Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# 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 ...................................................................................................... 4  
Routing Policies and BGP Communities .......................................................................................... 4  
  Routing Policies .......................................................................................................................... 4  
  BGP Communities ....................................................................................................................... 5  
Getting Started .................................................................................................................................. 6  
  Step 1: Sign Up for AWS .................................................................................................................. 6  
  Step 2: Submit AWS Direct Connect Connection Request ............................................................ 7  
    Accept Your Hosted Connection .................................................................................................. 8  
  Step 3: Download the LOA-CFA ................................................................................................... 9  
  Step 4: (Optional) Configure Redundant Connections ................................................................... 9  
  Step 5: Create a Virtual Interface .................................................................................................. 10  
  Step 6: Download Router Configuration ....................................................................................... 13  
  Step 7: Verify Your Virtual Interface ........................................................................................... 13  
Connections ...................................................................................................................................... 15  
  Creating a Connection .................................................................................................................... 16  
    Downloading the LOA-CFA ......................................................................................................... 16  
    Viewing Connection Details ......................................................................................................... 17  
  Deleting a Connection ....................................................................................................................... 17  
    Accepting a Hosted Connection .................................................................................................. 18  
Requesting Cross Connects ................................................................................................................ 20  
Virtual Interfaces ............................................................................................................................... 27  
  Prerequisites for Virtual Interfaces ................................................................................................. 28  
  Creating a Virtual Interface .............................................................................................................. 28  
    Downloading the Router Configuration File ............................................................................. 31  
  Viewing Virtual Interface Details ................................................................................................... 34  
  Deleting a Virtual Interface ............................................................................................................. 34  
  Creating a Hosted Virtual Interface .............................................................................................. 35  
    Accepting a Hosted Virtual Interface .......................................................................................... 36  
  Adding or Removing a BGP Peer .................................................................................................... 37  
  Associating a Virtual Interface ....................................................................................................... 39  
LAGs .................................................................................................................................................. 41  
  Creating a LAG ................................................................................................................................. 42  
  Updating a LAG ............................................................................................................................... 44  
  Associating a Connection with a LAG ............................................................................................ 44  
  Disassociating a Connection From a LAG ....................................................................................... 45  
  Deleting a LAG ................................................................................................................................. 45  
Using IAM ........................................................................................................................................ 47  
  AWS Direct Connect Actions .......................................................................................................... 47  
  AWS Direct Connect Resources ..................................................................................................... 47  
  AWS Direct Connect Keys ............................................................................................................. 48  
  Example Policy for AWS Direct Connect ....................................................................................... 48  
Using Tags ........................................................................................................................................ 49  
  Tag Restrictions ............................................................................................................................... 50  
  Working with Tags .......................................................................................................................... 50  
Using the AWS CLI ........................................................................................................................... 51  
  Step 1: Create a Connection ........................................................................................................... 51  
  Step 2: Download the LOA-CFA ................................................................................................... 52  
  Step 3: Create a Virtual Interface and get the Router Configuration ........................................... 52  
Logging API Calls ............................................................................................................................ 57
What is AWS Direct Connect?

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to 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.
AWS Direct Connect Components

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS region. For more information, see Connections (p. 15).</td>
</tr>
<tr>
<td>Virtual Interface</td>
<td>Create a virtual interface 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. 27) and Prerequisites for Virtual Interfaces (p. 28).</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual interfaces per AWS Direct Connect connection</td>
<td>50</td>
<td>This limit cannot be increased.</td>
</tr>
<tr>
<td>Active AWS Direct Connect connections per region per account</td>
<td>10</td>
<td>This limit can be increased upon request.</td>
</tr>
<tr>
<td>Routes per Border Gateway Protocol (BGP) session on a private virtual interface</td>
<td>100</td>
<td>This limit cannot be increased.</td>
</tr>
<tr>
<td>Routes per Border Gateway Protocol (BGP) session on a public virtual interface</td>
<td>1,000</td>
<td>This limit cannot be increased.</td>
</tr>
<tr>
<td>Number of connections per link aggregation group (LAG)</td>
<td>4</td>
<td>This limit can be increased upon request.</td>
</tr>
<tr>
<td>Number of link aggregation groups (LAGs) per region</td>
<td>10</td>
<td>This limit can be increased upon request.</td>
</tr>
</tbody>
</table>

Resources

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Direct Connect product information</td>
<td>General product overview.</td>
</tr>
<tr>
<td>Pricing</td>
<td>Calculate monthly costs.</td>
</tr>
<tr>
<td>AWS Developer Tools</td>
<td>Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.</td>
</tr>
<tr>
<td>AWS Direct Connect FAQ</td>
<td>The top questions asked about this product.</td>
</tr>
<tr>
<td>AWS Direct Connect Forum</td>
<td>A community-based forum for discussing technical questions related to AWS Direct Connect.</td>
</tr>
<tr>
<td>AWS Support Center</td>
<td>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.</td>
</tr>
<tr>
<td>Contact Us</td>
<td>A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.</td>
</tr>
</tbody>
</table>
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. 27).

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.

Routing Policies and BGP Communities

AWS Direct Connect applies inbound and outbound routing policies for a public AWS Direct Connect connection. You can also make use of Border Gateway Protocol (BGP) community tags on advertised Amazon routes and apply BGP community tags on the routes you advertise to Amazon.

Routing Policies

If you're using AWS Direct Connect to access public AWS services, you must specify the public IPv4 prefixes or IPv6 prefixes to advertise over BGP.

The following inbound routing policies apply:

- You must own the public prefixes and they must be registered as such in the appropriate regional internet registry.
- Traffic must be destined to Amazon public prefixes. Transitive routing between connections is not supported.
- AWS Direct Connect performs inbound packet filtering to validate that the source of the traffic originated from your advertised prefix.

