections

Create a LAG from new Connections

Select the AWS Direct Connect location in this region where you would like to connect, and the port speed you are requesting for the new Connections. If these choices don't fit your use case, for other options to connect you can [contact one of our partners](#).

Please note that for each new Connection, port hours are billed once the connection between your router and the AWS router is established, or 90 days after you ordered the port, whichever comes first. There is no additional charge for the LAG itself. For more information, [please see our FAQ](#).

Location: Equinix DA1 - DA3 & DA6, Dallas, TX ⓘ

LAG Name: DA-LAG ⓘ

Connection Bandwidth: 1 Gbps 10 Gbps ⓘ

Number of new Connections: 2 ⓘ

Cancel Create

4. Choose **Create**.

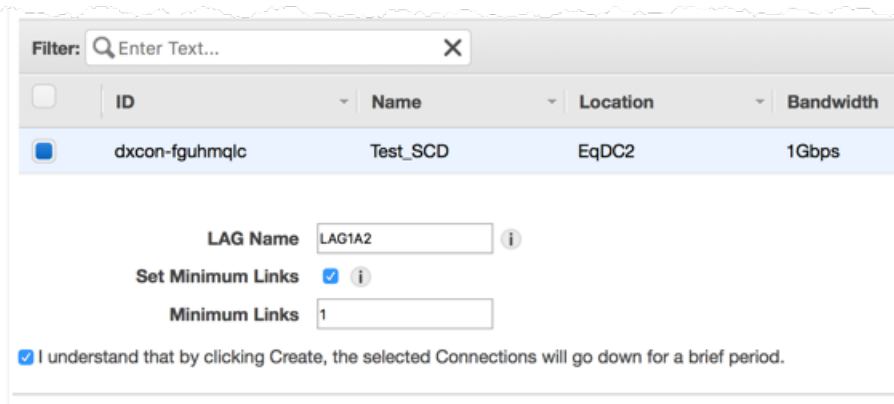
To create a LAG from existing connections, the connections must be on the same AWS device (terminate at the same AWS Direct Connect endpoint), and they must use the same bandwidth. You cannot migrate a connection from an existing LAG if removing the connection causes the original LAG to fall below its setting for minimum number of operational connections.

Important

For existing connections, connectivity to AWS is interrupted during the creation of the LAG.

To create a LAG from existing connections

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, **Create LAG**.
3. Choose **Use existing Connections**, and select the required connections.
4. For **LAG Name**, specify a name for the LAG. For **Set Minimum Links**, specify the minimum number of connections that must be operational for the LAG itself to be operational. If you do not specify a value, we assign a default value of 0.



Filter:

ID	Name	Location	Bandwidth
dxcon-fguhmqlc	Test_SCD	EqDC2	1Gbps

LAG Name:

Set Minimum Links:

Minimum Links:

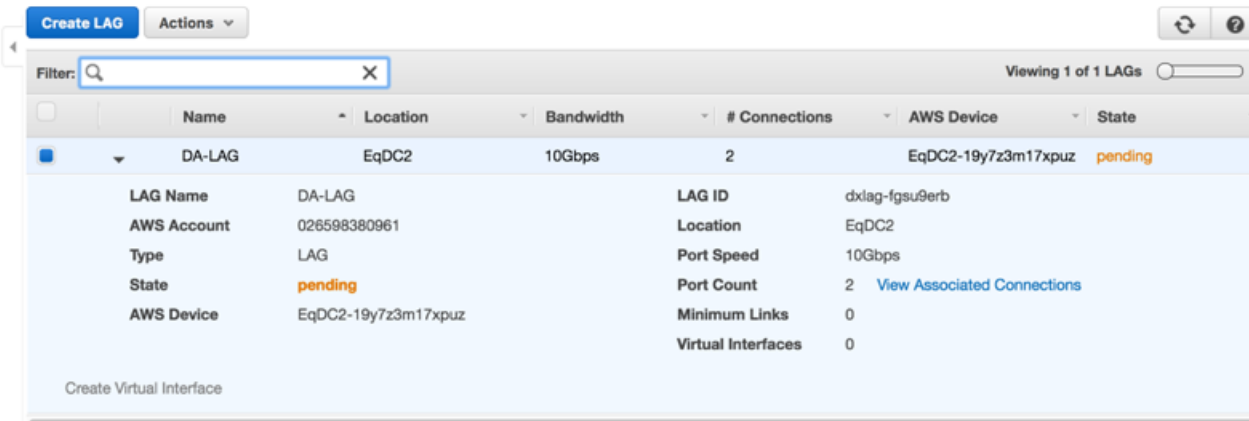
I understand that by clicking Create, the selected Connections will go down for a brief period.

