AWS Direct Connect

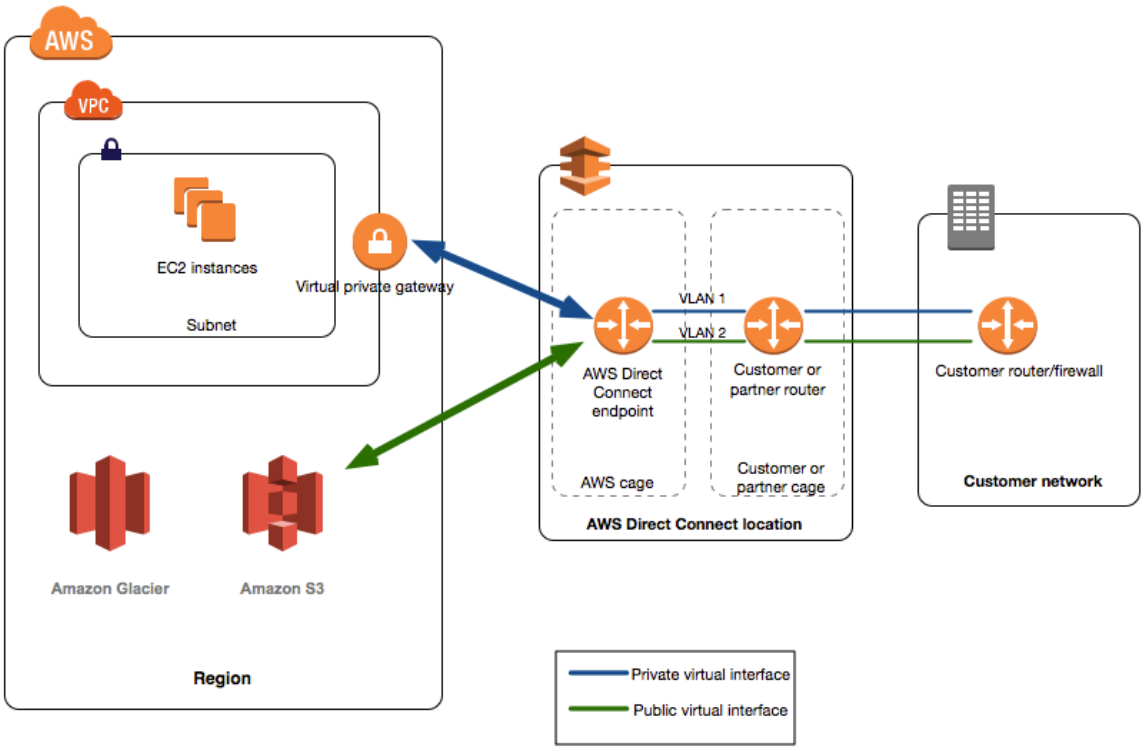
用户指南

Table of Contents

什么是 AWS Direct Connect？

AWS Direct Connect 通过标准的 1 Gb 或 10 Gb 以太网光纤电缆将您的内部网络链接到 AWS Direct Connect 位置。电缆的一端接到您的路由器，另一端接到 AWS Direct Connect 路由器。有了此连接以后，您就可以创建直接连接到公共 AWS 服务 (如 Amazon S3) 或 Amazon VPC 的虚拟接口，从而绕过您的网络路径中的 Internet 服务提供商。一个 AWS Direct Connect 位置提供对与它关联的区域中的 AWS 的访问权限，并且您可以使用公有区域或 AWS GovCloud (US) 中的单个连接访问所有其他公有区域中的公有 AWS 服务。

以下图表显示 AWS Direct Connect 如何连接您的网络。



内容

AWS Direct Connect 组件

以下是您将用于 AWS Direct Connect 的关键组件。

Connection	在 AWS Direct Connect 位置创建连接以建立从您的本地到 AWS 区域的网络连接。有关更多信息，请参阅 连接 (p. 15)。
虚拟接口	创建虚拟接口以启用对 AWS 服务的访问。公有虚拟接口允许对面向公众服务的访问，如 Amazon S3。私有虚拟接口允许对您 VPC 的访问。有关更多信息，请参阅 虚拟网关 (p. 26) 和 虚拟接口的先决条件 (p. 26)。

网络要求

要在 AWS Direct Connect 位置使用 AWS Direct Connect，您的网络必须满足以下条件之一：

- 您的网络托管于现有的 AWS Direct Connect 节点。有关可用 AWS Direct Connect 位置的更多信息，请参阅 AWS Direct Connect 产品详细信息。
- 您正与作为 AWS Partner Network (APN) 成员的 AWS Direct Connect 合作伙伴开展合作。有关信息，请参阅支持 AWS Direct Connect 的 APN 合作伙伴。
- 您正与独立的服务提供商合作连接到 AWS Direct Connect。

此外，您的网络必须符合以下条件：

- 您的网络必须使用具有适用于 1 Gb 以太网的 1000BASE-LX (1310nm) 收发器或适用于 10 Gb 以太网的 10GBASE-LR (1310nm) 收发器的单模光纤。
- 必须禁用端口的自动协商功能。必须手动配置端口速度和全双工模式。
- 必须跨整个连接 (包括中间设备) 支持 802.1Q VLAN 封装。
- 您的设备必须支持边界网关协议 (BGP) 和 BGP MD5 认证。
- (可选) 您可以在网络上配置双向转发检测 (BFD)。异步 BFD 对 AWS Direct Connect 虚拟接口自动启用，但直到您在路由器上配置它后才会生效。

AWS Direct Connect支持 IPv4 和 IPv6 通信协议。公共 AWS 服务提供的 IPv6 地址可通过 AWS Direct Connect 公有虚拟接口进行访问。

AWS Direct Connect 在物理连接层上支持的最大传输单位 (MTU) 高达 1522 字节 (14 字节以太网标头 + 4 字节 VLAN 标签 + 1500 字节 IP 数据报 + 4 字节 FCS)。

AWS Direct Connect 限制

下表列出了与 AWS Direct Connect 相关的限制。除非另外指明，否则您可使用 AWS Direct Connect 限制表单申请提高其中任何一项限制。

组建	限制	注释
每个 AWS Direct Connect 连接的虚拟接口数	50	不能提高此限制。
每个区域每个账户的活动 AWS Direct Connect 连接数	10	可以在请求时提高此限制。

组建	限制	注释
专用虚拟接口上每个边界网关协议 (BGP) 会话的路由数量	100	不能提高此限制。
公有虚拟接口上每个边界网关协议 (BGP) 会话的路由数量	1000	不能提高此限制。
每个链接聚合组 (LAG) 的连接数	4	可以在请求时提高此限制。
每个区域的链接聚合组 (LAG) 的数量	10	可以在请求时提高此限制。
每个账户的 Direct Connect 网关数	200	可以在请求时提高此限制。
每个 Direct Connect 网关的虚拟专用网关数	10	不能提高此限制。
每个 Direct Connect 网关的虚拟接口数	30	可以在请求时提高此限制。

资源

下列相关资源在您使用此服务的过程中会有所帮助。

资源	说明
AWS Direct Connect 产品信息	一般产品概述。
定价	计算月度费用。
AWS 开发人员工具	链接到开发人员工具、开发工具包、IDE 工具包和命令行工具，用于开发和管理 AWS 应用程序。
AWS Direct Connect 常见问题	有关此产品的热门问题。
AWS Direct Connect 论坛	社区论坛，在这里可以讨论关于 AWS Direct Connect 的技术性问题。
AWS 支持中心	用于创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 AWS Trusted Advisor。
联系我们	用于查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。

访问远程 AWS 区域

公有区域或 AWS GovCloud (US) 中的 AWS Direct Connect 位置可以访问任何其他公有区域 (不包括 中国（北京）) 中的公有服务。此外，可将公有区域或 AWS GovCloud (US) 中的 AWS Direct Connect 连接配置为访问您账户中在其他公有区域 (不包括 中国（北京）) 中的 VPC。因此，您可以使用单个 AWS Direct Connect 连接构建多区域服务。无论您是访问公有 AWS 服务还是其他区域中的 VPC，所有网络通信都保留在 AWS 全局骨干网上。

在远程区域外部进行的任何数据传输按远程区域数据传输费率计费。有关数据传输定价的更多信息，请参阅 AWS Direct Connect 详细信息页面上的定价部分。

有关路由策略以及 AWS Direct Connect 连接支持的 BGP 社区的更多信息，请参阅路由策略和 BGP 社区 (p. 4)。

访问远程 AWS 区域中的公有服务

要访问远程区域中的公有资源，您必须设置公有虚拟接口并建立边界网关协议 (BGP) 会话。有关更多信息，请参阅 虚拟网关 (p. 26)。

创建了公有虚拟接口并对其建立了 BGP 会话之后，您的路由器可得知其他公有 AWS 区域的路由。有关 AWS 当前公布的前缀的更多信息，请参阅Amazon Web Services 一般参考中的 AWS IP 地址范围。

访问远程区域中的 VPC

您可以在任何公有区域创建一个 Direct Connect 网关，并使用它将您的 AWS Direct Connect 通过私有虚拟接口连接到您账户中位于不同区域的 VPC。有关更多信息，请参阅 Direct Connect 网关 (p. 45)。

或者，您可以为您的 AWS Direct Connect 连接创建一个公有虚拟接口，然后建立一个到远程区域中的 VPC 的 VPN 连接。有关配置到 VPC 的 VPN 连接的更多信息，请参阅Amazon VPC 用户指南中的使用 Amazon Virtual Private Cloud 的情景。

路由策略和 BGP 社区

AWS Direct Connect 会对公有 AWS Direct Connect 连接应用入站和出站路由策略。您也可以在公布的 Amazon 路由上利用边界网关协议 (BGP) 社区标签，并针对您向 Amazon 公布的路由应用 BGP 社区标签。

路由策略

如果使用 AWS Direct Connect 访问公有 AWS 服务，您必须指定公有 IPv4 前缀或 IPv6 前缀来通过 BGP 进行公布。

下面的入站路由策略适用：

- 您必须拥有公有前缀，而且这些前缀必须在相应的区域 Internet 注册表中进行注册。
- 流量必须发往 Amazon 公有前缀。不支持在连接之间传递的路由。
- AWS Direct Connect 执行入站数据包筛选功能，以验证来自您公布的前缀的流量来源。

下面的出站路由策略适用：

- AS-PATH 用于确定路由路径，AWS Direct Connect 是源自 Amazon 流量的首选路径。内部仅使用公有 ASN 进行路由选择。
- AWS Direct Connect 会公布所有可用的本地和远程 AWS 区域前缀，并包含其他可用的 AWS 非区域接入点 (PoP) 的网内前缀，例如 CloudFront 和 Route 53。
- AWS Direct Connect 会公布最小路径长度为 3 的前缀。
- AWS Direct Connect 会公布知名 `NO_EXPORT` BGP 社区的所有公有前缀。
- 如果您有多个 AWS Direct Connect 连接，可以公布具有类似路径属性的前缀，从而调整入站流量的负载共享。
- 由 AWS Direct Connect 公布的前缀不得超过您的连接的网络边界进行公布；例如，这些前缀不得包含在任何公有 Internet 路由表中。

BGP 社区

AWS Direct Connect 支持一系列 BGP 社区标签来帮助控制流量的范围 (区域性或全球性) 和路由首选项。

范围 BGP 社区

对于您向 Amazon 公布的公有前缀，您可以应用 BGP 社区标签，指示可以在 Amazon 网络中将您的前缀传播到多远 — 仅限本地 AWS 区域、一个大陆内的所有区域或所有公有区域。

您的前缀可以使用以下 BGP 社区：

- `7224:9100` – 本地 AWS 区域
- `7224:9200` – 一个大陆的所有 AWS 区域 (例如，北美范围内)
- `7224:9300` – 全球 (所有公有 AWS 区域)

> **Note**
>
> 如果您未应用任何社区标签，则默认情况下前缀会广播给所有公共 AWS 地区 (全球)。

AWS Direct Connect 保留 `7224:1` – `7224:65535` 社区。

此外，公有和私有虚拟接口均支持知名的 `NO_EXPORT` BGP 社区。

AWS Direct Connect 还针对公布的 Amazon 路由提供 BGP 社区标签。如果您使用 AWS Direct Connect 访问公有 AWS 服务，就可以根据这些社区标签创建筛选条件。

AWS Direct Connect 为其公布的路由应用以下 BGP 社区：

- `7224:8100` – 源自关联了 AWS Direct Connect 接入点的 AWS 区域的路由。
- `7224:8200` – 源自关联了 AWS Direct Connect 接入点的大陆的路由。
- 无标签 – 全球 (所有公有 AWS 区域)。

已删除 AWS Direct Connect 公有连接不支持的社区。

本地首选项 BGP 社区

您可以使用本地首选项 BGP 社区标签来实现网络传入通信的负载平衡和路由首选项。对于通过 BGP 会话公布的每个前缀，您可以应用社区标签来指示返回通信的关联路径的优先级。私有虚拟接口支持本地首选项 BGP 社区标签。

以下本地首选项 BGP 社区标签受支持：

- `7224:7100` — 低首选项
- `7224:7200` — 中首选项
- `7224:7300` — 高首选项

本地首选项 BGP 社区标签是互斥的。要跨多个 AWS Direct Connect 连接对通信进行负载均衡，请跨连接的前缀应用相同的社区标签。要跨多个 AWS Direct Connect 连接支持故障切换，请对主要或活动虚拟接口的前缀应用具有更高首选项的社区标签。

本地首选项 BGP 社区标签将在任何 AS_PATH 属性之前进行评估，并且按照从最低到最高首选项 (优先选择最高首选项) 的顺序进行评估。

开始使用 AWS Direct Connect

AWS Direct Connect 让您能够将您的本地网络直接与位于 AWS Direct Connect 位置的设备连接。以下过程演示了开始设置 AWS Direct Connect 连接的常见场景。您还可以参阅文章如何配置 AWS Direct Connect 连接？。

您可以使用以下方法之一设置 AWS Direct Connect 连接。

Port speed	方法
1 Gbps 或更高	从您的路由器直接连接到位于 AWS Direct Connect 位置的 AWS 设备。
1 Gbps 或更高	与 AWS 合作伙伴网络 (APN) 中的合作伙伴或帮助您将路由器从数据中心、办公室或托管环境连接到 AWS Direct Connect 位置的网络提供商合作。该网络提供商不必是 APN 的成员就能为您提供连接。
低于 1 Gbps	与 AWS 合作伙伴网络 (APN) 中为您创建托管连接的合作伙伴合作。注册 AWS，然后按照说明操作来接受您的托管连接 (p. 8)。

内容

先决条件

对于端口速度为 1 Gbps 或更高的与 AWS Direct Connect 的连接，请确保您的网络满足以下要求。

- 您的网络必须使用具有适用于 1 Gb 以太网的 1000BASE-LX (1310nm) 收发器或适用于 10 Gb 以太网的 10GBASE-LR (1310nm) 收发器的单模光纤。
- 必须禁用端口的自动协商功能。必须手动配置端口速度和全双工模式。
- 必须跨整个连接 (包括中间设备) 支持 802.1Q VLAN 封装。
- 您的设备必须支持边界网关协议 (BGP) 和 BGP MD5 认证。
- (可选) 您可以在网络上配置双向转发检测 (BFD)。异步 BFD 对 AWS Direct Connect 虚拟接口自动启用，但直到您在路由器上配置它后才会生效。

步骤 1：注册 AWS

要使用 AWS Direct Connect，您需要一个 AWS 账户（如果还没有）。

如何注册 AWS 账户

1. 打开 https://aws.amazon.com/，然后选择 Create an AWS Account。

   Note

   如果您之前已登录 AWS 管理控制台，则可能无法在浏览器中执行此操作。在此情况下，请选择 Sign in to a different account，然后选择 Create a new AWS account。

2. 按照屏幕上的说明进行操作。

   作为注册流程的一部分，您会收到一个电话，需要您使用电话键盘输入一个 PIN 码。

步骤 2：请求 AWS Direct Connect 连接

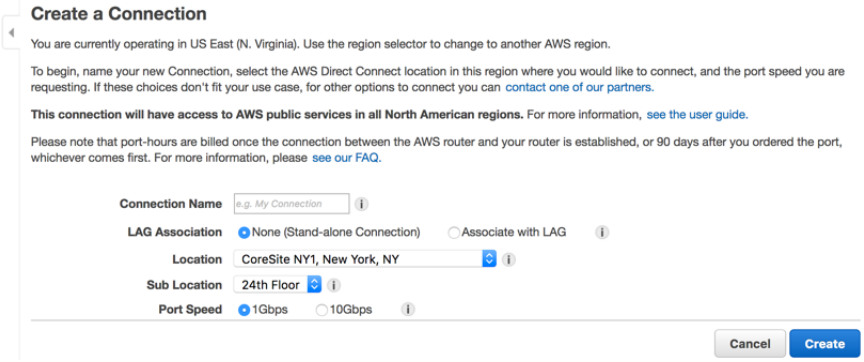
对于速度为 1 Gbps 或更高的连接，您可以使用 AWS Direct Connect 控制台提交连接请求。确保您具有以下信息：

- 您要求的端口速度：1 Gbps 或 10 Gbps。在您创建连接请求之后，无法更改端口速度。
- 将终止连接的 AWS Direct Connect 位置。

如果需要的端口速度低于 1 Gbps，您无法使用控制台请求连接。相反，您需要联系 APN 合作伙伴，由对方为您创建托管连接，然后您表示接受。请跳过以下步骤并转至(仅限低于 1 Gbps 的速度) 接受您的托管连接 (p. 8)。

如何创建新的 AWS Direct Connect 连接

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航栏中，选择要在其中连接到 AWS Direct Connect 的区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在 Welcome to AWS Direct Connect 屏幕上，选择 Get Started with Direct Connect。
4. 在 Create a Connection (创建连接) 对话框中，执行以下操作：



   a. 对于 Connection Name，输入连接的名称。

   b. 对于 LAG Association，请指定连接是否为独立的，或它是否应与您账户中的链接聚合组 (LAG) 关联。此选项仅在您在账户中有 LAG 时可用。要将此连接与 LAG 关联，请选择 LAG ID。创建此连接的端口速度和位置与 LAG 中所指定的相同。有关更多信息，请参阅链接聚合组 (p. 40)。

   c. 对于 Location，选择适当的 AWS Direct Connect 位置。

   d. 如果适用，对于 Sub Location (Sub 位置)，选择最接近您或您的网络提供商的楼层。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

   e. 选择适当的端口速度，然后单击 Create。

您的连接会列在 AWS Direct Connect 控制台的 Connections (连接) 窗格上。

AWS 审核您的请求并为您的连接配置端口可能需要长达 72 小时。在此期间，您可能会收到一封包含电子邮件，其中包含有关您的使用案例或指定位置的更多信息的请求。此电子邮件会发送到您注册 AWS 时使用的电子邮件地址。您必须在 7 日内回复，否则将删除该连接。

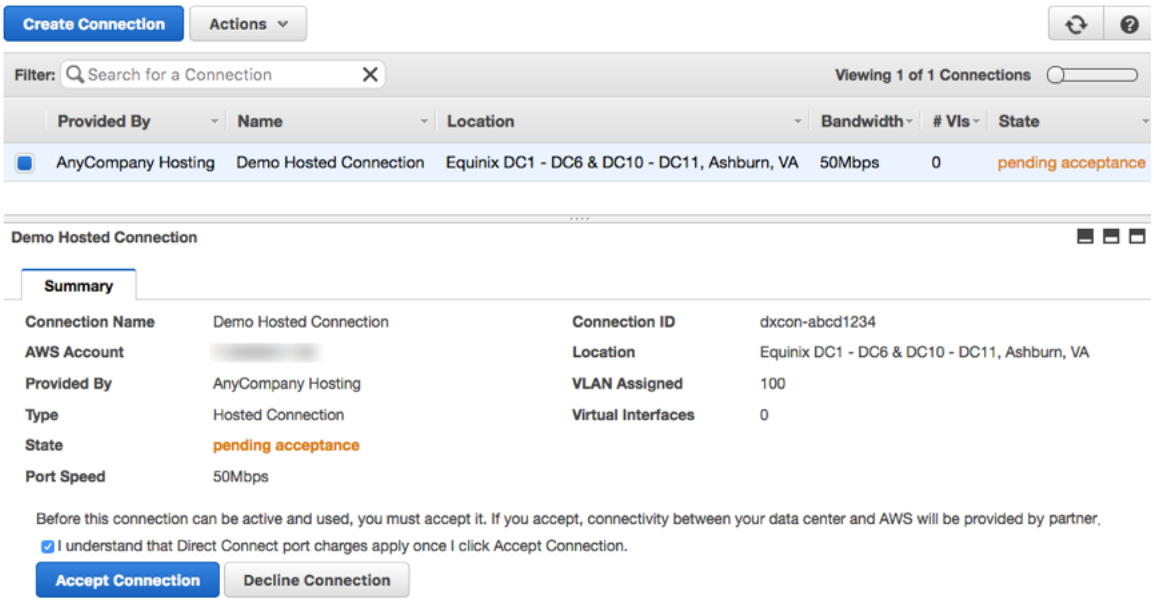
有关创建和使用 AWS Direct Connect 连接的更多信息，请参阅连接 (p. 15)。