The following outbound routing policies apply:

- Only AS-PATH is used to determine the routing path, and AWS Direct Connect is the preferred path for traffic sourced from Amazon. Only public ASNs are used internally for route selection.
- AWS Direct Connect advertises all local and remote AWS Region prefixes where available and includes on-net prefixes from other AWS non-region points of presence (PoP) where available; for example, CloudFront and Amazon Route 53.
- AWS Direct Connect advertises prefixes with a minimum path length of 3.
- AWS Direct Connect advertises all public prefixes with the well-known NO_EXPORT BGP community.
- If you have multiple AWS Direct Connect connections, you can adjust the load-sharing of inbound traffic by advertising prefixes with similar path attributes.
- The prefixes advertised by AWS Direct Connect must not be advertised beyond the network boundaries of your connection; for example, these prefixes must not be included in any public internet routing table.
BGP Communities

You can apply BGP community tags on the public prefixes you advertise to Amazon to indicate how far to propagate your prefixes in the Amazon network—for the local AWS Region only, or all North America regions.

You can use the following BGP communities for your prefixes:

- 7224:9100—Local AWS Region
- 7224:9200—North America–wide
- No tag—North America–wide

The communities 7224:1 – 7224:65535 are reserved by AWS Direct Connect.

In addition, the well-known NO_EXPORT BGP community is supported for both public and private virtual interfaces.

AWS Direct Connect also provides BGP community tags on advertised Amazon routes. If you're using AWS Direct Connect to access public AWS services, this enables you to create filters based on these community tags.

AWS Direct Connect applies the following BGP communities to its advertised routes:

- 7224:8100—Routes that originate from the same AWS Region in which the AWS Direct Connect point of presence is associated.
- 7224:8200—Routes that originate from the same continent with which the AWS Direct Connect point of presence is associated.
- No tag—Routes that originate from the same continent with which the AWS Direct Connect point of presence is associated.

Communities that are not supported for an AWS Direct Connect public connection are removed.
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 AWS (p. 6)
- Step 2: Submit AWS Direct Connect Connection Request (p. 7)
- Step 3: Download the LOA-CFA (p. 9)
- Step 4: (Optional) Configure Redundant Connections (p. 9)
- Step 5: Create a Virtual Interface (p. 10)
- Step 6: Download Router Configuration (p. 13)
- Step 7: Verify Your Virtual Interface (p. 13)

Step 1: Sign Up for AWS

To use AWS Direct Connect, you need an AWS account if you don’t already have one.
To sign up for an AWS account

1. Open https://aws.amazon.com/, and then choose Create an AWS Account.
   
   **Note**
   This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose Sign In to the Console, and then choose Create a new 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. 8).

**To create a new AWS Direct Connect connection**

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:
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

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 the hosted 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. 9) 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

2. In the navigation pane, choose Connections.
3. Choose Actions, 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.

4. 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. 20). 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. 28).
Note
A sub-1G connection only supports one virtual interface.

To provision a public virtual interface to non-VPC services

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.
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.
Step 5: Create a Virtual Interface

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. 13).

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**

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**.

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 **Virtual Private Gateway**, select the virtual private 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**.
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

2. In the Virtual Interfaces pane, select the virtual interface you created and then choose Actions, 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. 31).

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 traceroute and verify that the AWS Direct Connect identifier is in the network trace.
To verify your virtual interface connection to Amazon VPC

1. Using a pingable AMI, such as 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: 1000BASE-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. 44).

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. 27).

Topics
- Creating a Connection (p. 16)
- Viewing Connection Details (p. 17)
- Deleting a Connection (p. 17)
- Accepting a Hosted Connection (p. 18)
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**

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**:
   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**

2. In the navigation pane, choose **Connections**.
3. Choose **Actions, 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.

4. 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.

5. 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. 20).

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-12nikabcd) 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
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 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. 34).

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**

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**

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.
5. Select I understand that Direct Connect port charges apply once I click Accept 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. 21)
- Asia Pacific (Seoul) (p. 21)
- Asia Pacific (Singapore) (p. 21)
- Asia Pacific (Sydney) (p. 21)
- Asia Pacific (Mumbai) (p. 22)
- Canada (Central) (p. 22)
- China (Beijing) (p. 22)
- EU (Frankfurt) (p. 22)
- EU (Ireland) (p. 23)
- EU (London) (p. 23)
- South America (São Paulo) (p. 24)
- US East (N. Virginia) (p. 24)
- US East (Ohio) (p. 25)
## Asia Pacific (Tokyo)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equinix Osaka (Equinix OS1)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsddealreg@equinix.com">awsddealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix Tokyo (Equinix TY2)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsddealreg@equinix.com">awsddealreg@equinix.com</a>.</td>
</tr>
</tbody>
</table>

## Asia Pacific (Seoul)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>LG U+ Pyeong-Chon Mega Center, Seoul</td>
<td>Requests for cross connects can be made by submitting the LOA document to <a href="mailto:kidcadmin@lguplus.co.kr">kidcadmin@lguplus.co.kr</a> and <a href="mailto:center8@kidc.net">center8@kidc.net</a>.</td>
</tr>
</tbody>
</table>