5. Select the confirmation check box and choose **Create**.

After you've created a LAG, you can view its details in the AWS Direct Connect console.

To view information about your LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.
3. You can view information about the LAG, including its ID, the AWS Direct Connect endpoint on which the connections terminate (**AWS Device**), and the number of connections in the LAG (**Port Count**).



Create LAG Actions

Filter:

Viewing 1 of 1 LAGs

Name	Location	Bandwidth	# Connections	AWS Device	State
DA-LAG	EqDC2	10Gbps	2	EqDC2-19y7z3m17xpuz	pending

LAG Name: DA-LAG LAG ID: dxlag-fgsu9erb

AWS Account: 026598380961 Location: EqDC2

Type: LAG Port Speed: 10Gbps

State: pending Port Count: 2 [View Associated Connections](#)

AWS Device: EqDC2-19y7z3m17xpuz Minimum Links: 0

Virtual Interfaces: 0

Create Virtual Interface

After you've created a LAG, you can associate or disassociate connections from it. For more information, see [Associating a Connection with a LAG \(p. 41\)](#) and [Disassociating a Connection From a LAG \(p. 42\)](#).

To create a LAG using the command line or API

- [create-lag](#) (AWS CLI)
- [CreateLag](#) (AWS Direct Connect API)

To describe your LAGs using the command line or API

- [describe-lags](#) (AWS CLI)
- [DescribeLags](#) (AWS Direct Connect API)

To download the LOA-CFA using the command line or API

- [describe-loa](#) (AWS CLI)
- [DescribeLoa](#) (AWS Direct Connect API)

Updating a LAG

You can update a LAG to change its name, or to change the value for the minimum number of operational connections.

Note

If you adjust the threshold value for the minimum number of operational connections, ensure that the new value does not cause the LAG to fall below the threshold and become non-operational.

To update a LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.
3. Choose **Actions, Update LAG**.
4. For **LAG Name**, specify a new name for the LAG. For **Minimum Links**, adjust the value for the minimum number of operational connections.
5. Choose **Continue**.

To update a LAG using the command line or API

- [update-lag](#) (AWS CLI)
- [UpdateLag](#) (AWS Direct Connect API)

Associating a Connection with a LAG

You can associate an existing connection with a LAG. The connection can be standalone, or it can be part of another LAG. The connection must be on the same AWS device and must use the same bandwidth as the LAG. If the connection is already associated with another LAG, you cannot re-associate it if removing the connection causes the original LAG to fall below its threshold for minimum number of operational connections.

Associating a connection to a LAG automatically re-associates its virtual interfaces to the LAG.

Important

Connectivity to AWS over the connection is interrupted during association.

To associate a connection with a LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.
3. Choose **Actions, Associate Connection**.
4. Select the connection from the list of available connections.
5. Select the confirmation check box and choose **Continue**.

To associate a connection using the command line or API

- [associate-connection-with-lag](#) (AWS CLI)
- [AssociateConnectionWithLag](#) (AWS Direct Connect API)

Disassociating a Connection From a LAG

You can disassociate a connection from a LAG to convert it to a standalone connection. You cannot disassociate a connection if this will cause the LAG to fall below its threshold for minimum number of operational connections.

