



用户指南

AWS Direct Connect



AWS Direct Connect: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

| | |
|--|----|
| 什么是 Direct Connect ? | 1 |
| Direct Connect 的组件 | 1 |
| 网络要求 | 2 |
| 受支持的 Direct Connect 虚拟接口类型 | 3 |
| Direct Connect 的定价 | 4 |
| 访问远程 AWS 区域 | 4 |
| 访问远程区域中的公有服务 | 4 |
| 访问远程区域中的 VPC | 5 |
| 网络到 Amazon VPC 的连接选项 | 5 |
| Routing policies and BGP communities | 5 |
| 公有虚拟接口路由策略 | 5 |
| 公有虚拟接口 BGP 社区 | 7 |
| 私有虚拟接口和中转虚拟接口路由策略 | 8 |
| 长 ASN 支持 | 10 |
| 私有虚拟接口路由示例 | 11 |
| 连接选项 | 13 |
| 连接先决条件 | 13 |
| AWS Direct Connect 弹性工具包 | 15 |
| 可用的弹性模型 | 16 |
| AWS Direct Connect 弹性工具包先决条件 | 13 |
| 最大弹性 | 17 |
| 高弹性 | 18 |
| 开发和测试 | 19 |
| 失效转移测试 | 20 |
| 最大弹性配置 | 20 |
| 配置高弹性 | 30 |
| 配置开发和测试弹性 | 40 |
| Direct Connect 失效转移测试 | 50 |
| 经典连接 | 53 |
| 配置 Classic 连接 | 53 |
| Direct Connect 的维护 | 68 |
| 计划维护 | 68 |
| 紧急维护 | 69 |
| 第三方维护 | 69 |

| | |
|-----------------------------------|----|
| 维护活动的准备 | 70 |
| 弹性验证 | 70 |
| 维护活动延期 | 70 |
| MAC 安全 (MACsec) | 71 |
| MACsec 概念 | 71 |
| MACsec 密钥轮换 | 72 |
| 支持的连接 | 73 |
| 专用 连接 | 73 |
| LAGs | 74 |
| 合作伙伴互连 | 74 |
| 服务相关角色 | 75 |
| MACsec 预共享 CKN/CAK 密钥注意事项 | 75 |
| 开始使用 MACsec 专用连接 | 75 |
| 创建连接 | 75 |
| (可选) 创建 LAG | 75 |
| 将 CKN/CAK 与连接或 LAG 相关联 | 76 |
| 配置本地路由器 | 76 |
| 移除与连接或 LAG 之间的关联 CKN/CAK | 76 |
| 专用和托管连接 | 77 |
| 专用 连接 | 77 |
| 《授权和连接设备分配通知函 (LOA-CFA) 》 | 78 |
| 使用连接向导创建连接 | 79 |
| 创建 Classic 连接 | 81 |
| 下载 LOA-CFA | 82 |
| 将 MACsec CKN/CAK 与连接关联 | 83 |
| 移除 MACsec 密钥和连接之间的关联 | 83 |
| 托管 连接 | 84 |
| 接受托管连接 | 85 |
| 删除连接 | 86 |
| 更新连接 | 86 |
| 查看 连接详细信息 | 88 |
| 交叉连接 | 89 |
| 连接选项 | 89 |
| 美国东部 (俄亥俄州) | 91 |
| 美国东部 (弗吉尼亚州北部) | 91 |
| 美国西部 (加利福尼亚北部) | 92 |

| | |
|---------------------------------|-----|
| 美国西部 (俄勒冈州) | 93 |
| 非洲 (开普敦) | 94 |
| 亚太地区 (雅加达) | 94 |
| 亚太地区 (孟买) | 94 |
| 亚太地区 (首尔) | 95 |
| 亚太地区 (新加坡) | 95 |
| 亚太地区 (悉尼) | 96 |
| 亚太地区 (东京) | 96 |
| 加拿大 (中部) | 97 |
| 中国 (北京) | 97 |
| 中国 (宁夏) | 97 |
| 欧洲地区 (法兰克福) | 98 |
| 欧洲地区 (爱尔兰) | 99 |
| 欧洲地区 (米兰) | 99 |
| 欧洲地区 (伦敦) | 99 |
| 欧洲地区 (巴黎) | 100 |
| 欧洲地区 (斯德哥尔摩) | 100 |
| 欧洲 (苏黎世) | 100 |
| 以色列 (特拉维夫) | 100 |
| 中东 (巴林) | 101 |
| 中东 (阿联酋) | 101 |
| 南美洲 (圣保罗) | 101 |
| AWS GovCloud (美国东部) | 102 |
| AWS GovCloud (美国西部) | 102 |
| 虚拟接口和托管虚拟接口 | 103 |
| 公有虚拟接口前缀公布规则 | 103 |
| SiteLink | 104 |
| 虚拟接口的先决条件 | 105 |
| MTUs 用于私有虚拟接口或传输虚拟接口 | 110 |
| 虚拟接口 | 111 |
| 将虚拟接口中转到 Direct Connect 网关的先决条件 | 111 |
| 创建公有虚拟接口 | 112 |
| 创建私有虚拟接口 | 113 |
| 创建到 Direct Connect 网关的中转虚拟接口 | 115 |
| 下载路由器配置文件 | 117 |
| 托管的虚拟接口 | 119 |

| | |
|---------------------------------------|-----|
| 创建托管私有虚拟接口 | 122 |
| 创建托管公有虚拟接口 | 123 |
| 创建托管中转虚拟接口 | 125 |
| 查看虚拟接口详细信息 | 127 |
| 添加 BGP 对等体 | 127 |
| 删除 BGP 对等体 | 129 |
| 设置私有虚拟接口的 MTU | 130 |
| 添加或删除虚拟接口标签 | 130 |
| 删除虚拟接口 | 131 |
| 接受托管 虚拟接口 | 131 |
| 迁移虚拟接口 | 132 |
| 链接聚合组 (LAG) | 134 |
| MACsec 注意事项 | 135 |
| 创建 LAG | 136 |
| 查看 LAG 详细信息 | 138 |
| 更新 LAG | 138 |
| 将连接与 LAG 关联 | 140 |
| 解除连接与 LAG 的关联 | 141 |
| 将 MACsec CKN/CAK 与 LAG 关联 | 141 |
| 移除 MACsec 密钥和 LAG 之间的关联 | 142 |
| 删除 LAG | 143 |
| 网关 | 144 |
| Direct Connect 网关 | 144 |
| 场景 | 146 |
| 创建 Direct Connect 网关 | 149 |
| 从虚拟私有网关迁移到 Direct Connect 网关 | 150 |
| 删除 Direct Connect 网关 | 150 |
| 虚拟私有网关关联 | 151 |
| 创建虚拟专用网关 | 152 |
| 关联虚拟私有网关或解除其关联 | 153 |
| 创建到 Direct Connect 网关的私有虚拟接口 | 154 |
| 跨账户关联虚拟私有网关 | 157 |
| 中转网关关联 | 157 |
| 跨账户关联中转网关 | 158 |
| 将中转网关与 Direct Connect 关联或解除其关联。 | 158 |
| 创建到 Direct Connect 网关的中转虚拟接口 | 160 |

| | |
|---|-----|
| 创建中转网关关联提议 | 162 |
| 接受或拒绝中转网关关联提议 | 163 |
| 为中转网关关联更新允许的前缀 | 164 |
| 删除中转网关关联提议 | 165 |
| Cloud WAN 核心网络关联 | 165 |
| 先决条件 | 168 |
| 注意事项 | 168 |
| Direct Connect 网关与 Cloud WAN 核心网络关联 | 168 |
| 验证 Direct Connect 网关关联 | 169 |
| 允许的前缀交互 | 169 |
| 虚拟私有网关关联 | 169 |
| 中转网关关联 | 170 |
| 示例：允许在中转网关配置中添加前缀 | 171 |
| 标记资源 | 173 |
| 标签限制 | 174 |
| 通过 CLI 或 API 使用标签 | 174 |
| 示例 | 175 |
| 安全性 | 176 |
| 数据保护 | 176 |
| 互连网络流量隐私 | 177 |
| 加密 | 178 |
| 身份和访问管理 | 178 |
| 受众 | 179 |
| 使用身份进行身份验证 | 179 |
| 使用策略管理访问 | 180 |
| Direct Connect 如何与 IAM 结合使用 | 181 |
| Direct Connect 基于身份的策略示例 | 186 |
| 服务关联角色 | 196 |
| AWS 托管策略 | 199 |
| 问题排查 | 200 |
| 日志记录和监控 | 202 |
| 合规性验证 | 202 |
| Direct Connect 中的弹性 | 202 |
| 失效转移 | 203 |
| 基础结构安全性 | 203 |
| 边界网关协议 | 204 |

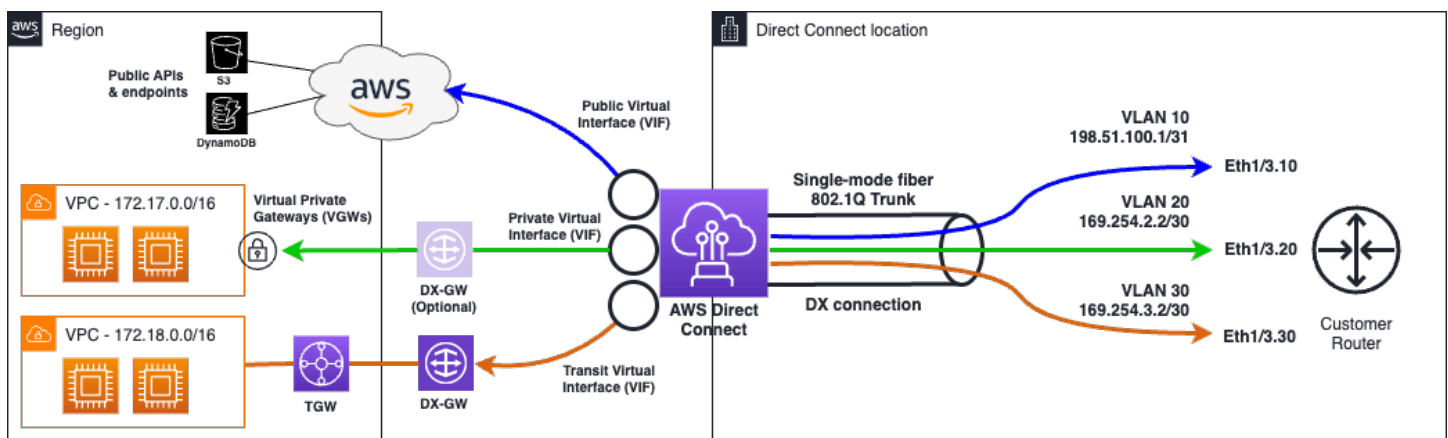
| | |
|---------------------------------------|---------|
| 使用 AWS CLI | 205 |
| 步骤 1：创建连接 | 205 |
| 步骤 2：下载 LOA-CFA | 206 |
| 步骤 3：创建虚拟接口，获取路由器配置 | 207 |
| 记录 API 调用 | 212 |
| Direct Connect 信息在 CloudTrail | 212 |
| 了解 Direct Connect 日志文件条目 | 213 |
| 监控 Direct Connect 资源 | 218 |
| 监控工具 | 218 |
| 自动监控工具 | 218 |
| 手动监控工具 | 219 |
| 使用 Amazon 进行监控 CloudWatch | 219 |
| Direct Connect 指标和维度 | 220 |
| 查看 Direct Connect CloudWatch 指标 | 225 |
| 创建警报以监控连接 | 226 |
| Direct Connect 的配额 | 228 |
| BGP 配额 | 230 |
| ASN 限制 | 231 |
| 负载均衡注意事项 | 231 |
| 故障排除 | 232 |
| 第 1 层（物理）问题 | 232 |
| 第 2 层（数据链路）问题 | 234 |
| 第 3/4 层（网络/传输）问题 | 235 |
| 长 ASN 问题 | 238 |
| 路由问题 | 239 |
| 文档历史记录 | 241 |
| | ccxlvii |

什么是 Direct Connect ?

Direct Connect 通过标准的以太网光纤电缆将您的内部网络链接到 Direct Connect 位置。电缆的一端接到您的路由器，另一端接到 Direct Connect 路由器。通过此连接，您可以创建直接连接到 AWS 公有服务（例如，连接到 Amazon S3）或 Amazon VPC 的虚拟接口，从而绕过网络路径中的互联网服务提供商。Direct Connect 位置在其关联的区域提供对 AWS 的访问。您可以在公有区域或 AWS GovCloud (US) 中使用单个连接访问所有其他公有区域中的公有 AWS 服务。

- 有关可供您连接至 Direct Connect 位置的列表，请参阅 [AWS Direct Connect Locations](#)。
- 有关 Direct Connect 问题的答案，请参阅 [Direct Connect FAQ](#)。

下图显示了 Direct Connect 如何与网络连接的高级概述。



内容

- [Direct Connect 组件](#)
- [网络要求](#)
- [受支持的 Direct Connect 虚拟接口类型](#)
- [Direct Connect 的定价](#)
- [访问远程 Direct Connect 区域](#)
- [Direct Connect 路由策略和 BGP 社区](#)

Direct Connect 组件

以下是您用于 Direct Connect 的关键组件：

连接

在 Direct Connect 位置创建连接以建立从本地到 AWS 区域的网络连接。有关更多信息，请参阅 [Direct Connect 专用连接和托管连接](#)。

虚拟接口

创建虚拟接口以启用对 AWS 服务的访问。公有虚拟接口允许访问公有服务，如 Amazon S3。私有虚拟接口允许对您 VPC 的访问。下文 [the section called “受支持的 Direct Connect 虚拟接口类型”](#) 介绍了支持的接口类型。有关受支持接口的更多详细信息，请参阅 [Direct Connect 虚拟接口和托管虚拟接口](#) 和 [虚拟接口的先决条件](#)。

网络要求

要在 Direct Connect 位置使用 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 Direct Connect 节点。有关可用 Direct Connect 位置的更多信息，请参阅 [AWS Direct Connect 产品详细信息](#)。
- 您正与属于 AWS 合作伙伴网络 (APN) 成员的 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](#)。
- 您正与独立的服务供应商合作连接到 Direct Connect。

此外，您的网络必须符合以下条件：

- 您的网络必须使用单模光纤，其中 1 GB 以太网使用 1000BASE-LX (1310 nm) 收发器，10 GB 以太网使用 10GBASE-LR (1310 nm) 收发器，100 GB 以太网使用 100GBASE-LR4 收发器，或者 400 Gbps 以太网使用 400GBASE-LR4。
- 但是，根据为连接提供服务的 AWS Direct Connect 端点，可能需要为任何专用连接启用或禁用本地设备自动协商。如果在 Direct Connect 连接开启时虚拟接口仍处于关闭状态，请参阅 [排查第 2 层 \(数据链路 \) 问题](#)。
- 整个连接 (包括中间设备) 都必须支持 802.1Q VLAN 封装。
- 您的设备必须支持边界网关协议 (BGP) 和 BGP MD5 身份验证。
- (可选) 您可以在网络上配置双向转发检测 (BFD)。每个 Direct Connect 虚拟接口自动启用异步 BFD。系统会对 Direct Connect 虚拟接口自动启用，但只有在路由器上配置后才会生效。有关更多信息，请参阅 [为 Direct Connect 连接启用 BFD](#)。

Direct Connect 支持 IPv4 和 IPv6 通信协议。可通过 Direct Connect 公有虚拟接口访问 AWS 公有服务提供的 IPv6 地址。

Direct Connect 在链路层支持 1522 或 9023 字节的以太网帧大小 (14 字节以太网标头 + 4 字节 VLAN 标记 + IP 数据报的字节 + 4 字节 FCS)。您可以设置私有虚拟接口的 MTU。有关更多信息，请参阅 [MTUs 用于私有虚拟接口或传输虚拟接口](#)。