(仅限低于 1 Gbps 的速度) 接受您的托管连接

如果您从所选合作伙伴请求了速度低于 1G 的连接，该合作伙伴将为您创建托管连接 (您无法自行创建该连接)。您必须在 AWS Direct Connect 控制台中接受该托管连接，然后才能创建虚拟接口。

如何接受托管连接

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如有必要，请选择托管连接所在的区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在 Connections 窗格中选择托管连接。



5. 选择 I understand that Direct Connect port charges apply once I click Accept Connection，然后选择 Accept Connection。
6. 转到步骤 4 (p. 9) 继续设置您的 AWS Direct Connect 连接。

步骤 3：下载 LOA-CFA

在您请求连接后，AWS 将提供《授权证书和连接设备分配 (LOA-CFA)》供您下载，也可能向您发送电子邮件要求您提供更多信息。LOA-CFA 是连接到 AWS 时使用的授权，主机托管提供商或您的网络提供商建立交叉网络连接 (cross-connect) 时需要此授权。

下载 LOA-CFA

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。

2. 在导航窗格中，选择 Connections，然后选择您的连接。
3. 选择 Actions、Download LOA-CFA。

   Note

   如果未启用链接，则 LOA-CFA 尚不可供您下载。查看您的电子邮件，了解是否要求您提供更多信息。如果仍不可用，或者您在 72 小时后仍未收到电子邮件，请联系 AWS Support。
4. 如果您希望将提供商名称作为请求者与公司名称一起显示在 LOA-CFA 中，可以选择输入您提供商的名称。选择 Download。LOA-CFA 以 PDF 文件格式下载到您的计算机中。
5. 在您下载 LOA-CFA 以后，请执行以下操作之一：

   - 如果您正在与 APN 成员或网络提供商合作，请向他们发送 LOA-CFA，以便他们能够在 AWS Direct Connect 位置为您订购交叉连接。如果他们无法为您订购交叉连接，您可以直接联系主机托管提供商 (p. 19)。
   - 如果您在 AWS Direct Connect 位置有设备，请联系主机托管提供商以请求交叉网络连接。您必须是主机托管提供商的客户，并且必须向主机托管提供商提供了授权与 AWS 路由器连接的 LOA-CFA，以及连接到您的网络时需要的信息。

作为多个站点列出的 AWS Direct Connect 位置 (例如，Equinix DC1-DC6 & DC10-DC11) 将设置为校园。如果您或您的网络提供商的设备位于任一这些站点中，您将能够请求交叉连接到所分配的端口，即使该端口位于校园内的不同建筑物中。

Important

园区被视为单个 AWS Direct Connect 位置。要实现高可用性，请配置与不同 AWS Direct Connect 位置的连接。

如果您或您的网络合作伙伴在建立物理连接时遇到问题，请参阅排查第 1 层 (物理) 问题 (p. 67)。

步骤 4：创建虚拟接口

要开始使用您的 AWS Direct Connect 连接，您必须创建一个虚拟接口。您可以创建私有虚拟接口以连接到 VPC，或者创建公有虚拟接口以连接到不在 VPC 中的公有 AWS 服务。创建与 VPC 的私有虚拟接口时，您需要所要连接到的各 VPC 的专用虚拟接口。例如，您需要三个专用虚拟接口连接到三个 VPC。

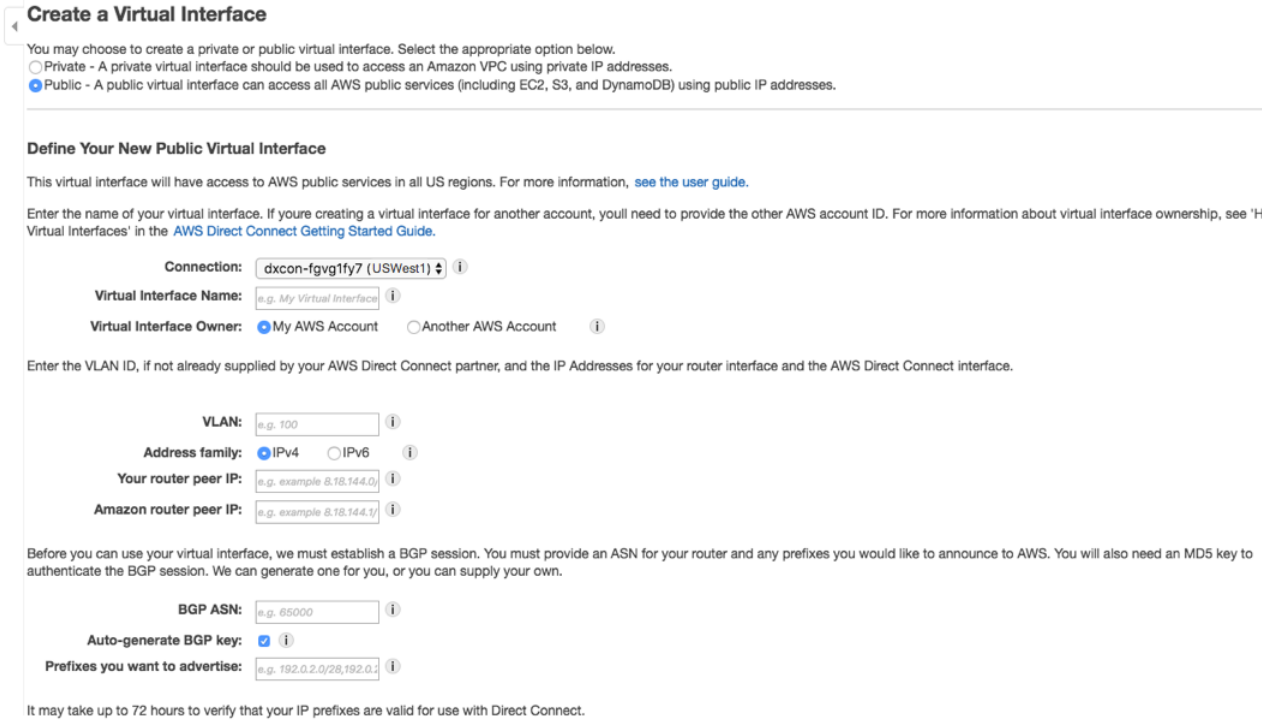
在您开始之前，请确保您已拥有以下信息：

- Connection：要为其创建虚拟接口的 AWS Direct Connect 连接或链路聚合组 (LAG)。
- Virtual interface name：虚拟接口名称。
- Virtual interface owner (虚拟接口所有者)：如果要为另一个账户创建虚拟接口，您需要其他账户的 AWS 账户 ID。
- (仅私有虚拟接口) Connection to：要连接到同一区域中的 VPC，您需要 VPC 的虚拟私有网关。BGP 会话的 Amazon 端的 ASN 是从虚拟私有网关继承的。当您创建虚拟私有网关时，您可以指定您自己的私有 ASN。否则，Amazon 会提供默认 ASN。有关更多信息，请参阅 Amazon VPC 用户指南 中的创建虚拟专用网关。要通过 Direct Connect 网关连接到 VPC，您需要 Direct Connect 网关。有关更多信息，请参阅 Direct Connect 网关。
- VLAN：未在您的连接上使用的唯一的虚拟局域网 (VLAN) 标记。该值必须介于 1 和 4094 之间且必须符合 Ethernet 802.1Q 标准。任何经过 AWS Direct Connect 连接的流量都必须有此标签。
- Address family (地址系列)：BGP 对等会话将基于 IPv4 还是 IPv6。
- Peer IP addresses (对等 IP 地址)：虚拟接口可以针对 IPv4、IPv6 或这二者 (双堆栈) 支持 BGP 对等会话。您无法在同一个虚拟接口上为同一 IP 地址系列创建多个 BGP 会话。IP 地址范围会分配到 BGP 对等会话的各个虚拟接口端。
  - IPv4:

  - (仅公有虚拟接口) 您必须指定您所拥有的唯一的公有 IPv4 地址 (/30)。
  - (仅私有虚拟接口) Amazon 可以为您生成私有 IPv4 地址。如果您自行指定，请确保仅为路由器接口和 AWS Direct Connect 接口指定私有 CIDR (例如，不要从本地网络中指定其他 IP 地址)。
- IPv6：Amazon 会自动为您分配一个 /125 IPv6 CIDR。您不能指定自己的对等 IPv6 地址。
- BGP 信息：
  - 用于 BGP 会话的您这一侧的公有或私有边界网关协议 (BGP) 自治系统编号 (ASN)。如果使用公有 ASN，您必须具有其所有权。如果使用私有 ASN，它必须在 64512 至 65535 的范围内。如果您对公有虚拟接口使用私有 ASN，则自治系统 (AS) 预置将不起作用。
  - MD5 BGP 身份验证密钥。您可以提供自己的密钥，或者让 Amazon 为您生成一个。
- (针对仅公有虚拟接口) Prefixes you want to advertise (您要公布的前缀)：要通过 BGP 公布的公有 IPv4 路由或 IPv6 路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。
  - IPv4：IPv4 CIDR 不能与通过 AWS Direct Connect 公布的其他公有 IPv4 CIDR 重叠。如果您不拥有公有 IPv4 地址，您的网络提供商也许能够为您提供一个公有 IPv4 CIDR。否则，联系 AWS Support 以请求一个 /31 公有 IPv4 CIDR (并且在您的请求中提供一个使用案例)。
  - IPv6：指定 /64 或更短的前缀长度。

配置与非 VPC 服务间的公有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections，再选择要使用的连接，然后依次选择 Actions 和 Create Virtual Interface。
3. 在 Create a Virtual Interface 窗格中，选择 Public。



4. 在 Define Your New Public Virtual Interface (定义新的公有虚拟接口) 对话框中，执行以下操作并选择 Continue (继续)：

   a. 对于 Connection，选择要用于创建虚拟接口的现有实体连接。

   b. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。

   c. 对于 Virtual Interface Owner，如果虚拟接口用于您的 AWS 账户，则选择 My AWS Account 选项。

d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
e. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：
   - 对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。
   - 对于 Amazon router peer IP，输入用于将流量发送到 Amazon 的 IPv4 CIDR 地址。
f. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。
g. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。
h. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

   要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。
i. 对于 Prefixes you want to advertise，输入通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号隔开)。

5. 下载您的路由器配置。有关更多信息，请参阅 步骤 5：下载路由器配置 (p. 12)。

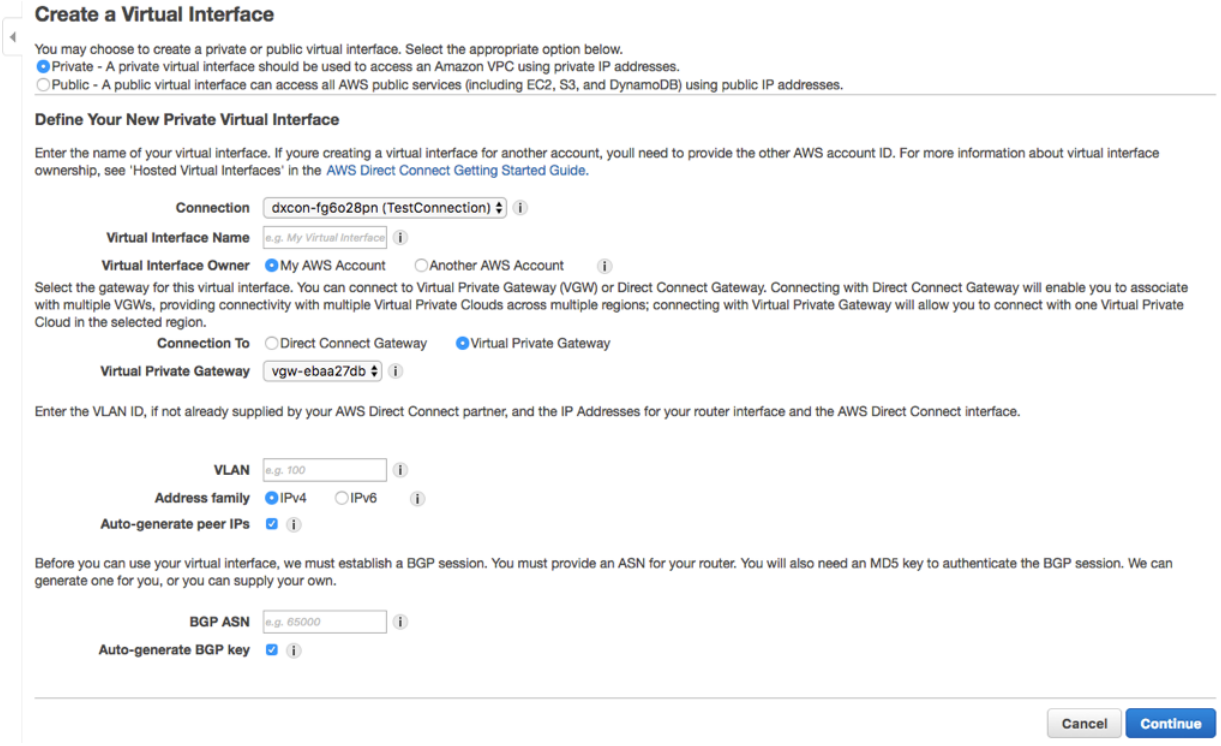
   Note

   如果您的公有前缀或 ASN 属于某个 ISP 或网络运营商，则 AWS 会请求您提供其他信息。这可以是使用公司抬头的文档，也可以是来自公司域名的用于验证该网络前缀/ASN 可能由您使用的电子邮件。

当您创建一个公有虚拟接口时，AWS 可能需要长达 72 小时来审核和批准您的请求。

配置与 VPC 间的私有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections (连接)，选择要使用的连接，然后依次选择 Actions (操作) 和 Create Virtual Interface (创建虚拟接口)。
3. 在 Create a Virtual Interface (创建虚拟接口) 窗格中，选择 Private (私有)。



4. 在 Define Your New Private Virtual Interface (定义您的新私有虚拟接口) 下，执行以下操作并选择 Continue (继续)：

   a. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。

   b. 对于 Virtual Interface Owner，如果虚拟接口用于您的 AWS 账户，则选择 My AWS Account 选项。

   c. 对于 Connection To (连接到)，选择 Virtual Private Gateway (虚拟私有网关)，然后选择要连接到的虚拟私有网关。

   d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。

   e. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：

      - 要让 AWS 生成您的路由器 IP 地址和 Amazon IP 地址，请选择 Auto-generate peer IPs (自动生成对等 IP)。
      - 要自行指定这些 IP 地址，请清除 Auto-generate peer IPs 复选框。对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。对于 Amazon router peer IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。

   f. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。

   g. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

   h. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

      要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

5. 下载您的路由器配置。有关更多信息，请参阅 步骤 5：下载路由器配置 (p. 12)。

   Note

   如果您使用 VPC 向导创建 VPC，系统将自动为您启用路线传播。通过路线传播，路线会自动添加到您 VPC 中的路线表。如果您愿意，您可以停用路线传播。有关更多信息，请参阅Amazon VPC 用户指南中的在路由表中启用路由传播。

步骤 5：下载路由器配置

当您为 AWS Direct Connect 连接创建了虚拟接口后，可以下载路由器配置文件。该文件包含将您的路由器配置为用于您的私有或公有虚拟接口所需的命令。

下载路由器配置

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在 Virtual Interfaces (虚拟接口) 窗格中，选择虚拟接口，然后选择 Actions (操作)、Download Router Configuration (下载路由器配置)。
3. 在 Download Router Configuration (下载路由器配置) 对话框中，执行以下操作：

   a. 对于 Vendor，选择您的路由器的生产商。

   b. 对于 Platform，选择您的路由器型号。

   c. 对于 Software，选择您的路由器软件版本。

4. 选择 Download，然后使用适合您路由器的配置，以确保您可以连接到 AWS Direct Connect。

有关示例配置文件，请参阅示例路由器配置文件。

在配置您的路由器后，虚拟接口的状态将变为 `UP`。如果虚拟接口保持断开并且您无法对 AWS Direct Connect 设备的对等 IP 地址执行 ping 操作，请参阅排查第 2 层 (数据链路) 问题 (p. 68)。如果您可以对

对等 IP 地址执行 ping 操作，请参阅排查第 3/4 层 (网络/传输) 问题 (p. 70)。如果 BGP 对等会话已建立但您无法路由流量，请参阅排查路由问题 (p. 72)。

步骤 6：确认您的虚拟接口

建立到 AWS 云或 Amazon VPC 的虚拟接口以后，可以通过以下步骤验证您的 AWS Direct Connect 连接。

确认您的虚拟接口连接到 AWS 云

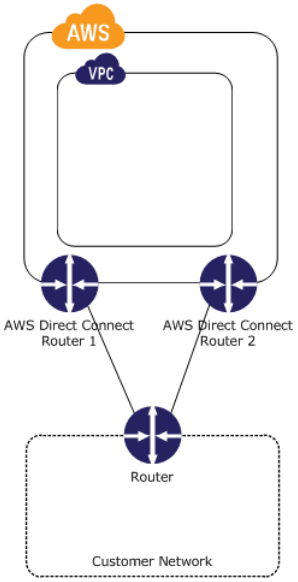
- 运行 `traceroute` 并确认 AWS Direct Connect 标识符在网络追踪范围内。

如何要确认您的虚拟接口连接到 Amazon VPC

1. 使用可以通过 Ping 操作访问的 AMI，例如 Amazon Linux AMI，将 EC2 实例启动到与虚拟专用网关连接的 VPC 中。当您使用 Amazon EC2 控制台中的实例启动向导时，可在 Quick Start 选项卡中使用 Amazon Linux AMI。有关更多信息，请参阅启动实例 (Amazon EC2 用户指南（适用于 Linux 实例）中）。确保与实例关联的安全组包含允许入站 ICMP 流量的规则（用于检测请求）。
2. 当实例开始运行后，获取其私有 IPv4 地址 (例如 10.0.0.4)。Amazon EC2 控制台显示的地址是实例详细信息的一部分。
3. Ping 私有 IPv4 地址并获得响应。

(可选) 配置冗余连接

为了提供故障转移，我们建议您申请并配置两个接到 AWS 的专用连接 (如下图所示)。这些连接会在您的网络中的一个或两个路由器上终止。



如果您配置两个专用连接，则可以有不同的配置选择：

- 主动/主动（BGP 多路径）。这是两个连接均为主动连接的默认配置。AWS Direct Connect 支持同一个位置中指向多个虚拟接口的多路径，流量基于流程在接口之间负载均衡。如果一个连接不可用，那么所有流量都会路由到另一个连接。
- 主动/被动（故障转移）。一个连接正在处理流量，另一个连接处于待命状态。如果主动连接不可用，所有流量都会路由到被动连接。您需要在您的一个链接上将 AS 路径附加到路由之前以使其成为被动链接。

您如何配置连接并不影响冗余，但是会影响策略，而该策略决定如何在两个连接间路由流量。我们建议您将两个连接配置为活跃状态。

如果您使用 VPN 连接实现冗余，请确保实施了运行状况检查和故障转移机制，并检查您的路由表路由。

要实现高可用性，强烈建议您配置与不同 AWS Direct Connect 位置的连接。有关高可用性选项的更多信息，请参阅多数据中心 HA 网络连接。

连接

要创建 AWS Direct Connect 连接，您需要以下信息：

- AWS Direct Connect 位置

  与 AWS Partner Network (APN) 中的伙伴合作，帮助您建立连接 AWS Direct Connect 节点和数据中心、办公室或托管环境的网络线路，或者在与 AWS Direct Connect 节点相同的设施内提供托管空间。如需属于 APN 的 AWS Direct Connect 合作伙伴列表，请参阅支持 AWS Direct Connect 的 APN 合作伙伴。
- Port speed