Disassociating a connection from a LAG does not automatically disassociate any virtual interfaces. You must associate the virtual interface with the connection separately. For more information, see [Associating a Virtual Interface with a Connection or LAG](#) (p. 36).

Important

Connectivity to AWS over the connection is interrupted during disassociation.

To disassociate a connection from a LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.
3. Choose **Actions, Disassociate Connection**.
4. Select the connection from the list of available connections.
5. Select the confirmation check box, and choose **Continue**.

To disassociate a connection using the command line or API

- [disassociate-connection-from-lag](#) (AWS CLI)
- [DisassociateConnectionFromLag](#) (AWS Direct Connect API)

Deleting a LAG

If you no longer need a LAG, you can delete it. You cannot delete a LAG if it has virtual interfaces associated with it—you must first delete the virtual interfaces, or associate them with a different LAG or connection. Deleting a LAG does not delete the connections in the LAG; you must delete the connections yourself. For more information, see [Deleting a Connection](#) (p. 17).

To delete a LAG

1. Open the AWS Direct Connect console at <https://console.aws.amazon.com/directconnect/>.
2. In the navigation pane, choose **LAGs**, and select the LAG.

3. Choose **Actions, Delete LAG**.
4. Select the confirmation check box and choose **Continue**.

To delete a LAG using the command line or API

- [delete-lag](#) (AWS CLI)
- [DeleteLag](#) (AWS Direct Connect API)

Using AWS Identity and Access Management with AWS Direct Connect

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

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

Important

Using AWS Direct Connect with IAM doesn't change how you use AWS Direct Connect. There are no changes to AWS Direct Connect actions, and no new AWS Direct Connect actions related to users and access control. For an example of a policy that covers AWS Direct Connect actions, see [Example Policy for AWS Direct Connect \(p. 45\)](#).

AWS Direct Connect Actions

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

AWS Direct Connect Resources

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

AWS Direct Connect Keys

AWS Direct Connect implements the following policy keys:

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

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

Note

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

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

For more information about policy keys, see [Condition](#) in *IAM User Guide*.

Example Policy for AWS Direct Connect

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

Note

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

Example

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

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

For more information about writing IAM policies, see [Overview of IAM Policies](#) in the *IAM User Guide*.

Using Tags with AWS Direct Connect

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

You can tag the following AWS Direct Connect resources.

Resource	Amazon Resource Name (ARN)
Connections	arn:aws:directconnect: <i>region</i> : <i>account-id</i> :dxcon/ <i>connection-id</i>
Virtual interfaces	arn:aws:directconnect: <i>region</i> : <i>account-id</i> :dxvif/ <i>virtual-interface-id</i>
Link aggregation group (LAG)	arn:aws:directconnect: <i>region</i> : <i>account-id</i> :dxlag/ <i>lag-id</i>

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

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

Tag Restrictions

The following rules and restrictions apply to tags:

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

Working with Tags

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

To add a tag using the AWS CLI

Use the `tag-resource` command:

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

To describe your tags using the AWS CLI

Use the `describe-tags` command:

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

To delete a tag using the AWS CLI

Use the `untag-resource` command:

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

Using the AWS CLI

You can use the AWS CLI to create and work with AWS Direct Connect resources.

The following example uses the AWS CLI commands to create an AWS Direct Connect connection, download the Letter of Authorization and Connecting Facility Assignment (LOA-CFA), and provision a private or public virtual interface.

Before you begin, ensure that you have installed and configured the AWS CLI. For more information, see the [AWS Command Line Interface User Guide](#).

Contents

- [Step 1: Create a Connection \(p. 48\)](#)
- [Step 2: Download the LOA-CFA \(p. 49\)](#)
- [Step 3: Create a Virtual Interface and get the Router Configuration \(p. 49\)](#)

Step 1: Create a Connection

The first step is to submit a connection request. Ensure that you know the port speed that you require and the AWS Direct Connect location. For more information, see [Connections \(p. 14\)](#).