## Asia Pacific (Singapore)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equinix Singapore (Equinix SG2)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsddealreg@equinix.com">awsddealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Global Switch, Singapore</td>
<td>Requests for cross connects can be submitted by contacting Global Switch at <a href="mailto:salessingapore@globalswitch.com">salessingapore@globalswitch.com</a>.</td>
</tr>
<tr>
<td>GPX Mumbai</td>
<td>Requests for cross connects can be submitted by contacting GPX at <a href="mailto:nkankane@gpxglobal.net">nkankane@gpxglobal.net</a>.</td>
</tr>
<tr>
<td>iAdvantage MEGA-i, Hong Kong</td>
<td>Requests for cross connects can be submitted by contacting iAdvantage at cs@iad advantage.net or by placing an order at iAdvantage Cabling Order e-Form.</td>
</tr>
<tr>
<td>Menara AIMS, Kuala Lumpur</td>
<td>Existing AIMS customers can request a X-Connect order via the Customer Service portal by filling out the Engineering Work Order Request Form and contacting <a href="mailto:service.delivery@aims.com.my">service.delivery@aims.com.my</a> if there are any problems submitting the request.</td>
</tr>
</tbody>
</table>

## Asia Pacific (Sydney)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equinix Sydney (Equinix SY3)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsddealreg@equinix.com">awsddealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Global Switch</td>
<td>Requests for cross connects can be submitted by contacting Global Switch at <a href="mailto:salessydney@globalswitch.com">salessydney@globalswitch.com</a>.</td>
</tr>
</tbody>
</table>
### Location

**How to request a connection**

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Global Switch SY6)</td>
<td></td>
</tr>
<tr>
<td>NEXTDC Melbourne (NEXTDC M1)</td>
<td>Requests for cross connects can be submitted by contacting NEXTDC at <a href="mailto:nxtops@nextdc.com">nxtops@nextdc.com</a>.</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td></td>
</tr>
<tr>
<td>GPX Mumbai</td>
<td>Requests for cross connects can be submitted by contacting GPX at <a href="mailto:nkankane@gpxglobal.net">nkankane@gpxglobal.net</a>.</td>
</tr>
<tr>
<td>Sify Rabale, Mumbai</td>
<td>Requests for cross connects can be submitted by contacting Sify at <a href="mailto:aws.directconnect@sifycorp.com">aws.directconnect@sifycorp.com</a>.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
</tr>
<tr>
<td>Allied 250 Front St W, Toronto</td>
<td>Requests for cross connects can be submitted by contacting <a href="mailto:driches@alliedreit.com">driches@alliedreit.com</a>.</td>
</tr>
<tr>
<td>Cologix Montreal</td>
<td>Requests for cross connects can be submitted by contacting Cologix at <a href="mailto:aws@cologix.com">aws@cologix.com</a>.</td>
</tr>
<tr>
<td>Netelligent Montreal</td>
<td>Requests for cross connects can be submitted by contacting Netelligent at <a href="mailto:directconnect@netelligent.ca">directconnect@netelligent.ca</a>.</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td></td>
</tr>
<tr>
<td>Sinnet Jiuxianqiao IDC</td>
<td>Requests for cross connects can be submitted by contacting Sinnet at <a href="mailto:dx-order@sinnet.com.cn">dx-order@sinnet.com.cn</a>.</td>
</tr>
<tr>
<td>EU (Frankfurt)</td>
<td></td>
</tr>
<tr>
<td>CE Colo, Prague</td>
<td>Requests for cross connects can be submitted by contacting CE Colo at <a href="mailto:info@cecolo.com">info@cecolo.com</a>.</td>
</tr>
<tr>
<td>Equinix Amsterdam (Equinix AM3)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix Frankfurt (Equinix FR4 and FR5)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix Munich (Equinix MU1 and MU3)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Location</td>
<td>How to request a connection</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Equinix Warsaw (Equinix WA1)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>IPB, Berlin</td>
<td>Requests for cross connects can be submitted by contacting IPB at <a href="mailto:kontakt@ipb.de">kontakt@ipb.de</a>.</td>
</tr>
<tr>
<td>Interxion Frankfurt</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Interxion Madrid</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Interxion Marseille</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Interxion Stockholm</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Interxion Vienna</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Interxion Zurich</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
<tr>
<td>Telehouse Voltaire, Paris (TH2)</td>
<td>Requests for cross connects can be submitted by creating a request at the Customer Portal. <a href="#">DFM/SFM Layout/Connectivity/MMR Circuit Commissioning</a>.</td>
</tr>
</tbody>
</table>

**EU (Ireland)**

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Realty (UK) (Sovereign House and London Meridian Gate)</td>
<td>Requests for cross connects can be submitted by contacting Digital Realty (UK) at <a href="mailto:amazon.orders@digitalrealty.com">amazon.orders@digitalrealty.com</a>.</td>
</tr>
<tr>
<td>Eircom Clonshaugh</td>
<td>Requests for cross connects can be submitted by contacting Eircom at <a href="mailto:awsorders@eircom.ie">awsorders@eircom.ie</a>.</td>
</tr>
<tr>
<td>Equinix London (Slough) (Equinix LD4-LD6)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Interxion Dublin</td>
<td>Requests for cross connects can be submitted by contacting Interxion at <a href="mailto:customer.services@interxion.com">customer.services@interxion.com</a>.</td>
</tr>
</tbody>
</table>