  AWS Direct Connect 支持两种端口速度：1 Gbps：通过单模光纤的 1000BASE-LX (1310nm)，和 10 Gbps：通过单模光纤的 10GBASE-LR (1310nm)。在您创建连接请求之后，无法更改端口速度。如果需要更改端口速度，您必须创建并配置新的连接。

  对于速度低于 1 Gbps 的端口，您不能使用控制台请求连接。而是可以联系支持 AWS Direct Connect 并可以为您预配置托管连接的 APN 合作伙伴。

在您请求了连接后，AWS 将提供《授权证书和连接设备分配 (LOA-CFA)》供您下载，也可能向您发送电子邮件要求您提供更多信息。如果收到提供更多信息的请求，您必须在 7 日内回复，否则将删除该连接。LOA-CFA 是用于连接到 AWS 的授权，您的网络提供商需要它来为您订购交叉连接。如果您在 AWS Direct Connect 位置没有设备，就无法为自己订购交叉连接；您的网络提供商为您执行此操作。

有关将连接与链接聚合组 (LAG) 关联的信息，请参阅将连接与 LAG 关联 (p. 43)。

创建连接之后，创建虚拟接口以连接到公有和私有 AWS 资源。有关更多信息，请参阅 虚拟网关 (p. 26)。

主题

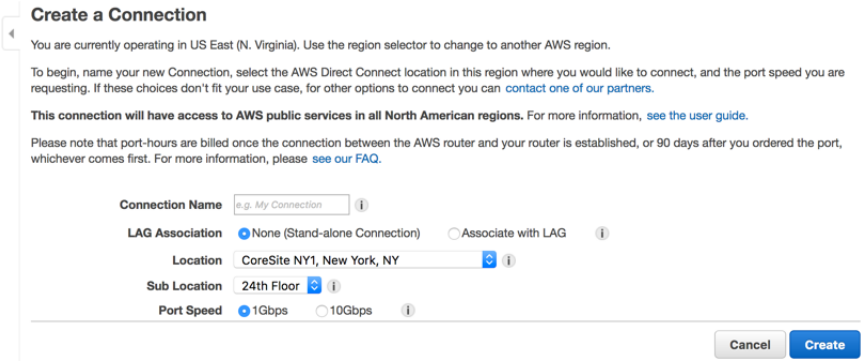
创建连接

您可以创建独立的连接，或者创建连接来与您账户中的 LAG 关联。如果您将连接与 LAG 关联，则将使用在 LAG 中指定的相同端口速度和位置来创建该连接。

如果您在 AWS Direct Connect 位置没有设备，请先在 AWS 合作伙伴网络 (APN) 联系 AWS 合作伙伴。有关更多信息，请参阅支持 AWS Direct Connect 的 APN 合作伙伴。

创建新连接

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航栏中，选择要在其中连接到 AWS Direct Connect 的区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，依次选择 Connections、Create Connection。
4. 在 Create a Connection 对话框中，输入以下值，然后选择 Create：



a. 对于 Connection Name，输入连接的名称。

b. 对于 LAG Association，指定连接是独立的还是应该与 LAG 关联。如果您将此连接与 LAG 关联，请选择 LAG ID。

c. 对于 Location，选择适当的 AWS Direct Connect 位置。

d. 如果适用，对于 Sub Location (Sub 位置)，选择最接近您或您的网络提供商的楼层。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

e. 选择与现有网络兼容的合适端口速度。

使用命令行或 API 创建 连接

- create-connection (AWS CLI)
- CreateConnection (AWS Direct Connect API)

下载 LOA-CFA

AWS 处理您的连接请求之后，您可以下载《授权证书和连接设备分配 (LOA-CFA)》。

下载 LOA-CFA

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections。
3. 选择 Actions、Download LOA-CFA。

   Note

   如果未启用链接，则 LOA-CFA 尚不可供您下载。查看您的电子邮件，了解是否要求您提供更多信息。如果仍不可用，或者您在 72 小时后仍未收到电子邮件，请联系 AWS Support。
4. 在对话框中，如果您希望将提供商名称作为请求者与公司名称一起显示在 LOA-CFA 中，可以选择输入您的提供商名称。选择 Download。LOA-CFA 以 PDF 文件格式下载到您的计算机中。
5. 将 LOA-CFA 发送到网络提供商或主机托管提供商，以便其为您订购交叉连接。各托管供应商的联系流程可能会不同。有关更多信息，请参阅 要求在 AWS Direct Connect 节点交叉连接 (p. 19)。

LOA-CFA 在 90 天后失效。如果您的连接未在 90 天后建立，我们将向您发送电子邮件，提醒您 LOA-CFA 已失效。要使用新的发布日期刷新 LOA-CFA，请从 AWS Direct Connect 控制台重新下载。如果您不采取任何操作，我们将删除连接。

Note

在您创建连接 90 天之后或者您的路由器与 AWS Direct Connect 终端节点之间建立连接之后 (以先到者为准)，将开始端口小时计费。有关更多信息，请参阅 AWS Direct Connect 定价。如果您在

重新发行 LOA-CFA 之后不再需要连接，您必须自行删除该连接。有关更多信息，请参阅 删除连接 (p. 17)。

使用命令行或 API 下载 LOA-CFA

- describe-loa (AWS CLI)
- DescribeLoa (AWS Direct Connect API)

查看连接详细信息

您可以查看您当前的连接状态。您还可以查看连接 ID (例如，`dxcon-12nikabc`) 并验证它与您所接收或下载的《授权证书和连接设备分配 (LOA-CFA)》上的连接 ID 匹配。

如何查看连接的详细信息

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在 Connections 窗格中选择一个连接，查看其详细信息。

   Provided By (提供者) 列中会列出与该连接相关联的服务提供商。

使用命令行或 API 创建连接

- describe-connections (AWS CLI)
- DescribeConnections (AWS Direct Connect API)

删除连接

只要连接没有连接虚拟接口，您就可以删除该连接。删除您的连接会终止该连接的所有端口的小时计费。AWS Direct Connect 数据传输费用与虚拟接口相关联。所有交叉连接或网络线路费用都与 AWS Direct Connect 没有关系，因此必须逐个删除。有关如何删除虚拟接口的详细信息，请参阅 删除虚拟接口 (p. 33)。

如果连接是链接聚合组 (LAG) 的一部分，则您无法删除连接，因为这将导致 LAG 低于其设置的最小运行连接数。

如何删除连接

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在 Connections 窗格中，依次选择要删除的连接、Actions 和 Delete Connection。
5. 在 Delete Connection 对话框中，选择 Delete。

使用命令行或 API 删除 连接

- delete-connection (AWS CLI)
- DeleteConnection (AWS Direct Connect API)

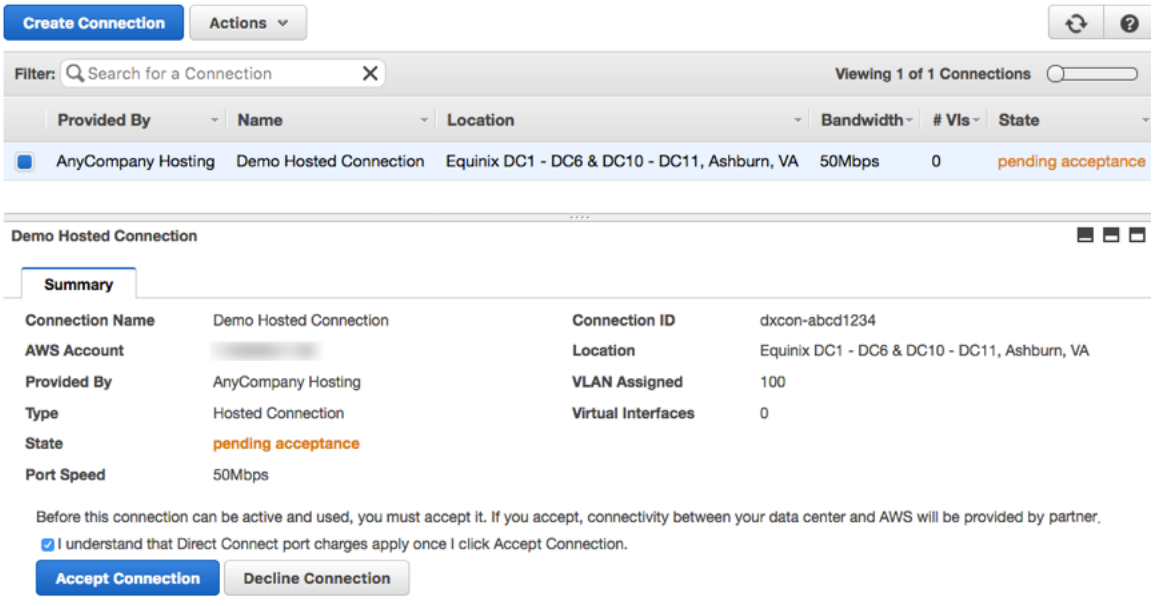
接受托管连接

如果您对购买托管连接感兴趣，则必须联系 AWS 合作伙伴网络 (APN) 中的合作伙伴。该合作伙伴会为您配置连接。配置连接后，连接会出现在 AWS Direct Connect 控制台中的 Connections (连接) 窗格中。

在您开始使用托管连接前，必须接受该连接。

如何接受托管连接

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在 Connections 窗格中选择一个连接。



5. 选择 I understand that Direct Connect port charges apply once I click Accept Connection，然后选择 Accept Connection。

使用命令行或 API 接受托管连接

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

要求在 AWS Direct Connect 节点交叉连接

当您下载了《授权和连接设备分配 (LOA-CFA) 通知函》后，您需要完成交叉网络连接（即交叉连接）。如果您在 AWS Direct Connect 节点已经有设备，请与相应的供应商联系，以便完成交叉连接。有关各供应商的具体说明，请参阅下表。有关交叉连接定价，请联系您的供应商。建立交叉连接后，可以使用 AWS Direct Connect 控制台创建虚拟界面。

一些位置设置为园区。有关更多信息，请参阅 AWS Direct Connect 位置。

如果您在 AWS Direct Connect 节点还没有设备，您可以与 AWS Partner Network (APN) 中的一位合作伙伴合作，帮助您连接到 AWS Direct Connect 节点。要查看 APN 中有 AWS Direct Connect 连接经验的合作伙伴的列表，请参阅支持 AWS Direct Connect的 APN 合作伙伴。您将需要与您选中的供应商共享 LOA-CFA，以便顺利完成交叉连接。

AWS Direct Connect 连接可提供对其他区域中的资源的访问权限。有关更多信息，请参阅 访问远程 AWS 区域 (p. 3)。

> **Note**
>
> 如果交叉连接在 90 天内未完成，LOA-CFA 授予的权限将失效。要更新已失效的 LOA-CFA，您可以从 AWS Direct Connect 控制台再次下载它。有关更多信息，请参阅 下载 LOA-CFA (p. 16)。

亚太区域（东京）

地点	如何申请连接
AT Tokyo Chuo Data Center，东京	要提交交叉连接申请，可以与 Ikenishi 联系，邮箱为：ikenishi.junko@attokyo.co.jp。

地点	如何申请连接
是方电讯，台北	要提交交叉连接申请，可以与是方电讯联系，电子邮件地址为：vicky_chan@chief.com.tw。
Equinix OS1，大阪	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix TY2，东京	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。

亚太区域（首尔）

地点	如何申请连接
KINX Gasan Data Center，首尔	要提交交叉连接申请，可以与 KINX 联系，邮箱为：sales@kinx.net。
LG U+ Pyeong-Chon Mega Center，首尔	要申请交叉连接，可以向 kidcadmin@lguplus.co.kr 和 center8@kidc.net 提交 LOA 文档。

亚太区域（新加坡）

地点	如何申请连接
Equinix SG2，新加坡	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Global Switch，Singapore	要提交交叉连接申请，可以与 Global Switch 联系，电子邮箱：salessingapore@globalswitch.com。
GPX Mumbai	要提交交叉连接申请，可以与 GPX 联系，电子邮箱：nkankane@gpxglobal.net。
iAdvantage MEGA-i，香港	可以通过 cs@iadvantage.net 联系 iAdvantage 或者在 iAdvantage 布线订单电子表格上下订单来提交交叉连接的申请。
Menara AIMS，吉隆坡	现有 AIMS 客户可以通过客户服务门户填写工程工作订单请求表，请求交叉连接订单；如果提交请求遇到任何问题，请与 service.delivery@aims.com.my 联系。

亚太区域（悉尼）

地点	如何申请连接
Equinix SY3，悉尼	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Global Switch SY6，悉尼	要提交交叉连接申请，可以与 Global Switch 联系，电子邮箱：salessydney@globalswitch.com。
NEXTDC C1，堪培拉	要提交交叉连接申请，可以与 NEXTDC 联系，电子邮件地址为：nxtops@nextdc.com。
NEXTDC M1，墨尔本	要提交交叉连接申请，可以与 NEXTDC 联系，电子邮件地址为：nxtops@nextdc.com。

地点	如何申请连接
NEXTDC P1，珀斯	要提交交叉连接申请，可以与 NEXTDC 联系，电子邮件地址为：nxtops@nextdc.com。

亚太地区（孟买）

地点	如何申请连接
GPX Mumbai	要提交交叉连接申请，可以与 GPX 联系，电子邮箱：nkankane@gpxglobal.net。
NetMagic DC2，班加罗尔	要提交交叉连接申请，可以与 NetMagic 销售和市场营销联系，免费电话为 18001033130，邮箱为 marketing@netmagicsolutions.com。
Sify Rabale, Mumbai	要提交交叉连接申请，可以与 Sify 联系，电子邮箱：aws.directconnect@sifycorp.com。
STT GDC Pvt. Ltd. VSB，钦奈	要提交交叉连接申请，可以与 STT 联系，电子邮件地址为：enquiry.AWSDX@sttelemediagdc.in

加拿大 (中部)

地点	如何申请连接
Allied 250 Front St W, Toronto	交叉连接申请可提交至：driches@alliedreit.com。
Cologix MTL3，蒙特利尔	要提交交叉连接申请，可以与 Cologix 联系，电子邮件地址为：aws@cologix.com。
Cologix VAN2，温哥华	要提交交叉连接申请，可以与 Cologix 联系，电子邮件地址为：aws@cologix.com。
eStruxture，蒙特利尔	要提交交叉连接申请，可以与 eStruxture 联系，电子邮件地址为：directconnect@estruxture.com。

中国（北京）

地点	如何申请连接
Sinnet Jiuxianqiao IDC	要提交交叉连接申请，可以与 Sinnet 联系，电子邮箱：dx-order@sinnet.com.cn。

欧洲（法兰克福）

地点	如何申请连接
CE Colo，布拉格	要提交交叉连接申请，可以与 CE Colo 联系，邮箱为：info@cecolo.com。
Equinix AM3，阿姆斯特丹	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix FR5，法兰克福	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。

地点	如何申请连接
Equinix HE6，赫尔辛基	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix ITConic MD2，马德里	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix MU1，慕尼黑	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix WA1，华沙	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
IPB，柏林	要提交交叉连接申请，可以与 IPB 联系，邮箱为：kontakt@ipb.de。
Interxion FRA6，法兰克福	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion MAD2，马德里	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion MRS1，马赛	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion STO1，斯德哥尔摩	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion VIE2，维也纳	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion ZUR1，苏黎世	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Telehouse Voltaire，巴黎	要提交交叉连接请求，可以在客户门户网站创建请求。 请求类型：DFM/SFM 布局/连接/MMR 电路调试

欧洲（爱尔兰）

地点	如何申请连接
Digital Realty (UK), Docklands	要提交交叉连接申请，可以与 Digital Realty (UK) 联系，电子邮箱：amazon.orders@digitalrealty.com。
Eircom Clonshaugh	要提交交叉连接申请，可以与 Eircom 联系，电子邮箱：awsorders@eircom.ie。
Equinix LD5，伦敦 (Slough)	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Interxion DUB2，都柏林	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Interxion MRS1，马赛	要提交交叉连接申请，可以与 Interxion 联系，电子邮箱：customer.services@interxion.com。
Teraco CT1，开普敦	要提交交叉连接申请，可以与 Teraco 联系，邮箱为 support@teraco.co.za（针对现有 Teraco 客户）和 connect@teraco.co.za（针对新客户）。

地点	如何申请连接
Teraco JB1，约翰内斯堡	要提交交叉连接申请，可以与 Teraco 联系，邮箱为 support@teraco.co.za（针对现有 Teraco 客户）和 connect@teraco.co.za（针对新客户）。

欧洲 (伦敦)

地点	如何申请连接
Digital Realty (UK), Docklands	要提交交叉连接申请，可以与 Digital Realty (UK) 联系，电子邮箱：amazon.orders@digitalrealty.com。
Equinix LD5，伦敦 (Slough)	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix MA3，曼彻斯特	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Telehouse West，伦敦	要提交交叉连接申请，可以与 Telehouse UK 联系，电子邮件地址为：sales.support@uk.telehouse.net。

欧洲 (巴黎)

地点	如何申请连接
Equinix PA3，巴黎	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Telehouse Voltaire，巴黎	要提交交叉连接请求，可以在客户门户网站创建请求。 请求类型：DFM/SFM 布局/连接/MMR 电路调试

南美洲（圣保罗）

地点	如何申请连接
Equinix RJ2，里约热内卢	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix SP4，圣保罗	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Tivit	要提交交叉连接申请，可以与 Tivit 联系，邮箱为：aws@tivit.com.br。

美国东部（弗吉尼亚北部）

地点	如何申请连接
165 Halsey Street, Newark	请参考位于 http://www.165halsey.com/colocation-services/connectivity/ 的资源，或联系 operations@165halsey.com。
CoreSite NY1，纽约	要提交交叉连接申请，可以在 CoreSite 客户门户网站下订单。当您完成表单后，请检查订单的准确性，然后使用 MyCoreSite Web 站点审批订单。

地点	如何申请连接
CoreSite VA1，雷斯顿	要提交交叉连接申请，可以在 CoreSite 客户门户网站下订单。当您完成表单后，请检查订单的准确性，然后使用 MyCoreSite Web 站点审批订单。
Digital Realty ATL1，亚特兰大	要提交交叉连接申请，可以与 Digital Realty 联系，邮箱为：amazon.orders@digitalrealty.com。
Equinix DC2/DC11，阿什本	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix DA2，达拉斯	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix MI1，迈阿密	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Lightower, Philadelphia	要提交交叉连接申请，可以与 Lightower 联系，邮箱为：awsorders@lightower.com。
Markley，One Summer Street，波士顿	可以在客户门户网站上提交交叉连接申请：https://portal.markleygroup.com。对于新查询，请联系 sales@markleygroup.com。

美国东部（俄亥俄州）

地点	如何申请连接
Cologix COL2，哥伦布市	要提交交叉连接申请，可以与 Cologix 联系，电子邮件地址为：aws@cologix.com。
Cologix MIN3，明尼阿波利斯	要提交交叉连接申请，可以与 Cologix 联系，电子邮件地址为：aws@cologix.com。
CyrusOne West III，休斯顿	可以在客户门户网站上提交交叉连接申请和信息申请：https://cyrusone.com/about-enterprise-data-center-provider/customer-support/。
Equinix CH2，芝加哥	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
QTS 芝加哥	要提交交叉连接申请，可以与 QTS 联系，电子邮箱：AConnect@qtsdatacenters.com。

AWS GovCloud (US)

地点	如何申请连接
Equinix SV5，圣荷西	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。

美国西部（加利福尼亚北部）

地点	如何申请连接
CoreSite LA1，洛杉矶	要提交交叉连接申请，可以在 CoreSite 客户门户网站下订单。当您完成表单后，请检查订单的准确性，然后使用 MyCoreSite Web 站点审批订单。
CoreSite SV4，圣克拉拉	要提交交叉连接申请，可以在 CoreSite 客户门户网站下订单。当您完成表单后，请检查订单的准确性，然后使用 MyCoreSite Web 站点审批订单。
Equinix LA3，埃尔塞贡多	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
Equinix SV5，圣荷西	要提交交叉连接申请，可以与 Equinix 联系，电子邮箱：awsdealreg@equinix.com。
PhoenixNAP，菲尼克斯	要提交交叉连接申请，可以与 phoenixNAP Provisioning 联系，电子邮件地址为：provisioning@phoenixnap.com。