受支持的 Direct Connect 虚拟接口类型

AWS Direct Connect 支持以下三种虚拟接口 (VIF) 类型：

- 私有虚拟接口

此类接口用于使用私有 IP 地址访问 Amazon Virtual Private Cloud (VPC)。使用私有虚拟接口，您可以

- 将每个私有虚拟接口直接连接到单个 VPC，即可使用同一区域的私有 IP 访问这些资源。
- 将私有虚拟接口连接到 Direct Connect 网关，即可访问任何账户和 AWS 区域 (AWS 中国区域除外) 的多个虚拟私有网关。

- 公有虚拟接口

此类虚拟接口用于使用公有 IP 地址访问所有 AWS 公有服务。通过公有虚拟接口，您可以连接到全球所有 AWS 公有 IP 地址和服务。

- 中转虚拟接口

此类接口用于访问与 Direct Connect 网关关联的一个或多个 Amazon VPC 中转网关。使用中转虚拟接口，您可以跨多个账户和 AWS 区域 (AWS 中国区域除外) 连接多个 Amazon VPC 中转网关。

Note

Direct Connect 网关和虚拟接口之间不同类型的关联有数量限制。有关具体限制的更多信息，请参阅 [Direct Connect 的配额](#) 页面。

有关虚拟接口的更多信息，请参阅 [虚拟接口和托管虚拟接口](#)。

Direct Connect 的定价

AWS Direct Connect 具有两个计费元素：端口小时费和出站数据传输费。端口小时定价由容量和连接类型（专用连接或托管连接）确定。

专用接口和传输虚拟接口的数据传出费用将分配给负责数据传输的 AWS 账户。使用多账户 AWS Direct Connect 网关不会产生额外的费用。

对于可公开寻址的 AWS 资源（例如，Amazon S3 存储桶、Classic EC2 实例或通过互联网网关的 EC2 流量），如果出站流量的目的地是由同一个 AWS 付款人账户拥有的公有前缀，并且出站流量通过 Direct Connect 公有虚拟接口主动发布到 AWS，则数据传出（DTO）使用量按 Direct Connect 数据传输速率向资源所有者计量。

有关更多信息，请参阅 [AWS Direct Connect 定价](#)。

访问远程 Direct Connect 区域

公有区域或 AWS GovCloud (US) 中的 Direct Connect 位置，可以访问任何其他公有区域 [不包括中国（北京和宁夏）] 中的公有服务。此外，可将公有区域或 AWS GovCloud (US) 中的 Direct Connect 连接配置为：访问您账户中在任何其他公有区域 [不包括中国（北京和宁夏）] 中的 VPC。因此，您可以使用单个 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，所有网络流量都保留在 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 Direct Connect 连接支持的 BGP 社区的更多信息，请参阅 [Routing policies and BGP communities](#)。

访问远程区域中的公有服务

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 [虚拟接口和托管虚拟接口](#)。

创建公有虚拟接口并对其建立 BGP 会话之后，您的路由器将获知其他公有 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中创建 Direct Connect 网关。使用它将您的 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 或连接到中转网关。有关更多信息，请参阅 [Direct Connect 网关](#)。

或者，您可以为您的 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 的场景](#)。

网络到 Amazon VPC 的连接选项

以下配置可用于将远程网络连接到您的 Amazon VPC 环境。这些选项有利于将 AWS 资源与您现有的现场服务集成：

- [Amazon Virtual Private Cloud Connectivity Options](#)

Direct Connect 路由策略和 BGP 社区

Direct Connect 为公共 Direct Connect 连接应用入站（来自您的本地数据中心）和出站（来自您 AWS 所在区域）的路由策略。您也可以在 Amazon 公布的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。

公有虚拟接口路由策略

如果您使用 Direct Connect 访问公共 AWS 服务，则必须指定要通过 BGP 进行通告的公共 IPv4 IPv6 前缀或前缀。

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。
- Direct Connect 执行入站数据包过滤，以验证流量来源是否来自您通告的前缀。

下面的出站路由策略适用：

- AS_PATH 和最长前缀匹配用于确定路由路径。AWS Direct Connect 如果向互联网和公共虚拟接口通告相同的前缀，则建议使用更具体的路由。

- Direct Connect 在可用时公布所有本地和远程 AWS 区域前缀，并包括来自其他 AWS 非区域接入点 (PoP) 的网络前缀 (例如 Route 53)。CloudFront

Note

- 中国区域 AWS 的 IP 地址范围 JSON 文件 ip-ranges.json 中列出的前缀仅在中国 AWS 区域中公布。AWS
 - 商业区域 AWS 的 IP 地址范围 JSON 文件 ip-ranges.json 中列出的前缀仅在 AWS 商业区域中公布。AWS
- 有关 ip-ranges.json 文件的更多信息，请参阅《AWS 一般参考》中的 [AWS IP 地址范围](#)。

- Direct Connect 通告前缀的最小路径长度为 3。
- Direct Connect 向知名的 NO_EXPORT BGP 社区通告所有公共前缀。
- 如果您使用两个不同的公共虚拟接口从两个不同的区域通告相同的前缀，并且两者都具有相同的 BGP 属性和最长的前缀长度，则 AWS 将优先考虑主区域的出站流量。
- 如果您有多个 Direct Connect 连接，则可以通过广告具有相同路径属性的前缀来调整入站流量的负载分担。
- 所通告的前缀 Direct Connect 不得在连接的网络边界之外进行通告。例如，这些前缀不得包含在任何公有 Internet 路由表中。
- Direct Connect 保留买家在 Amazon 网络中宣传的前缀。我们不会将从公有 VIF 获取的客户前缀重新公布到以下任何位置：
 - 其他 Direct Connect 客户
 - 与 AWS 全球网络对等的网络
 - Amazon 中转提供商
- 使用公有接口时，您可以使用公有或私有 ASN。但是，有重要的注意事项：
 - 公开 ASNs：您必须拥有 ASN 并有权公布。AWS 将验证您对 ASN 的所有权。同时支持 ASNs (1-2147483647) 和做多 ASNs (1-4294967295)。
 - 私人 ASNs：您可以使用以下范围内的私 ASN 有模式：
 - 私人 ASNs：64512-65534
 - 私募多头 ASNs：420000000000-4294967294

但是，在向其他 AWS 客户或互联网宣传您的前缀时，Direct Connect 会将私有 AWS ASN 替换为 ASN (7224)。

- **ASN 前置：**

- 使用公有 ASN (包括 ASN 和长 ASN)，前置将按预期工作，并且您的前置 ASN 将对其他网络可见。
- 使用私有 ASN (包括 ASN 和长 ASN)，当用 7224 AWS 替换您的私有 ASN 时，您所做的任何前置都将被删除。这意味着，除了在公共虚拟接口上使用私有 ASN AWS 时，预置 ASN 并不能有效影响路由决策。
- 通过 AWS 公共虚拟接口建立 BGP 对等会话时，请使用 7224 作为自治系统编号 (ASN)，以便在侧面建立 BGP 会话。AWS 您的路由器或客户网关设备上的 ASN 应与该 ASN 不同。您的客户 ASN 可以是 ASN (1-2147483647，不包括保留范围)，也可以是长 ASN (1-4294967295，不包括保留范围)。

公有虚拟接口 BGP 社区

Direct Connect 支持 scope BGP 社区标签，以帮助控制公共虚拟接口上流量的范围 (区域或全局) 和路由首选项。AWS 将从公共 VIF 接收的所有路由视为标有 NO_EXPORT BGP 社区标签，这意味着只有 AWS 网络才会使用该路由信息。

作用域 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。

AWS 区域 社区

对于入站路由策略，您的前缀可以使用以下 BGP 社区：

- 7224:9100—本地 AWS 区域
- 7224:9200—一切 AWS 区域 为了一个大陆：
 - 整个北美
 - 亚太地区
 - 欧洲、中东和非洲
- 7224:9300—全球 (所有公共 AWS 区域)

Note

如果您不应用任何社区标签，则默认情况下，会向所有公共 AWS 区域 (全球) 发布前缀。标有同一社区并且带有相同的 AS_PATH 属性的前缀适合多路径传输。

Direct Connect保留 7224:1 - 7224:65535 社区。

对于出站路由策略，Direct Connect 将以下 BGP 社区应用于其通告的路由：

- 7224:8100—来自与接入 Direct Connect 点 AWS 关联的同一区域的路由。
- 7224:8200—起源于与入 Direct Connect 点关联的同一大陆的路线。
- 无标签：来自其他欧洲大陆的路由。

Note

要接收所有 AWS 公共前缀，请不要应用任何过滤器。

不支持 Direct Connect 公共连接的社区将被移除。

NO_EXPORT BGP 社区

对于出站路由策略，公有虚拟接口支持 NO_EXPORT BGP 社区标签。

Direct Connect 还在宣传的 Amazon 路线上提供 BGP 社区标签。如果您使用 Direct Connect 访问公共 AWS 服务，则可以基于这些社区标签创建过滤器。

对于公共虚拟接口，向客户 Direct Connect 通告的所有路由都标有 NO_EXPORT 社区标签。

私有虚拟接口和中转虚拟接口路由策略

如果您使用 AWS Direct Connect 访问私有 AWS 资源，则必须指定要通过 BGP 进行通告的 IPv4 或 IPv6 前缀。上述前缀可以是公有前缀或私有前缀。

基于通告的前缀，适用以下出站路由规则：

- AWS 首先评估最长的前缀长度。AWS 如果所需的路由路径用于连接，则建议使用多个 Direct Connect 虚拟接口发布更具体的 active/passive 路由。有关更多信息，请参阅 [Influencing Traffic over Hybrid Networks using Longest Prefix Match](#)。
- 当所需的路由路径用于 active/passive 连接并且通告的前缀长度相同时，建议使用本地优先级的 BGP 属性。AWS 区域使用 7224:7200 —Medium本地偏好社区值，将每个区域设置为具有相同关联的首选[AWS Direct Connect 位置](#)。如果本地区域未与 Direct Connect 位置关联，则将其设置为较低的值。只有未分配本地首选项社区标签时才适用。
- 当前缀长度和本地首选项相同时，AS_PATH 长度才可用于确定路由路径。

- 当前缀长度、本地首选项和 AS_PATH 相同时，多出口鉴别器 (MED) 可用于确定路由路径。AWS 不建议使用 MED 值，因为它们在评估中的优先级较低。
- AWS 当前缀具有相同的 AS_PATH 长度和 BGP 属性时，使用跨多个传输或私有虚拟接口的等价多路径 (ECMP) 路由。前缀的 AS_PATH ASNs 中的不需要匹配。

私有虚拟接口和中转虚拟接口 BGP 社区

当通过 Direct Connect 私有接口或传输虚拟接口将流量 AWS 区域 路由到本地位置时，Direct Connect 位置的关联 AWS 区域 会影响 ECMP 的使用。AWS 区域 默认情况下，首选相同关联的 Direct Connect AWS 区域 t 位置。查看 [AWS Direct Connect 位置](#) 以识别任一 Direct Connect 位置的关联 AWS 区域。

如果未应用本地首选项社区标签，则在以下情况下，Direct Connect 支持在两条或更多路径中，通过私有或中转虚拟接口，对 AS_PATH 长度和 MED 值相同的前缀应用 ECMP。

- AWS 区域 发送流量有两条或多条来自相同关联位置的虚拟接口路径 AWS 区域，无论是在相同的主机托管设施中还是在不同的主机托管设施中。
- AWS 区域 发送流量有两条或多条来自不在同一区域的虚拟接口路径。

有关更多信息，请参阅[如何设置 AWS 从私有或传输虚拟接口到的 Active/Active 或 Active/Passive Direct Connect 连接？](#)

Note

这对 AWS 区域 从本地位置传送的 ECMP 没有影响。

要控制路由首选项，Direct Connect 支持本地首选项 BGP 社区标签，以便用于私有虚拟接口和中转虚拟接口。

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。

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。要对位于相同或不同 AWS 区域的多个 Direct Connect 连接（主动/主动）之间的流量进行负载平衡，请在连接的前缀中应用相同的社区标签；例如，7224:7200（中等偏好）。如果其中一个连接失败，则系统将使用 ECMP 在剩余的主动连接之间实现流量负载均衡，无论其主区域关联如何。要支持跨多个 Direct Connect 连接（主动/被动）的失效转移，请对主要或主动虚拟接口的前缀应用具有高首选项的社区标签，并对备份或被动虚拟接口的前缀应用具有低首选项的社区标签。例如，将主要虚拟接口或主动虚拟接口的 BGP 社区标签设置为 7224:7300（高首选项），将被动虚拟接口的 BGP 社区标签设置为 7224:7100（低首选项）。

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。

长期支持 ASN Direct Connect

Support for long ASNs（4 字节）允许您将长自治系统编号 (ASNs) 配置为 AWS 网络设备和网络设备之间建立的 BGP 会话的参数的一部分。此功能是按账户启用或禁用的。

您可以在主机上或通过设置 ASN 或长 ASN 范围。 APIs

- 使用控制台时，ASN 字段支持两者 ASNs 兼而有之。 ASNs 您可以添加从 1 到 4294967294 之间的任何范围。
- 使用创建虚拟接口时，您可以指定 ASN (asn) 或长 ASN (asnLong)，但不能同时指定两者。 APIs 有关使用 ASN 或长 ASN 的更多信息，请参阅 [Direct Connect API](#) 参考 APIs 中的以下内容：
 - BGPPeer
 - DeleteBGPPeerRequest
 - NewBGPPeer
 - NewPrivateVirtualInterface
 - NewPrivateVirtualInterfaceAllocation
 - NewPublicVirtualInterface
 - NewPublicVirtualInterfaceAllocation
 - NewTransitVirtualInterface
 - NewTransitVirtualInterfaceAllocation
 - VirtualInterface

注意事项

选择使用 ASN 或长 ASN 时，请注意以下几点：

- 向后兼容：Direct Connect 会自动处理与支持 ASN 的路由器和支持长 ASN 的路由器的 BGP 会话。如果您的路由器不支持长时间 ASNs，则 BGP 会话将在 ASN 模式下运行。
- ASN 格式：您可以用普通格式（例如）4200000000或 asdot 格式（例如）指定 4 字节 ASNs。64086.59904Direct Connect 接受这两种格式，但 ASNs 以纯格式显示
- 私有 ASN 范围：使用私有 long ASNs (4200000000-4294967294) 时，适用与私 ASNs 有相同的替换行为。在向其他网络通告时，Direct Connect 会将您的私有 ASN 替换为 7224。
- BGP 社区标签：所有现有的 BGP 社区标签 (7224:xxxx) 均可使用 long。ASNs 社区标签格式保持不变。
- 监控和故障排除：为了保持一致性，CloudWatch 指标、BGP 会话日志和故障排除工具 ASNs 以普通格式长显示。

可用性和定价

要获得长期 ASN 支持，请注意以下几点：Direct Connect

- 可用性：长 ASN 在所有受支持的 AWS 地区都可 Direct Connect 用。
- 定价：除标准定 Direct Connect 价外，长期 ASN 支持不收取任何额外费用。