To create a connection request

1. Describe the AWS Direct Connect locations for your current region. In the output that's returned, take note of the location code for the location in which you want to establish the connection.

```
aws directconnect describe-locations
```

```
{
  "locations": [
    {
      "locationName": "NAP do Brasil, Barueri, Sao Paulo",
      "locationCode": "TNDB"
    },
    {
      "locationName": "Tivit - Site Transamerica (Sao Paulo)",
      "locationCode": "TIVIT"
    }
  ]
}
```

```
}
```

2. Create the connection and specify a name, the port speed, and the location code. In the output that's returned, take note of the connection ID. You need the ID to get the LOA-CFA in the next step.

```
aws directconnect create-connection --location TIVIT --bandwidth 1Gbps --connection-name "Connection to AWS"
```

```
{  
  "ownerAccount": "123456789012",  
  "connectionId": "dxcon-fg31dyv6",  
  "connectionState": "requested",  
  "bandwidth": "1Gbps",  
  "location": "TIVIT",  
  "connectionName": "Connection to AWS",  
  "region": "sa-east-1"  
}
```

Step 2: Download the LOA-CFA

After you've requested a connection, you can get the LOA-CFA using the `describe-loa` command. The output is base64-encoded. You must extract the relevant LOA content, decode it, and create a PDF file.

To get the LOA-CFA using Linux or Mac OS X

In this example, the final part of the command decodes the content using the `base64` utility, and sends the output to a PDF file.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query loaContent|base64 --decode > myLoaCfa.pdf
```

To get the LOA-CFA using Windows

In this example, the output is extracted to a file called `myLoaCfa.base64`. The second command uses the `certutil` utility to decode the file and send the output to a PDF file.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

After you've downloaded the LOA-CFA, send it to your network provider or colocation provider.

Step 3: Create a Virtual Interface and get the Router Configuration

After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to begin using it. You can create a private virtual interface to connect to your VPC, or you can create a public virtual interface to connect to AWS services that aren't in a VPC. You can create a virtual interface that supports IPv4 or IPv6 traffic.

Before you begin, ensure that you've read the prerequisites in [Prerequisites for Virtual Interfaces \(p. 25\)](#).

When you create a virtual interface using the AWS CLI, the output includes generic router configuration information. If you want router configuration that's specific to your device, use the AWS Direct Connect console. For more information, see [Downloading the Router Configuration File \(p. 29\)](#).

To create a private virtual interface

1. Get the ID of the virtual private gateway (vgw-xxxxxxx) that's attached to your VPC. You need the ID to create the virtual interface in the next step.

```
aws ec2 describe-vpn-gateways
```

```
{
  "VpnGateways": [
    {
      "State": "available",
      "Tags": [
        {
          "Value": "DX_VGW",
          "Key": "Name"
        }
      ],
      "Type": "ipsec.1",
      "VpnGatewayId": "vgw-ebaa27db",
      "VpcAttachments": [
        {
          "State": "attached",
          "VpcId": "vpc-24f33d4d"
        }
      ]
    }
  ]
}
```

2. Create a private virtual interface. You must specify a name, a VLAN ID, and a BGP Autonomous System Number (ASN).

For IPv4 traffic, you need private IPv4 addresses for each end of the BPG peering session. You can specify your own IPv4 addresses, or you can let Amazon generate the addresses for you. In the following example, the IPv4 addresses are generated for you.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
  "virtualInterfaceState": "pending",
  "asn": 65000,
  "vlan": 101,
  "customerAddress": "192.168.1.2/30",
  "ownerAccount": "123456789012",
  "connectionId": "dxcon-fg31dyv6",
  "addressFamily": "ipv4",
  "virtualGatewayId": "vgw-ebaa27db",
  "virtualInterfaceId": "dxvif-ffhkh74f",
  "authKey": "asdf34example",
  "routeFilterPrefixes": [],
  "location": "TIVIT",
  "bgpPeers": [
    {
      "bgpStatus": "down",
```