美国西部（俄勒冈）

地点	如何申请连接
CoreSite DE1，丹佛	要提交交叉连接申请，可以在 CoreSite 客户门户网站下订单。当您完成表单后，请检查订单的准确性，然后使用 MyCoreSite Web 站点审批订单。
EdgeConneX，波特兰	要提交交叉连接申请，可以在 EdgeOS 客户门户网站上下订单。在提交表单之后，EdgeConneX 将提供服务订单表进行审批。您可以将问题发送到 cloudaccess@edgeconnex.com。
Equinix SE2，西雅图	要提交交叉连接申请，可以与 Equinix 联系，邮箱为：support@equinix.com。
Pittock Block，波特兰	要提交交叉连接申请，可发送电子邮件至 crossconnect@pittock.com，或致电 +1 503 226 6777。
Switch SUPERNAP 8, Las Vegas	要提交交叉连接申请，可以与 Switch SUPERNAP 联系，电子邮箱：orders@supernap.com。
TierPoint Seattle	要提交交叉连接申请，可以与 TierPoint 联系，电子邮箱：sales@tierpoint.com。

虚拟网关

您必须创建一个虚拟接口，才能开始使用您的 AWS Direct Connect 连接。您可以创建私有虚拟接口以连接到 VPC，或者创建公有虚拟接口以连接到不在 VPC 中的 AWS 服务，例如 Amazon S3 和 Amazon Glacier。您可以在单个 AWS Direct Connect 连接上配置多个虚拟接口。对于私有虚拟接口，每个 VPC 都需要一个私有虚拟接口，以从 AWS Direct Connect 连接进行连接，或者您可以使用 Direct Connect 网关。有关更多信息，请参阅 Direct Connect 网关。

要使用 IPv6 地址连接到其他 AWS 服务，请检查服务文档以确保支持 IPv6 寻址。

我们将向您公布适当的 Amazon 前缀，以便您可以连接您的 VPC 或其他 AWS 服务。您可以通过该区域访问所有 AWS 前缀，例如，Amazon EC2、Amazon S3 和 Amazon.com。您无权访问 Amazon 前缀。有关 AWS 公布的前缀的最新列表，请参阅Amazon Web Services 一般参考中的 AWS IP 地址范围。

> Note
>
> 我们建议您使用防火墙筛选条件 (根据数据包的源/目标地址) 来控制流量传入和传出某些前缀。如果您使用前缀筛选条件 (路由映射)，请确保它接受精确匹配或更长的前缀。从 AWS Direct Connect 公布的前缀可能会聚合，也可能与前缀筛选条件中定义的前缀不同。

要通过其他 AWS 账户使用您的 AWS Direct Connect 连接，可以为相应账户创建托管虚拟接口。其他账户的所有者在开始使用它之前必须接受托管虚拟接口。托管虚拟接口与标准虚拟端口的工作方式相同，可以连接至公有资源或 VPC。

一个 Sub-1G 连接仅支持一个虚拟接口。

内容

虚拟接口的先决条件

要创建虚拟接口，您需要以下信息：

- Connection：要为其创建虚拟接口的 AWS Direct Connect 连接或链路聚合组 (LAG)。
- Virtual interface name：虚拟接口名称。
- Virtual interface owner (虚拟接口所有者)：如果要为另一个账户创建虚拟接口，您需要其他账户的 AWS 账户 ID。
- (仅私有虚拟接口) Connection to：要连接到同一区域中的 VPC，您需要 VPC 的虚拟私有网关。BGP 会话的 Amazon 端的 ASN 是从虚拟私有网关继承的。当您创建虚拟私有网关时，您可以指定您自己的私有

ASN。否则，Amazon 会提供默认 ASN。有关更多信息，请参阅 Amazon VPC 用户指南 中的创建虚拟专用网关。要通过 Direct Connect 网关连接到 VPC，您需要 Direct Connect 网关。有关更多信息，请参阅 Direct Connect 网关。

- VLAN：未在您的连接上使用的唯一的虚拟局域网 (VLAN) 标记。该值必须介于 1 和 4094 之间且必须符合 Ethernet 802.1Q 标准。任何经过 AWS Direct Connect 连接的流量都必须有此标签。
- Address family (地址系列)：BGP 对等会话将基于 IPv4 还是 IPv6。
- Peer IP addresses (对等 IP 地址)：虚拟接口可以针对 IPv4、IPv6 或这二者 (双堆栈) 支持 BGP 对等会话。您无法在同一个虚拟接口上为同一 IP 地址系列创建多个 BGP 会话。IP 地址范围会分配到 BGP 对等会话的各个虚拟接口端。
  - IPv4:
    - (仅公有虚拟接口) 您必须指定您所拥有的唯一的公有 IPv4 地址 (/30)。
    - (仅私有虚拟接口) Amazon 可以为您生成私有 IPv4 地址。如果您自行指定，请确保仅为路由器接口和 AWS Direct Connect 接口指定私有 CIDR (例如，不要从本地网络中指定其他 IP 地址)。
  - IPv6：Amazon 会自动为您分配一个 /125 IPv6 CIDR。您不能指定自己的对等 IPv6 地址。
- BGP 信息：
  - 用于 BGP 会话的您这一侧的公有或私有边界网关协议 (BGP) 自治系统编号 (ASN)。如果使用公有 ASN，您必须具有其所有权。如果使用私有 ASN，它必须在 64512 至 65535 的范围内。如果您对公有虚拟接口使用私有 ASN，则自治系统 (AS) 预置将不起作用。
  - MD5 BGP 身份验证密钥。您可以提供自己的密钥，或者让 Amazon 为您生成一个。
- (针对仅公有虚拟接口) Prefixes you want to advertise (您要公布的前缀)：要通过 BGP 公布的公有 IPv4 路由或 IPv6 路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。
  - IPv4：IPv4 CIDR 不能与通过 AWS Direct Connect 公布的其他公有 IPv4 CIDR 重叠。如果您不拥有公有 IPv4 地址，您的网络提供商也许能够为您提供一个公有 IPv4 CIDR。否则，联系 AWS Support 以请求一个 /31 公有 IPv4 CIDR (并且在您的请求中提供一个使用案例)。
  - IPv6：指定 /64 或更短的前缀长度。

创建虚拟接口

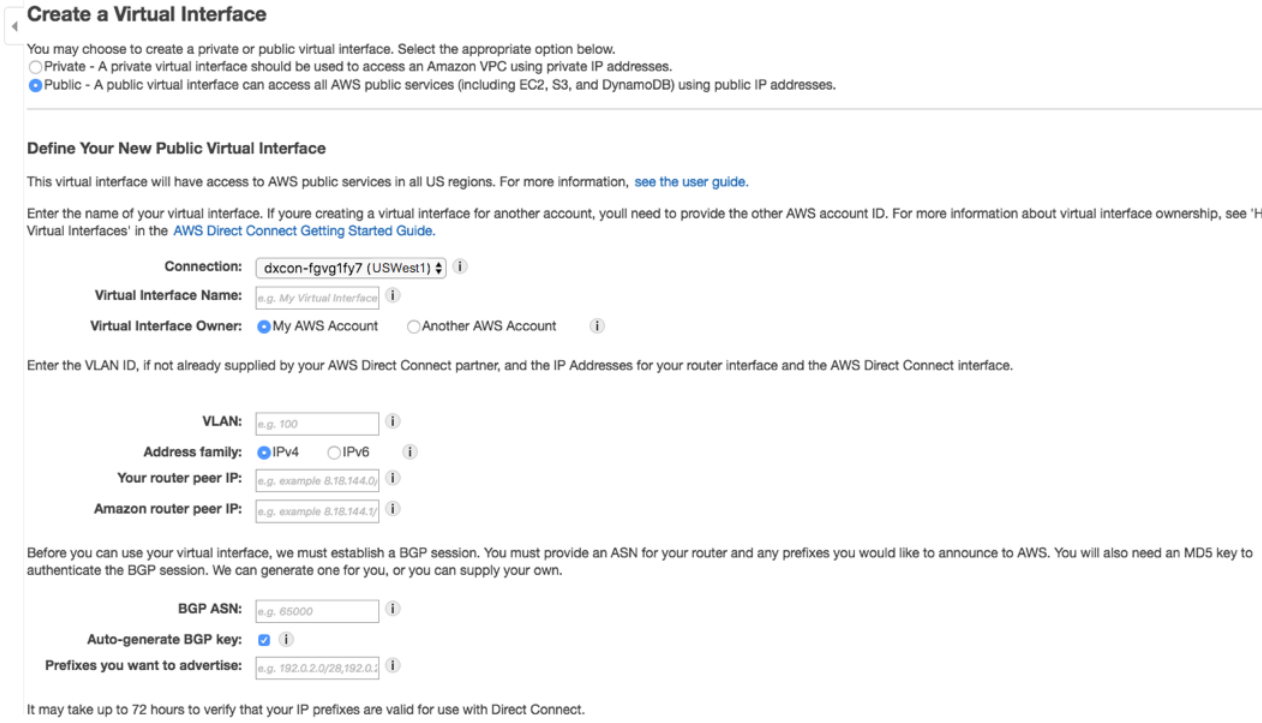
您可以创建一个公有虚拟接口从而连接至公有资源 (非 VPC 服务)，或创建一个私有虚拟接口从而连接至您的 VPC。

在您开始之前，请确保您阅读了 虚拟接口的先决条件 (p. 26)中的信息。

创建公有虚拟接口

预配置公有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections，再选择要使用的连接，然后依次选择 Actions 和 Create Virtual Interface。
3. 在 Create a Virtual Interface 窗格中，选择 Public。



4. 在 Define Your New Public Virtual Interface (定义新的公有虚拟接口) 对话框中，执行以下操作并选择 Continue (继续)：

   a. 对于 Connection，选择要用于创建虚拟接口的现有实体连接。

   b. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。

   c. 对于 Virtual Interface Owner，如果虚拟接口用于您的 AWS 账户，则选择 My AWS Account 选项。

   d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。

   e. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：

      - 对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。
      - 对于 Amazon router peer IP，输入用于将流量发送到 Amazon 的 IPv4 CIDR 地址。

   f. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。

   g. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

   h. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

      要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

   i. 对于 Prefixes you want to advertise，输入通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号隔开)。

5. 为您的设备下载路由器配置。有关更多信息，请参阅 下载路由器配置文件 (p. 30)。

使用命令行或 API 创建公有虚拟接口

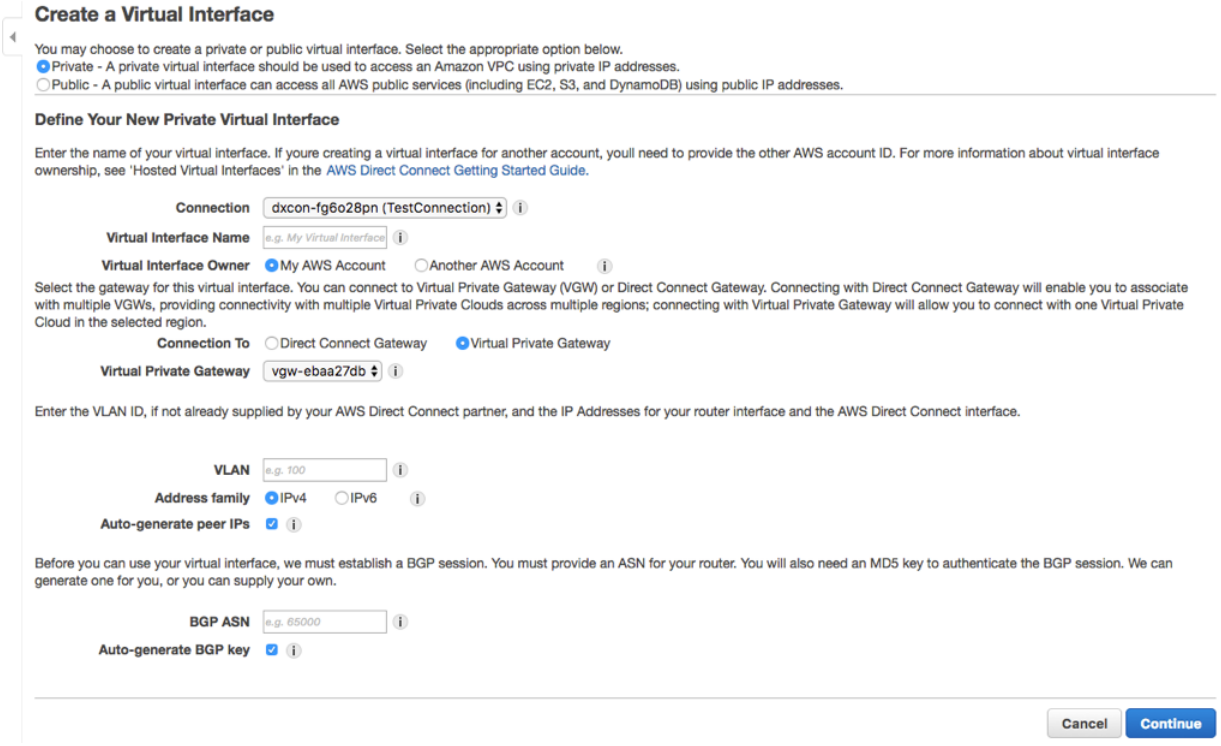
- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface (AWS Direct Connect API)

创建私有虚拟接口

您可以为您的 AWS Direct Connect 连接所在的区域中的虚拟专用网关配置一个私有虚拟接口。有关配置到 Direct Connect 网关的私有虚拟接口的更多信息，请参阅Direct Connect 网关 (p. 45)。

配置与 VPC 间的私有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections (连接)，选择要使用的连接，然后依次选择 Actions (操作) 和 Create Virtual Interface (创建虚拟接口)。
3. 在 Create a Virtual Interface (创建虚拟接口) 窗格中，选择 Private (私有)。



4. 在 Define Your New Private Virtual Interface (定义您的新私有虚拟接口) 下，执行以下操作并选择 Continue (继续)：

   a. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。
   b. 对于 Virtual Interface Owner，如果虚拟接口用于您的 AWS 账户，则选择 My AWS Account 选项。
   c. 对于 Connection To (连接到)，选择 Virtual Private Gateway (虚拟私有网关)，然后选择要连接到的虚拟私有网关。
   d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
   e. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：
      - 要让 AWS 生成您的路由器 IP 地址和 Amazon IP 地址，请选择 Auto-generate peer IPs (自动生成对等 IP)。
      - 要自行指定这些 IP 地址，请清除 Auto-generate peer IPs 复选框。对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。对于 Amazon router peer IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。
   f. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。
   g. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

h. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

Note

如果您使用 VPC 向导创建 VPC，系统将自动为您启用路线传播。通过路线传播，路线会自动添加到您 VPC 中的路线表。如果您愿意，您可以停用路线传播。有关更多信息，请参阅Amazon VPC 用户指南中的在路由表中启用路由传播。

创建了虚拟接口后，您可以为设备下载路由器配置。有关更多信息，请参阅 下载路由器配置文件 (p. 30)。

使用命令行或 API 创建私有虚拟接口

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

下载路由器配置文件

在创建虚拟接口后，您可以为您的路由器下载路由器配置文件。

下载路由器配置

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在 Virtual Interfaces (虚拟接口) 窗格中，选择虚拟接口，然后选择 Actions (操作)、Download Router Configuration (下载路由器配置)。
3. 在 Download Router Configuration (下载路由器配置) 对话框中，执行以下操作：
   a. 对于 Vendor，选择您的路由器的生产商。
   b. 对于 Platform，选择您的路由器型号。
   c. 对于 Software，选择您的路由器软件版本。
4. 选择 Download，然后使用适合您路由器的配置，以确保您可以连接到 AWS Direct Connect。

路由器配置文件示例

以下是路由器配置文件示例提取。

Cisco IOS

```
interface GigabitEthernet0/1
no ip address

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

router bgp CUSTOMER_BGP_ASN
neighbor AWS_PEER_IP remote-as AWS_ASN
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 AWS_ASN
    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 AWS_ASN
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

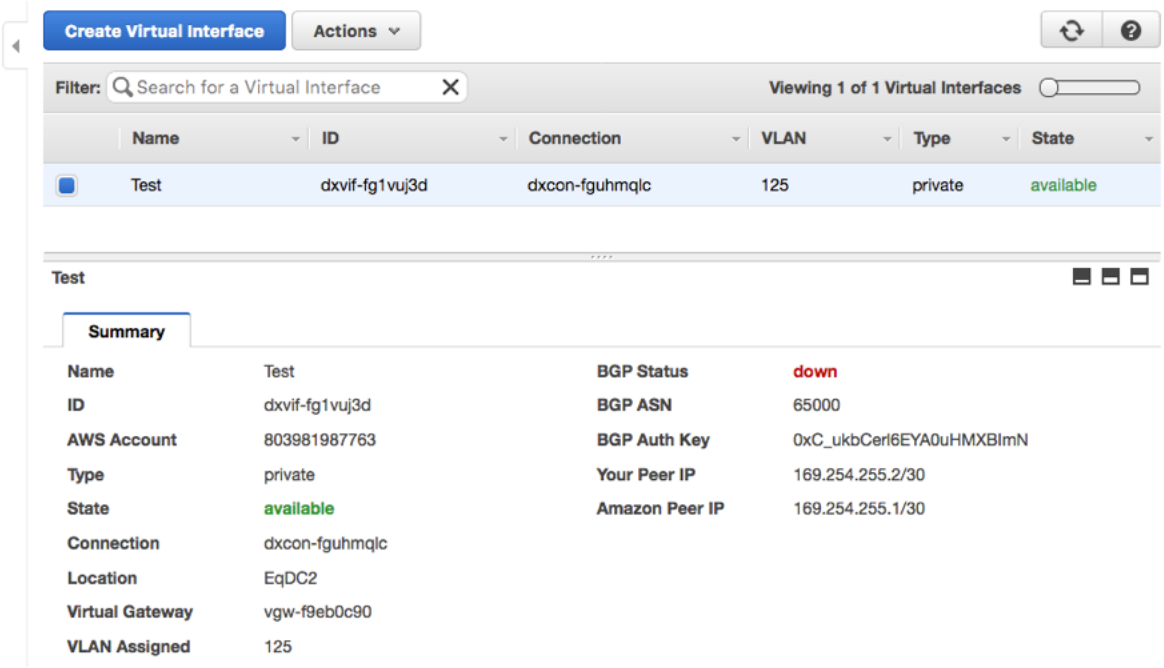
```
configure exclusive
edit interfaces ge-0/0/1
set description "Direct Connect to your Amazon VPC or AWS Cloud"
set flexible-vlan-tagging
set mtu 1522
edit unit 0
set vlan-id VLAN_NUMBER
set family inet mtu 1500
set family inet address YOUR_PEER_IP
top