Note

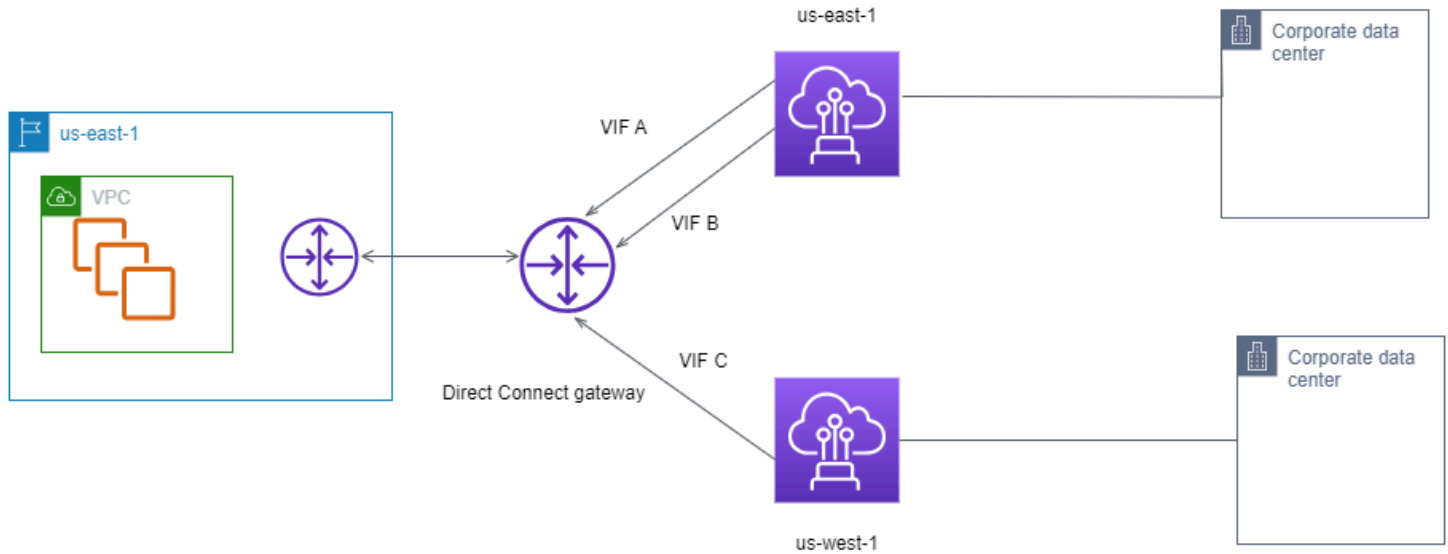
长期 ASN 启用适用于您的整个 AWS 账户。您不能为单个虚拟接口或 BGP 对等体启用长 ASN 支持。

Direct Connect 私有虚拟接口路由示例

考虑一下 Direct Connect 位置 1 的主区域与 VPC 主区域相同的配置。另一个区域中有一个冗余 Direct Connect 位置。从位置 1 VIFs (us-east-1) 到 Direct Connect 网关有两个私有 Direct Connect 位置 (VIF A 和 VIF B)。从 Direct Connect 位置 (us-west-1) 到 Direct Connect 网关之间有一个私有 VIF (VIF C)。要在 VIF A 之前通过 VIF B 进行 AWS 路由，请将 VIF B 的 AS_PATH 属性设置为比 VIF A AS_PATH 属性短。

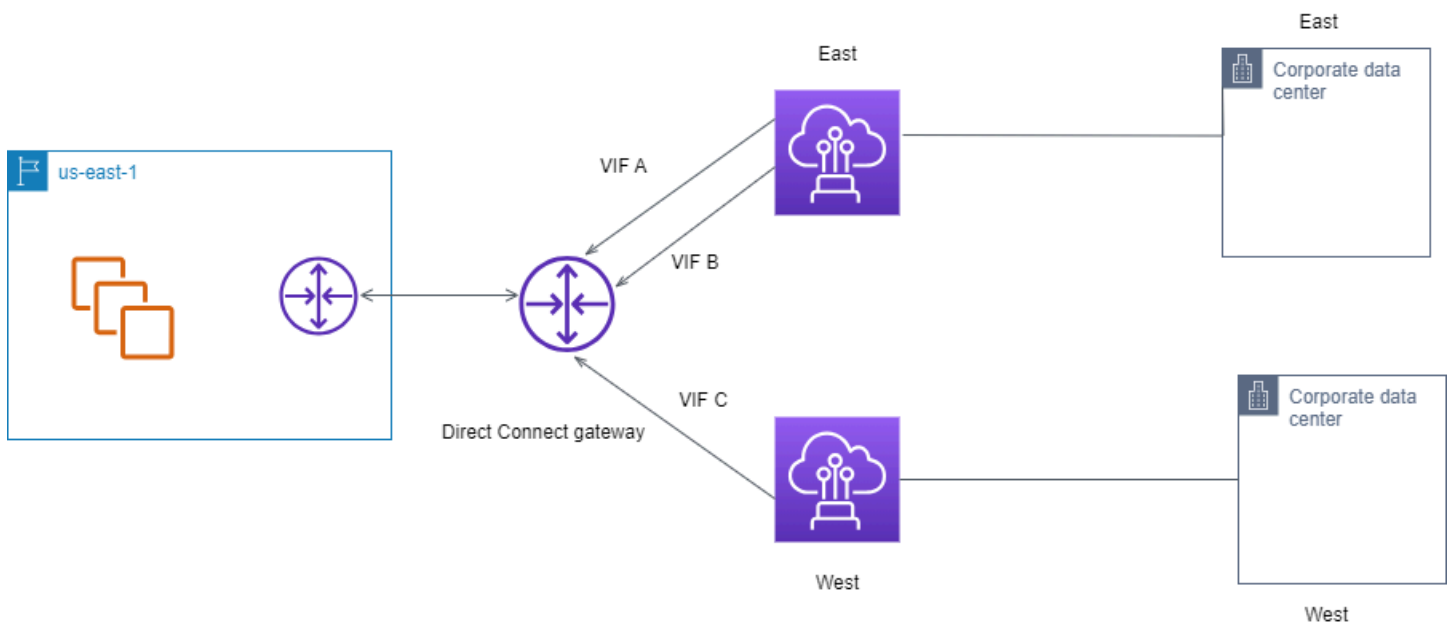
它们 VIFs 具有以下配置：

- VIF A (位于 us-east-1) 公布 172.16.0.0/16 , 其 AS_PATH 属性为 65001, 65001, 65001
- VIF B (位于 us-east-1) 公布 172.16.0.0/16 , 其 AS_PATH 属性为 65001, 65001
- VIF C (位于 us-west-1) 公布 172.16.0.0/16 , 其 AS_PATH 属性为 65001



如果更改 VIF C 的 CIDR 范围配置，则属于 VIF C CIDR 范围的路由将使用 VIF C，因为其具有最长前缀长度。

- VIF C (位于 us-west-1) 公布 172.16.0.0/24 , 其 AS_PATH 属性为 65001



Direct Connect 连接选项

AWS 让客户能够在 Amazon Virtual Private Cloud (Amazon VPC) 与其本地基础设施之间实现高度弹性的网络连接。AWS Direct Connect 弹性工具包提供了一个包含多个弹性模型的连接向导。这些模型可帮助您确定，然后订购专用连接数量，以便满足 SLA 目标。您选择一个弹性模型，然后 Resiliency Toolkit 将指导您完成专用的连接订购流程。AWS Direct Connect 这些弹性模型旨在确保您在多个位置具有适当数量的专用连接。

以下连接选项可用于 Direct Connect。

- **最大弹性**：此模型位于 AWS Direct Connect 弹性工具包中，可让您订购专用连接以实现 99.99% 的 SLA。要求您满足 [Direct Connect 服务水平协议](#) 中指定的实现 SLA 的所有要求。有关更多信息，请参阅 [AWS Direct Connect 弹性工具包](#)。
- **高弹性**：此模型可在 AWS Direct Connect 弹性工具包中找到，它为您提供了一种订购专用连接的方法，以实现 99.9% 的 SLA。要求您满足 [Direct Connect 服务水平协议](#) 中指定的实现 SLA 的所有要求。有关更多信息，请参阅 [AWS Direct Connect 弹性工具包](#)。
- **开发和测试**：此模型位于 AWS Direct Connect 弹性工具包中，可让您通过使用在一个位置中的不同设备上终止的单独连接来实现非关键工作负载的开发和测试弹性。有关更多信息，请参阅 [AWS Direct Connect 弹性工具包](#)。
- **经典**：经典连接无需 AWS Direct Connect 弹性工具包即可创建连接。此选项面向已有连接且想要不使用工具包来添加更多连接的用户。此模型有 95% 的 SLA，但不提供弹性或冗余。有关更多信息，请参阅 [经典连接](#)。

主题

- [连接先决条件](#)
- [AWS Direct Connect 弹性工具包](#)
- [Direct Connect 经典连接](#)

连接先决条件

Direct Connect 通过单模光纤支持以下端口速度：用于 1 千兆以太网的 1000BASE-LX (1310 nm) 收发器、用于 10 千兆位以太网的 10GBASE-LR (1310 nm) 收发器、用于 100 千兆位以太网的 100GBASE-LX (1310 nm) 收发器或用于 400 Gbase 以太网的 400GBASE-LR (1310 nm) 收发器。LR4 LR4

您可以通过以下方式之一使用 AWS Direct Connect 弹性工具包或经典连接来设置连接：Direct Connect

| 模型 | 带宽 | 方法 |
|------|--|--|
| 专用连接 | 1 Gbps、10 Gbps、100 Gbps 和 400 Gbps | 与 Direct Connect 合作伙伴或网络提供商合作，将路由器从您的数据中心、办公室或托管环境连接到某个 Direct Connect 位置。网络提供商不必是 AWS Direct Connect 合作伙伴 即可将您连接到专用连接。Direct Connect 专用连接通过单模光纤支持以下端口速度：1 Gbps：1000 BASE-LX (1310 nm)、10 Gbps：10Gbase-LR (1310 nm)、100Gbps：100Gbase-或 400 Gbase-以太网。LR4 LR4 |
| 托管连接 | 50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps 和 25 Gbps。 | 与合作伙伴 计划中的AWS Direct Connect 合作伙伴合作 ，将路由器从您的数据中心、办公室或托管环境连接到某个 Direct Connect 地点。 只有某些合作伙伴提供更高容量的连接。 |

对于 Direct Connect 带宽为 1 Gbps 或更高的连接，请确保您的网络满足以下要求：

- 您的网络必须使用带有 1000BASE-LX (1310 nm) 收发器的单模光纤用于千兆以太网，10GBASE-LR (1310 nm) 收发器用于万兆以太网，100GBASE-LR (1310 nm) 收发器用于100千兆以太网，或者使用400GBASE-用于400 Gbase-以太网。LR4 LR4

- 根据为您的连接提供服务的 Direct Connect 端点，可能需要为任何专用连接启用或禁用本地设备自动协商。如果在 Direct Connect 连接开启时虚拟接口仍处于关闭状态，请参阅 [排查第 2 层 \(数据链路\) 问题](#)。
- 整个连接 (包括中间设备) 都必须支持 802.1Q VLAN 封装。
- 您的设备必须支持边界网关协议 (BGP) 和 B MD5 GP 身份验证。
- (可选) 您可以在网络上配置双向转发检测 (BFD)。自动为每个 Direct Connect 虚拟接口启用异步 BFD。系统会对 Direct Connect 虚拟接口自动启用，但只有在路由器上配置后才会生效。有关更多信息，请参阅 [为 Direct Connect 连接启用 BFD](#)。

在开始配置之前，请确保您具有以下信息：

- 您不创建经典连接时要使用的弹性模型。有关 AWS Direct Connect 弹性工具包的连接选项，请参阅 [AWS Direct Connect 弹性工具包](#)
- 所有连接的速度、位置和合作伙伴。

您只需要获知一个连接的速度。

AWS Direct Connect 弹性工具包

AWS 让客户能够在 Amazon Virtual Private Cloud (Amazon VPC) 与其本地基础设施之间实现高度弹性的网络连接。AWS Direct Connect 弹性工具包提供了一个包含多个弹性模型的连接向导。这些模型可帮助您确定，然后订购专用连接数量，以便满足 SLA 目标。您选择一个弹性模型，然后 Resiliency Toolkit 将指导您完成专用的连接订购流程。AWS Direct Connect 这些弹性模型旨在确保您在多个位置具有适当数量的专用连接。

AWS Direct Connect 弹性工具包具有以下优点：

- 提供有关如何依次确定和订购适当的冗余 Direct Connect 专用连接的指导。
- 确保冗余专用连接具有相同的速度。
- 自动配置专用连接名称。
- 当您拥有现有 AWS 账户并选择已知 AWS Direct Connect 合作伙伴时，会自动批准您的专用连接。授权书 (LOA) 可供即时下载。
- 当您是新 AWS 客户或选择了未知 (其他) 合作伙伴时，自动创建支持请求以获得专属连接批准。
- 提供专用连接的订单摘要，以及可实现的 SLA 与所订购专用连接的端口小时成本。

- 创建链路聚合组 (LAGs)，LAGs 当您选择 1 Gbps、10 Gbps、100 Gbps 或 400 Gbps 以外的速度时，将相应数量的专用连接添加到中。
- 提供 LAG 摘要，以及可实现的专用连接 SLA 与作为 LAG 的一部分的每个所订购专用连接的总端口小时成本。
- 防止您终止同一 Direct Connect 设备上的专用连接。
- 为您提供一种测试配置弹性的方法。您可以使用 AWS 关闭 BGP 对等会话，以验证流量是否路由到其中一个冗余虚拟接口。有关更多信息，请参阅 [the section called “Direct Connect 失效转移测试”](#)。
- 提供 Amazon 的连接和虚拟接口 CloudWatch 指标。有关更多信息，请参阅 [监控 Direct Connect 资源](#)。

选择弹性模型后，弹性工具包将引导您完成以下步骤：

- 选择专用连接的数量
- 选择连接容量和专用网络位置
- 订购专用连接
- 验证专用连接是否已可供使用
- 为每个专用连接下载授权书 (LOA-CFA)
- 验证您的配置是否满足弹性要求

可用的弹性模型

弹性工具包中提供了以下 AWS Direct Connect 弹性模型：

- 最大弹性：此模型可让您订购专用连接以实现 99.99% 的 SLA。要求您满足 [Direct Connect 服务水平协议](#) 中指定的实现 SLA 的所有要求。
- 高弹性：此模型可让您订购专用连接以实现 99.9% 的 SLA。要求您满足 [Direct Connect 服务水平协议](#) 中指定的实现 SLA 的所有要求。
- 开发和测试：此模型可让您通过使用在一个位置中的不同设备上终止的单独连接来实现非关键工作负载的开发和测试弹性。