AWS Direct Connect User Guide

Step 3: Create a Virtual Interface and get the Router Configuration

```
    "customerAddress": "192.168.1.2/30",
    "addressFamily": "ipv4",
    "authKey": "asdf34example",
    "bgpPeerState": "pending",
    "amazonAddress": "192.168.1.1/30",
    "asn": 65000
  }
  "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhkh74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
<amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
<bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>\n
<connection_type>private</connection_type>\n</logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
  }
}
```

To create a private virtual interface that supports IPv6 traffic, use the same command as above and specify `ipv6` for the `addressFamily` parameter. You cannot specify your own IPv6 addresses for the BGP peering session; Amazon allocates you IPv6 addresses.

3. To view the router configuration information in XML format, describe the virtual interface you created. Use the `--query` parameter to extract the `customerRouterConfig` information, and the `--output` parameter to organize the text into tab-delimited lines.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhkh74f --
query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhkh74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

To create a public virtual interface

1. To create a public virtual interface, you must specify a name, a VLAN ID, and a BGP Autonomous System Number (ASN).

For IPv4 traffic, you must also specify public IPv4 addresses for each end of the BGP peering session, and public IPv4 routes that you will advertise over BGP. The following example creates a public virtual interface for IPv4 traffic.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/30,custo
{cidr=203.0.113.4/30}]
```

```
{
  "virtualInterfaceState": "verifying",
  "asn": 65000,
  "vlan": 2000,
  "customerAddress": "203.0.113.2/30",
```

AWS Direct Connect User Guide

Step 3: Create a Virtual Interface and get the Router Configuration

```
"ownerAccount": "123456789012",
"connectionId": "dxcon-fg31dyv6",
"addressFamily": "ipv4",
"virtualGatewayId": "",
"virtualInterfaceId": "dxvif-fgh0hcrk",
"authKey": "asdf34example",
"routeFilterPrefixes": [
  {
    "cidr": "203.0.113.0/30"
  },
  {
    "cidr": "203.0.113.4/30"
  }
],
"location": "TIVIT",
"bgpPeers": [
  {
    "bgpStatus": "down",
    "customerAddress": "203.0.113.2/30",
    "addressFamily": "ipv4",
    "authKey": "asdf34example",
    "bgpPeerState": "verifying",
    "amazonAddress": "203.0.113.1/30",
    "asn": 65000
  }
],
"customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<logical_connection id=\"dxvif-fgh0hcrk\">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
  </logical_connection>
  <amazonAddress> \"203.0.113.1/30\",
  <virtualInterfaceType> \"public\",
  <virtualInterfaceName> \"PublicVirtualInterface\"
}>
```

To create a public virtual interface that supports IPv6 traffic, you can specify IPv6 routes that you will advertise over BGP. You cannot specify IPv6 addresses for the peering session; Amazon allocates IPv6 addresses to you. The following example creates a public virtual interface for IPv6 traffic.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFilterPrefixes=[{cidr:2001:db8:64ce:ba01::/64}]
```

2. To view the router configuration information in XML format, describe the virtual interface you created. Use the `--query` parameter to extract the `customerRouterConfig` information, and the `--output` parameter to organize the text into tab-delimited lines.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk --
query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
```

AWS Direct Connect User Guide
Step 3: Create a Virtual Interface
and get the Router Configuration

```
</logical_connection>
```


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 \(p. 54\)](#)
- [Understanding AWS Direct Connect Log File Entries \(p. 55\)](#)

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.