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

set routing-options autonomous-system CUSTOMER_BGP_ASN

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

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
commit and-quit
```

查看虚拟接口详细信息

您可以查看虚拟接口的当前状态；连接状态、名称和节点；VLAN 和 BGP 的详细信息以及对等 IP 地址。

如何查看有关虚拟接口的详细信息

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Virtual Interfaces。
4. 在 Virtual Interfaces 窗格中，选择一个虚拟接口查看其详细信息。



使用命令行或 API 描述虚拟接口

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

删除虚拟接口

您必须先删除虚拟接口，然后才能删除连接。Connection 窗格中的 # VIs 列中列出了连接上配置的虚拟接口数量。删除虚拟接口会终止对与虚拟接口相关 AWS Direct Connect 数据传输收费。

如何删除虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Virtual Interfaces。
4. 在 Virtual Interfaces 窗格中，依次选择虚拟接口、Actions 和 Delete Virtual Interface。
5. 在 Delete Virtual Interface 对话框中，选择 Delete。

使用命令行或 API 删除虚拟接口

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

创建托管虚拟接口

您可以创建公有或私有托管虚拟接口。在您开始之前，请确保您阅读了 虚拟接口的先决条件 (p. 26)中的信息。

创建托管私有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在连接窗格中，选择要添加虚拟接口的连接，然后选择操作、创建虚拟接口。
5. 选择私有选项。
6. 在 Define Your New Private Virtual Interface (定义您的新私有虚拟接口) 下，执行以下操作：
   a. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。
   b. 对于 Virtual Interface Owner，选择 Another AWS Account。对于 Account ID，输入 AWS 账户 ID 号以作为此虚拟接口的所有者进行关联。
   c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
   d. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：
      - 要让 AWS 生成您的路由器 IP 地址和 Amazon IP 地址，请选择 Auto-generate peer IPs (自动生成对等 IP)。
      - 要自行指定这些 IP 地址，请清除 Auto-generate peer IPs 复选框。对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。对于 Amazon router peer IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。
   e. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。
   f. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。
   g. 如果您希望 AWS 为您生成 BGP 密钥，请选中 Auto-generate BGP key 复选框。

      要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。
7. 选择 Continue (继续)。新接口将添加至 Virtual Interfaces 窗格上的虚拟接口列表中。
8. 在其他 AWS 账户的所有者接受托管虚拟接口之后，您可下载路由器配置文件 (p. 30)。

创建托管公有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Connections。
4. 在连接窗格中，选择要添加虚拟接口的连接，然后选择操作、创建虚拟接口。
5. 选择公有选项。
6. 在 Define Your New Public Virtual Interface (定义新的公有虚拟接口) 对话框中，执行以下操作：
   a. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。

b. 对于 Virtual Interface Owner，选择 Another AWS Account。对于 Account ID，输入 AWS 账户 ID 号以作为此虚拟接口的所有者进行关联。

c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。

d. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：

- 对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。
- 对于 Amazon router peer IP，输入用于将流量发送到 Amazon 的 IPv4 CIDR 地址。

e. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。

f. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

g. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

h. 对于 Prefixes you want to advertise，输入通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号隔开)。

7. 选择 Continue (继续)。新接口将添加至 Virtual Interfaces 窗格上的虚拟接口列表中。
8. 在其他 AWS 账户的所有者接受托管虚拟接口之后，您可下载路由器配置文件 (p. 30)。

使用命令行或 API 创建托管私有虚拟接口

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

使用命令行或 API 创建托管公有虚拟接口

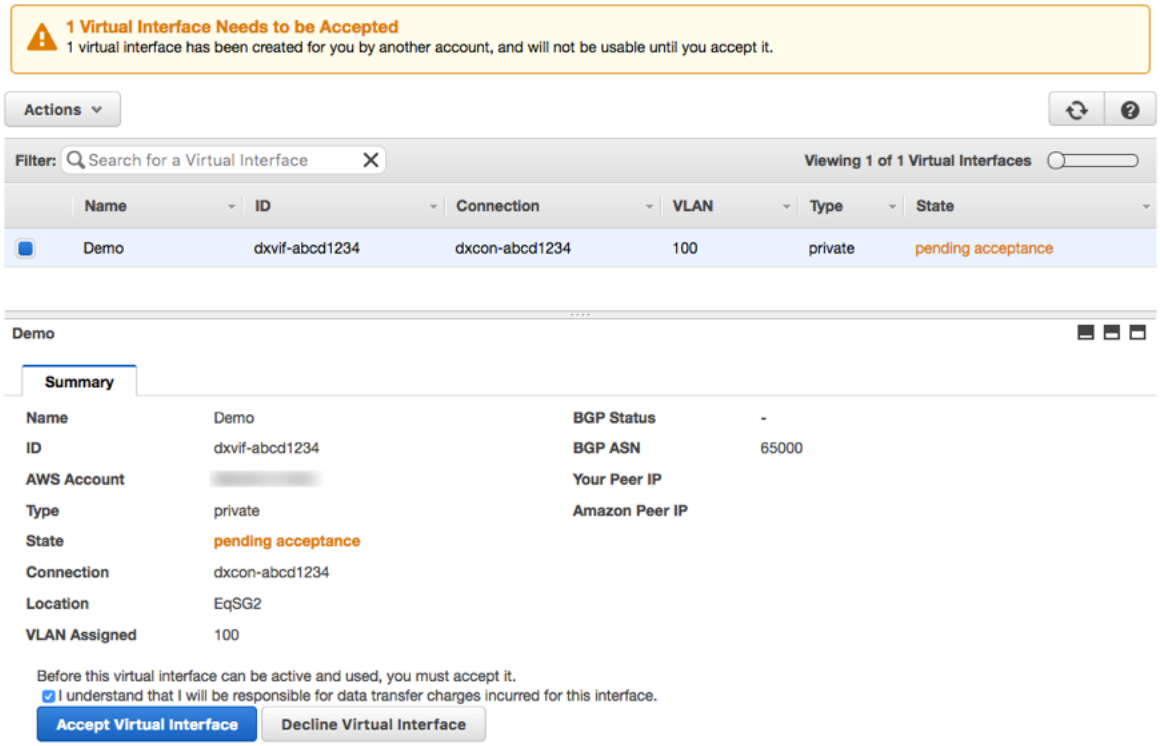
- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface (AWS Direct Connect API)

接受托管虚拟接口

在开始使用托管虚拟接口之前，必须先接受该虚拟接口。对于私有虚拟接口，您还必须已有一个虚拟专用网关或 Direct Connect 网关。

如何接受托管虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 如果需要，在导航栏中更改区域。有关更多信息，请参阅 AWS 区域和终端节点。
3. 在导航窗格中，选择 Virtual Interfaces。
4. 在 Virtual Interfaces 窗格中，选择虚拟接口查看其详细信息。



5. 选中 I understand that I will be responsible for data transfer charges incurred for this interface 复选框，然后选择 Accept Virtual Interface。
6. (私有虚拟接口) 在接受虚拟接口对话框中，选择虚拟专用网关或 Direct Connect 网关，然后选择接受。
7. 在您接受托管虚拟接口之后，AWS Direct Connect 连接的所有者可下载路由器配置文件。Download Router Configuration 选项对接受托管虚拟接口的账户不可用。

使用命令行或 API 接受托管私有虚拟接口

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

使用命令行或 API 接受托管公有虚拟接口

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

添加或删除 BGP 对等

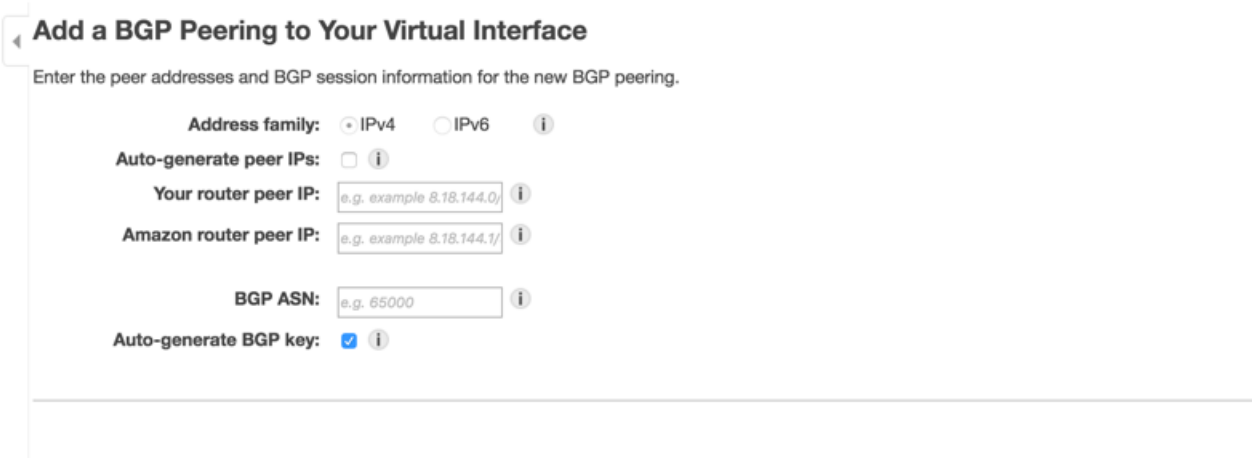
虚拟接口可以支持单个 IPv4 BGP 对等会话和单个 IPv6 BGP 对等会话。您可以将 IPv6 BGP 对等会话添加到具有现有的 IPv4 BGP 对等会话的虚拟接口。此外，您可以将 IPv4 BGP 对等会话添加到具有现有的 IPv6 BGP 对等会话的虚拟接口。

您无法为 IPv6 BGP 对等会话指定您自己的对等体 IPv6 地址。Amazon 会自动为您分配一个 /125 IPv6 CIDR。

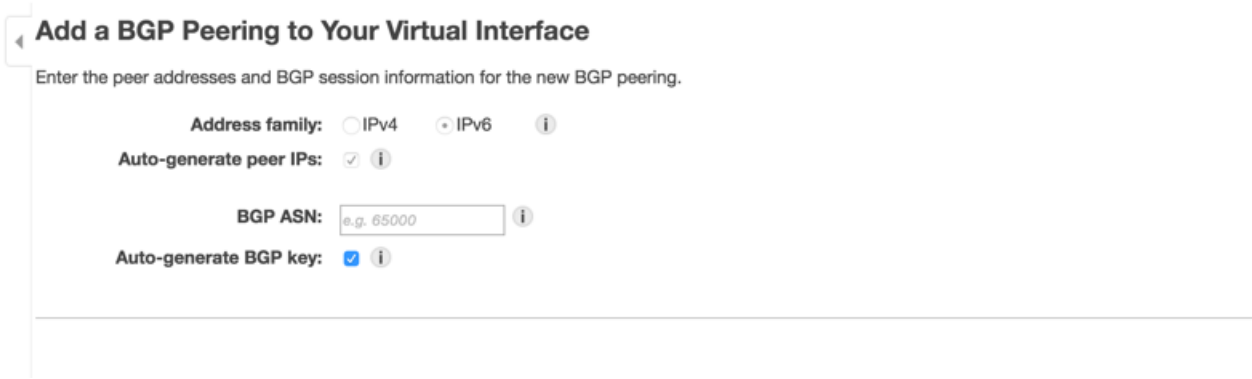
不支持多协议 BGP。IPv4 和 IPv6 在虚拟接口的双堆栈模式下运行。

添加 BGP 对等体

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Virtual Interfaces，然后选择所需的虚拟接口。
3. 依次选择 Actions (操作) 和 Add Peering (添加对等体)。
4. (私有虚拟接口) 要添加 IPv4 BGP 对等体，请执行以下操作：
   - 要让 AWS 生成您的路由器 IP 地址和 Amazon IP 地址，请选择 Auto-generate peer IPs (自动生成对等 IP)。
   - 要自行指定这些 IP 地址，请清除 Auto-generate peer IPs 复选框。对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。在 Amazon router peer IP 字段中，输入用来向 AWS 发送流量的 IPv4 CIDR 地址。



5. (公有虚拟接口) 要添加 IPv4 BGP 对等体，请执行以下操作：
   - 对于 Your router peer IP，输入发送流量的 IPv4 CIDR 目标地址。
   - 对于 Amazon router peer IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。
6. (私有或公有虚拟接口) 要添加 IPv6 BGP 对等体，Auto-generate peer IPs (自动生成对等 IP) 在选择默认情况下处于选定状态。对等 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配；您无法指定自定义 IPv6 地址。



7. 在 BGP ASN 字段中，输入网关的边界网关协议 (BGP) 自治系统编号 (ASN)，例如一个 1 到 65534 之间的数字。对于公有虚拟接口，ASN 必须为私有或已针对该虚拟接口加入了白名单。
8. 选中 Auto-generate BGP key 复选框可让 AWS 为您生成一个 BGP 密钥。

要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

9. 选择 Continue (继续)。

如果您的虚拟接口有 IPv4 和 IPv6 BGP 对等会话，您可以删除一个 BGP 对等会话 (但不能两者都删除)。

删除 BGP 对等体

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Virtual Interfaces，然后选择所需的虚拟接口。
3. 依次选择 Actions (操作) 和 Delete Peering (删除对等体)。
4. 要删除 IPv4 BGP 对等体，请选择 IPv4。要删除 IPv6 BGP 对等体，请选择 IPv6。
5. 选择 Delete。

使用命令行或 API 创建 BGP 对等

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

使用命令行或 API 删除 BGP 对等

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

将虚拟接口与连接或 LAG 关联

您可将虚拟接口与链接聚合组 (LAG) 或其他连接关联。

如果目标连接或 LAG 具有包含下列匹配属性的现有关联虚拟接口，则您无法关联虚拟接口：

- 冲突的 VLAN 编号
- (公有虚拟接口) Amazon 路由器或客户路由器的 IP 地址范围相同
- (专用虚拟接口) Amazon 路由器或客户路由器的虚拟专用网关和 IP 地址范围相同

您无法取消虚拟接口与连接或 LAG 的关联，但您可重新关联虚拟接口或删除它。有关更多信息，请参阅 删除虚拟接口 (p. 33)。

> **Important**
>
> 与 AWS 的连接在关联过程中临时中断。

将虚拟接口与连接关联

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Virtual Interfaces，然后选择虚拟接口。
3. 依次选择 Actions 和 Associate Connection or LAG。
4. 选择所需连接，选中确认复选框，然后选择 Continue。

您可使用与上面相同的过程将虚拟接口与 LAG 关联。此外，也可以使用 LAGs 屏幕。

将虚拟接口与 LAG 关联

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 LAGs，然后选择 LAG。
3. 依次选择 Actions 和 Associate Virtual Interface。
4. 选择所需虚拟接口，选中确认复选框，然后选择 Continue。

使用命令行或 API 关联虚拟接口

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

链接聚合组

链接聚合组 (LAG) 是一个逻辑接口，使用链接聚合控制协议 (LACP) 在一个 AWS Direct Connect 终端节点处聚合多个 1 GB 或 10 GB 连接，从而允许您将这些连接视为一个托管连接。

您可从现有连接创建 LAG，也可配置新连接。在创建 LAG 之后，您可将现有连接 (无论是独立连接还是其他 LAG 的一部分) 与 LAG 关联。

以下规则适用：

- LAG 中的所有连接都必须使用相同的带宽。支持下列带宽：1 Gbps 和 10 Gbps。
- LAG 中最多可有 4 个连接。LAG 中的每个连接都会计入区域的整体连接限制。
- LAG 中的所有连接都必须终止于同一 AWS Direct Connect 终端节点。

创建 LAG 时，您可以从 AWS Direct Connect 控制台分别为每个新的物理连接下载《授权证书和连接设备分配 (LOA-CFA)》。有关更多信息，请参阅 下载 LOA-CFA (p. 16)。

所有 LAG 都有一个属性，该属性确定要让 LAG 本身运行，LAG 中必须运行的连接的最小数量。默认情况下，新 LAG 的此属性设置为 0。您可更新 LAG 以指定不同的值 - 这样做意味着您的整个 LAG 将在运行连接数低于此阈值时变得无法运行。此属性可用于防止过度使用剩余连接。

LAG 中的所有连接以主动/主动模式运行。

> Note
>
> 当您创建 LAG 或将多个连接与 LAG 关联时，我们可能无法保证给定 AWS Direct Connect 终端节点上有足够的可用端口。

主题

正在创建 LAG

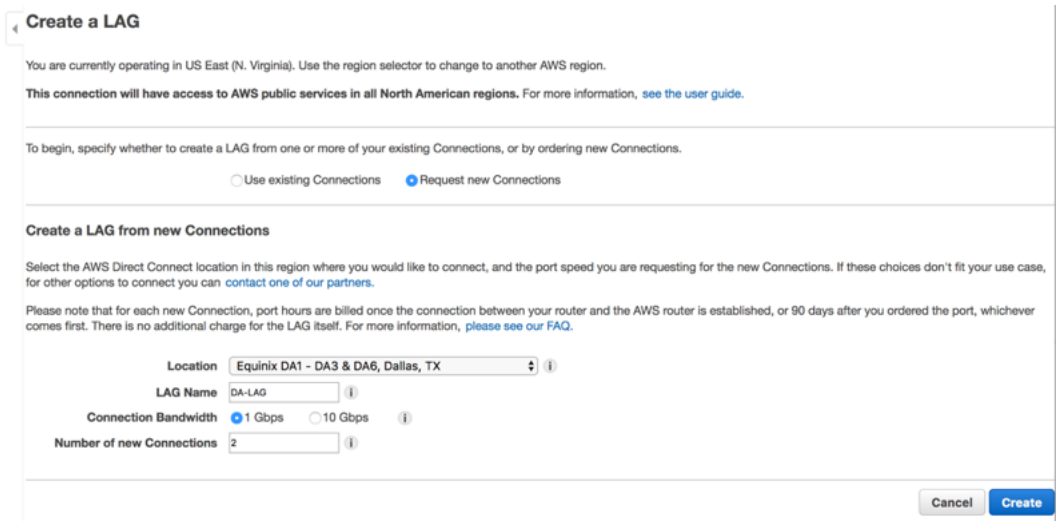
您可通过配置新连接或聚合现有连接来创建 LAG。

如果这导致您超出区域的整体连接限制，则您无法利用新连接创建 LAG。

利用新连接创建 LAG

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，依次选择 LAGs 和 Create LAG。
3. 选择 Request new Connections，然后提供以下信息。
   - Location：选择 LAG 的位置。
   - LAG Name：为 LAG 指定名称。
   - Connection Bandwidth：选择连接的端口速度。

- Number of new Connections：指定必须在 LAG 中配置的连接的数量。



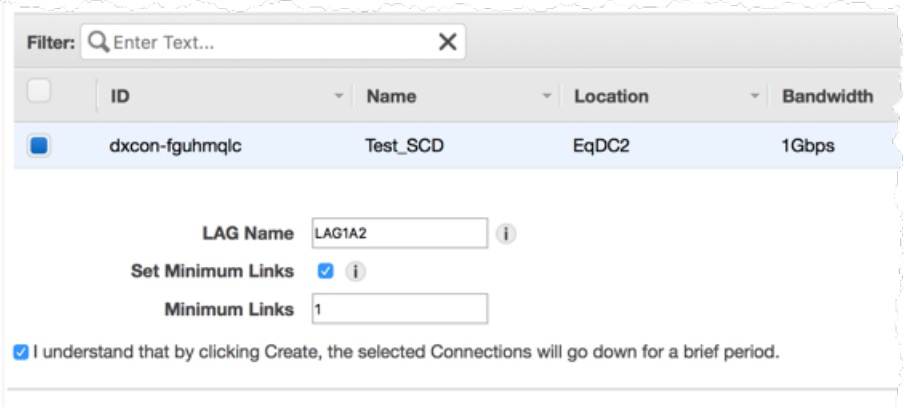
4. 选择 Create。

要通过现有连接创建 LAG，连接必须位于同一 AWS 设备上 (终止于同一 AWS Direct Connect 终端节点)，它们必须使用相同的带宽。如果删除连接导致原始 LAG 低于其设置的最小运行连接数，则您无法从现有 LAG 迁移连接。

> **Important**
>
> 对于现有连接，与 AWS 的连接将在创建 LAG 时中断。

通过现有连接创建 LAG

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，依次选择 LAGs 和 Create LAG。
3. 选择 Use existing Connections，然后选择所需连接。
4. 对于 LAG Name，为 LAG 指定名称。对于 Set Minimum Links，指定要让 LAG 本身运行，必须运行的连接的最小数量。如果您未指定值，我们将分配默认值 0。

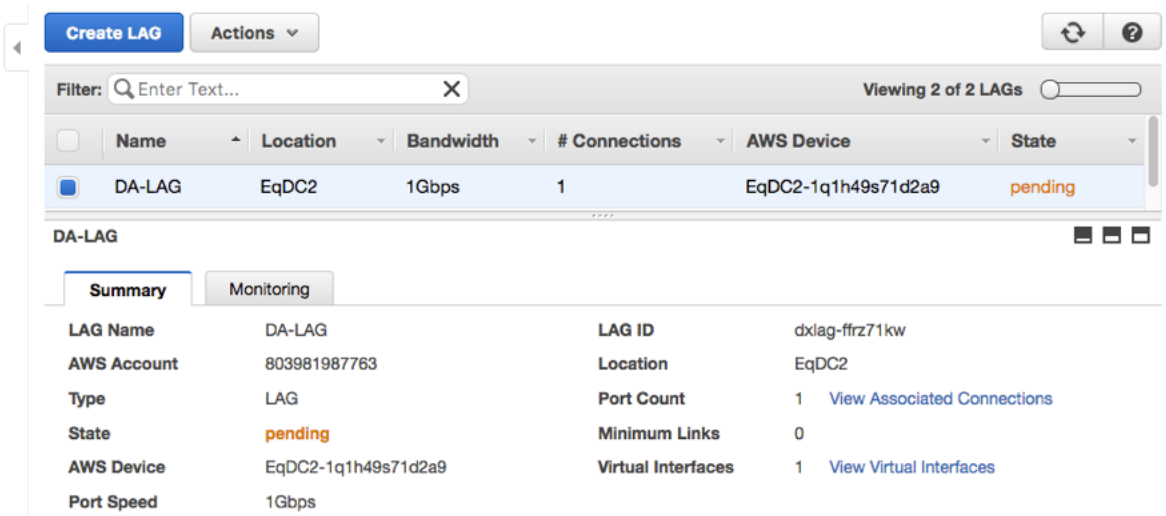


5. 选中确认复选框，然后选择 Create。

创建 LAG 后，您可以在 AWS Direct Connect 控制台中查看其详细信息。

查看有关您的 LAG 的信息

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 LAGs，然后选择 LAG。
3. 您可以查看 LAG 的相关信息，包括 ID、终止连接的 AWS Direct Connect 终端节点 (AWS 设备) 和 LAG 中的连接数量 (端口数量)。



创建 LAG 后，您可将连接关联到 LAG 或取消两者的关联。有关更多信息，请参阅 将连接与 LAG 关联 (p. 43) 和 取消连接与 LAG 的关联 (p. 43)。

使用命令行或 API 创建 LAG

- create-lag (AWS CLI)
- CreateLag (AWS Direct Connect API)

使用命令行或 API 描述 LAG

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

使用命令行或 API 下载 LOA-CFA

- describe-loa (AWS CLI)
- DescribeLoa (AWS Direct Connect API)

更新 LAG

您可更新 LAG 以更改其名称或更改最小运行连接数的值。

Note

如果您调整最小运行连接数的阈值，请确保新值不会导致 LAG 低于此阈值并且变得无法运行。

更新 LAG

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。

2. 在导航窗格中，选择 LAGs，然后选择 LAG。
3. 依次选择 Actions 和 Update LAG。
4. 使用 LAG Name 为 LAG 指定新名称。对于 Minimum Links，调整最小运行连接数的值。
5. 选择 Continue (继续)。

使用命令行或 API 更新 LAG

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

将连接与 LAG 关联

您可将现有连接与 LAG 关联。连接可以是独立的，也可以是其他 LAG 的一部分。连接必须在同一 AWS 设备上并且必须使用与 LAG 相同的带宽。如果连接已与另一 LAG 关联，并且删除连接将导致原始 LAG 低于其最小运行连接数的阈值，则您无法重新关联该连接。

将某个连接与 LAG 关联，会自动将其虚拟接口重新关联到 LAG。

> **Important**
>
> 通过该连接与 AWS 建立的连接将在关联过程中中断。

将连接与 LAG 关联

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 LAGs，然后选择 LAG。
3. 依次选择 Actions 和 Associate Connection。
4. 从可用连接的列表中选择连接。
5. 选中确认复选框，然后选择 Continue。

使用命令行或 API 关联连接

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

取消连接与 LAG 的关联

您可取消连接与 LAG 的关联以将其转换为独立连接。如果取消关联连接将导致 LAG 低于其最小运行连接数的阈值，则无法执行此操作。