最佳做法是使用 AWS Direct Connect 弹性工具包中的连接向导来实现您的 SLA 目标。

Note

如果您不想使用弹性工具包创建 AWS Direct Connect 弹性模型，则可以创建经典连接。有关经典连接的更多信息，请参阅 [经典连接](#)。

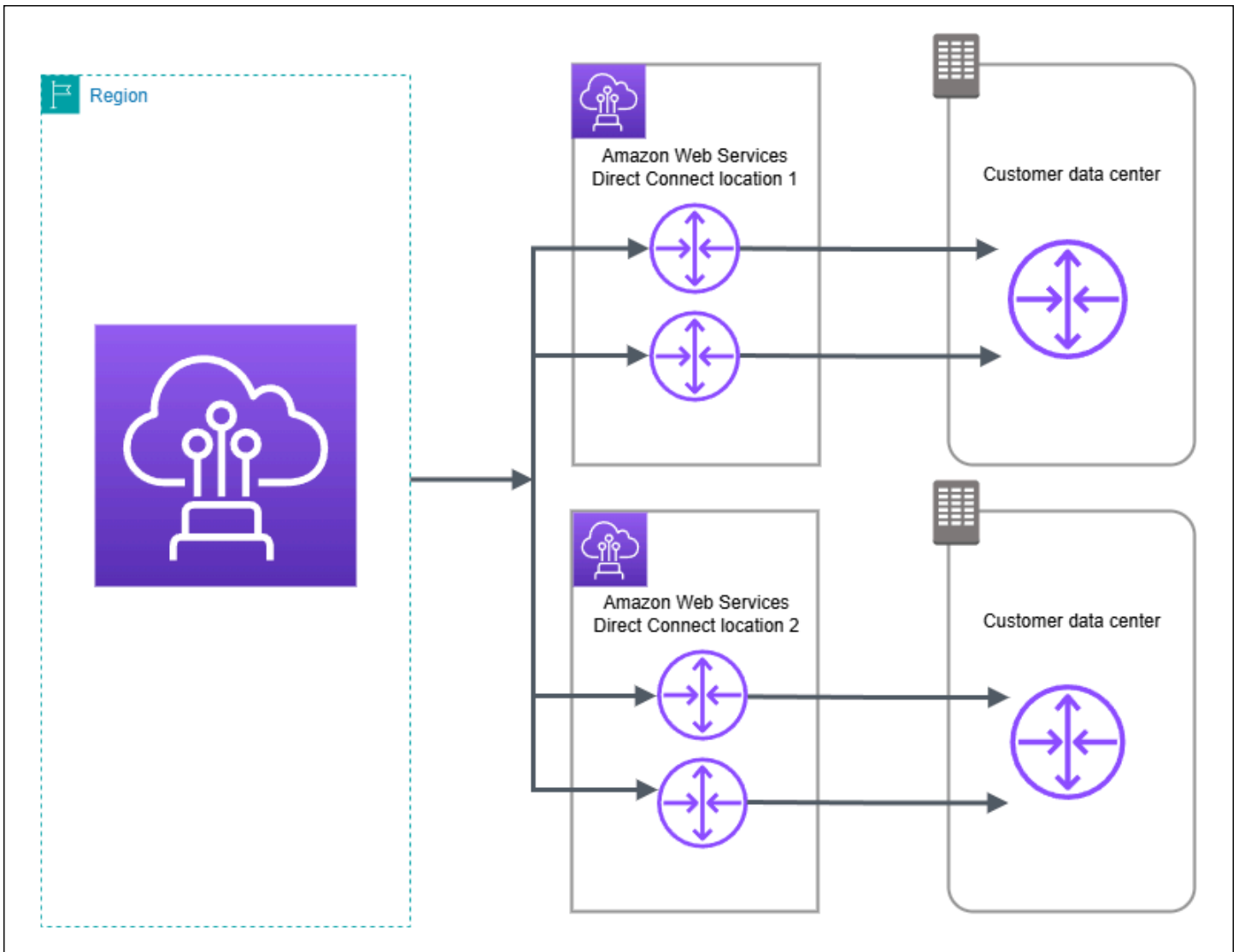
AWS Direct Connect 弹性工具包先决条件

在开始配置之前，请注意以下信息：

- 熟悉 [连接先决条件](#)。
- 要使用的可用弹性模型。

最大弹性

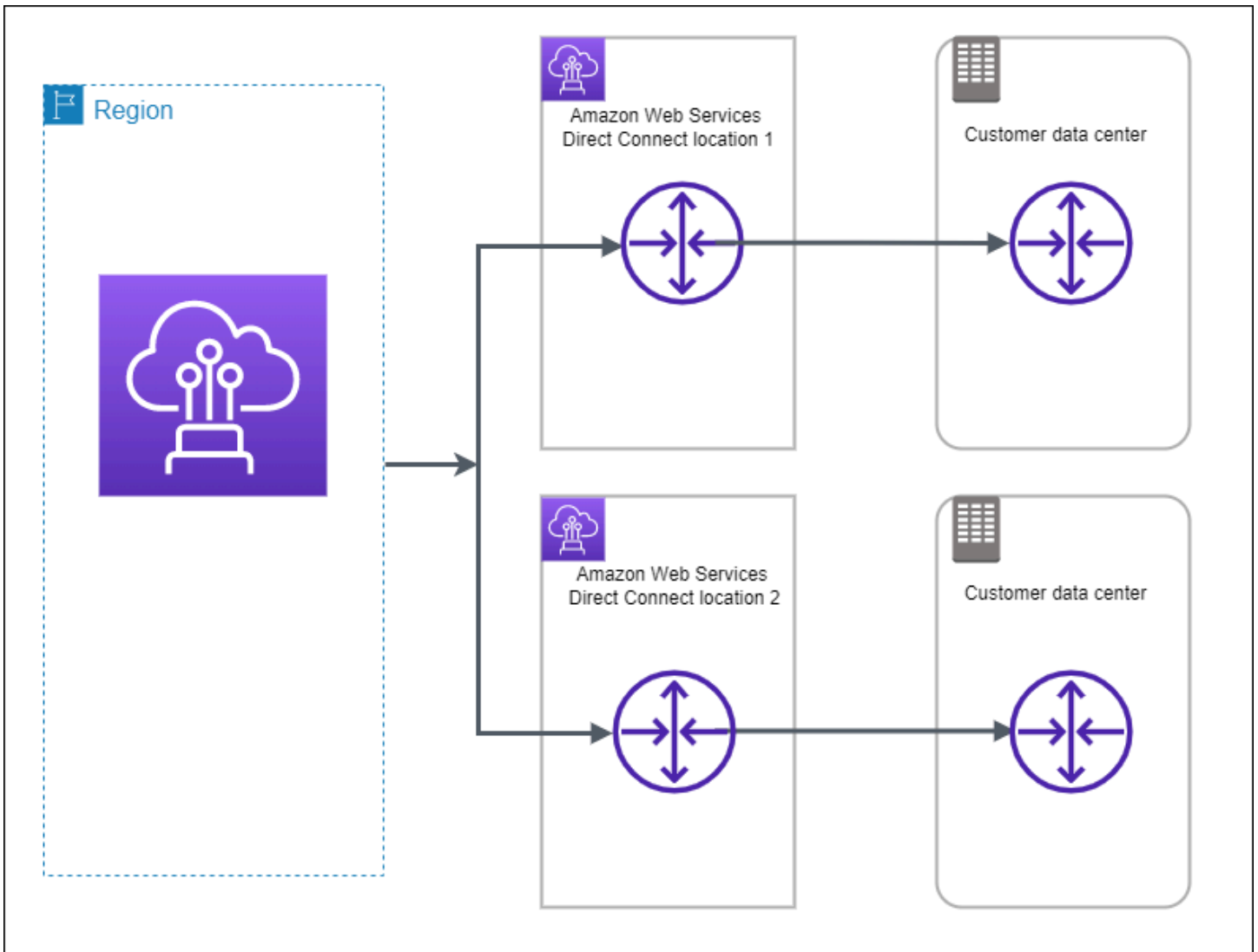
通过使用在多个位置中的不同设备上终止的不同连接，您可以实现关键工作负载的最大弹性（如下图所示）。该模型针对设备、连接性和完整位置故障均提供了弹性。下图显示了从每个客户数据中心到相同 Direct Connect 位置的两个连接。您可以选择将客户数据中心的每个连接连接到不同的位置。



有关使用弹性工具包配置最大 AWS Direct Connect 弹性模型的过程，请参阅。[最大弹性配置](#)

高弹性

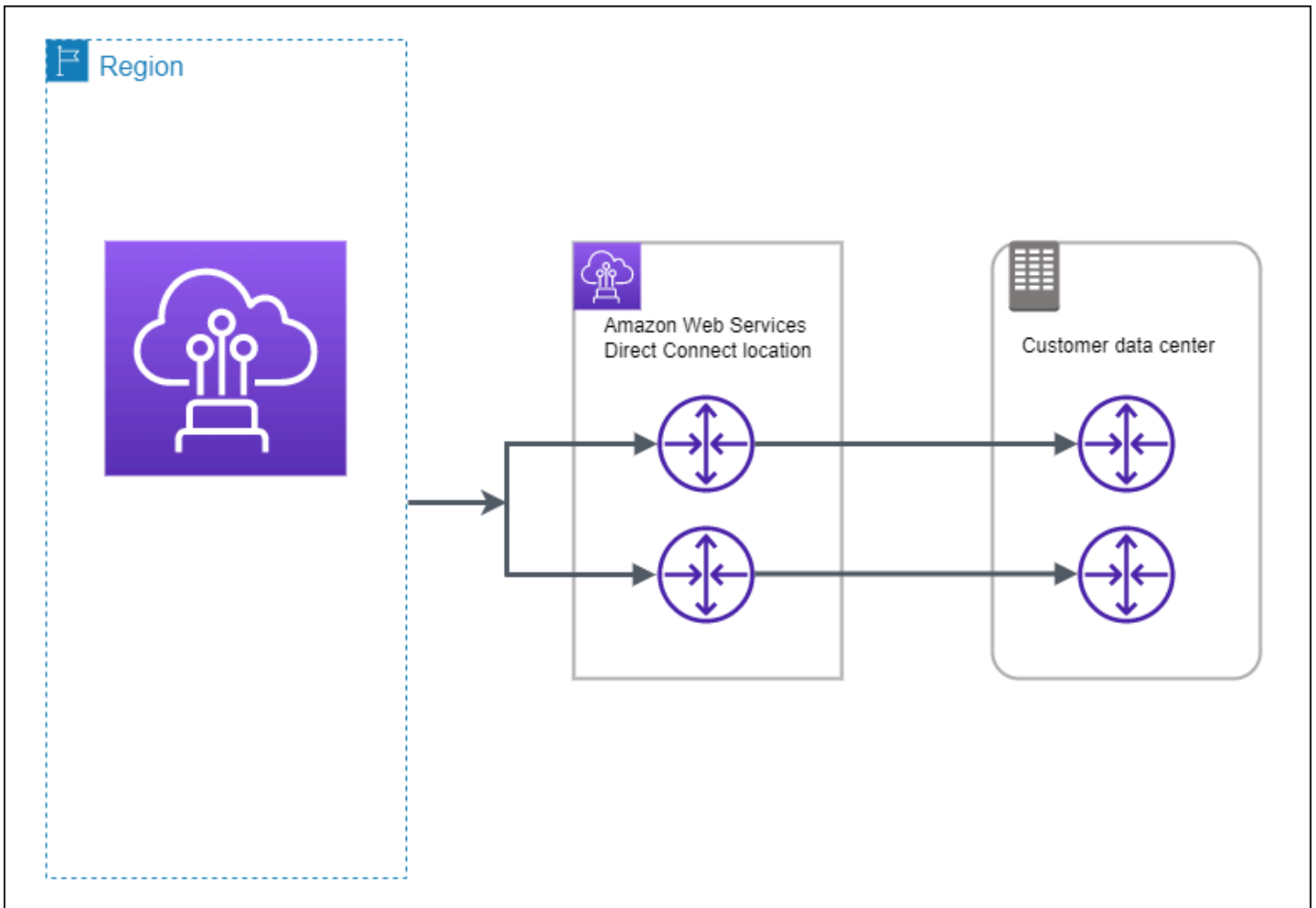
通过使用到多个位置的两个单一连接，可以为关键工作负载实现高弹性（如下图所示）。此模型可针对因光纤切断或设备故障而导致的连接故障提供弹性。它还有助于防止完整位置故障。



有关使用弹性工具包配置高 AWS Direct Connect 弹性模型的过程，请参阅 [配置高弹性](#)

开发和测试

通过使用在一个位置中的不同设备上终止的单独连接，您可以实现非关键工作负载的开发和测试弹性（如下图所示）。此模型提供了针对设备故障的弹性，但没有提供针对位置故障的弹性。



有关使用弹性工具包配置最大 AWS Direct Connect 弹性模型的过程，请参阅 [配置开发和测试弹性](#)

AWS Direct Connect FailoverTest

使用 AWS Direct Connect 弹性工具包来验证交通路线，以及这些路线是否符合您的弹性要求。

有关使用 AWS Direct Connect 弹性工具包执行故障转移测试的过程，请参阅 [Direct Connect 失效转移测试](#)。

使用弹性工具包配置 Direct Connect 以获得最大的 AWS Direct Connect 弹性

在本示例中，Direct Connect 弹性工具包用于配置最大弹性模型

任务

- [第 1 步：注册 AWS](#)

- [步骤 2：配置弹性模型](#)
- [步骤 3：创建您的虚拟接口](#)
- [步骤 4：验证您的虚拟接口弹性配置](#)
- [步骤 5：验证您的虚拟接口连接](#)

第 1 步：注册 AWS

要使用 Direct Connect，如果您还没有 AWS 帐户，则需要一个帐户。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/注册>。
2. 按照屏幕上的说明操作。

在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建 AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 <https://aws.amazon.com/> 并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS 管理控制台](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台 \)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户 [登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Create a permission set](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Add groups](#)。

步骤 2：配置弹性模型

配置最大弹性模型

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择连接，然后选择创建连接。
3. 在 Connection ordering type (连接订购类型) 下，选择 Connection wizard (连接向导)。

4. 在 Resiliency level (弹性级别) 下，选择 Maximum Resiliency (最大弹性)，然后选择 Next (下一步)。
5. 在 Configure connections (配置连接) 窗格上，在 Connection settings (连接设置) 下，执行以下操作：

- a. 对于 Bandwidth (带宽)，选择专用连接带宽。

此带宽适用于所有已创建的连接。

- b. 对于第一位置服务提供商，请为专用连接选择适当 Direct Connect 的位置。
- c. 如果适用，对于 First Sub location (第一子位置)，选择最接近您或您的网络提供商的楼层。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
- d. 如果您为第一位置服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- e. 对于第二位置服务提供商，请选择相应 Direct Connect 的地点。
- f. 如果适用，对于 Second Sub location (第二子位置)，选择最接近您或您的网络提供商的楼层。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
- g. 如果您为第二位置服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- h. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签) ，然后执行以下操作：

- 对于 Key (键) ，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

6. 选择下一步。
7. 检查您的连接，然后选择 Continue (继续)。

如果您已 LOAs 准备就绪，则可以选择“下载 LOA”，然后单击“继续”。

最多可能需要 72 个工作小时 AWS 才能审核您的请求并为您的连接配置端口。在此期间，您可能会收到一封电子邮件，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。电子邮件将发送到您注册时使用的电子邮件地址 AWS。您必须在 7 日内回复，否则将删除该连接。

步骤 3：创建您的虚拟接口

您可以创建一个私有虚拟接口来连接到您的 VPC。或者，您可以创建一个公共虚拟接口来连接不在 VPC 中的公共 AWS 服务。在创建与 VPC 的私有虚拟接口时，您需要将连接到的每个 VPC 的私有虚拟接口。例如，您需要三个私有虚拟接口才能连接到三个私有虚拟接口 VPCs。

在您开始之前，请确保您已拥有以下信息：

| 资源 | 所需信息 |
|-----------------|---|
| Connection | 您要为其创建虚拟接口的 Direct Connect 连接或链路聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 虚拟接口所有者 | 如果您要为另一个账户创建虚拟界面，则需要另一个 AWS 账户的账户 ID。 |
| (仅限私有虚拟接口) 连接 | 要连接到同一 AWS 区域的 VPC，您需要为自己的 VPC 提供虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关时，您可以指定自己的私有 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 创建虚拟私有网关 。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 | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果您有托管连接，则您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |
| 对等 IP 地址 | <p>虚拟接口可以支持 IPv4、IPv6 或其中一个 (双栈) 的 BGP 对等会话。请勿使用 Amazon 池中的 Elastic IPs (EIPs) 或自带 IP 地址 (BYOIP) 来创建公共虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> IPv4: <ul style="list-style-type: none"> (仅限公共虚拟接口) 您必须指定自己拥有的唯一公有 IPv4 地址。值可以是以下之一： <ul style="list-style-type: none"> 客户拥有 IPv4 的 CIDR |

| 资源 | 所需信息 |
|------|---|
| | <p>它们可以是任何公用 IPs（客户拥有或由提供 AWS），但是对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /31 范围，例如 203.0.113.0/31，则可以将其 203.0.113.0 用于对等 IP 和 203.0.113.1 对 AWS 等 IP。或者，如果您分配了一个 /24 范围，例如 198.51.100.0/24，则可以将其 198.51.100.10 用于对等 IP 和 198.51.100.20 对 AWS 等 IP。</p> <ul style="list-style-type: none"> 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权 AWS 提供的 /31 CIDR。联系 Support 申请公共 IPv4 CIDR（并在请求中提供用例） <div data-bbox="496 737 1507 953" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>我们不能保证我们能够满足所有关于 AWS 提供公共 IPv4 地址的请求。</p> </div> <ul style="list-style-type: none"> （仅限私有虚拟接口）Amazon 可以为您生成私有 IPv4 地址。如果您自己指定，请确保 CIDRs 为路由器接口指定私有接口，并且仅为 Direct Connect 接口指定私有接口。例如，请勿指定本地网络中的其他 IP 地址。与公共虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /30 范围，例如 192.168.0.0/30，则可以将其 192.168.0.1 用于对等 IP 和 192.168.0.2 对 AWS 等 IP。 IPv6: 亚马逊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。 |
| 地址系列 | BGP 对等会话是否会结束 IPv4 还是 IPv6 |

| 资源 | 所需信息 |
|---|---|
| <p>BGP 信息</p> <p>(仅限公有虚拟接口) 您要公布的前缀</p> | <ul style="list-style-type: none"> • 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (AS N) 。如果您使用的是公有 ASN ，则必须拥有其所有权。如果您使用的是私有 ASN ，则可以设置自定义 ASN 值。对于 16 位 ASN ，该值必须在 64512 到 65534 范围内。对于 32 位 ASN ，该值必须在 1 到 4294967294 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。 • AWS MD5 默认情况下启用。您无法修改此选项。 • MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 <p>要通过 BGP 发布的公共 IPv4 IPv6 路由或路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。</p> <ul style="list-style-type: none"> • IPv4: 当以下任一条件为真 Direct Connect 时，IPv4 CIDR IPv4 R 可以与使用宣布的另一个公共 CIDR 重叠： <ul style="list-style-type: none"> • CIDRs 他们来自不同 AWS 的地区。确保在公有前缀上应用 BGP 社区标签。 • 如果配置中有公用 ASN ，则可以使用 AS_PATH。 active/passive <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> • 通过 Direct Connect 公共虚拟接口，您可以为其指定从 /1 到 /32 以及从 /1 到 /6 IPv4 之间的任意前缀长度。 IPv6 • 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |
| <p>(仅限私有和中转虚拟接口) 巨型帧</p> | <p>数据包的最大传输单位 (MTU)。 Direct Connect 默认为 1500。将虚拟接口的 MTU 设置为 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。巨型帧仅适用于来自的传播路由。 Direct Connect 如果在路由表中添加指向虚拟私有网关的静态路由，则通过静态路由传输的流量将使用 1500 MTU 发送。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口“常规配置”页面上找到支持巨型帧。</p> |