```
{
  "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-fhajolly",
    "newPrivateVirtualInterface": {
      "virtualInterfaceName": "MyVirtualInterface",
      "customerAddress": "[PROTECTED]",
      "authKey": "[PROTECTED]",
      "asn": -1,
      "virtualGatewayId": "vgw-bb09d4a5",
      "amazonAddress": "[PROTECTED]",
      "vlan": 123
    }
  },
  "responseElements": {
    "virtualInterfaceId": "dxvif-fgq61m6w",
    "authKey": "[PROTECTED]",
    "virtualGatewayId": "vgw-bb09d4a5",
    "customerRouterConfig": "[PROTECTED]",
    "virtualInterfaceType": "private",
    "asn": -1,
    "routeFilterPrefixes": [],
    "virtualInterfaceName": "MyVirtualInterface",
    "virtualInterfaceState": "pending",
    "customerAddress": "[PROTECTED]",
    "vlan": 123,
    "ownerAccount": "123456789012",
    "amazonAddress": "[PROTECTED]",
    "connectionId": "dxcon-fhajolly",
    "location": "EqSE2"
  }
},
...additional entries
]
}
```

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

```
{
  "Records": [
    {
      "eventVersion": "1.0",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice",
```

```
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-04-04T12:23:05Z"
      }
    }
  },
  "eventTime": "2014-04-04T17:27:28Z",
  "eventSource": "directconnect.amazonaws.com",
  "eventName": "DescribeConnections",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "Coral/Jakarta",
  "requestParameters": null,
  "responseElements": null
},
...additional entries
]
}
```

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

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

Troubleshooting AWS Direct Connect

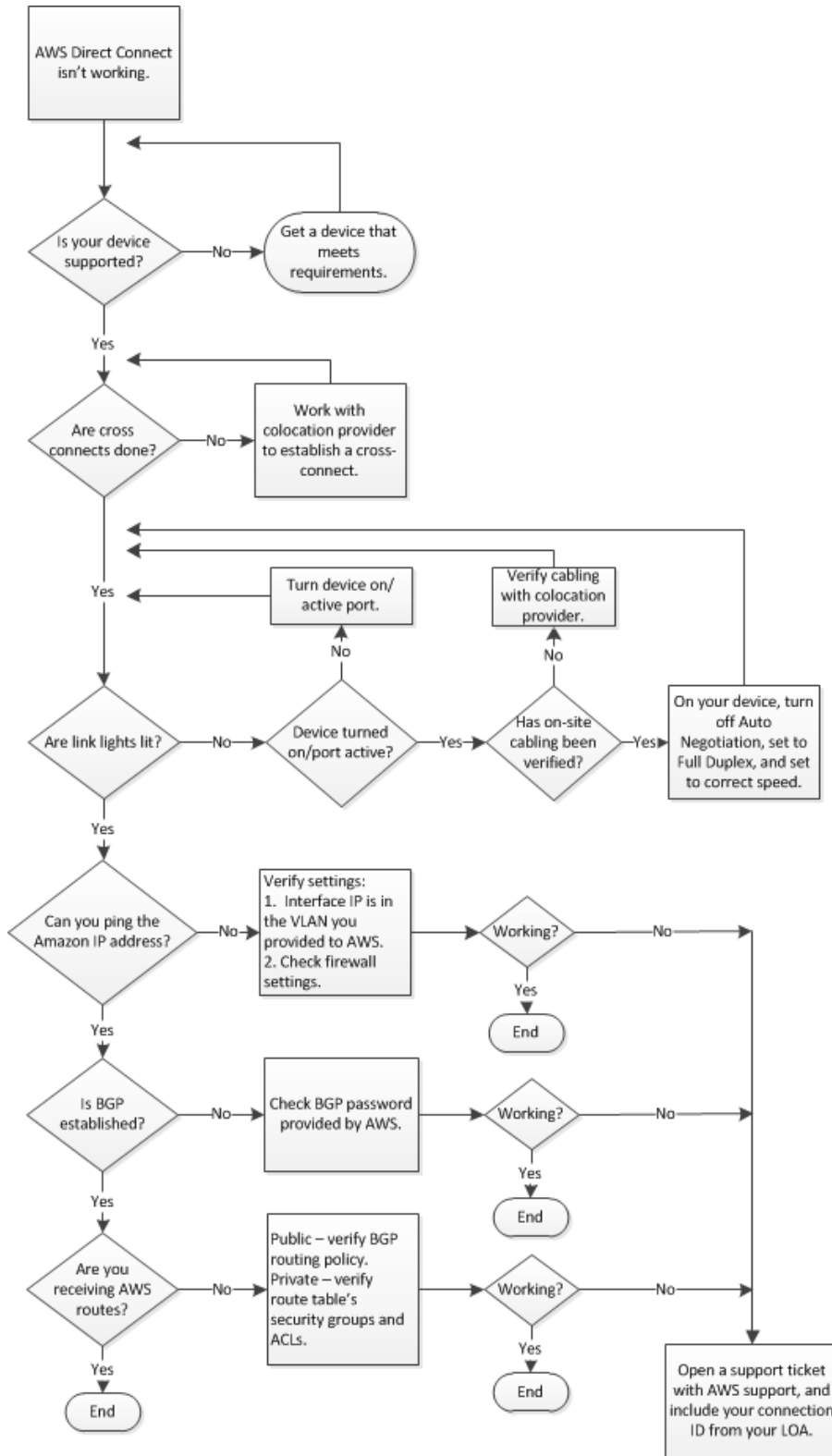