取消某个连接与 LAG 的关联不会自动取消关联任何虚拟接口。您必须单独将虚拟接口与该连接关联。有关更多信息，请参阅 将虚拟接口与连接或 LAG 关联 (p. 38)。

> **Important**
>
> 通过该连接与 AWS 建立的连接将在取消关联过程中中断。

取消连接与 LAG 的关联

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 LAGs，然后选择 LAG。

3. 依次选择 Actions 和 Disassociate Connection。
4. 从可用连接的列表中选择连接。
5. 选中确认复选框，然后选择 Continue。

使用命令行或 API 取消关联连接

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

删除 LAG

如果您不再需要 LAG，则可以删除它。如果 LAG 具有相关联的虚拟接口，则您无法删除 LAG - 您必须先删除虚拟接口，或者将虚拟接口与其他 LAG 或连接关联。删除 LAG 不会删除 LAG 中的连接；您必须亲自删除这些连接。有关更多信息，请参阅 删除连接 (p. 17)。

删除 LAG

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 LAGs，然后选择 LAG。
3. 依次选择 Actions 和 Delete LAG。
4. 选中确认复选框，然后选择 Continue。

使用命令行或 API 删除 LAG

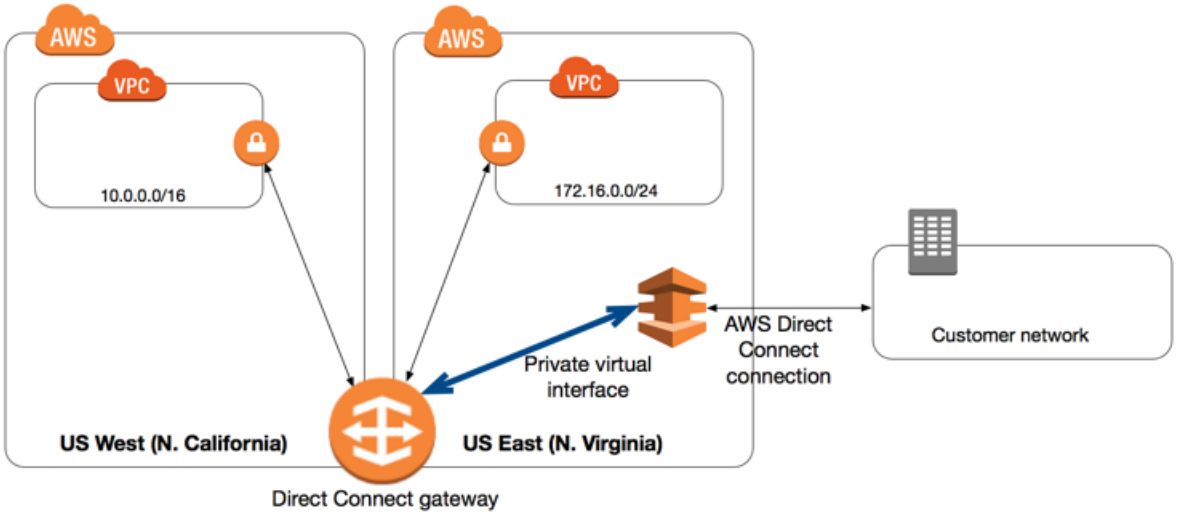
- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect API)

Direct Connect 网关

您可以使用 AWS Direct Connect 网关将您的 AWS Direct Connect 通过私有虚拟接口连接到您账户中位于相同或不同区域的一个或多个 VPC。您将 Direct Connect 网关与 VPC 的虚拟专用网关关联，然后创建一个私有虚拟接口，以将您的 AWS Direct Connect 连接到 Direct Connect 网关。您可以将多个私有虚拟接口附加到您的 Direct Connect 网关。

Direct Connect 网关是全球可用资源。您可以在任何公有区域中创建 Direct Connect 网关，并从所有其他公有区域访问它。

在下图中，Direct Connect 网关能让您使用 美国东部（弗吉尼亚北部） 区域中的 AWS Direct Connect 连接访问您账户中在 美国东部（弗吉尼亚北部） 和 美国西部（加利福尼亚北部） 区域的 VPC。



以下规则适用：

- 您无法使用 Direct Connect 网关连接到 中国 区域中的 VPC。
- 您无法使用位于您账户中的 Direct Connect 网关连接到位于其他 AWS 账户中的 VPC。要将 Direct Connect 网关与虚拟专用网关关联，前者必须与后者位于同一账户中。
- 创建和使用 Direct Connect 网关是有限制的。有关更多信息，请参阅 AWS Direct Connect 限制 (p. 2)。
- 您通过 Direct Connect 网关连接到的 VPC 不能具有重叠 CIDR 块。如果您将 IPv4 CIDR 块连接到一个与 Direct Connect 网关关联的 VPC，请确保该 CIDR 块不会与任何其他关联 VPC 的现有 CIDR 块重叠。有关更多信息，请参阅 Amazon VPC 用户指南 中的向 VPC 中添加 IPv4 CIDR 块。
- 您不能创建一个到 Direct Connect 网关的公有虚拟接口。
- Direct Connect 网关支持附加私有虚拟接口与关联虚拟专用网关之间的通信。以下流量不受支持：
  - 与 Direct Connect 网关关联的 VPC 之间的直接通信。
  - 附加到 Direct Connect 网关的虚拟接口之间的直接通信。
  - 附加到 Direct Connect 网关的虚拟接口和与同一 Direct Connect 网关关联的虚拟专用网关上的 VPN 连接之间的直接通信。
- 您不能将一个虚拟专用网关与多个 Direct Connect 网关关联，而且不能将一个私有虚拟接口附加到多个 Direct Connect 网关。
- 与 Direct Connect 网关关联的虚拟专用网关必须附加到 VPC。

- 您不能标记 Direct Connect 网关。

要将 AWS Direct Connect 连接到仅在同一区域中的 VPC，您可以创建 Direct Connect 网关，也可以创建私有虚拟接口并将其附加到 VPC 的虚拟专用网关。有关更多信息，请参阅创建私有虚拟接口 (p. 29)和 VPN CloudHub。

要通过其他账户中的 VPC 使用您的 AWS Direct Connect 连接，可以为相应账户创建一个托管私有虚拟接口。当其他账户的所有者接受该托管虚拟接口时，他们可以选择将其附加到其账户中的虚拟专用网关或 Direct Connect 网关。有关更多信息，请参阅 虚拟网关 (p. 26)。

内容

创建 Direct Connect 网关

您可以在任何受支持的公有区域中创建 Direct Connect 网关。

创建 Direct Connect 网关

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Direct Connect Gateways。
3. 选择 Create Direct Connect Gateway。
4. 指定以下信息，然后选择 Create。
   - Name：输入一个名称以帮助您标识 Direct Connect 网关。
   - Amazon side ASN：为 BGP 会话的 Amazon 端指定 ASN。该 ASN 必须位于 64,512 到 65,534 范围或 4,200,000,000 个到 4,294,967,294 范围。

使用命令行或 API 创建 Direct Connect 网关

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway (AWS Direct Connect API)

关联和取消关联虚拟专用网关

要将虚拟专用网关与 Direct Connect 网关关联，您必须位于虚拟专用网关所在的区域。虚拟专用网关必须附加到您要连接到的 VPC。有关更多信息，请参阅 Amazon VPC 用户指南 中的创建虚拟专用网关。

> **Note**
>
> 如果您计划对 Direct Connect 网关和动态 VPN 连接使用虚拟私有网关，请将虚拟私有网关上的 ASN 设置为 VPN 连接的所需值。否则，虚拟私有网关上的 ASN 可以设置为任何允许的值。Direct Connect 网关会通过分配给它的 ASN 公布给所有连接的 VPC。

关联虚拟专用网关

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。

2. 使用区域选择器选择您的虚拟专用网关所在的区域。
3. 在导航窗格中，选择 Direct Connect Gateways，然后选择所需的 Direct Connect 网关。
4. 依次选择 Actions、Associate Virtual Private Gateway。
5. 选择要关联的虚拟专用网关，然后选择 Associate。

您可以通过选择 Virtual Gateway Associations 查看与 Direct Connect 网关关联的所有区域中的所有虚拟专用网关。要取消虚拟专用网关与 Direct Connect 网关的关联，您必须位于虚拟专用网关所在的区域。

取消关联虚拟专用网关

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 使用区域选择器切换到您的虚拟专用网关所在的区域。
3. 在导航窗格中，选择 Direct Connect Gateways，然后选择所需的 Direct Connect 网关。
4. 依次选择 Actions、Disassociate Virtual Private Gateway。
5. 选择要取消关联的虚拟专用网关，然后选择 Disassociate。

使用命令行或 API 关联虚拟专用网关

- create-direct-connect-gateway-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

使用命令行或 API 查看与 Direct Connect 网关关联的虚拟专用网关

- describe-direct-connect-gateway-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (AWS Direct Connect API)

使用命令行或 API 取消关联虚拟专用网关

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (AWS Direct Connect API)

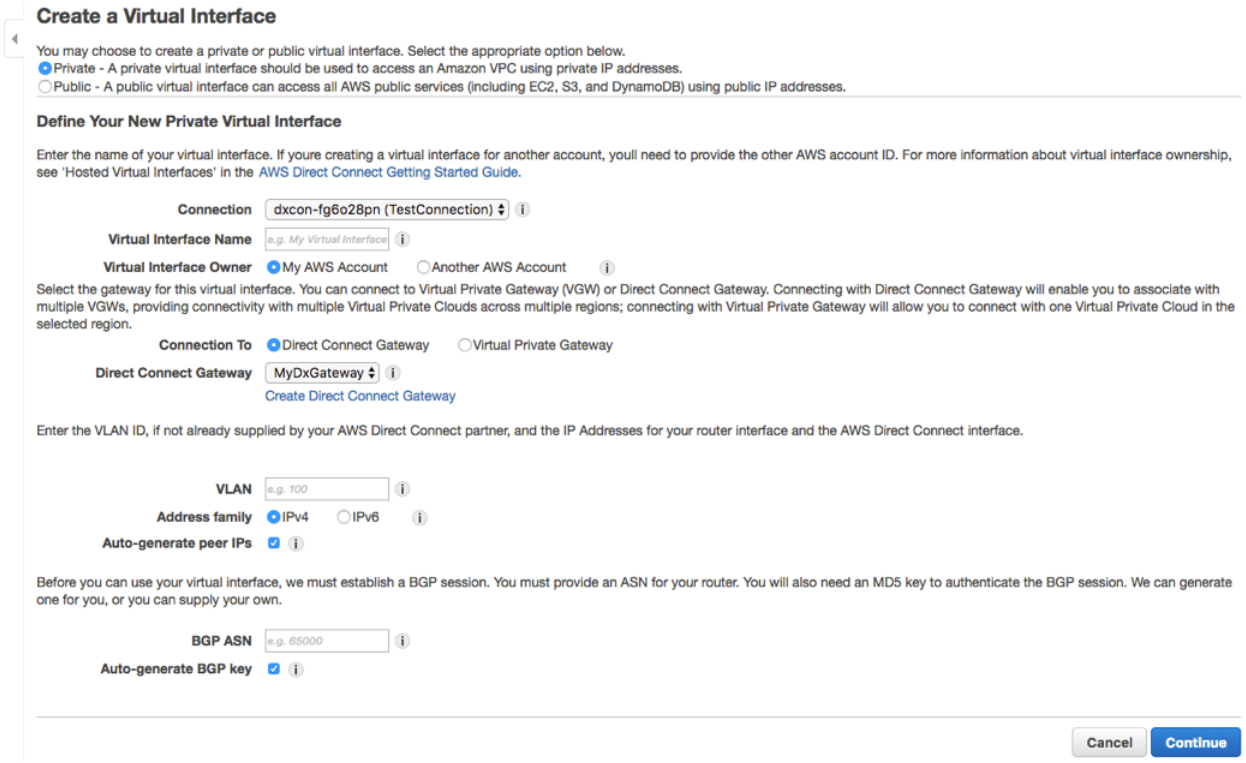
创建到 Direct Connect 网关的私有虚拟接口

要将 AWS Direct Connect 连接到远程 VPC，您必须为连接创建私有虚拟接口，并指定要连接到的 Direct Connect 网关。

> **Note**
>
> 如果您接受了某个托管私有虚拟接口，则可以将其与您账户中的 Direct Connect 网关关联。有关更多信息，请参阅 接受托管虚拟接口 (p. 35)。

为 Direct Connect 网关配置私有虚拟接口

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections (连接)，选择要使用的连接，然后依次选择 Actions (操作) 和 Create Virtual Interface (创建虚拟接口)。
3. 在 Create a Virtual Interface (创建虚拟接口) 窗格中，选择 Private (私有)。



4. 在 Define Your New Private Virtual Interface (定义您的新私有虚拟接口) 下，执行以下操作并选择 Continue (继续)：

   a. 对于 Virtual Interface Name (虚拟接口名称)，输入虚拟接口名称。
   b. 对于 Virtual Interface Owner，如果虚拟接口用于您的 AWS 账户，则选择 My AWS Account 选项。
   c. 对于 Connection To (连接到)，请选择 Direct Connect Gateway (Direct Connect 网关)，然后选择 Direct Connect 网关。
   d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
   e. 如果您要配置 IPv4 BGP 对等体，请选择 IPv4，然后执行以下操作：
      - 要让 AWS 生成您的路由器 IP 地址和 Amazon IP 地址，请选择 Auto-generate peer IPs (自动生成对等 IP)。
      - 要自行指定这些 IP 地址，请清除 Auto-generate peer IPs 复选框。对于 Your router peer IP，输入 Amazon 应将流量发送到的 IPv4 CIDR 目标地址。对于 Amazon router peer IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。
   f. 如果您要配置 IPv6 BGP 对等体，请选择 IPv6。对等体 IPv6 地址会从 Amazon 的 IPv6 地址池自动分配。您无法指定自定义 IPv6 地址。
   g. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。
   h. 要让 AWS 生成 BGP 密钥，选中 Auto-generate BGP key 复选框。

      要提供您自己的 BGP 密钥，清除 Auto-generate BGP key 复选框。对于 BGP Authentication Key，输入您的 BGP MD5 密钥。

创建了虚拟接口后，您可以为设备下载路由器配置。有关更多信息，请参阅 下载路由器配置文件 (p. 30)。

使用命令行或 API 创建私有虚拟接口

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

使用命令行或 API 查看附加到 Direct Connect 网关的虚拟接口

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

删除 Direct Connect 网关

如果您不再需要某一 Direct Connect 网关，可将其删除。您必须先取消关联 (p. 46)所有关联的虚拟专用网关并删除 (p. 33)附加的私有虚拟接口。

删除 Direct Connect 网关

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Direct Connect Gateways，然后选择所需的 Direct Connect 网关。
3. 依次选择 Actions、Delete Direct Connect Gateway。
4. 选择 Delete。

使用命令行或 API 删除 Direct Connect 网关

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway (AWS Direct Connect API)

使用 AWS Identity and Access Management 控制对 AWS Direct Connect 的访问

您可以使用 AWS Identity and Access Management 的功能来指定您的 AWS 账户下的用户可以执行哪些 AWS Direct Connect 操作。例如，您可以创建 IAM 策略，只向您组织中的特定用户授予相应的权限，允许他们使用 `DescribeConnections` 操作来检索有关您的 AWS Direct Connect 连接的数据。

使用 IAM 授予的权限涵盖您使用 AWS Direct Connect 涉及的所有 AWS 资源。您无法使用 IAM 来控制针对特定 AWS 资源的访问权限（也称为资源级权限）。例如，您无法授予用户仅针对特定虚拟接口的数据的访问权限。

AWS Direct Connect 操作

在 IAM 策略中，您可以指定 AWS Direct Connect 提供的某项或所有操作。操作名称必须包含小写字母前缀 `directconnect:`。例如：`directconnect:DescribeConnections`、`directconnect:CreateConnection` 或 `directconnect:*`（针对所有 AWS Direct Connect 操作）。有关操作的列表，请参阅 AWS Direct Connect API Reference。

AWS Direct Connect 资源

AWS Direct Connect 不支持资源级权限；因此，您无法控制对特定 AWS Direct Connect 资源的访问权限。当您编写策略来控制对 AWS Direct Connect 操作的访问权限时，必须使用星号 (*) 指定资源。

AWS Direct Connect 密钥

AWS Direct Connect 实施以下策略密钥：

- `aws:CurrentTime`（用于日期/时间条件）
- `aws:EpochTime`（用新纪元或 UINX 时间表示的日期，用于日期/时间条件）
- `aws:SecureTransport`（表示请求是否使用 SSL 发送的布尔值）
- `aws:SourceIp`（请求者的 IP 地址，用于 IP 地址条件）
- `aws:UserAgent`（有关请求者客户端应用程序的信息，用于字符串条件）

如果您使用 `aws:SourceIp`，且申请来自 Amazon EC2 实例，则实例的公有 IP 地址用于决定是否允许访问。

对于仅使用 SSL 的服务（如 Amazon Relational Database Service 和 Amazon Route 53），`aws:SecureTransport` 键无意义。

有关更多信息，请参阅 IAM 用户指南 中的 Condition。

AWS Direct Connect 示例策略

以下示例策略授予针对 AWS Direct Connect 的读取权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

以下示例策略授予针对 AWS Direct Connect 的完全访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

有关编写 IAM 策略的更多信息，请参阅 IAM 用户指南 中的 IAM 策略。

针对 AWS Direct Connect 使用标签

您可以选择为您的 AWS Direct Connect 资源分配标签，对其进行分类或管理。每个标签都包含您定义的一个键和一个可选值。

您可以为以下 AWS Direct Connect 资源添加标签。

资源	Amazon 资源名称 (ARN)
连接	arn:aws:directconnect:*region*:*account-id*:dxcon/*connection-id*
虚拟接口	arn:aws:directconnect:*region*:*account-id*:dxvif/*virtual-interface-id*
链接聚合组 (LAG)	arn:aws:directconnect:*region*:*account-id*:dxlag/*lag-id*

例如，在一个区域中有两个 AWS Direct Connect 连接，每个连接处于不同的位置。连接 `dxcon-11aa22bb` 是服务生产流量的连接，与虚拟接口 `dxvif-33cc44dd` 相关联。连接 `dxcon-abcabcab` 是冗余（备份）连接，与虚拟接口 `dxvif-12312312` 相关联。您可以选择用以下方式为连接和虚拟接口添加标签来进行区分：

资源 ID	标记密钥	标记值
`dxcon-11aa22bb`	目的	生产
	地点	阿姆斯特丹
`dxvif-33cc44dd`	目的	生产
`dxcon-abcabcab`	目的	备份
	地点	法兰克福
`dxvif-12312312`	目的	备份

标签限制

下面是适用于标签的规则和限制：

- 每个资源的最大标签数：50
- 最大密钥长度：128 个 Unicode 字符
- 最大值长度：265 个 Unicode 字符
- 标签密钥和值要区分大小写。
- `aws:` 前缀供 AWS 预留使用 — 您无法创建或删除带有此前缀的标签键或值。具有此前缀的标签不计入每个资源的标签数限制。
- 允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符：+ - = . _ : / @
- 不支持成本分配标签，因此，您应用到 AWS Direct Connect 资源的标签无法用于成本分配跟踪。

使用标签

目前可使用 AWS Direct Connect API、AWS CLI、适用于 Windows PowerShell 的 AWS 工具 或单独的 AWS SDK 处理标签。要应用或删除标签，您必须为资源指定亚马逊资源名称 (ARN)。有关更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon 资源名称 (ARN) 和 AWS 服务命名空间。

使用 AWS CLI 添加标签

使用 tag-resource 命令：

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

使用 AWS CLI 描述您的标签

使用 describe-tags 命令：

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

使用 AWS CLI 删除标签

使用 untag-resource 命令：

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

使用 AWS CLI

您可以使用 AWS CLI 创建和使用 AWS Direct Connect 资源。

以下示例使用 AWS CLI 命令创建 AWS Direct Connect 连接、下载《授权证书和连接设备分配 (LOA-CFA)》以及预配置私有或公有虚拟接口。

在开始之前，请确保您已经安装并配置 AWS CLI。有关更多信息，请参阅 AWS Command Line Interface 用户指南。

内容

第 1 步：创建连接

第一步是提交连接请求。确保您知道所需的端口速度和 AWS Direct Connect 位置。有关更多信息，请参阅连接 (p. 15)。

创建连接请求

1. 描述您当前区域中的 AWS Direct Connect 位置。在返回的输出中，记录您要建立连接的位置的位置代码。