如果您的公共前缀或 ASNs 属于互联网服务提供商或网络运营商，我们会要求您提供更多信息。这可以是使用公司官方信头的文档，也可以是来自公司域名的电子邮件，确认 prefix/ASN 您可以使用该网络。

创建公共虚拟接口时，最多可能需要 72 个工作小时 AWS 才能审核和批准您的请求。

配置与非 VPC 服务间的公有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。
5. 在 Public virtual interface settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - d. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在 Additional settings (其他设置) 下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。
 - b. 要提供自己的 BGP 密钥，请输入您的 BGP MD5 密钥。

如果您不输入值，我们将生成一个 BGP 密钥。

- c. 要向 Amazon 宣传前缀，对于要宣传的前缀，请输入应通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址（用逗号分隔）。
- d. （可选）添加或删除标签。

[添加标签] 选择 Add tag（添加标签），然后执行以下操作：

- 对于 Key（键），输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface（创建虚拟接口）。

配置与 VPC 间的私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface（创建虚拟接口）。
4. 在虚拟接口类型下，对于类型，选择私有。
5. 在私有虚拟接口设置下，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 Connection（连接），选择要用于此接口的 Direct Connect 连接。
 - c. 对于网关类型，选择虚拟私有网关或 Direct Connect 网关。
 - d. 对于虚拟接口所有者，选择其他 AWS 帐户，然后输入该 AWS 帐户。
 - e. 对于虚拟私有网关，选择要用于此接口的虚拟私有网关。
 - f. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - g. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs（1-2147483647）和多头（1-4294967294）。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。 AWS

⚠ Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。 IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接地址。 point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 9001 (巨型帧)，请选择巨型帧 MTU (MTU 大小 9001)。
- (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。
- (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

步骤 4：验证您的虚拟接口弹性配置

建立通往 AWS 云或 Amazon VPC 的虚拟接口后，请执行虚拟接口故障转移测试，以验证您的配置是否符合您的弹性要求。有关更多信息，请参阅 [the section called “Direct Connect 失效转移测试”](#)。

步骤 5：验证您的虚拟接口连接

建立与 AWS 云或 Amazon VPC 的虚拟接口后，您可以使用以下步骤验证您的 AWS Direct Connect 连接。

验证您的虚拟接口与 AWS 云端的连接

- 运行 `tracert` 并验证标 Direct Connect 标识符是否在网络跟踪中。

要验证您的虚拟接口是否连接到 Amazon VPC

1. 使用可执行 ping 操作的 AMI（比如 Amazon Linux AMI），在连接到虚拟私有网关的 VPC 中启动 EC2 实例。当您在亚马逊 EC2 控制台使用实例启动向导时，Amazon Linux AMIs 可在快速入门选项卡中找到。有关更多信息，请参阅《Amazon EC2 用户指南》中的[启动实例](#)。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 地址并获得回复。

使用弹性工具包配置 Direct Connect 以实现高 AWS Direct Connect 弹性

在本示例中，Direct Connect 弹性工具包用于配置高弹性模型

任务

- [第 1 步：注册 AWS](#)
- [步骤 2：配置弹性模型](#)
- [步骤 3：创建您的虚拟接口](#)
- [步骤 4：验证您的虚拟接口弹性配置](#)
- [步骤 5：验证您的虚拟接口连接](#)

第 1 步：注册 AWS

要使用 Direct Connect，如果您还没有 AWS 帐户，则需要一个帐户。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/>注册。
2. 按照屏幕上的说明操作。

在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 <https://aws.amazon.com/> 并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS 管理控制台](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台 \)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Create a permission set](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Add groups](#)。

步骤 2：配置弹性模型

配置高弹性模型

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择连接，然后选择创建连接。
3. 在 Connection ordering type (连接订购类型) 下，选择 Connection wizard (连接向导)。
4. 在 Resiliency level (弹性级别) 下，选择 High Resiliency (高弹性)，然后选择 Next (下一步)。
5. 在 Configure connections (配置连接) 窗格上，在 Connection settings (连接设置) 下，执行以下操作：

- a. 对于 bandwidth (带宽)，选择连接带宽。

此带宽适用于所有已创建的连接。

- b. 对于第一位置服务提供商，请选择相应 Direct Connect 的地点。
- c. 如果适用，对于 First Sub location (第一子位置)，选择最接近您或您的网络提供商的楼层。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
- d. 如果您为第一位置服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- e. 对于第二位置服务提供商，请选择相应 Direct Connect 的地点。

- f. 如果适用，对于 Second Sub location (第二子位置)，选择最接近您或您的网络提供商的楼层。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
- g. 如果您为第二位置服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- h. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

6. 选择下一步。
7. 检查您的连接，然后选择 Continue (继续)。

如果您已 LOAs 准备就绪，则可以选择“下载 LOA”，然后单击“继续”。

最多可能需要 72 个工作小时 AWS 才能审核您的请求并为您的连接配置端口。在此期间，您可能会收到一封电子邮件，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。电子邮件将发送到您注册时使用的电子邮件地址 AWS。您必须在 7 日内回复，否则将删除该连接。


步骤 3：创建您的虚拟接口

您可以创建一个私有虚拟接口来连接到您的 VPC。或者，您可以创建一个公共虚拟接口来连接不在 VPC 中的公共 AWS 服务。在创建与 VPC 的私有虚拟接口时，您需要将连接到的每个 VPC 的私有虚拟接口。例如，您需要三个私有虚拟接口才能连接到三个私有虚拟接口 VPCs。

在您开始之前，请确保您已拥有以下信息：

| 资源 | 所需信息 |
|-----------------|---|
| Connection | 您要为其创建虚拟接口的 Direct Connect 连接或链路聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 虚拟接口所有者 | 如果您要为另一个账户创建虚拟界面，则需要另一个 AWS 账户的账户 ID。 |
| (仅限私有虚拟接口) 连接 | 要连接到同一 AWS 区域的 VPC，您需要为自己的 VPC 提供虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关 |

| 资源 | 所需信息 |
|------|--|
| | <p>时，您可以指定自己的私有 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》中的创建虚拟私有网关。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。</p> |
| VLAN | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果您有托管连接，则您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |

| 资源 | 所需信息 |
|----------|---|
| 对等 IP 地址 | <p>虚拟接口可以支持 IPv4、IPv6 或其中一个（双栈）的 BGP 对等会话。请勿使用 Amazon 池中的 Elastic IPs (EIPs) 或自带 IP 地址 (BYOIP) 来创建公共虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> IPv4: <ul style="list-style-type: none"> （仅限公共虚拟接口）您必须指定自己拥有的唯一公有 IPv4 地址。值可以是以下之一： <ul style="list-style-type: none"> 客户拥有 IPv4 的 CIDR <p>它们可以是任何公用 IPs（客户拥有或由提供 AWS），但是对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /31 范围，例如 203.0.113.0/31，则可以将其 203.0.113.0 用于对等 IP 和 203.0.113.1 对 AWS 等 IP。或者，如果您分配了一个 /24 范围，例如 198.51.100.0/24，则可以将其 198.51.100.10 用于对等 IP 和 198.51.100.20 对 AWS 等 IP。</p> 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权 AWS 提供的 /31 CIDR。联系 Su AWS support 申请公共 IPv4 CIDR（并在请求中提供用例） <div data-bbox="496 1220 1507 1436" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>我们不能保证我们能够满足所有关于 AWS 提供公共 IPv4 地址的请求。</p> </div> <ul style="list-style-type: none"> （仅限私有虚拟接口）Amazon 可以为您生成私有 IPv4 地址。如果您自己指定，请确保 CIDRs 为路由器接口指定私有接口，并且仅为 Direct Connect 接口指定私有接口。例如，请勿指定本地网络中的其他 IP 地址。与公共虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /30 范围，例如 192.168.0.0/30，则可以将其 192.168.0.1 用于对等 IP 和 192.168.0.2 对 AWS 等 IP。 |

| 资源 | 所需信息 |
|----------------------|---|
| | <ul style="list-style-type: none"> IPv6: 亚马逊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。 |
| 地址系列 | BGP 对等会话是否会结束 IPv4 还是 IPv6 |
| BGP 信息 | <ul style="list-style-type: none"> 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (AS N)。如果您使用的是公有 ASN，则必须拥有其所有权。如果您使用的是私有 ASN，则可以设置自定义 ASN 值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 1 到 4294967294 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。 AWS MD5 默认情况下启用。您无法修改此选项。 MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 |
| (仅限公有虚拟接口) 您要公布的前缀 | <p>要通过 BGP 发布的公共 IPv4 IPv6 路由或路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。</p> <ul style="list-style-type: none"> IPv4: 当以下任一条件为真 Direct Connect 时，IPv4 CIDR IPv4 R 可以与使用宣布的另一个公共 CIDR 重叠： <ul style="list-style-type: none"> CIDRs 他们来自不同 AWS 的地区。确保在公有前缀上应用 BGP 社区标签。 如果配置中有公用 ASN，则可以使用 AS_PATH。 active/passive <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> 通过 Direct Connect 公共虚拟接口，您可以为其指定从 /1 到 /32 以及从 /1 到 /6 IPv4 之间的任意前缀长度。 IPv6 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |

| 资源 | 所需信息 |
|---------------------|---|
| (仅限私有和中转虚拟接口) 巨型帧 | 数据包的最大传输单位 (MTU)。Direct Connect默认为 1500。将虚拟接口的 MTU 设置为 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。巨型帧仅适用于来自的传播路由。Direct Connect如果在路由表中添加指向虚拟私有网关的静态路由，则通过静态路由传输的流量将使用 1500 MTU 发送。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口“常规配置”页面上找到支持巨型帧。 |

如果您的公共前缀或 ASNs 属于互联网服务提供商或网络运营商，AWS 请您提供更多信息。这可以是使用公司官方信头的文档，也可以是来自公司域名的电子邮件，确认 prefix/ASN 您可以使用该网络。

创建公共虚拟接口时，最多可能需要 72 个工作小时 AWS 才能审核和批准您的请求。

配置与非 VPC 服务间的公有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。
5. 在 Public virtual interface settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - d. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在 Additional settings (其他设置) 下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。 AWS

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要提供自己的 BGP 密钥，请输入您的 BGP MD5 密钥。

如果您不输入值，我们将生成一个 BGP 密钥。

- c. 要向 Amazon 宣传前缀，对于要宣传的前缀，请输入应通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址（用逗号分隔）。
- d. （可选）添加或删除标签。

[添加标签] 选择 Add tag（添加标签），然后执行以下操作：

- 对于 Key（键），输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface（创建虚拟接口）。

配置与 VPC 间的私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface（创建虚拟接口）。
4. 在虚拟接口类型下，对于类型，选择私有。
5. 在私有虚拟接口设置下，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 Connection（连接），选择要用于此接口的 Direct Connect 连接。
 - c. 对于网关类型，选择虚拟私有网关或 Direct Connect 网关。
 - d. 对于虚拟接口所有者，选择其他 AWS 帐户，然后输入该 AWS 帐户。
 - e. 对于虚拟私有网关，选择要用于此接口的虚拟私有网关。
 - f. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - g. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。


有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：

a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

 Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接地址。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 9001 (巨型帧)，请选择巨型帧 MTU (MTU 大小 9001)。

c. (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。

d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

步骤 4：验证您的虚拟接口弹性配置

建立通往 AWS 云或 Amazon VPC 的虚拟接口后，请执行虚拟接口故障转移测试，以验证您的配置是否符合您的弹性要求。有关更多信息，请参阅 [the section called “Direct Connect 失效转移测试”](#)。

步骤 5：验证您的虚拟接口连接

建立与 AWS 云或 Amazon VPC 的虚拟接口后，您可以使用以下步骤验证您的 AWS Direct Connect 连接。

验证您的虚拟接口与 AWS 云端的连接

- 运行 traceroute 并验证标 Direct Connect 识符是否在网络跟踪中。

要验证您的虚拟接口是否连接到 Amazon VPC

1. 使用可执行 ping 操作的 AMI (比如 Amazon Linux AMI) ，在连接到虚拟私有网关的 VPC 中启动 EC2 实例。当您在亚马逊 EC2 控制台中使用实例启动向导时，Amazon Linux AMIs 可在快速入门选项卡中找到。有关更多信息，请参阅《Amazon EC2 用户指南》中的 [启动实例](#)。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 地址并获得回复。

使用弹 AWS Direct Connect 性工具包配置开发和测试 AWS Direct Connect 弹性

在此示例中，Direct Connect 弹性工具包用于配置开发和测试弹性模型

任务

- [第 1 步：注册 AWS](#)
- [步骤 2：配置弹性模型](#)

- [步骤 3：创建虚拟接口](#)
- [步骤 4：验证您的虚拟接口弹性配置](#)
- [步骤 5：验证您的虚拟接口](#)

第 1 步：注册 AWS

要使用 Direct Connect，如果您还没有 AWS 帐户，则需要一个帐户。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/注册>。
2. 按照屏幕上的说明操作。

在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建 AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 <https://aws.amazon.com/> 并选择“我的账户”，查看当前账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS 管理控制台](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA) 。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户 \(控制台\) 启用虚拟 MFA 设备](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》IAM Identity Center 目录中的[使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Create a permission set](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Add groups](#)。

步骤 2：配置弹性模型

配置弹性模型

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择连接，然后选择创建连接。
3. 在 Connection ordering type (连接订购类型) 下，选择 Connection wizard (连接向导)。

4. 在 Resiliency level (弹性级别) 下，选择 Development and test (开发和测试)，然后选择 Next (下一步)。
5. 在 Configure connections (配置连接) 窗格上，在 Connection settings (连接设置) 下，执行以下操作：

- a. 对于 bandwidth (带宽)，选择连接带宽。

此带宽适用于所有已创建的连接。

- b. 对于第一定位服务提供商，请选择相应 Direct Connect 的地点。
- c. 如果适用，对于 First Sub location (第一子位置)，选择最接近您或您的网络提供商的楼层。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
- d. 如果您为第一位置服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- e. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

6. 选择下一步。
7. 检查您的连接，然后选择 Continue (继续)。

如果您已 LOAs 准备就绪，则可以选择“下载 LOA”，然后单击“继续”。

最多可能需要 72 个工作小时 AWS 才能审核您的请求并为您的连接配置端口。在此期间，您可能会收到一封电子邮件，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。电子邮件将发送到您注册时使用的电子邮件地址 AWS。您必须在 7 日内回复，否则将删除该连接。