The following table lists troubleshooting resources that you'll find useful as you work with AWS Direct Connect.

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

Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect

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

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



Troubleshooting a Cross Connection to AWS Direct Connect

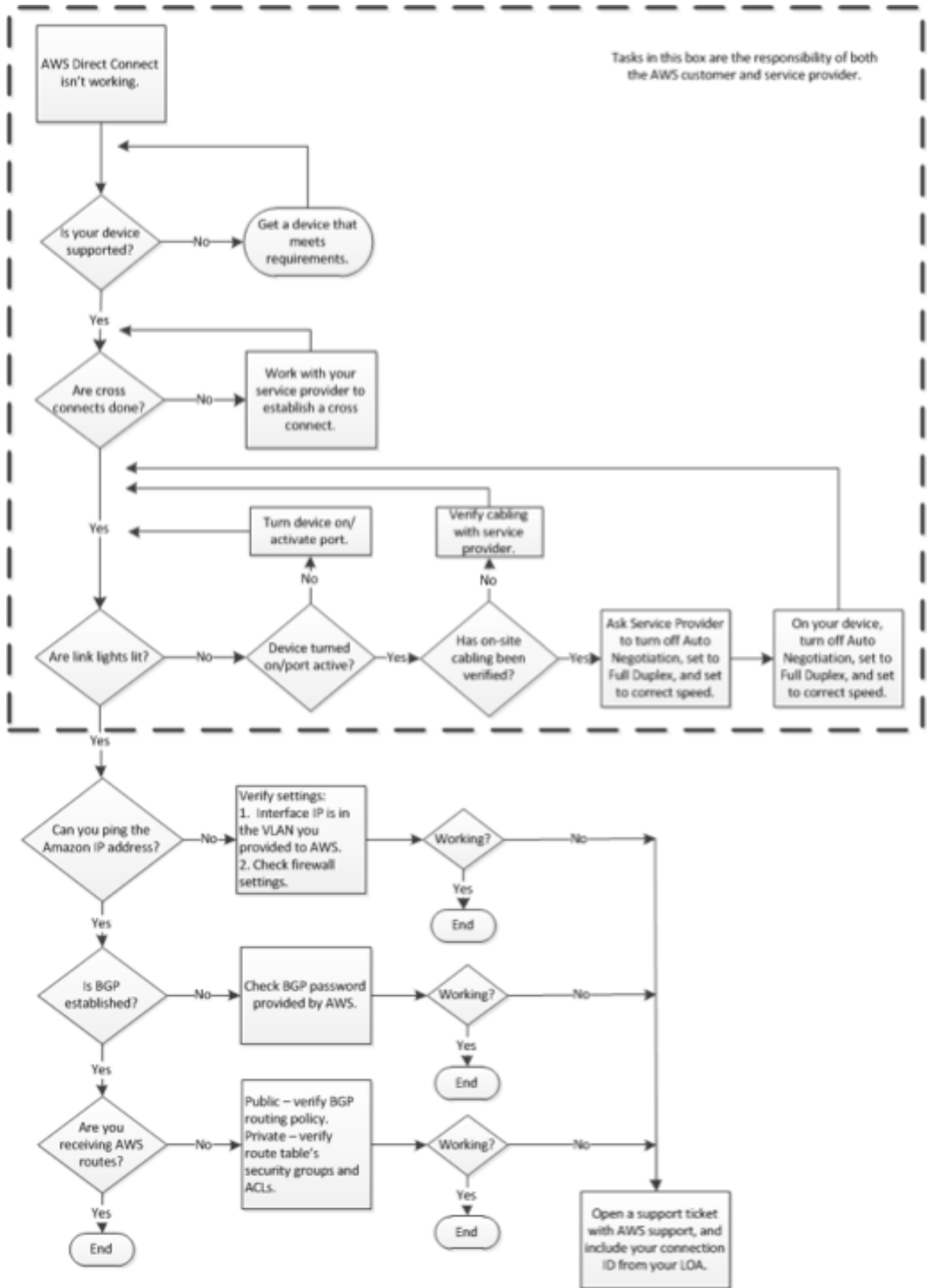
You can use the following tasks to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility. To see these tasks in a flow chart, see [Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect \(p. 58\)](#).

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

Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect

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

AWS Direct Connect 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 \(p. 60\)](#).

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

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
Link aggregation groups	You can create a link aggregation group (LAG) to aggregate multiple AWS Direct Connect connections. For more information, see Link Aggregation Groups (p. 38) .	2017-02-13
IPv6 support	Your virtual interface can now support an IPv6 BGP peering session. For more information, see Adding or Removing a BGP Peer (p. 34) .	2016-12-01
Tagging support	You can now tag your AWS Direct Connect resources. For more information, see Using Tags with AWS Direct Connect (p. 46) .	2016-11-04
Self-service LOA-CFA	You can now download your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) using the AWS Direct Connect console or API.	2016-06-22