```
aws directconnect describe-locations
```

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

2. 创建连接并指定名称、端口速度和位置代码。在返回的输出中，记录连接 ID。您需要该 ID 在下一步获取 LOA-CFA。

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

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

```
}
```

步骤 2：下载 LOA-CFA

在请求连接后，您就可以使用 `describe-loa` 命令获取 LOA-CFA。输出为 base64 编码。您必须提取相关的 LOA 内容、进行解码并创建 PDF 文件。

使用 Linux 或 Mac OS X 获取 LOA-CFA

在此示例中，命令的最后一部分使用 base64 实用工具解码内容并将输出发送到 PDF 文件。

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

使用 Windows 获取 LOA-CFA

在本示例中，输出将提取到名为 myLoaCfa.base64 的文件。第二个命令使用 `certutil` 实用工具解码文件并将输出发送到 PDF 文件。

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

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

下载 LOA-CFA 之后，将其发送到网络提供商或主机托管提供商。

步骤 3：创建虚拟接口，获取路由器配置

订购 AWS Direct Connect 连接以后，您必须创建虚拟接口以开始使用。您可以创建私有虚拟接口以连接到 VPC，或者创建公有虚拟接口以连接到不在 VPC 中的 AWS 服务。您可以创建支持 IPv4 或 IPv6 流量的接口。

在开始之前，请您务必阅读 虚拟接口的先决条件 (p. 26) 中的先决条件。

使用 AWS CLI 创建虚拟接口时，输出包括通用路由器配置信息。如果您希望路由器配置特定于您的设备，请使用 AWS Direct Connect 控制台。有关更多信息，请参阅 下载路由器配置文件 (p. 30)。

创建私有虚拟接口

1. 获取附加到您 VPC 的虚拟专用网关的 ID (vgw-xxxxxxxx)。您需要该 ID 在下一步创建虚拟接口。

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

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

```
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. 创建私有虚拟接口。您必须指定名称、VLAN ID 和 BGP 自治系统编号 (ASN)。

   对于 IPv4 流量，您需要为 BGP 对等会话的每一端都指定私有 IPv4 地址。您可以指定自己的 IPv4 地址，也可以让 Amazon 为您生成地址。在以下示例中，将为您生成 IPv4 地址。

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

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-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\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>\n
 <connection_type>private</connection_type>\n</logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

   要创建支持 IPv6 流量的私有虚拟接口，请使用上述命令并为 `addressFamily` 参数指定 `ipv6`。您不能为 BGP 对等会话指定自己的 IPv6 地址；Amazon 向您分配 IPv6 地址。

3. 要查看 XML 格式的路由器配置信息，请描述您创建的虚拟接口。使用 `--query` 参数可提取 `customerRouterConfig` 信息，使用 `--output` 参数可将文本排列到以制表符分隔的行中。

```
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>
```

创建公有虚拟接口

1. 要创建公有虚拟接口，您必须指定名称、VLAN ID 和 BGP 自治系统编号 (ASN)。

   对于 IPv4 流量，您还必须为 BGP 对等会话的每一端都指定公有 IPv4 地址，以及您通过 BGP 公布的公有 IPv4 路由。以下示例为 IPv4 流量创建公有虚拟接口。

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

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

```
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

要创建支持 IPv6 流量的公有虚拟接口，您可以指定将通过 BGP 公布的 IPv6 路由。您不能为对等会话指定 IPv6 地址；Amazon 向您分配 IPv6 地址。以下示例为 IPv6 流量创建公有虚拟接口。

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

2. 要查看 XML 格式的路由器配置信息，请描述您创建的虚拟接口。使用 `--query` 参数可提取 `customerRouterConfig` 信息，使用 `--output` 参数可将文本排列到以制表符分隔的行中。

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

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

在 AWS CloudTrail 中记录 AWS Direct Connect API 调用

AWS Direct Connect 与 AWS CloudTrail 集成在一起，后者是一个可捕获由 AWS 账户或代表 AWS 账户进行的 API 调用的服务。此信息在收集后写入存储在您指定的 Amazon Simple Storage Service (S3) 存储桶中的日志文件。当您使用 AWS Direct Connect API、AWS Direct Connect 控制台、后端控制台或 AWS CLI 时，将会记录 API 调用。使用由 CloudTrail 收集的信息，您可以确定向 AWS Direct Connect 发出了什么请求、发出请求的源 IP 地址、谁发出的请求以及发出请求的时间等。

要了解有关 CloudTrail 的更多信息（包括如何配置和启用它），请参阅 AWS CloudTrail 用户指南。

主题

CloudTrail 中的 AWS Direct Connect 信息

如果启用了 CloudTrail 日志记录，则会将对所有 AWS Direct Connect 操作的调用捕获在日志文件中。AWS Direct Connect API Reference 中记载了所有 AWS Direct Connect 操作。例如，对 CreateConnection、CreatePrivateVirtualInterface 和 DescribeConnections 操作的调用会在 CloudTrail 日志文件中生成相应条目。

每个日志条目都包含有关生成请求的人员的信息。例如，如果发出了创建与 AWS Direct Connect 间的新连接的请求 (CreateConnection)，那么 CloudTrail 将记录发出该请求的人或服务的用户身份。用户身份信息有助于您确定该请求是使用根证书、AWS Identity and Access Management (IAM) 用户证书、适用于某个角色或联合身份用户的临时安全证书发出的，还是由 AWS 中的另一个服务发出的。有关 CloudTrail 字段的更多信息，请参阅 AWS CloudTrail 用户指南中的 CloudTrail 事件参考。

日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。

了解 AWS Direct Connect 日志文件条目

CloudTrail 日志文件可包含一个或多个日志条目，每个条目由多个 JSON 格式的事件组成。一个日志条目表示来自任何源的一个请求，并包括所请求的操作、所有输入参数以及操作的日期和时间等信息。日志条目不按任何特定顺序显示。也就是说，它们不表示公用 API 调用的有序堆栈跟踪。

以下日志文件记录显示一个用户调用了 CreateConnection 操作。

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

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

以下日志文件记录显示一个用户调用了 CreatePrivateVirtualInterface 操作。

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
```

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

以下日志文件记录显示一个用户调用了 DescribeConnections 操作。

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

以下日志文件记录显示一个用户调用了 DescribeVirtualInterfaces 操作。

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

监控 AWS Direct Connect

监控是维护 AWS Direct Connect 资源可靠性、可用性和性能的重要环节。您应从 AWS 解决方案的所有部分收集监控数据，以便更轻松地调试出现的多点故障。不过，在开始监控 AWS Direct Connect 之前，您应制定监控计划并在计划中回答下列问题：

- 您的监控目标是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

下一步是通过测量不同时间和不同负载条件下的性能，在您的环境中建立正常 AWS Direct Connect 性能的基准。在监控 AWS Direct Connect 时，存储历史监控数据，以便将此数据与当前性能数据进行比较，确定正常性能模式和性能异常，并设计解决问题的方法。

要建立基准，您应监控 AWS Direct Connect 物理连接的使用情况、状态和运行状况。

主题

监控工具

AWS 为您提供了各种可以用来监控 AWS Direct Connect 连接的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动化监控工具来监控 AWS Direct Connect 并在出现错误时报告：

- Amazon CloudWatch 警报 – 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。操作是向 Amazon SNS 主题发送的通知。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态；该状态必须改变并在指定数量的时间段内一直保持。有关更多信息，请参阅 使用 Amazon CloudWatch 进行监控 (p. 64)。
- AWS CloudTrail 日志监控 – 在账户间共享日志文件，通过将 CloudTrail 日志文件发送到 CloudWatch Logs 对它们进行实时监控，在 Java 中编写日志处理应用程序，以及验证您的日志文件在被 CloudTrail 交付后未发生更改。有关更多信息，请参阅 AWS CloudTrail User Guide 中的在 AWS CloudTrail 中记录 AWS Direct Connect API 调用 (p. 59)和使用 CloudTrail 日志文件。

手动监控工具

监控 AWS Direct Connect 连接时的另一个重要环节是手动监控 CloudWatch 警报未涵盖的那些项。AWS Direct Connect 和 CloudWatch 控制台控制面板提供您的 AWS 环境状态的概览视图。

- 该 AWS Direct Connect 控制台显示：
  - 连接状态 (请参阅 State 列)

  - 虚拟接口状态 (请参阅 State 列)
- CloudWatch 主页将显示以下内容：
  - 当前警报和状态
  - 警报和资源的图表
  - 服务运行状况

  此外，您还可以使用 CloudWatch 执行以下操作：
  - 创建自定义控制面板以监控您关心的服务
  - 绘制指标数据图，以排除问题并弄清楚趋势
  - 搜索并浏览您所有的 AWS 资源指标
  - 创建和编辑警报以接收有关问题的通知

使用 Amazon CloudWatch 进行监控

您可以使用 CloudWatch 监控 AWS Direct Connect 物理连接，该工具可从 AWS Direct Connect 中收集原始数据并将其处理为可读的、近乎实时的指标。默认情况下，CloudWatch 以 5 分钟为间隔提供 AWS Direct Connect 指标数据。您也可以选择以 1 分钟为间隔查看数据。

有关 Amazon CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南。

> **Note**
>
> 如果您的连接是来自 AWS Direct Connect 合作伙伴的托管连接，您无法查看该托管连接的 CloudWatch 指标。

主题

AWS Direct Connect 维度和指标

AWS Direct Connect 会以 30 秒为间隔向 Amazon CloudWatch 发送有关您的 AWS Direct Connect 连接的以下指标。然后 Amazon CloudWatch 会以 1 分钟或 5 分钟的时间间隔聚合这些数据点。您可以按照以下步骤查看 AWS Direct Connect 连接的指标。

使用 CloudWatch 控制台查看指标

指标的分组首先依据服务命名空间，然后依据每个命名空间内的各种维度组合。

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Metrics。
3. 在 All metrics 下，选择 DX 指标命名空间。
4. 选择 Connection Metrics，然后选择指标维度，以查看指标 (例如，AWS Direct Connect 连接)。
5. (可选) 要以 1 分钟为间隔返回所选指标的数据，请选择 Graphed metrics，然后从 Period 列表中选择 1 Minute。

使用 AWS Direct Connect 控制台查看指标

1. 通过以下网址打开 AWS Direct Connect 控制台：https://console.aws.amazon.com/directconnect/。
2. 在导航窗格中，选择 Connections，然后选择您的连接。

3. Monitoring 选项卡会显示您的连接的指标。

使用 AWS CLI 查看指标

- 在命令提示符处，输入以下命令：

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

AWS Direct Connect 中包含以下指标。这些指标目前只可用于 AWS Direct Connect 物理连接。

指标	描述
ConnectionState	连接的状态。0 表示 DOWN，1 表示 UP。 单位：布尔值
ConnectionBpsEgress	AWS 连接侧出站数据的比特率。 报告的数量是指定时间段 (默认为 5 分钟，最短 1 分钟) 内的总计。 单位：每秒比特数
ConnectionBpsIngress	AWS 连接侧入站数据的比特率。 报告的数量是指定时间段 (默认为 5 分钟，最短 1 分钟) 内的总计。 单位：每秒比特数
ConnectionPpsEgress	AWS 连接侧出站数据的数据包速率。 报告的数量是指定时间段 (默认为 5 分钟，最短 1 分钟) 内的总计。 单位：每秒数据包数
ConnectionPpsIngress	AWS 连接侧入站数据的数据包速率。 报告的数量是指定时间段 (默认为 5 分钟，最短 1 分钟) 内的总计。 单位：每秒数据包数
ConnectionCRCErrorCount	对于在连接处接收到的数据，观察到的循环冗余校验 (CRC) 错误数。 单位：整数
ConnectionLightLevelTx	指示 AWS 连接侧出口 (出站) 流量的光纤连接的运行状况。 该指标只适用于 10 Gbps 端口速率的连接。 单位：dBm
ConnectionLightLevelRx	指示 AWS 连接侧入口 (入站) 流量的光纤连接的运行状况。

指标	描述
	该指标只适用于 10 Gbps 端口速率的连接。 单位：dBm

可使用以下维度来筛选 AWS Direct Connect 数据。

维度	描述
`ConnectionId`	该维度按 AWS Direct Connect 连接筛选数据。

创建 CloudWatch 警报以监控 AWS Direct Connect 连接

您可以创建 CloudWatch 警报，以在警报改变状态时发送 Amazon SNS 消息。在您指定的时间段内，警报会监控单一指标，然后根据若干这样的时间段内相对于给定阈值的指标值，向 Amazon SNS 主题发送通知。

例如，您可以创建警报来监控 AWS Direct Connect 连接的状态，并在连接状态于连续 5 个 1 分钟时间段内为 DOWN 时发送通知。

创建 连接状态的警报

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择 Alarms 和 Create Alarm。
3. 选择 DX Metrics (DX 指标) 类别。
4. 选择 AWS Direct Connect 连接，然后选择 ConnectionState 指标。选择 Next。
5. 按如下所示配置警报，然后在完成后选择 Create Alarm：
   - 在 Alarm Threshold 下，输入警报的名称和说明。对于 Whenever，选择 < 并输入 `1`。输入 5 作为连续周期数。
   - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
   - 在 Alarm Preview 下，选择以 1 分钟为时间段。

有关创建警报的更多示例，请参阅 Amazon CloudWatch 用户指南 中的创建 Amazon CloudWatch 警报。

对 AWS Direct Connect 进行问题排查

以下主题可帮助您排查与您的 AWS Direct Connect 连接相关的问题。

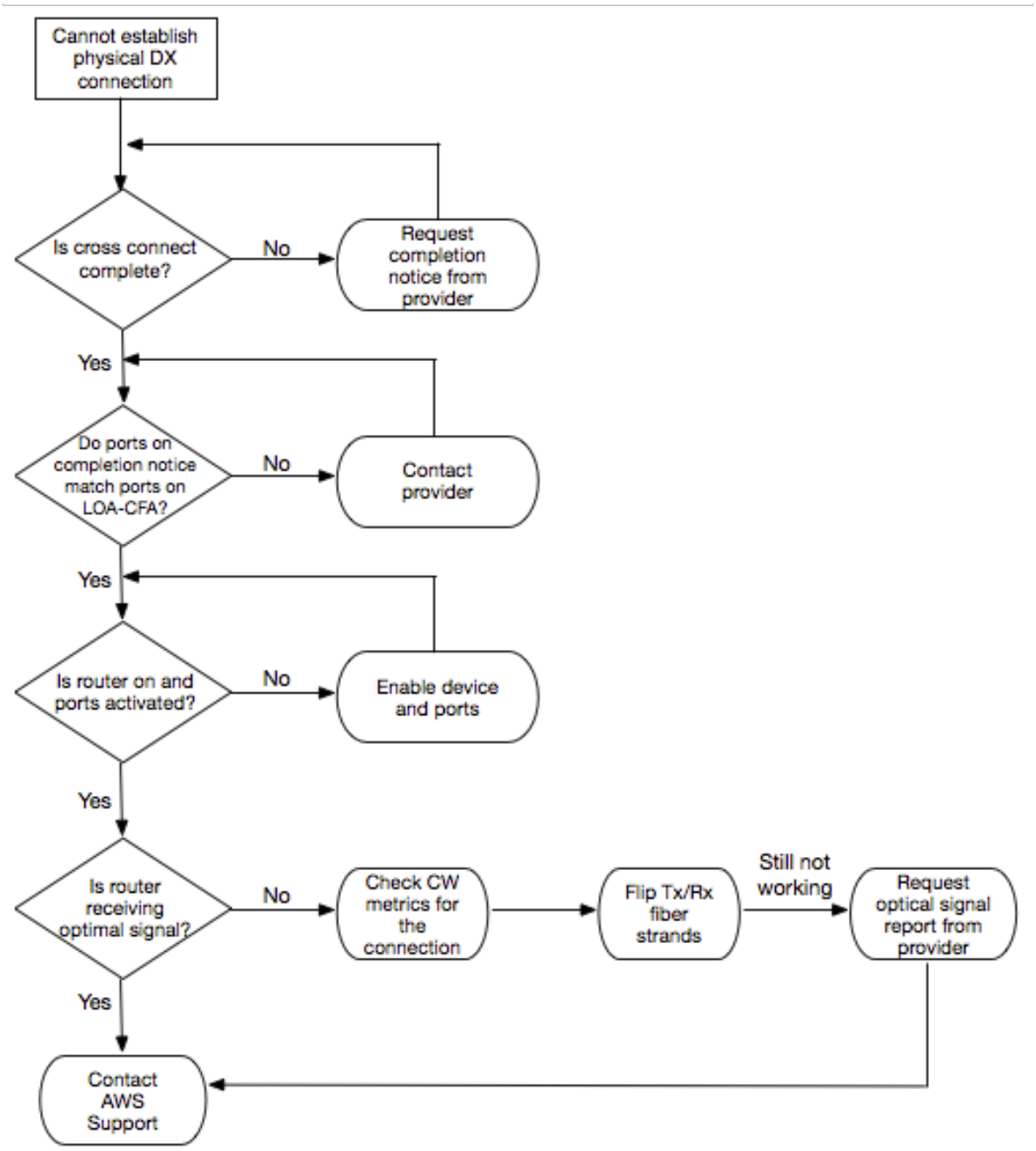
主题

排查第 1 层 (物理) 问题

如果您或您的网络提供商在建立与 AWS Direct Connect 设备的物理连接时遇到困难，请使用以下步骤排查该问题。

1. 与主机托管提供商一起验证交叉连接是否已完成。要求主机托管提供商或您的网络提供商为您提供交叉连接完成通知并将端口与在 LOA-CFA 上列出的端口进行比较。
2. 验证您的路由器或您的提供商的路由器是否已打开，端口是否已激活。
3. 确保这些路由器使用的是正确的光学收发器，已禁用自动协商功能并且已手动配置端口速度和全双工模式。有关更多信息，请参阅网络要求。
4. 验证路由器是否正在通过交叉连接接收可接受的光信号。
5. 尝试翻转 (也称为“滚动”) Tx/Rx 光纤束。
6. 检查 AWS Direct Connect 的 Amazon CloudWatch 指标。您可以验证 AWS Direct Connect 设备的 Tx/Rx 光学读数 (仅 10-Gbps 端口速度)、物理错误计数和运行状态。有关更多信息，请参阅使用 Amazon CloudWatch 进行监控。
7. 联系主机托管提供商并请求跨交叉连接的 Tx/Rx 光信号的书面报告。
8. 如果上述步骤未解决物理连接问题，请联系 AWS Support 并提供来自主机托管提供商的交叉连接完成通知和光信号报告。