步骤 3：创建虚拟接口

要开始使用您的 Direct Connect 连接，必须创建一个虚拟接口。您可以创建一个私有虚拟接口来连接到您的 VPC。或者，您可以创建一个公共虚拟接口来连接不在 VPC 中的公共 AWS 服务。在创建与 VPC 的私有虚拟接口时，您需要将连接到的每个 VPC 的私有虚拟接口。例如，您需要三个私有虚拟接口才能连接到三个私有虚拟接口 VPCs。

在您开始之前，请确保您已拥有以下信息：

| 资源 | 所需信息 |
|-----------------|--|
| Connection | 您要为其创建虚拟接口的 Direct Connect 连接或链路聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 虚拟接口所有者 | 如果您要为另一个账户创建虚拟界面，则需要另一个 AWS 账户的账户 ID。 |
| (仅限私有虚拟接口) 连接 | 要连接到同一 AWS 区域的 VPC，您需要为自己的 VPC 提供虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关时，您可以指定自己的私有 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 创建虚拟私有网关 。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 | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果您有托管连接，则您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |
| 对等 IP 地址 | <p>虚拟接口可以支持 IPv4、IPv6 或其中一个 (双栈) 的 BGP 对等会话。请勿使用 Amazon 池中的 Elastic IPs (EIPs) 或自带 IP 地址 (BYOIP) 来创建公共虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> • IPv4: <ul style="list-style-type: none"> • (仅限公共虚拟接口) 您必须指定自己拥有的唯一公有 IPv4 地址。值可以是以下之一： <ul style="list-style-type: none"> • 客户拥有 IPv4 的 CIDR <p>它们可以是任何公用 IPs (客户拥有或由提供 AWS)，但是对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /31 范围，例如 203.0.113.0/31，则可以将其 203.0.113.0 用于对等 IP 和 203.0.113.1 对 AWS 等 IP。或者，如果您分配了一个 /24 范围，例如 198.51.100.0/24，则可以将其 198.51.100.10 用于对等 IP 和 198.51.100.20 对 AWS 等 IP。</p> |

| 资源 | 所需信息 |
|--------|---|
| | <ul style="list-style-type: none"> • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权 • AWS提供的 /31 CIDR。联系 Support 申请公共 IPv4 CIDR (并在请求中提供用例) <div data-bbox="496 443 1507 659" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>我们不能保证我们能够满足所有关于 AWS提供公共 IPv4 地址的请求。</p> </div> <ul style="list-style-type: none"> • (仅限私有虚拟接口) Amazon 可以为您生成私有 IPv4 地址。如果您自己指定，请确保 CIDRs 为路由器接口指定私有接口，并且仅为 Direct Connect 接口指定私有接口。例如，请勿指定本地网络中的其他 IP 地址。与公共虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /30 范围，例如 192.168.0.0/30，则可以将其 192.168.0.1 用于对等 IP 和 192.168.0.2 对 AWS 等 IP。 • IPv6: 亚马逊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。 |
| 地址系列 | BGP 对等会话是否会结束 IPv4 还是 IPv6 |
| BGP 信息 | <ul style="list-style-type: none"> • 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (ASN)。如果您使用的是公有 ASN，则必须拥有其所有权。如果您使用的是私有 ASN，则可以设置自定义 ASN 值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 1 到 4294967294 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。 • AWS MD5 默认情况下启用。您无法修改此选项。 • MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 |

| 资源 | 所需信息 |
|----------------------|---|
| (仅限公有虚拟接口) 您要公布的前缀 | <p>要通过 BGP 发布的公共 IPv4 IPv6 路由或路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。</p> <ul style="list-style-type: none"> IPv4: 当以下任一条件为真 Direct Connect 时，IPv4 CIDR IPv4 R 可以与使用宣布的另一个公共 CIDR 重叠： <ul style="list-style-type: none"> CIDRs 他们来自不同 AWS 的地区。确保在公有前缀上应用 BGP 社区标签。 如果配置中有公用 ASN，则可以使用 AS_PATH。 active/passive <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> 通过 Direct Connect 公共虚拟接口，您可以为其指定从 /1 到 /32 以及从 /1 到 /6 IPv4 4 之间的任意前缀长度。 IPv6 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |
| (仅限私有和中转虚拟接口) 巨型帧 | <p>数据包的最大传输单位 (MTU)。 Direct Connect默认为 1500。将虚拟接口的 MTU 设置为 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。巨型帧仅适用于来自的传播路由。 Direct Connect如果在路由表中添加指向虚拟私有网关的静态路由，则通过静态路由传输的流量将使用 1500 MTU 发送。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口“常规配置”页面上找到支持巨型帧。</p> |

如果您的公共前缀或 ASNs 属于互联网服务提供商或网络运营商，我们会要求您提供更多信息。这可以是使用公司官方信头的文档，也可以是来自公司域名的电子邮件，确认 prefix/ASN 您可以使用该网络。

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

配置与非 VPC 服务间的公有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。

3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。
5. 在 Public virtual interface settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - d. 对于 BGP ASN，输入您网关的边界网关协议 (BGP) 自治系统编号 (ASN)。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在 Additional settings (其他设置) 下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要提供自己的 BGP 密钥，请输入您的 BGP MD5 密钥。

如果您不输入值，我们将生成一个 BGP 密钥。

- c. 要向 Amazon 宣传前缀，对于要宣传的前缀，请输入应通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号分隔)。
- d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

配置与 VPC 间的私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在虚拟接口类型下，对于类型，选择私有。
5. 在私有虚拟接口设置下，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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于网关类型，选择虚拟私有网关或 Direct Connect 网关。
 - d. 对于虚拟接口所有者，选择其他 AWS 账户，然后输入 AWS 账户。
 - e. 对于虚拟私有网关，选择要用于此接口的虚拟私有网关。
 - f. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - g. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

Important

配置 Di AWS rect Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit

Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 9001 (巨型帧)，请选择巨型帧 MTU (MTU 大小 9001)。
- (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。
- (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

- 选择 Create virtual interface (创建虚拟接口)。

步骤 4：验证您的虚拟接口弹性配置

建立通往 AWS 云或 Amazon VPC 的虚拟接口后，请执行虚拟接口故障转移测试，以验证您的配置是否符合您的弹性要求。有关更多信息，请参阅 [the section called “Direct Connect 失效转移测试”](#)。

步骤 5：验证您的虚拟接口

建立与 AWS 云或 Amazon VPC 的虚拟接口后，您可以使用以下步骤验证您的 AWS Direct Connect 连接。

验证您的虚拟接口与 AWS 云端的连接

- 运行 traceroute 并验证标 Direct Connect 识符是否在网络跟踪中。

要验证您的虚拟接口是否连接到 Amazon VPC

- 使用可执行 ping 操作的 AMI (比如 Amazon Linux AMI)，在连接到虚拟私有网关的 VPC 中启动 EC2 实例。当您在亚马逊 EC2 控制台中使用实例启动向导时，Amazon Linux AMIs 可在快速入门

选项卡中找到。有关更多信息，请参阅《Amazon EC2 用户指南》中的[启动实例](#)。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 地址并获得回复。

Direct Connect 故障转移测试

AWS Direct Connect 弹性工具包弹性模型旨在确保您在多个位置拥有适当数量的虚拟接口连接。完成向导后，使用 AWS Direct Connect 弹性工具包失效转移测试关闭 BGP 对等会话，以便验证流量是否路由到其中一个冗余虚拟接口，并满足您的弹性要求。

使用测试确保在虚拟接口停止服务时，可通过冗余虚拟接口路由流量。可以通过选择虚拟接口、BGP 对等会话以及运行测试的时间来启动测试。AWS 将所选虚拟接口 BGP 对等会话置于关闭状态。当接口处于此状态时，流量应该通过冗余虚拟接口路由。如果您的配置不包含适当的冗余连接，则 BGP 对等会话将会失败，并且不会路由流量。当测试完成后，或者您手动停止测试时，AWS 将恢复 BGP 会话。测试完成后，可以使用 AWS Direct Connect 弹性工具包调整您的配置。

Note

请勿在 Direct Connect 维护期间使用此功能，因为在维护期间或维护之后，BGP 会话可能会提早恢复。

测试历史记录

AWS 将在 365 天后删除测试历史记录。测试历史记录包括在所有 BGP 对等上运行的测试的状态。历史记录包括测试了哪些 BGP 对等会话、开始和结束时间以及测试状态，可以是以下任意值：

- 正在进行中 - 测试当前正在运行。
- 已完成 - 测试已在您指定的时间内运行。
- 已取消 - 测试已在指定时间之前取消。
- 失败 - 测试未在您指定的时间运行。当路由器出现问题时，会发生这种情况。

有关更多信息，请参阅 [the section called “查看虚拟接口失效转移测试历史记录”](#)。

验证权限

具有故障转移测试运行权限的唯一账户是拥有虚拟接口的账户。账户所有者通过 AWS CloudTrail 接收已在虚拟接口上运行测试的指示。

主题

- [开始 AWS Direct Connect 弹性工具包虚拟接口故障转移测试](#)
- [查看 AWS Direct Connect 弹性工具包虚拟接口故障转移测试历史记录](#)
- [停止 AWS Direct Connect 弹性工具包虚拟接口故障转移测试](#)

开始 AWS Direct Connect 弹性工具包虚拟接口故障转移测试

您可以使用 Direct Connect 控制台或启动虚拟接口故障切换测试 AWS CLI。

从 Direct Connect 控制台启动虚拟接口故障切换测试

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 选择虚拟接口。
3. 选择虚拟接口，然后依次选择操作、关闭 BGP。

可以在公有、私有或传输虚拟接口上运行测试。

4. 在开始故障测试对话框中，执行以下操作：
 - a. 例如，要将 Peerings 归结为测试，请选择要测试的对等互连会话。IPv4
 - b. 在测试时间上限中，输入测试将会持续的分钟数。

最大值为 4320 分钟 (72 工作小时)。

默认值为 180 分钟 (3 小时)。

- c. 对于 To confirm test (确认测试)，请输入确认。
- d. 选择确认。

BGP 对等会话将置于“关闭”状态。您可以发送流量以便验证是否出现中断情况。如果需要，您可以立即停止测试。

要启动虚拟接口故障切换测试，请使用 AWS CLI

使用 [StartBgpFailoverTest](#)。

查看 AWS Direct Connect 弹性工具包虚拟接口故障转移测试历史记录

您可以使用 Direct Connect 控制台或查看虚拟接口故障切换测试历史记录 AWS CLI。

从 Direct Connect 控制台查看虚拟接口故障切换测试历史记录

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 选择虚拟接口。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。
4. 选择测试历史记录。

控制台显示您已为虚拟接口执行的虚拟接口测试。

5. 要查看特定测试的详细信息，请选择测试 ID。

要查看虚拟接口故障切换测试历史记录，请使用 AWS CLI

使用 [ListVirtualInterfaceTestHistory](#)。

停止 AWS Direct Connect 弹性工具包虚拟接口故障转移测试

您可以使用 Direct Connect 控制台停止虚拟接口故障切换测试，或者 AWS CLI。

从 Direct Connect 控制台停止虚拟接口故障切换测试

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 选择虚拟接口。
3. 选择虚拟接口，然后依次选择操作、取消测试。
4. 选择确认。

AWS 恢复 BGP 对等会话。测试历史记录将显示“已取消”测试。

要停止虚拟接口故障切换测试，请使用 AWS CLI

使用 [StopBgpFailoverTest](#)。

Direct Connect 经典连接

经典连接提供了一种简单方法在本地基础设施和 AWS 之间建立专用网络连接。这种连接类型非常适合希望管理自己的网络配置并拥有现有 Direct Connect 基础设施的组织。经典连接不依赖于 AWS Direct Connect 弹性工具包。

如果您已有连接并且想要添加额外连接，请选择“经典”。经典连接的 SLA 为 95%。但是，它不提供弹性或冗余，这只能在创建连接时在 AWS Direct Connect 弹性工具包中找到。

Note

在配置经典连接之前，请熟悉 [连接先决条件](#)。

任务

- [配置 Direct Connect 经典连接](#)

配置 Direct Connect 经典连接

如果您已有 Direct Connect 连接，请配置 Classic 连接。

第 1 步：注册 AWS

要使用 Direct Connect，如果您还没有帐户，则需要一个帐户。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/>注册。
2. 按照屏幕上的说明操作。

在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建 AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 <https://aws.amazon.com/> 并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS 管理控制台](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台 \)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Enabling. AWS IAM Identity Center](#)

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Create a permission set](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Add groups](#)。

步骤 2：申请 Direct Connect 专用连接

对于专用连接，您可以使用 Direct Connect 控制台提交连接请求。对于托管连接，请与 AWS Direct Connect 合作伙伴合作申请托管连接。确保您具有以下信息：

- 您需要的端口速度。在您创建连接请求之后，将无法更改端口速度。
- 连接的终止 Direct Connect 位置。

Note

您不能使用 Direct Connect 控制台请求托管连接。相反，请联系 AWS Direct Connect 合作伙伴，合作伙伴可以为您创建托管连接，然后您接受该连接。请跳过以下步骤并转至[接受托管连接](#)。

创建新 Direct Connect 连接

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择连接，然后选择创建连接。
3. 选择 Classic。
4. 在 Create Connection (创建连接) 窗格上，在 Connection settings (连接设置) 下，执行以下操作：
 - a. 对于 Name (名称)，输入连接的名称。
 - b. 对于 Location (位置)，选择适当的 Direct Connect 位置。
 - c. 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。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
 - d. 对于 Port Speed (端口速度)，选择连接带宽。

- e. 对于本地，当您使用此连接连接到您的数据中心时，请选择“通过 Direct Connect 合作伙伴连接”。
- f. 对于服务提供商，请选择 AWS Direct Connect 合作伙伴。如果您使用的合作伙伴不在列表中，请选择 Other (其他)。
- g. 如果您为服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
- h. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

5. 选择创建连接。

最多可能需要 72 个工作小时 AWS 才能审核您的请求并为您的连接配置端口。在此期间，您可能会收到一封电子邮件，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。电子邮件将发送到您注册时使用的电子邮件地址 AWS。您必须在 7 日内回复，否则将删除该连接。

有关更多信息，请参阅 [Direct Connect 专用连接和托管连接](#)。

接受托管连接

必须先在 Direct Connect 控制台中接受托管连接，然后才能创建虚拟接口。此步骤仅适用于托管连接。

如何接受托管虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择托管连接，然后选择接受。

选择 Accept (接受)。

(专用连接) 步骤 3 : 下载 LOA-CFA

在您请求连接后，我们会向您提供授权证书和连接设备分配 (LOA-CFA) 供您下载，或通过电子邮件向您请求更多信息。LOA-CFA 是连接的授权 AWS，托管提供商或您的网络提供商需要它才能建立跨网络连接 (交叉连接)。

下载 LOA-CFA

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择连接，然后选择 View Details (查看详细信息)。
4. 选择下载 LOA-CFA。

LOA-CFA 以 PDF 文件格式下载到您的计算机中。

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消息。如果仍不可用，或者您在 72 工作小时后仍未收到电子邮件，请联系 [AWS 支持](#)。

5. 在您下载 LOA-CFA 以后，执行以下操作之一：
 - 如果您正在与 AWS Direct Connect 合作伙伴或网络提供商合作，请向他们发送 LOA-CFA，以便他们可以在该地点为您订购交叉连接。Direct Connect 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](#)。
 - 如果您在该 Direct Connect 地点有设备，请联系托管服务提供商申请跨网络连接。您必须为托管供应商的客户。您还必须向他们出示授权连接 AWS 路由器的 LOA-CFA 以及连接到您的网络所需的必要信息。

Direct Connect 列为多个站点 (例如 Equinix DC1-DC6 和 DC10-DC11) 的地点被设置为校园。如果您或您的网络提供商的设备位于其中任一站点中，您可以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

校园被视为单一 Direct Connect 地点。要实现高可用性，请配置与不同 Direct Connect 位置的连接。


如果您或您的网络提供商在建立物理连接时遇到问题，请参阅[排查第 1 层（物理）问题](#)。

步骤 4：创建虚拟接口

要开始使用您的 Direct Connect 连接，必须创建一个虚拟接口。您可以创建一个私有虚拟接口来连接到您的 VPC。或者，您可以创建一个公共虚拟接口来连接不在 VPC 中的公共 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 的私有虚拟接口。例如，您需要三个私有虚拟接口才能连接到三个 VPCs。