**EU (London)**

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Realty (UK)</td>
<td>Requests for cross connects can be submitted by contacting Digital Realty (UK) at <a href="mailto:amazon.orders@digitalrealty.com">amazon.orders@digitalrealty.com</a>.</td>
</tr>
<tr>
<td>Location</td>
<td>How to request connection</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>(Sovereign House and London Meridian Gate)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix London (Slough) (Equinix LD4-LD6)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix São Paulo (Equinix SP4)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Tivit</td>
<td>Requests for cross connects can be submitted by contacting Tivit at <a href="mailto:aws@tivit.com.br">aws@tivit.com.br</a>.</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>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.</td>
</tr>
<tr>
<td>165 Halsey Street, Newark</td>
<td>Refer to the resources on <a href="http://www.165halsey.com/colocation-services/connectivity/">http://www.165halsey.com/colocation-services/connectivity/</a> or contact <a href="mailto:operations@165halsey.com">operations@165halsey.com</a>.</td>
</tr>
<tr>
<td>CoreSite 32 Avenue of the Americas, New York</td>
<td>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.</td>
</tr>
<tr>
<td>CoreSite Northern Virginia (CoreSite VA1 and VA2)</td>
<td>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.</td>
</tr>
<tr>
<td>Digital Realty, Atlanta (ATL1 and ATL2)</td>
<td>Requests for cross connects can be submitted by contacting Digital Realty at <a href="mailto:amazon.orders@digitalrealty.com">amazon.orders@digitalrealty.com</a>.</td>
</tr>
<tr>
<td>Equinix Ashburn (Equinix DC1-DC6, and DC10-DC11)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix Dallas (Equinix DA1-DA3, and DA6)</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Lightower, Philadelphia</td>
<td>Requests for cross connects can be submitted by contacting Lightower at <a href="mailto:awsorders@lightower.com">awsorders@lightower.com</a>.</td>
</tr>
</tbody>
</table>
### US East (Ohio)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cologix COL2, Columbus</td>
<td>Requests for cross connects can be submitted by contacting Cologix at <a href="mailto:aws@cologix.com">aws@cologix.com</a>.</td>
</tr>
<tr>
<td>Equinix Chicago</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>QTS Chicago</td>
<td>Requests for cross connects can be submitted by contacting QTS at <a href="mailto:AConnect@qtsdatacenters.com">AConnect@qtsdatacenters.com</a>.</td>
</tr>
</tbody>
</table>

### AWS GovCloud (US)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equinix Silicon Valley</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
</tbody>
</table>

### US West (N. California)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoreSite One Wilshire and 900 North Alameda</td>
<td>Requests for cross connects can be submitted by placing an order at the <a href="https://www.coresite.com">CoreSite Customer Portal</a>. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.</td>
</tr>
<tr>
<td>CoreSite Silicon Valley</td>
<td>Requests for cross connects can be submitted by placing an order at the <a href="https://www.coresite.com">CoreSite Customer Portal</a>. After you complete the form, review the order for accuracy, and then approve it using the MyCoreSite website.</td>
</tr>
<tr>
<td>Equinix Los Angeles</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
<tr>
<td>Equinix Silicon Valley</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:awsdealreg@equinix.com">awsdealreg@equinix.com</a>.</td>
</tr>
</tbody>
</table>

### US West (Oregon)

<table>
<thead>
<tr>
<th>Location</th>
<th>How to request a connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>EdgeConneX, Portland, OR</td>
<td>Requests for cross connects can be submitted by placing an order on the <a href="https://www.edgeconnex.com">EdgeOS Customer Portal</a>. After you have submitted the form, EdgeConneX will provide a service order form for approval. You can send questions to <a href="mailto:cloudaccess@edgeconnex.com">cloudaccess@edgeconnex.com</a>.</td>
</tr>
<tr>
<td>Equinix Seattle</td>
<td>Requests for cross connects can be submitted by contacting Equinix at <a href="mailto:support@equinix.com">support@equinix.com</a>.</td>
</tr>
<tr>
<td>Location</td>
<td>How to request a connection</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pittock Block, Portland, OR</td>
<td>Requests for cross connects can be submitted by email at <a href="mailto:crossconnect@pittock.com">crossconnect@pittock.com</a>, or by phone at +1 503 226 6777.</td>
</tr>
<tr>
<td>Switch SUPERNAP 8, Las Vegas, NV</td>
<td>Requests for cross connects can be submitted by contacting Switch SUPERNAP at <a href="mailto:orders@supernap.com">orders@supernap.com</a>.</td>
</tr>
<tr>
<td>TierPoint Seattle</td>
<td>Requests for cross connects can be submitted by contacting TierPoint at <a href="mailto:sales@tierpoint.com">sales@tierpoint.com</a>.</td>
</tr>
</tbody>
</table>
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-Amazon prefixes or prefixes outside of your region. For the current list of IP prefixes advertised on AWS Direct Connect public connections, see the list in the AWS Direct Connect Discussion Forum.

**Note**
We recommend that you use a firewall filter (based on the source/destination address of packets) to control traffic to and from some prefixes. If you're using a prefix filter (route map), ensure that it accepts prefixes with an exact match or longer. Prefixes advertised from AWS Direct Connect may be aggregated and may differ from the prefixes defined in your prefix filter.

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. 28)
- Creating a Virtual Interface (p. 28)
- Viewing Virtual Interface Details (p. 34)
- Deleting a Virtual Interface (p. 34)
- Creating a Hosted Virtual Interface (p. 35)
- Accepting a Hosted Virtual Interface (p. 36)
- Adding or Removing a BGP Peer (p. 37)
- Associating a Virtual Interface with a Connection or LAG (p. 39)
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) for your side of the BGP session. 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. The ASN for the Amazon side of the BGP session is inherited from the virtual private gateway. When you create a virtual private gateway, you can specify your own private ASN. Otherwise, Amazon provides a default ASN. For more information, see AWS Managed VPN Connections 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 1,000 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. 28).

To provision a public virtual interface

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.
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. 31).

**To provision a private virtual interface to a VPC**

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**.

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 **Virtual Private Gateway**, select the virtual private 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**.
After you've created the virtual interface, you can download the router configuration file for your device. For more information, see Downloading the Router Configuration File (p. 31).