以下流程图包含诊断物理连接问题的步骤。



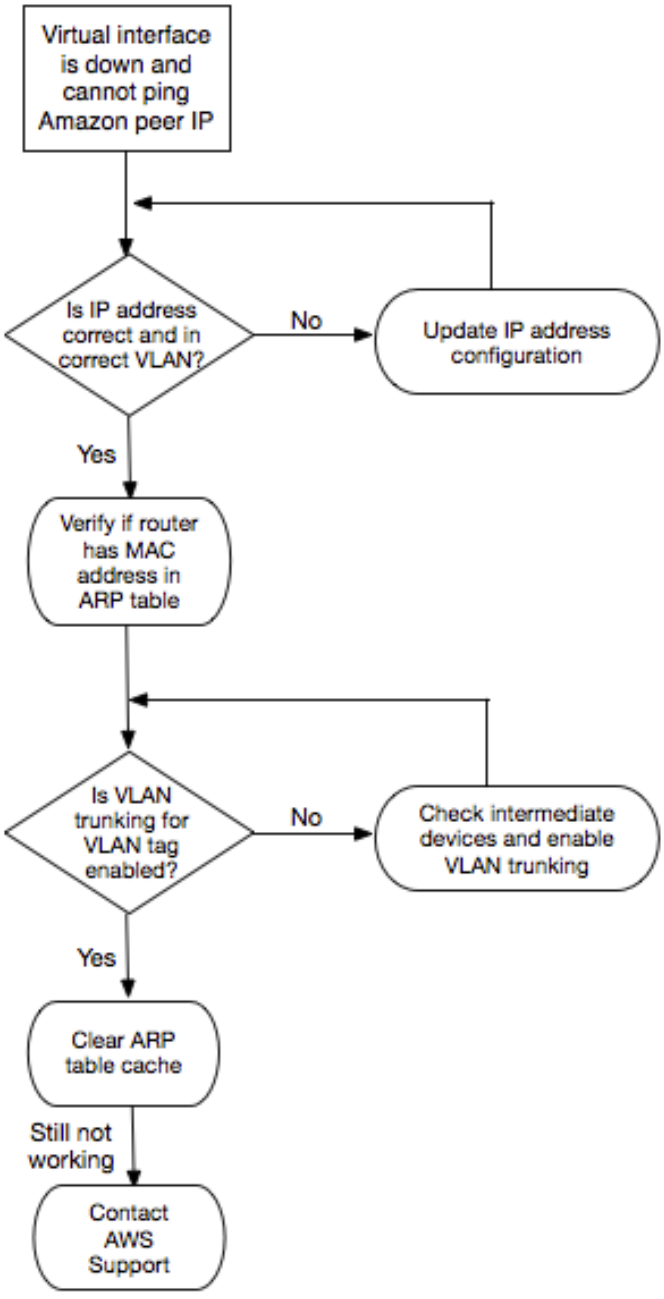
排查第 2 层 (数据链路) 问题

如果您的 AWS Direct Connect 物理连接已开启但虚拟接口已关闭，请使用以下步骤排查该问题。

1. 如果无法对 Amazon 对等 IP 地址执行 ping 操作，请验证您的对等 IP 地址是否已正确配置且位于正确的 VLAN 中。确保在 VLAN 子接口而不是物理接口 (例如，GigabitEthernet0/0.123 而不是 GigabitEthernet0/0) 中配置了该 IP 地址。
2. 验证路由器是否具有来自您的地址解析协议 (ARP) 表中 AWS 终端节点的 MAC 地址条目。

3. 确保终端节点之间的任何中间设备都已针对您的 802.1Q VLAN 标签启用 VLAN 中继。在 AWS 端无法建立 ARP，直到 AWS 接收标记的流量。
4. 清除您或您的提供商的 ARP 表缓存。
5. 如果上述步骤未建立 ARP 或您仍无法对 Amazon 对等 IP 执行 ping 操作，请联系 AWS Support。

以下流程图包含诊断数据链路问题的步骤。



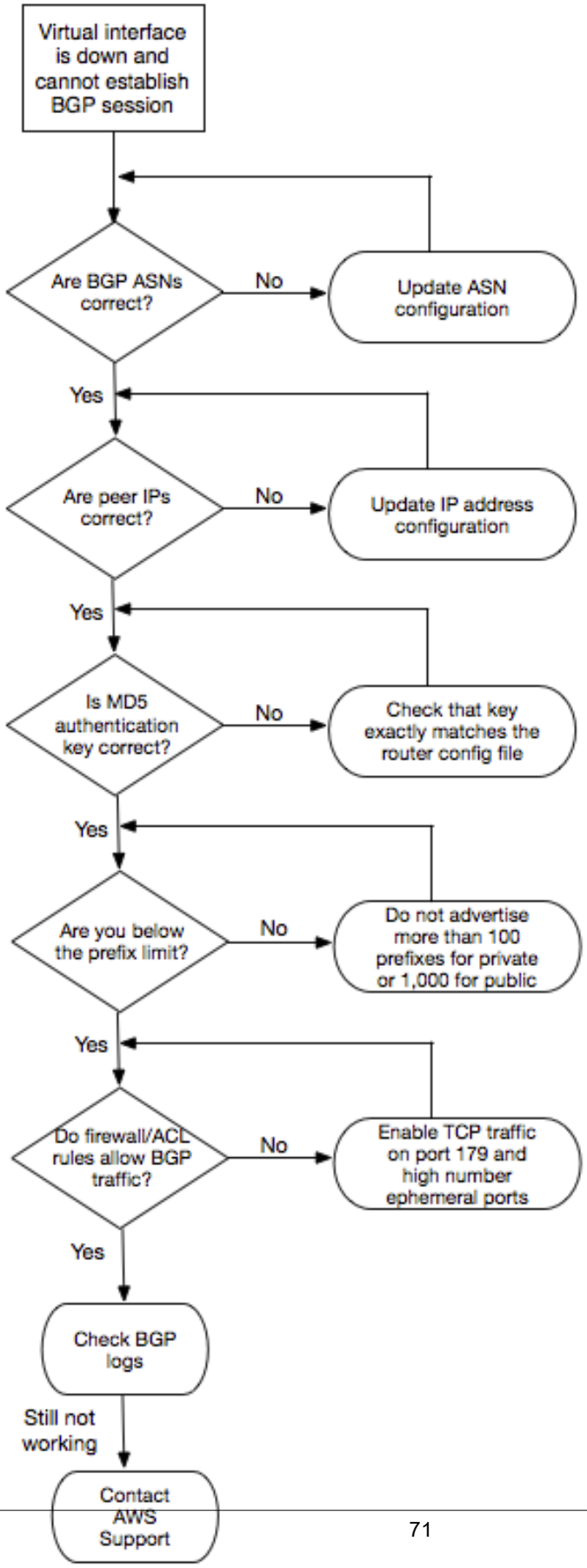
如果在验证这些步骤后仍无法建立 BGP 会话，请参阅排查第 3/4 层 (网络/传输) 问题 (p. 70)。如果已建立 BGP 会话但您遇到了路由问题，请参阅排查路由问题 (p. 72)。

排查第 3/4 层 (网络/传输) 问题

如果您的 AWS Direct Connect 物理连接已开启并且您可以对 Amazon 对等 IP 地址执行 ping 操作，但您的虚拟接口已关闭且 BGP 对等会话无法建立，请使用以下步骤排查该问题。

1. 确保您的 BGP 本地自治系统编号 (ASN) 和 Amazon 的 ASN 已正确配置。
2. 确保 BGP 对等会话两端的对等 IP 已正确配置。
3. 确保您的 MD5 身份验证密钥已配置且与下载的路由器配置文件中的密钥完全匹配。检查是否有多余的空格或字符。
4. 验证您或您的提供商是否没有为私有虚拟接口公布超过 100 个前缀或为公共虚拟接口公布超过 1,000 个前缀。这些是硬性限制，不得超出。
5. 确保没有阻止 TCP 端口 179 或任何大数字临时 TCP 端口的防火墙或 ACL 规则。这些端口对于 BGP 在这些对等项之间建立 TCP 连接是必需的。
6. 检查您的 BGP 日志中是否有任何错误或警告消息。
7. 如果上述步骤未建立 BGP 对等会话，请联系 AWS Support。

以下流程图包含诊断 BGP 对等会话问题的步骤。


Virtual interface is down and cannot establish BGP session
Are BGP ASNs correct?
No
Update ASN configuration
Yes
Are peer IPs correct?
No
Update IP address configuration
Yes
Is MD5 authentication key correct?
No
Check that key exactly matches the router config file
Yes
Are you below the prefix limit?
No
Do not advertise more than 100 prefixes for private or 1,000 for public
Yes
Do firewall/ACL rules allow BGP traffic?
No
Enable TCP traffic on port 179 and high number ephemeral ports
Yes
Check BGP logs
Still not working
Contact AWS Support

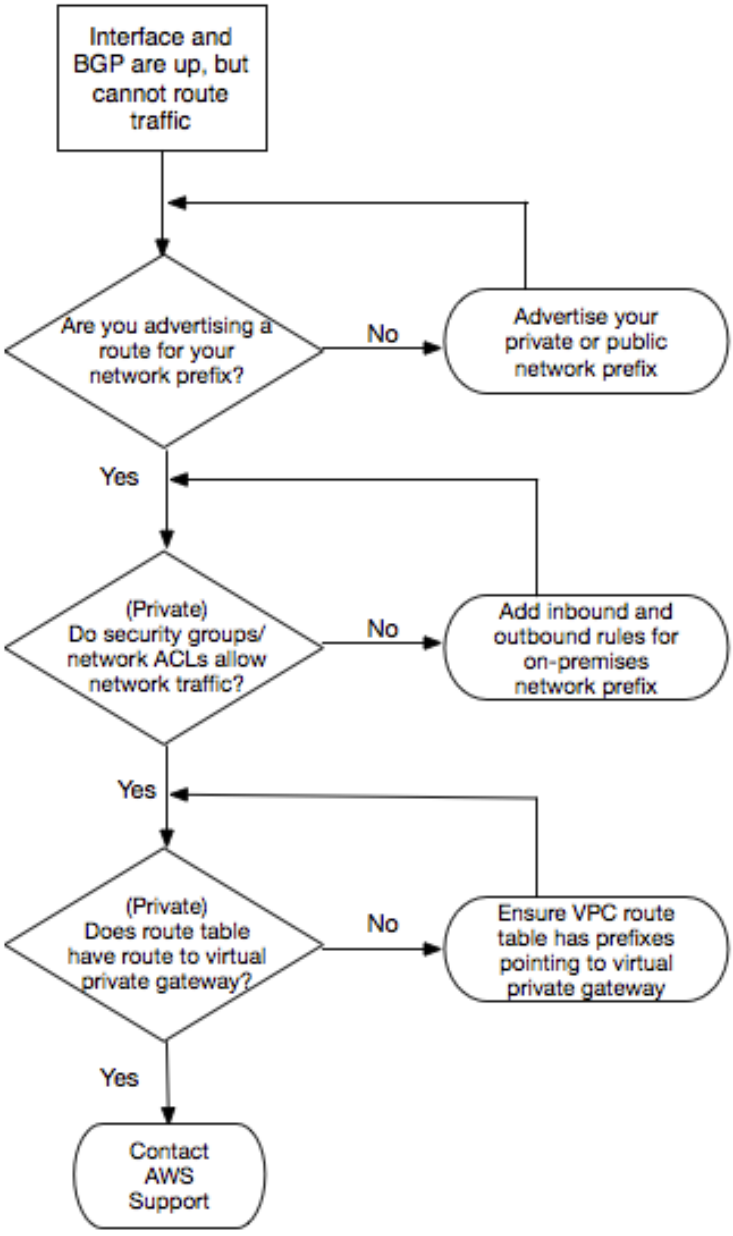
如果已建立 BGP 对等会话但您遇到了路由问题，请参阅排查路由问题 (p. 72)。

排查路由问题

如果您的虚拟接口已开启并且您已建立 BGP 对等会话，但无法通过该虚拟接口路由流量，请使用以下步骤排查该问题。

1. 确保您通过 BGP 会话为您的本地网络前缀公布路由。对于私有虚拟接口，这可以是私有或公有网络前缀。对于公有虚拟接口，这必须是您的公共可路由的网络前缀。
2. 对于私有虚拟接口，请确保您的 VPC 安全组和网络 ACL 针对您的本地网络前缀允许入站和出站流量。有关更多信息，请参阅 Amazon VPC 用户指南 中的安全组和网络 ACL。
3. 对于私有虚拟接口，请确保您的 VPC 路由表具有指向您的私有虚拟接口所连接到的虚拟专用网关的前缀。例如，如果您更喜欢默认情况下让您的所有流量路由到您的本地网络，则可以添加默认路由 (0.0.0.0/0 和/或 ::/0)，同时将该虚拟专用网关作为您的 VPC 路由表中的目标。
   - 或者，启用路由传播以基于您的动态 BGP 路由通告自动更新路由表中的路由。您对每个路由表可以拥有最多 100 个传播路由。不能提高此限制。有关更多信息，请参阅 Amazon VPC 用户指南 中的启用和禁用路由传播。
4. 如果上述步骤未解决您的路由问题，请联系 AWS Support。

以下流程图包含诊断路由问题的步骤。


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact AWS Support

文档历史记录

- API 版本：2012-10-25

下表描述了上次发布 AWS Direct Connect User Guide 以来的重要更改。

更改	描述	发行日期
本地首选项 BGP 社区	您可以使用本地首选项 BGP 社区标签来实现网络传入通信的负载平衡和路由首选项。有关更多信息，请参阅 本地首选项 BGP 社区 (p. 5)。	2018-02-06
AWS Direct Connect 网关	您可以使用 Direct Connect 网关将您的 AWS Direct Connect 连接到远程区域中的 VPC。有关更多信息，请参阅 Direct Connect 网关 (p. 45)。	2017-11-01
Amazon CloudWatch 指标	您可以查看 AWS Direct Connect 连接的 CloudWatch 指标。有关更多信息，请参阅 使用 Amazon CloudWatch 进行监控 (p. 64)。	2017 年 6 月 29 日
链接聚合组	您可创建一个链接聚合组 (LAG) 来聚合多个 AWS Direct Connect 连接。有关更多信息，请参阅 链接聚合组 (p. 40)。	2017-02-13
IPv6 支持	您的虚拟接口现在可以支持 IPv6 BGP 对等会话。有关更多信息，请参阅 添加或删除 BGP 对等 (p. 36)。	2016-12-01
标记支持	现在您可以标记您的 AWS Direct Connect 资源。有关更多信息，请参阅 针对 AWS Direct Connect 使用标签 (p. 52)。	2016-11-04
自助服务 LOA-CFA	现在，您可以使用 AWS Direct Connect 控制台或 API 下载《授权证书和连接设备分配 (LOA-CFA) 通知函》。	2016-06-22
硅谷新增节点	更新了主题，以包括 美国西部（加利福尼亚北部） 区域中新增的硅谷节点。	2016-06-03
阿姆斯特丹新增节点	更新了主题，以包括 欧洲（法兰克福） 区域中新增的阿姆斯特丹节点。	2016-05-19
俄勒冈州波特兰和新加坡新增节点	更新了主题，以包括 美国西部（俄勒冈） 和 亚太区域（新加坡） 区域中新增的俄勒冈州波特兰和新加坡节点。	2016-04-27
巴西圣保罗新增节点	更新了主题，以包括 南美洲（圣保罗） 区域中新增的巴西圣保罗节点。	2015-12-09
达拉斯、伦敦、硅谷和孟买新增节点	更新了主题，以包括在达拉斯（美国东部（弗吉尼亚北部） 区域）、伦敦（欧洲（爱尔兰） 区域）、硅谷（AWS GovCloud (US) 区域）和孟买（亚太区域（新加坡） 区域）新增的节点。	2015-11-27
中国（北京）区域新增节点	更新了主题，以包括 中国（北京） 区域中新增的北京节点。	2015-04-14
位于美国西部（俄勒冈）区域的拉斯维加斯新增节点	更新了主题，以包括在美国西部（俄勒冈）区域中新增的 AWS Direct Connect 拉斯维加斯节点。	2014-11-10

更改	描述	发行日期
欧洲（法兰克福）区域新增节点	更新了主题，以包括为欧洲（法兰克福）区域提供服务的新增 AWS Direct Connect 节点。	2014-10-23
亚太地区（悉尼）区域新增节点	更新了主题，以包括为亚太地区（悉尼）区域提供服务的新增 AWS Direct Connect 节点	2014-07-14
支持 AWS CloudTrail	增加了一个新主题，用于说明如何在 AWS Direct Connect 中使用 CloudTrail 记录活动。有关更多信息，请参阅 在 AWS CloudTrail 中记录 AWS Direct Connect API 调用 (p. 59)。	2014-04-04
支持访问远程 AWS 区域	添加了一个新主题，用于说明如何访问远程区域中的公有资源。有关更多信息，请参阅 访问远程 AWS 区域 (p. 3)。	2013-12-19
支持托管连接	更新主题，以涵盖对托管连接的支持。	2013-10-22
欧洲（爱尔兰）区域新增节点	更新了主题，以包括为欧洲（爱尔兰）区域提供服务的新增 AWS Direct Connect 节点。	2013-06-24
位于美国西部（俄勒冈）区域的西雅图新增节点	更新了主题，以包括位于西雅图的、为美国西部（俄勒冈）区域提供服务的新增 AWS Direct Connect 节点。	2013 年 5 月 8 日
支持结合 AWS Direct Connect 使用 IAM	添加了关于结合 AWS Direct Connect 使用 AWS Identity and Access Management 的主题。有关更多信息，请参阅 使用 AWS Identity and Access Management 控制对 AWS Direct Connect 的访问 (p. 50)。	2012 年 12 月 21 日
亚太地区（悉尼）区域新增节点	更新了主题，以包括为亚太地区（悉尼）区域提供服务的新增 AWS Direct Connect 节点。	2012 年 12 月 14 日
新 AWS Direct Connect 控制台和美国东部（弗吉利亚北部）和南美（圣保罗）区域	使用“AWS Direct Connect User Guide”取代了“AWS Direct Connect Getting Started Guide”。添加了新主题，以涵盖新的 AWS Direct Connect 控制台；添加了计费主题；添加了路由器配置信息；更新了主题，添加了为美国东部（弗吉尼亚北部）和南美洲（圣保罗）区域提供服务的两个新增 AWS Direct Connect 节点。	2012 年 8 月 13 日
欧盟（爱尔兰）、亚太地区（新加坡）和亚太地区（东京）区域的支持	添加了新的问题排查章节，并更新了主题，添加了为美国西部（加利福尼亚北部）、欧洲（爱尔兰）、亚太地区（新加坡）和亚太地区（东京）区域提供服务的四个新增的 AWS Direct Connect 节点。	2012 年 1 月 10 日
美国西部（加利福利亚北部）区域的支持	更新了主题，以包含增加的美国西部（加利福利亚北部）区域。	2011 年 9 月 8 日
公开发布	首次发行 AWS Direct Connect。	2011 年 8 月 3 日

AWS 词汇表

有关最新 AWS 术语，请参阅 AWS General Reference 中的 AWS 词汇表。