在您开始之前，请确保您已拥有以下信息：

| 资源 | 所需信息 |
|-----------------|---|
| Connection | 您要为其创建虚拟接口的 Direct Connect 连接或链路聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 虚拟接口所有者 | 如果您要为另一个账户创建虚拟界面，则需要另一个 AWS 账户的账户 ID。 |
| (仅限私有虚拟接口) 连接 | 要连接到同一 AWS 区域的 VPC，您需要为自己的 VPC 提供虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关时，您可以指定自己的私有 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 创建虚拟私有网关 。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 | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果您有托管连接，则您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |

| 资源 | 所需信息 |
|----------|--|
| 对等 IP 地址 | <p>虚拟接口可以支持 IPv4、IPv6 或其中一个（双栈）的 BGP 对等会话。请勿使用 Amazon 池中的 Elastic IPs (EIPs) 或自带 IP 地址 (BYOIP) 来创建公共虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> IPv4: <ul style="list-style-type: none"> （仅限公共虚拟接口）您必须指定自己拥有的唯一公有 IPv4 地址。值可以是以下之一： <ul style="list-style-type: none"> 客户拥有 IPv4 的 CIDR <p>它们可以是任何公用 IPs（客户拥有或由提供 AWS），但是对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /31 范围，例如 203.0.113.0/31，则可以将其 203.0.113.0 用于对等 IP 和 203.0.113.1 对 AWS 等 IP。或者，如果您分配了一个 /24 范围，例如 198.51.100.0/24，则可以将其 198.51.100.10 用于对等 IP 和 198.51.100.20 对 AWS 等 IP。</p> 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权 AWS 提供的 /31 CIDR。联系 Su AWS pp ort 申请公共 IPv4 CIDR（并在请求中提供用例） <div data-bbox="496 1220 1507 1436" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>我们不能保证我们能够满足所有关于 AWS 提供公共 IPv4 地址的请求。</p> </div> <ul style="list-style-type: none"> （仅限私有虚拟接口）Amazon 可以为您生成私有 IPv4 地址。如果您自己指定，请确保 CIDRs 为路由器接口指定私有接口，并且仅为 Di AWS rect Connect 接口指定私有接口。例如，请勿指定本地网络中的其他 IP 地址。与公共虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /30 范围，例如 192.168.0.0/30，则可以将其 192.168.0.1 用于对等 IP 和 192.168.0.2 对 AWS 等 IP。 |

| 资源 | 所需信息 |
|----------------------|---|
| | <ul style="list-style-type: none"> IPv6: 亚马逊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。 |
| 地址系列 | BGP 对等会话是否会结束 IPv4 还是 IPv6 |
| BGP 信息 | <ul style="list-style-type: none"> 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (AS N)。如果您使用的是公有 ASN，则必须拥有其所有权。如果您使用的是私有 ASN，则可以设置自定义 ASN 值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 1 到 4294967294 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。 AWS MD5 默认情况下启用。您无法修改此选项。 MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 |
| (仅限公有虚拟接口) 您要公布的前缀 | <p>要通过 BGP 发布的公共 IPv4 IPv6 路由或路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。</p> <ul style="list-style-type: none"> IPv4: 当以下任一条件为真 Direct Connect 时，IPv4 CIDR IPv4 R 可以与使用宣布的另一个公共 CIDR 重叠： <ul style="list-style-type: none"> CIDRs 他们来自不同 AWS 的地区。确保在公有前缀上应用 BGP 社区标签。 如果配置中有公用 ASN，则可以使用 AS_PATH。 active/passive <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> 通过 Direct Connect 公共虚拟接口，您可以为其指定从 /1 到 /32 以及从 /1 到 /6 IPv4 之间的任意前缀长度。 IPv6 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |

| 资源 | 所需信息 |
|---------------------|---|
| (仅限私有和中转虚拟接口) 巨型帧 | 数据包的最大传输单位 (MTU)。Direct Connect默认为 1500。将虚拟接口的 MTU 设置为 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。巨型帧仅适用于来自的传播路由。Direct Connect如果在路由表中添加指向虚拟私有网关的静态路由，则通过静态路由传输的流量将使用 1500 MTU 发送。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口“常规配置”页面上找到支持巨型帧。 |

如果您的公共前缀或 ASNs 属于互联网服务提供商或网络运营商，我们会要求您提供更多信息。这可以是使用公司官方信头的文档，也可以是来自公司域名的电子邮件，证明您 prefix/ASN 可能正在使用该网络。

对于私有虚拟接口和公有虚拟接口，网络连接的最大传输单元 (MTU) 是可以通过连接传递的数据包的最大允许大小 (以字节为单位)。私有虚拟接口的 MTU 可以是 1500 或 9001 (巨型帧)。中转虚拟接口的 MTU 可以是 1500 或 8500 (巨型帧)。您可以在创建接口时指定 MTU，也可以在创建接口后对其进行更新。将虚拟接口的 MTU 设置为 8500 (巨型帧) 或 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在“摘要”选项卡上找到“支持巨型帧”。

创建公共虚拟接口时，最多可能需要 72 个工作小时 AWS 才能审核和批准您的请求。

配置与非 VPC 服务间的公有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。
5. 在 Public virtual interface settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。

- d. 对于 BGP ASN，请输入新虚拟接口的本地对等路由器的边界网关协议自治系统编号。有效值为 1 到 4294967294。这包括对 ASNs (1-2147483647) 和多头 (1-4294967294) 的支持。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。
6. 在 Additional settings (其他设置) 下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择IPv4并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

[IPv6] 要配置 IPv6 BGP 对等体，请选择IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。
 - b. 要提供自己的 BGP 密钥，请输入您的 BGP MD5 密钥。

如果您不输入值，我们将生成一个 BGP 密钥。
 - c. 要向 Amazon 宣传前缀，对于要宣传的前缀，请输入应通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号分隔)。
 - d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

 - 对于 Key (键)，输入键名称。
 - 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。
 7. 选择 Create virtual interface (创建虚拟接口)。

配置与 VPC 间的私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在虚拟接口类型下，对于类型，选择私有。
5. 在私有虚拟接口设置下，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 Connection (连接), 选择要用于此接口的 Direct Connect 连接。
- c. 对于网关类型, 选择虚拟私有网关或 Direct Connect 网关。
- d. 对于虚拟接口所有者, 选择其他 AWS 帐户, 然后输入该 AWS 帐户。
- e. 对于虚拟私有网关, 选择要用于此接口的虚拟私有网关。
- f. 对于 VLAN, 输入您的虚拟局域网 (VLAN) 的 ID 号。
- g. 对于 BGP ASN, 输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。


有效值为 1 到 4294967294。这包括对 ASNs (1-2147483647) 和多头 (1-4294967294) 的支持。ASNs 有关 ASNs 和详细内容的更多信息, ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下, 执行以下操作:

- a. 要配置 IPv4 BGP 或对 IPv6 等体, 请执行以下操作:

[IPv4] 要配置 IPv4 BGP 对等体, 请选择IPv4并执行以下任一操作:

- 要自己指定这些 IP 地址, 请在您的路由器对等 IP 中, 输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP, 请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

 Important

配置 Di AWS rect Connect 虚拟接口时, 您可以使用 RFC 1918 指定自己的 IP 地址, 使用其他寻址方案, 或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point这些 point-to-point连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的, 例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect, AWS 建议使用客户网关路由器上的环回或局域网接口作为源地地址或目标地址, 而不是连接。 point-to-point

- 有关 RFC 1918 的更多信息, 请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息, 请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体, 请选择IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 9001 (巨型帧) ，请选择巨型帧 MTU (MTU 大小 9001) 。
- c. (可选) 在 “启用” 下 SiteLink ，选择 “启用” 以启用 Direct Connect 接入点之间的直接连接。
- d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签) ，然后执行以下操作：

- 对于 Key (键) ，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

7. 选择 Create virtual interface (创建虚拟接口)。
8. 您需要使用 BGP 设备来公布用于公有 VIF 连接的网络。

步骤 5：下载路由器配置

为 Direct Connect 连接创建虚拟接口后，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. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择连接，然后选择 View Details (查看详细信息)。
4. 选择 Download router configuration (下载路由器配置)。
5. 对于下载路由器配置，执行以下操作：
 - a. 对于 Vendor (供应商)，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。
6. 选择下载，然后使用适合您的路由器的配置，以确保您可以连接到 Direct Connect。

有关手动配置路由器的更多信息，请参阅 [下载路由器配置文件](#)。

在配置您的路由器后，虚拟接口的状态将变为 UP。如果虚拟接口一直处于关闭状态，并且您无法 ping Direct Connect 设备的对等 IP 地址，请参阅[排查第 2 层 \(数据链路\) 问题](#)。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](#)。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](#)。

步骤 6：确认您的虚拟接口

建立与 AWS 云或 Amazon VPC 的虚拟接口后，您可以使用以下步骤验证您的 AWS Direct Connect 连接。

验证您的虚拟接口与 AWS 云端的连接

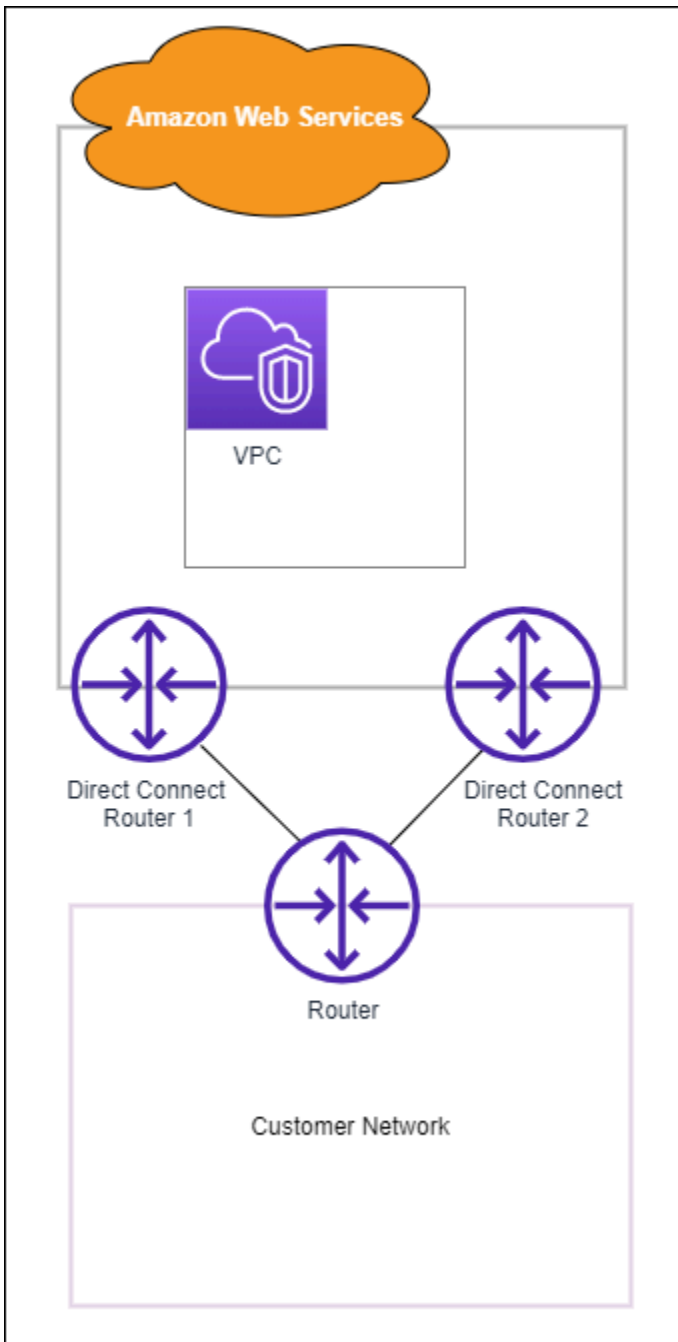
- 运行 traceroute 并验证标 Direct Connect 识符是否在网络跟踪中。

验证您的虚拟接口是否连接到 Amazon VPC

1. 使用可连接 ping 的 AMI（例如 Amazon Linux AMI），在连接到您的虚拟私有网关的 VPC 中启动 EC2 实例。当您在亚马逊 EC2 控制台中使用实例启动向导时，Amazon Linux AMIs 可在快速入门选项卡中找到。有关更多信息，请参阅 Amazon EC2 用户指南中的[启动实例](#)。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. 实例运行后，获取其私有 IPv4 地址（例如 10.0.0.4）。Amazon EC2 控制台将地址显示为实例详情的一部分。
3. ping 私有 IPv4 地址并获得回复。

（推荐）步骤 7：配置冗余连接

为了提供故障转移，我们建议您请求并配置两个专用连接 AWS，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）。这是默认配置，其中两个连接都处于活动状态。Direct Connect 支持多路径到同一位置内的多个虚拟接口，并且流量根据流量在接口之间进行负载共享。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。如果您使用以下任一配置，则需要检查[路由表路由](#)以路由到新的网络接口。

- 您使用自己的实例进行路由，例如实例是防火墙的情况。
- 您使用自己的实例终止 VPN 连接。

为了实现高可用性，我们强烈建议您配置与不同 Direct Connect 位置的连接。

有关 Direct Connect 弹性的更多信息，请参阅[Direct Connect 弹性建议](#)。

Direct Connect 维护

Direct Connect 致力于确保服务的安全性、可用性和可扩展性。为了保持这些标准，需要对硬件网络设备进行定期维护。Direct Connect 维护分为两种类型：计划维护和紧急维护。

这些维护活动包括解决安全漏洞和硬件问题、执行设备迁移以符合标准、修复缺陷以及提供新功能。通过遵循 [维护活动的准备](#) 中描述的做法，您可以更好地为 Direct Connect 环境做好准备，以免在维护活动期间出现中断。如果您的网络设置不具有弹性，或者只有一个连接，则您的本地网络和 AWS 资源之间的连接将中断。

Direct Connect 会将有关计划内和紧急维护事件的电子邮件通知发送到与拥有 Direct Connect 连接或虚拟接口资源的 AWS 账户关联的电子邮件地址。如果您使用与其中一个 Direct Connect 交付合作伙伴的 Direct Connect 托管连接，则系统会向您和合作伙伴账户发送有关维护活动的电子邮件通知。您还可以添加其他电子邮件地址或通讯组列表来接收通知。有关更多信息，[请参阅更新 AWS 账户的备用联系人](#)。

维护活动

- [Direct Connect 计划维护](#)
- [Direct Connect 紧急维护](#)
- [第三方维护](#)
- [维护活动的准备](#)
- [请求延期或取消维护活动](#)

Direct Connect 计划维护

计划维护活动涉及网络升级，例如操作系统修补和硬件设备端点的配置更新，这些都是提高可用性和提供新功能所必需的。

这些维护活动是提前 14 天安排的，通常发生在设备端点所在的 Direct Connect 位置的四小时内，即流量较低的时段。维护活动通常在整整四小时时段到期之前完成，工作完成后您将收到通知。在极少数情况下，如果因为出现不可预见的情况而需要延长维护时段，我们会单独发送一份通知，其中包含修改后的预计完工时间。

按照以下计划，初始通知和提醒通知将发送到拥有该资源的 AWS 账户：

- 计划维护活动前 14 个日历日，

- 计划维护活动前 7 个日历日，
- 计划维护活动前 1 天。

Note

日历日包括非工作日和当地节假日。

此外，

- 通过与 AWS Health 集成，在您的监控或开单系统中接收通知。要进行集成 AWS Health，请参阅 [AWS Health 用户指南中的 AWS Health 使用 Amazon EventBridge 监控事件](#)。
- 在 [Health Dashboard](#) 上查看计划维护时间表。