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

2. In the Virtual Interfaces pane, select the virtual interface, and then choose Actions, 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.

### Example Router Configuration Files

The following are example extracts of router configuration files.

**Cisco IOS**

```plaintext
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

! NAT Configuration for Public Virtual Interfaces (Optional)

ip access-list standard NAT-ACL
 permit any
 exit

ip nat inside source list NAT-ACL interface GigabitEthernet0/1.VLAN_NUMBER overload

interface GigabitEthernet0/1.VLAN_NUMBER
 ip nat outside
 exit

interface interface-towards-customer-local-network
 ip nat inside
 exit

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

! NAT Configuration for Public Virtual Interfaces (Optional)

ip access-list standard NAT-ACL
 permit any any
 exit

ip nat inside source list NAT-ACL VlanVLAN_NUMBER overload

interface VlanVLAN_NUMBER
ip nat outside
exit

interface interface-towards-customer-local-network
ip nat inside
exit

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
download
edit unit 0
set vlan-id VLAN_NUMBER
set family inet mtu 1500
set family inet address YOUR_PEER_IP

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

download
set routing-options autonomous-system CUSTOMER_BGP_ASN

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

download
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

# NAT Configuration for Public Virtual Interfaces (Optional)

set security policies from-zone trust to-zone untrust policy PolicyName match source-address any
set security policies from-zone trust to-zone untrust policy PolicyName match destination-address any
set security policies from-zone trust to-zone untrust policy PolicyName match application any
set security policies from-zone trust to-zone untrust policy PolicyName then permit

set security nat source rule-set SNAT-RS from zone trust
set security nat source rule-set SNAT-RS to zone untrust
set security nat source rule-set SNAT-RS rule SNAT-Rule match source-address 0.0.0.0/0
set security nat source rule-set SNAT-RS rule SNAT-Rule then source-nat interface

commit check
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

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 to view its details.

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

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. 28).

To create a hosted virtual interface
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. 31).
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**

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 virtual interface to view its details.
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**

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.
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 AWS.

6. (Private or public virtual interface) To add an IPv6 BGP peer, the **Auto-generate peer IPs** is selected by default. The peer IPv6 addresses are automatically assigned from Amazon’s pool of IPv6 addresses; you cannot specify custom IPv6 addresses.

7. In the **BGP ASN** field, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534. For a public virtual interface, the ASN must be private or already whitelisted for the virtual interface.

8. Select the **Auto-generate BGP key** check box 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**

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. 34).

Important
Connectivity to AWS is temporarily interrupted during the association process.

To associate a virtual interface with a connection
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
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. 42)
- Updating a LAG (p. 44)
- Associating a Connection with a LAG (p. 44)
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

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.
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

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.

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**

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**).

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. 44) and **Disassociating a Connection From a LAG** (p. 45).

**To create a LAG using the command line or API**

- **create-lag** (AWS CLI)
AWS Direct Connect User Guide

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 if 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**

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**

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. 39).

Important
Connectivity to AWS over the connection is interrupted during disassociation.

To disassociate a connection from a LAG
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
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 AWS 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 AWS 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. 48)](#).

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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Amazon Resource Name (ARN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections</td>
<td>arn:aws:directconnect:region:account-id:dxcon/connection-id</td>
</tr>
<tr>
<td>Link aggregation group (LAG)</td>
<td>arn:aws:directconnect:region:account-id:dxlag/lag-id</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Resource ID</th>
<th>Tag key</th>
<th>Tag value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dxcon-11aa22bb</td>
<td>Purpose</td>
<td>Production</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Amsterdam</td>
</tr>
<tr>
<td>dxvif-33cc44dd</td>
<td>Purpose</td>
<td>Production</td>
</tr>
<tr>
<td>dxcon-abcabcab</td>
<td>Purpose</td>
<td>Backup</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Frankfurt</td>
</tr>
<tr>
<td>dxvif-12312312</td>
<td>Purpose</td>
<td>Backup</td>
</tr>
</tbody>
</table>
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: `+ - = . _ : / @`
- Cost allocation tags are not supported; therefore, tags that you apply to AWS Direct Connect resources cannot be used for cost allocation tracking.

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:

```bash
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:

```bash
```

To delete a tag using the AWS CLI

Use the `untag-resource` command:

```bash
```
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. 51)
- Step 2: Download the LOA-CFA (p. 52)
- Step 3: Create a Virtual Interface and get the Router Configuration (p. 52)

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. 15).

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.

```bash
aws directconnect describe-locations
```

```json
{
  "locations": [
    {
      "locationName": "NAP do Brasil, Barueri, Sao Paulo",
      "locationCode": "TNDB"
    },
    {
      "locationName": "Tivit - Site Transamerica (Sao Paulo)",
      "locationCode": "TIVIT"
    }
  ]
}
```
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 directconnect 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. 28).
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. 31).

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.

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

   ```json
   {
   "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.

   ```bash
   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
   ```

   ```json
   {
   "virtualInterfaceState": "pending",
   "asn": 65000,
   "vlan": 101,
   "customerAddress": "192.168.1.2/30",
   "ownerAccount": "123456789012",
   "connectionId": "dxcon-fg31dyv6",
   "addressFamily": "ipv4",
   "virtualGatewayId": "vgw-ebaa27db",
   "virtualInterfaceId": "dxvif-ffhhk74f",
   "authKey": "asdf34example",
   "routeFilterPrefixes": [],
   "location": "TIVIT",
   "bgpPeers": [
   {
   "bgpStatus": "down",
   ```
"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"?>
<logical_connection id="dxvif-ffhhk74f">
  <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>
"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-ffhhk74f --query virtualInterfaces[*].customerRouterConfig --output text
```

<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <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, customerAddress=203.0.113.2/30
```

```json
{
  "virtualInterfaceState": "verifying",
  "asn": 65000,
  "vlan": 2000,
  "customerAddress": "203.0.113.2/30",
  "amazonAddress": "203.0.113.1/30",
  "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.

```bash
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:ba00::/64},
{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.

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

```xml
<?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>
```
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. 57)
- Understanding AWS Direct Connect Log File Entries (p. 58)

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.