New location in Silicon Valley	Updated topic to include the addition of the new Silicon Valley location in the US West (N. California) region.	2016-06-03
New location in Amsterdam	Updated topic to include the addition of the new Amsterdam location in the EU (Frankfurt) region.	2016-05-19
New locations in Portland, Oregon and Singapore	Updated topic to include the addition of the new Portland, Oregon and Singapore locations in the US West (Oregon) and Asia Pacific (Singapore) regions.	2016-04-27
New location in Sao Paulo, Brasil	Updated topic to include the addition of the new Sao Paulo location in the South America (São Paulo) region.	2015-12-09
New locations in Dallas, London, Silicon	Updated topics to include the addition of the new locations in Dallas (US East (N. Virginia) region), London (EU (Ireland) region),	2015-11-27

Change	Description	Release Date
Valley, and Mumbai	Silicon Valley (AWS GovCloud (US) region), and Mumbai (Asia Pacific (Singapore) region).	
New location in the China (Beijing) region	Updated topics to include the addition of the new Beijing location in the China (Beijing) region.	2015-04-14
New Las Vegas location in the US West (Oregon) region	Updated topics to include the addition of the new AWS Direct Connect Las Vegas location in the US West (Oregon) region.	2014-11-10
New EU (Frankfurt) region	Updated topics to include the addition of the new AWS Direct Connect locations serving the EU (Frankfurt) region.	2014-10-23
New 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. 54) .	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 North America (p. 3) .	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. 44) .	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*.