```json
{
    "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": "2014-04-04T12:05Z"
                    }
                }
            },
            "eventTime": "2014-04-04T17:28:16Z",
            "eventSource": "directconnect.amazonaws.com",
            "eventName": "CreateConnection",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "127.0.0.1",
            "userAgent": "Coral/Jakarta",
            "requestParameters": {
                "location": "EqSE2",
                "connectionName": "MyExampleConnection",
                "bandwidth": "1Gbps"
            },
            "responseElements": {
                "location": "EqSE2",
                "region": "us-west-2",
                "connectionState": "requested",
                "bandwidth": "1Gbps",
                "ownerAccount": "123456789012",
                "connectionId": "dxcon-fhajolyy",
                "connectionName": "MyExampleConnection"
            }
        },
        ...
    ]
}
```

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

```json
{
    "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": "2014-04-04T12:05Z"
                    }
                }
            },
            "eventTime": "2014-04-04T17:28:16Z",
            "eventSource": "directconnect.amazonaws.com",
            "eventName": "CreatePrivateVirtualInterface",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "127.0.0.1",
            "userAgent": "Coral/Jakarta",
            "requestParameters": {
                "location": "EqSE2",
                "region": "us-west-2",
                "connectionState": "requested",
                "bandwidth": "1Gbps",
                "ownerAccount": "123456789012",
                "connectionId": "dxcon-fhajolyy",
                "connectionName": "MyExampleConnection"
            },
            "responseElements": {
                "location": "EqSE2",
                "region": "us-west-2",
                "connectionState": "requested",
                "bandwidth": "1Gbps",
                "ownerAccount": "123456789012",
                "connectionId": "dxcon-fhajolyy",
                "connectionName": "MyExampleConnection"
            }
        }
    ]
}
```
"principalId": "EX_PRINCIPAL_ID",
"arn": "arn:aws:iam::123456789012:user/Alice",
"accountId": "123456789012",
"accessKeyId": "EXAMPLE_KEY_ID",
"userName": "Alice",
"sessionContext": {
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2014-04-04T12:00:00Z"
  }
},
"eventTime": "2014-04-04T17:39:55Z",
"eventSource": "directconnect.amazonaws.com",
"eventName": "CreatePrivateVirtualInterface",
"awsRegion": "us-west-2",
"sourceIPAddress": "127.0.0.1",
" userAgent": "Coral/Jakarta",
"requestParameters": {
  "connectionId": "dxcon-fhajolyy",
  "newPrivateVirtualInterface": {
    "virtualInterfaceName": "MyVirtualInterface",
    "customerAddress": "[PROTECTED]",
    "authKey": "[PROTECTED]",
    "asn": -1,
    "virtualGatewayId": "vgw-bb09d4a5",
    "amazonAddress": "[PROTECTED]",
    "vlan": 123
  }
},
"responseElements": {
  "virtualInterfaceId": "dxvif-fgg616m6w",
  "authKey": "[PROTECTED]",
  "virtualGatewayId": "vgw-bb09d4a5",
  "customerRouterConfig": "[PROTECTED]",
  "virtualInterfaceType": "private",
  "asn": -1,
  "routeFilterPrefixes": [],
  "virtualInterfaceName": "MyVirtualInterface",
  "virtualInterfaceState": "pending",
  "customerAddress": "[PROTECTED]",
  "vlan": 123,
  "ownerAccount": "123456789012",
  "amazonAddress": "[PROTECTED]",
  "connectionId": "dxcon-fhajolyy",
  "location": "EqSE2"
}
],
...additional entries
]

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

```json
{
  "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",
```
The following log file record shows that a user called the **DescribeVirtualInterfaces** action.

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

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS Direct Connect resources. You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. Before you start monitoring AWS Direct Connect; however, you should create a monitoring plan that includes answers to the following questions:

• What are your monitoring goals?
• What resources will you monitor?
• How often will you monitor these resources?
• What monitoring tools will you use?
• Who will perform the monitoring tasks?
• Who should be notified when something goes wrong?

The next step is to establish a baseline for normal AWS Direct Connect performance in your environment, by measuring performance at various times and under different load conditions. As you monitor AWS Direct Connect, store historical monitoring data so that you can compare it with current performance data, identify normal performance patterns and performance anomalies, and devise methods to address issues.

To establish a baseline, you should monitor the usage, state, and health of your physical AWS Direct Connect connections.

Topics

• Monitoring Tools (p. 61)
• Monitoring with Amazon CloudWatch (p. 62)

Monitoring Tools

AWS provides various tools that you can use to monitor an AWS Direct Connect connection. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.
Automated Monitoring Tools

You can use the following automated monitoring tools to watch AWS Direct Connect and report when something is wrong:

- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see Monitoring with Amazon CloudWatch (p. 62).

- **AWS CloudTrail Log Monitoring** – Share log files between accounts, monitor CloudTrail log files in real time by sending them to CloudWatch Logs, write log processing applications in Java, and validate that your log files have not changed after delivery by CloudTrail. For more information, see Logging AWS Direct Connect API Calls in AWS CloudTrail (p. 57) and Working with CloudTrail Log Files in the AWS CloudTrail User Guide.

Manual Monitoring Tools

Another important part of monitoring an AWS Direct Connect connection involves manually monitoring those items that the CloudWatch alarms don’t cover. The AWS Direct Connect and CloudWatch console dashboards provide an at-a-glance view of the state of your AWS environment.

- The AWS Direct Connect console shows:
  - Connection status (see the **State** column)
  - Virtual interface status (see the **State** column)
- The CloudWatch home page shows:
  - Current alarms and status
  - Graphs of alarms and resources
  - Service health status

In addition, you can use CloudWatch to do the following:

- Create customized dashboards to monitor the services you care about
- Graph metric data to troubleshoot issues and discover trends
- Search and browse all your AWS resource metrics
- Create and edit alarms to be notified of problems

Monitoring with Amazon CloudWatch

You can monitor physical AWS Direct Connect connections using CloudWatch, which collects and processes raw data from AWS Direct Connect into readable, near real-time metrics. By default, CloudWatch provides AWS Direct Connect metric data in 5-minute intervals. You can optionally view data in 1-minute intervals.

For more information about Amazon CloudWatch, see the Amazon CloudWatch User Guide.

**Note**

If your connection is a hosted connection from an AWS Direct Connect partner, you cannot view CloudWatch metrics for the hosted connection.
AWS Direct Connect Metrics and Dimensions

AWS Direct Connect sends the following metrics about your AWS Direct Connect connections at 30-second intervals to Amazon CloudWatch. Amazon CloudWatch then aggregates these data points to 1-minute or 5-minute intervals. You can use the following procedures to view the metrics for AWS Direct Connect connections.

To view metrics using the CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

2. In the navigation pane, choose Metrics.
3. Under All metrics, choose the DX metric namespace.
4. Choose Connection Metrics, and select the metric dimension to view the metrics (for example, for the AWS Direct Connect connection).
5. (Optional) To return data for the selected metric in 1-minute intervals, choose Graphed metrics, and select 1 Minute from the Period list.

To view metrics using the AWS Direct Connect console

2. In the navigation pane, choose Connections and select your connection.
3. The Monitoring tab displays the metrics for your connection.

To view metrics using the AWS CLI

- At a command prompt, use the following command:

  ```bash
  aws cloudwatch list-metrics --namespace "AWS/DX"
  ```

The following metrics are available from AWS Direct Connect. Metrics are currently available for AWS Direct Connect physical connections only.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionState</td>
<td>The state of the connection. 0 indicates DOWN and 1 indicates UP.</td>
</tr>
<tr>
<td></td>
<td>Units: Boolean</td>
</tr>
<tr>
<td>ConnectionBpsEgress</td>
<td>The bit rate for outbound data from the AWS side of the connection.</td>
</tr>
<tr>
<td></td>
<td>The number reported is the aggregate over the specified time period (5 minutes by default, 1 minute minimum).</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConnectionBpsIngress</td>
<td>The bit rate for inbound data to the AWS side of the connection. The number reported is the aggregate over the specified time period (5 minutes by default, 1 minute minimum). Units: Bits per second</td>
</tr>
<tr>
<td>ConnectionPpsEgress</td>
<td>The packet rate for outbound data from the AWS side of the connection. The number reported is the aggregate over the specified time period (5 minutes by default, 1 minute minimum). Units: Packets per second</td>
</tr>
<tr>
<td>ConnectionPpsIngress</td>
<td>The packet rate for inbound data to the AWS side of the connection. The number reported is the aggregate over the specified time period (5 minutes by default, 1 minute minimum). Units: Packets per second</td>
</tr>
<tr>
<td>ConnectionCRCErrorCount</td>
<td>The number of times cyclic redundancy check (CRC) errors are observed for the data received at the connection. Units: Integer</td>
</tr>
<tr>
<td>ConnectionLightLevelTx</td>
<td>Indicates the health of the fiber connection for egress (outbound) traffic from the AWS side of the connection. This metric is available for connections with 10 Gbps port speeds only. Units: dBm</td>
</tr>
<tr>
<td>ConnectionLightLevelRx</td>
<td>Indicates the health of the fiber connection for ingress (inbound) traffic to the AWS side of the connection. This metric is available for connections with 10 Gbps port speeds only. Units: dBm</td>
</tr>
</tbody>
</table>

You can filter the AWS Direct Connect data using the following dimensions.

<table>
<thead>
<tr>
<th><strong>Dimension</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionId</td>
<td>This dimension filters the data by the AWS Direct Connect connection.</td>
</tr>
</tbody>
</table>
Creating CloudWatch Alarms to Monitor AWS Direct Connect Connections

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period that you specify, and sends a notification to an Amazon SNS topic based on the value of the metric relative to a given threshold over a number of time periods.

For example, you can create an alarm that monitors the state of an AWS Direct Connect connection and sends a notification when the connection state is DOWN for 5 consecutive 1-minute periods.

To create an alarm for connection state

2. In the navigation pane, choose Alarms, Create Alarm.
3. Choose DX Metrics.
4. Select the AWS Direct Connect connection and choose the ConnectionState metric. Choose Next.
5. Configure the alarm as follows, and choose Create Alarm when you are done:
   - Under Alarm Threshold, enter a name and description for your alarm. For Whenever, choose < and enter 1. Enter 5 for the consecutive periods.
   - Under Actions, select an existing notification list or choose New list to create a new one.
   - Under Alarm Preview, select a period of 1 minute.

For more examples of creating alarms, see Creating Amazon CloudWatch Alarms in the Amazon CloudWatch User Guide.
Troubleshooting AWS Direct Connect

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Chart: Troubleshooting a Cross Connection to AWS Direct Connect (p. 66)</td>
<td>Flow chart that provides the steps necessary to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility.</td>
</tr>
<tr>
<td>Troubleshooting a Cross Connection to AWS Direct Connect (p. 68)</td>
<td>Task list that provides the steps necessary to diagnose, troubleshoot, and repair a faulty cross connection to AWS Direct Connect within a colocation facility.</td>
</tr>
<tr>
<td>Flow Chart: Troubleshooting a Remote Connection to AWS Direct Connect (p. 68)</td>
<td>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.</td>
</tr>
<tr>
<td>Troubleshooting a Remote Connection to AWS Direct Connect (p. 70)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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. 68).
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. 66).

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 AWS 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. 70).
AWS Direct Connect User Guide
Flow Chart: 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. 68).

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

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon CloudWatch metrics</td>
<td>You can view CloudWatch metrics for your AWS Direct Connect connections. For more information, see Monitoring with Amazon CloudWatch (p. 62).</td>
<td>2017-06-29</td>
</tr>
<tr>
<td>Link aggregation groups</td>
<td>You can create a link aggregation group (LAG) to aggregate multiple AWS Direct Connect connections. For more information, see Link Aggregation Groups (p. 41).</td>
<td>2017-02-13</td>
</tr>
<tr>
<td>IPv6 support</td>
<td>Your virtual interface can now support an IPv6 BGP peering session. For more information, see Adding or Removing a BGP Peer (p. 37).</td>
<td>2016-12-01</td>
</tr>
<tr>
<td>Tagging support</td>
<td>You can now tag your AWS Direct Connect resources. For more information, see Using Tags with AWS Direct Connect (p. 49).</td>
<td>2016-11-04</td>
</tr>
<tr>
<td>Self-service LOA-CFA</td>
<td>You can now download your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) using the AWS Direct Connect console or API.</td>
<td>2016-06-22</td>
</tr>
<tr>
<td>New location in Silicon Valley</td>
<td>Updated topic to include the addition of the new Silicon Valley location in the US West (N. California) region.</td>
<td>2016-06-03</td>
</tr>
<tr>
<td>New location in Amsterdam</td>
<td>Updated topic to include the addition of the new Amsterdam location in the EU (Frankfurt) region.</td>
<td>2016-05-19</td>
</tr>
<tr>
<td>New locations in Portland, Oregon and Singapore</td>
<td>Updated topic to include the addition of the new Portland, Oregon and Singapore locations in the US West (Oregon) and Asia Pacific (Singapore) regions.</td>
<td>2016-04-27</td>
</tr>
<tr>
<td>New location in Sao Paulo, Brasil</td>
<td>Updated topic to include the addition of the new Sao Paulo location in the South America (São Paulo) region.</td>
<td>2015-12-09</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>New locations in Dallas, London, Silicon Valley, and Mumbai</td>
<td>Updated topics to include the addition of the new locations in Dallas (US East (N. Virginia) region), London (EU (Ireland) region), Silicon Valley (AWS GovCloud (US) region), and Mumbai (Asia Pacific (Singapore) region).</td>
<td>2015-11-27</td>
</tr>
<tr>
<td>New location in the China (Beijing) region</td>
<td>Updated topics to include the addition of the new Beijing location in the China (Beijing) region.</td>
<td>2015-04-14</td>
</tr>
<tr>
<td>New Las Vegas location in the US West (Oregon) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect Las Vegas location in the US West (Oregon) region.</td>
<td>2014-11-10</td>
</tr>
<tr>
<td>New EU (Frankfurt) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect locations serving the EU (Frankfurt) region.</td>
<td>2014-10-23</td>
</tr>
<tr>
<td>New locations in the Asia Pacific (Sydney) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect locations serving the Asia Pacific (Sydney) region.</td>
<td>2014-07-14</td>
</tr>
<tr>
<td>Support for AWS CloudTrail</td>
<td>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. 57).</td>
<td>2014-04-04</td>
</tr>
<tr>
<td>Support for accessing remote AWS regions</td>
<td>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. 4).</td>
<td>2013-12-19</td>
</tr>
<tr>
<td>Support for hosted connections</td>
<td>Updated topics to include support for hosted connections.</td>
<td>2013-10-22</td>
</tr>
<tr>
<td>New location in the EU (Ireland) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect location serving the EU (Ireland) region.</td>
<td>2013-06-24</td>
</tr>
<tr>
<td>New Seattle location in the US West (Oregon) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect location in Seattle serving the US West (Oregon) region.</td>
<td>2013-05-08</td>
</tr>
<tr>
<td>Support for using IAM with AWS Direct Connect</td>
<td>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. 47).</td>
<td>2012-12-21</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>New Asia Pacific (Sydney) region</td>
<td>Updated topics to include the addition of the new AWS Direct Connect location serving the Asia Pacific (Sydney) region.</td>
<td>2012-12-14</td>
</tr>
<tr>
<td>New AWS Direct Connect console, and the US East (N. Virginia) and South America (Sao Paulo) regions</td>
<td>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.</td>
<td>2012-08-13</td>
</tr>
<tr>
<td>Support for the EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo) regions</td>
<td>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.</td>
<td>2012-01-10</td>
</tr>
<tr>
<td>Support for the US West (Northern California) region</td>
<td>Updated topics to include the addition of the US West (Northern California) region.</td>
<td>2011-09-08</td>
</tr>
<tr>
<td>Public release</td>
<td>The first release of AWS Direct Connect.</td>
<td>2011-08-03</td>
</tr>
</tbody>
</table>
AWS Glossary

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