在极少数情况下，计划维护活动无法如期进行。如果发生这种情况，我们将发送取消通知，并在将来按照与上述相同的流程重新安排活动。

Direct Connect 紧急维护

紧急维护活动是紧急启动的，以防止即将发生的影响服务的事件或解决已经导致连接中断的损坏。在这种情况下，必须立即采取措施将受影响的端点恢复到正常状态。

虽然我们努力尽可能提前通知，但有些情况可能需要立即开始维护。当紧急维护已计划或正在进行时，您会收到通知，并在紧急维护完成时再次收到通知。

这些活动通常发生在设备端点所在的 Direct Connect 位置的两小时时段内。维护活动通常在此时段内完成。如果不可预见的情况需要延长维护时段，例如更换硬件，我们将单独发送一份通知，其中包含修改后的预计完工时间。

第三方维护

除了 AWS 启动的维护事件外，您的 Direct Connect Delivery 合作伙伴或提供从您的本地到 Direct Connect 位置的网络连接的网络服务提供商可能会执行维护活动。Direct Connect Delivery 合作伙伴会收到来自的维护事件通知，AWS 这样他们就可以计划自己的维护计划以避免重叠。AWS 无法了解合作伙伴的维护活动，因此您需要向他们询问他们的日程安排流程、通知方法和最佳实践。

维护活动的准备

为确保生产工作负载在维护期间继续运行，Direct Connect 建议您使用 Direct Connect 弹性工具包来配置网络连接，以实现最大的弹性。有关最大弹性的示例模型，请参阅 [最大弹性](#)。

利用最大的弹性，连接分布在至少两个 Direct Connect 位置，并在每个 Direct Connect 位置内的两个唯一设备端点上终止。这提供了多层冗余，从而降低了单个端点故障的风险，并有助于在维护活动期间保持连接。Direct Connect 绝不会安排会同时切断您的冗余连接的计划维护活动。有关使用弹性工具包配置最大 AWS Direct Connect 弹性的步骤，请参阅 [最大弹性配置](#)。

在计划维护活动中，Direct Connect 会排出正在进行维护的连接端点的流量，并强制流量使用您的冗余连接。如果未配置最大弹性，则无需手动干预即可实现更无缝的网络流量重新路由。或者，您可以选择使用本地首选边界网关协议 (BGP) 社区在维护时段内控制冗余连接之间的流量重新路由。有关 BGP 社区的更多信息，请参阅 [Routing policies and BGP communities](#)。

使用最大弹性模型配置 Direct Connect 环境有助于确保您的业务在维护活动和基础设施故障期间不受影响。正确实施和测试后，您通常无需对这些维护活动采取任何操作。

弹性验证

如果您已将 Direct Connect 环境配置为具有弹性，请定期验证您的流量在连接时是否通过其他冗余连接进行路由。定期的主动测试可以帮助识别和解决任何潜在问题，以免它们在实际维护活动或故障情况下影响生产工作负载。这将确保在维护活动期间对网络的可靠性更有信心。使用 Direct Connect 失效转移测试来验证冗余连接的弹性。有关使用 Direct Connect 失效转移测试的步骤，请参阅 [Direct Connect 失效转移测试](#)。

您还可以利用 Amazon CloudWatch 网络监控器主动监控您的 Direct Connect 连接。有关更多信息，请参阅 [使用 Amazon CloudWatch 网络综合监控器监控混合连接](#)。

请求延期或取消维护活动

Direct Connect 设备在多个客户之间共享。因此，我们不接受重新安排或取消维护的具体要求。为一个客户重新安排或取消请求可能会对使用该端点的其他客户产生负面影响。这也可能给及时缓解可用性或安全问题带来风险。

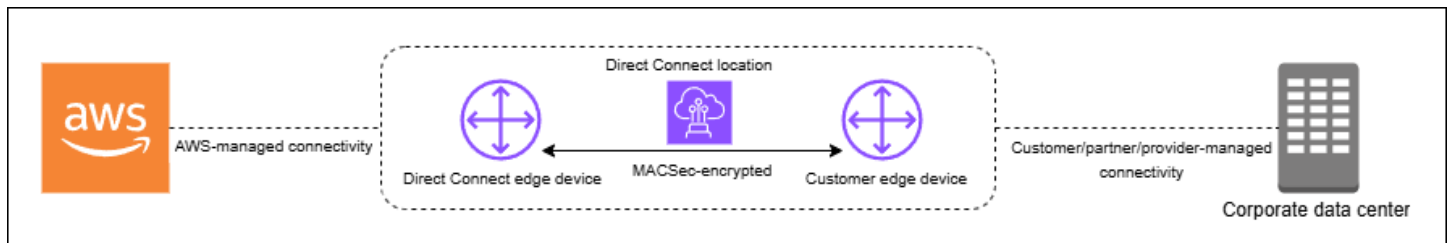
MAC 安全在 Direct Connect

MAC Security (MACsec) 是一项 IEEE 标准，可提供数据机密性、数据完整性和数据来源真实性。MACsec 通过交叉连接提供第 2 层 point-to-point 加密 AWS，在两台第 3 层路由器之间运行。虽然 MACsec 可以保护您的路由器与第 2 层的 Direct Connect 位置之间的连接，但通过在 Direct Connect 地点和区域之间通过网络传输的所有数据时，对物理层的所有数据进行加密，从而 AWS 提供额外的安全性。AWS 这创建了一种分层安全方法，在这种方法中，您的流量在初始进入网络期间 AWS 和通过 AWS 网络传输期间都受到保护。

在下图中，Direct Connect 交叉连接必须连接到客户边缘设备上 MACsec 支持连接的接口。MACsec over Direct Connect 为 Direct Connect 边缘设备和客户边缘设备之间的 point-to-point 流量提供第 2 层加密。这种加密是在交叉连接两端的接口之间交换和验证安全密钥之后进行的。

Note

MACsec 为以太网链路提供 point-to-point 安全性；因此，它不提供跨多个连续以太网或其他网段的 end-to-end 加密。



MACsec 概念

以下是以下关键概念 MACsec：

- MAC 安全 (MACsec) — IEEE 802.1 第 2 层标准，提供数据机密性、数据完整性和数据来源真实性。有关该协议的更多信息，请参阅 [802.1AE : MAC 安全 \(\) MACsec](#)。
- 安全关联密钥 (SAK)-一种会话密钥，用于在 MACsec 客户本地路由器与 Direct Connect 位置的连接端口之间建立连接。SAK 不是预共享的，而是通过加密密钥生成过程从 CKN/CAK 配对中自动派生的。在您提供和配置配对之后，这种推导发生在连接的 CKN/CAK 两端。出于安全考虑，无论何时建立会 MACsec 话，SAK 都会定期重新生成。

- 连接关联密钥名称 (CKN) 和连接关联密钥 (CAK)-这对中的值用于生成 MACsec 密钥。您可以生成配对值，将其与 Direct Connect 连接关联，然后在 Direct Connect 连接结束时在边缘设备上配置。Direct Connect 仅支持静态 CAK 模式，但不支持动态 CAK 模式。由于仅支持静态 CAK 模式，因此建议您在密钥生成、分发和轮换时遵循自己的密钥管理策略。
- 密钥格式：密钥格式应使用十六进制字符，长度恰好为 64 个字符。Direct Connect 仅支持用于专用连接的高级加密标准 (AES) 256 位密钥，该密钥对应于 64 个字符的十六进制字符串。
- 加密模式 — Direct Connect 支持两种 MACsec 加密模式：
 - `must_encrypt` — 在此模式下，连接需要对所有 MACsec 流量进行加密。如果 MACsec 协商失败或无法建立加密，则连接将不会传输任何流量。此模式提供了最高的安全保障，但如果存在任何 MACsec 相关问题，可能会影响可用性。
 - `should_encrypt` — 在此模式下，连接尝试建立 MACsec 加密，但如果 MACsec 协商失败，连接将回退到未加密的通信。此模式提供了更大的灵活性和更高的可用性，但在某些失败情况下，可能会允许未加密的流量。

加密模式可以在连接配置期间设置，也可以在以后进行修改。默认情况下，新 MACsec 启用的连接设置为 “`should_encrypt`” 模式，以防止在初始设置期间出现潜在的连接问题。

MACsec 密钥轮换

• CNN/CAK 轮换 (手动)

Direct Connect MACsec 支持最多可存储三 CKN/CAK 对 MACsec 密钥。这样，您就可以在不中断连接的情况下手动轮换这些长期密钥。使用 `associate-mac-sec-key` 命令关联新 CKN/CAK 配对时，必须在设备上配置相同的配对。Direct Connect 设备尝试使用最近添加的密钥。如果该密钥与您设备的密钥不匹配，它将回退到之前的工作密钥，从而确保轮换期间的连接稳定性。

有关使用的信息 `associate-mac-sec-key`，请参阅 [associate-mac-sec-key](#)。

• 安全关联密钥 (SAK) 轮换 (自动)

源自活动 CKN/CAK 对的 SAK 会根据以下条件进行自动旋转：

- 时间间隔
- 加密流量的总量
- MACsec 会话建立

这种轮换由协议自动处理，在不中断连接的情况下以透明方式进行，并且不需要手动干预。SAK 从不永久存储，而是通过符合 IEEE 802.1X 标准的安全密钥派生过程重新生成。

支持的连接

MACsec 适用于专用 Direct Connect 连接和链路聚合组：

支持的 MACsec 连接

- [专用 连接](#)
- [LAGs](#)
- [合作伙伴互连](#)

Note

使用受支持设备的合作伙伴可以使用 MACsec 加密其边缘网络设备和 Direct Connect 设备之间的第 2 层连接。启用该功能的合作伙伴可以加密通过安全链接的所有流量。MACsec 加密在第 2 层的两个特定设备之间运行，托管连接不支持加密。

有关如何订购支持的连接的信息 MACsec，请参阅[AWS Direct Connect](#)。

专用 连接

以下内容可帮助您熟悉 MACsec Direct Connect 专用连接。使用不收取任何额外费用 MACsec。有关在专用连接 MACsec 上进行配置的步骤，请参阅[开始使用 MACsec 专用连接](#)。

合作伙伴互连操作遵循与专用连接相同的程序。当您为伙伴互连运行 CLI 或 SDK 命令时，响应将包括 MACsec 相关信息（如果适用）。

MACsec 专用连接的先决条件

请注意专用连接 MACsec 的以下要求：

- MACsec 在选定的接入点支持 10 Gbps、100 Gbps 和 400 Gbps 的专用 Direct Connect 连接。对于这些连接，支持以下 MACsec 密码套件：
 - 对于 10 Gbps 连接，请使用 GCM-AES-256 和 GCM-AES-XPB-256。
 - 对于 100 Gbps 和 400 Gbps 的连接，GCM-AES-XPB-256。
- 仅支持 256 位 MACsec 密钥。

- 100 Gbps 和 400 Gbps 连接需要扩展数据包编号 (XPN)。对于 10Gbps 连接，Direct Connect 同时支持 GCM-AES-256 和 GCM-AES-XPN -256。高速连接 (例如 100 Gbps 和 400 Gbps 的专用连接) 可能会很快耗尽最初 MACsec 的 32 位数据包编号空间，这将要求您每隔几分钟轮换一次加密密钥才能建立新的连接关联。为了避免这种情况，IEEE Std 802. AEbw 1-2013 修正案引入了扩展的数据包编号，将编号空间增加到 64 位，从而放宽了密钥轮换的及时性要求。
- 安全通道标识符 (SCI) 是必填项，必须处于打开状态。此设置无法调整。
- 不支持 IEEE 802.1Q (Dot q/VLAN) tag offset/dot 1q-in-clear) 将 VLAN 标签移到加密有效负载之外。

此外，在专用连接 MACsec 上进行配置之前，还应完成以下任务。

- 为 MACsec 密钥创建 CKN/CAK 一对。

您可以使用开放标准工具创建该对。该对必须满足 [the section called “配置本地路由器”](#) 中指定的要求。

- 确保您的连接端有支持的设备 MACsec。
- 必须开启安全通道标识符 (SCI)。
- 仅支持 256 位 MACsec 密钥，提供最新的高级数据保护。

LAGs

以下要求可帮助您熟悉 MACsec 专用 Direct Connect 链路聚合组 (LAGs)：

- LAGs 必须由支持 MACsec 加密 MACsec 的专用连接组成
- LAG 内的所有连接必须具有相同的带宽和支持 MACsec
- MACsec 配置统一应用于 LAG 中的所有连接
- 启用 LAG 创建，MACsec 可以同时完成
- 任何时候只能在所有 LAG 链路上使用一个 MACsec 密钥。支持多个 MACsec 密钥的功能仅用于密钥轮换目的。

合作伙伴互连

拥有互连的合作伙伴账户可以在该物理连接或 LAG MACsec 上使用。这些操作与专用连接相同，但是它们是使用合作伙伴特定的 API/SDK 呼叫执行的。

服务相关角色

Direct Connect 使用 AWS Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。Direct Connect 服务相关角色由服务预定义 Direct Connect，包括该服务代表您调用其他 AWS 服务所需的所有权限。服务相关角色使设置变得 Direct Connect 更加容易，因为您不必手动添加必要的权限。Direct Connect 定义其服务相关角色的权限，除非另有定义，否则 Direct Connect 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。有关更多信息，请参阅 [the section called “服务关联角色”](#)。

MACsec 预共享 CKN/CAK 密钥注意事项

AWS Direct Connect CMKs 对与连接关联的预共享密钥使用 AWS 托管或 LAGs。Secrets Manager 将您预共享的 CKN 和 CAK 对，存储为 Secrets Manager 根密钥加密的密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》CMKs 中的 [AWS 托管](#)。

存储的密钥在设计上是只读的，但您可以使用 S AWS secrets Manager 控制台或 API 安排七到三十天的删除。当您计划删除时，无法读取 CKN，这可能会影响网络连接。发生这种情况时，我们会采用以下规则：

- 如果连接处于待处理状态，我们会解除 CKN 与连接的关联。
- 如果连接处于可用状态，我们会通过电子邮件通知连接所有者。如果您在 30 天内未采取任何行动，我们会解除 CKN 与连接的关联。

当我们解除最后一个 CKN 与连接的关联，并且连接加密模式设置为“必须加密”时，我们会将模式设置为“should_encrypt”，以防止突然丢包。

开始在专用 Direct Connect 连接 MACsec 上使用

以下任务可以让你开始设置 MACsec 在 Direct Connect 专用连接上使用

步骤 1：创建连接

要开始使用 MACsec，您必须在创建专用连接时开启该功能。

(可选) 步骤 2：创建链接聚合组 (LAG)

如果您使用多个连接实现冗余，则可以创建支持的 LAG MACsec。有关更多信息，请参阅 [MACsec 注意事项](#) 和 [Create a LAG](#)。

步骤 3：将 CKN/CAK 与连接或 LAG 关联

创建支持的连接或 LAG 后 MACsec，需要将 CKN/CAK 与该连接关联。有关更多信息，请参阅以下任一文档：

- [将 MACsec CKN/CAK 与连接关联](#)
- [将 MACsec CKN/CAK 与 LAG 关联](#)

步骤 4：配置本地路由器

使用 MACsec 密钥更新您的本地路由器。本地路由器上的 MACsec 密钥和 Direct Connect 位置的密钥必须匹配。有关更多信息，请参阅 [下载路由器配置文件](#)。

步骤 5：（可选）移除与连接或 LAG 之间的关联 CKN/CAK

您可以选择移除与连接或 LAG 之间的关联。如果需要移除关联，请参阅以下内容之一：CKN/CAK

- [移除 MACsec 密钥和连接之间的关联](#)
- [移除 MACsec 密钥和 LAG 之间的关联](#)

Direct Connect 专用连接和托管连接

Direct Connect 使您能够在您的网络和其中一个 Direct Connect 位置之间建立专用的网络连接。

有两种类型的连接：

- 专用连接：与单个客户关联的物理以太网连接。客户可以通过 Direct Connect 控制台、CLI 或 API 请求专用连接。有关更多信息，请参阅 [专用连接](#)。
- 托管连接：AWS Direct Connect 合作伙伴代表客户配置的物理以太网连接。客户通过联系 AWS Direct Connect 合作伙伴计划中负责预置连接的合作伙伴，来请求托管连接。有关更多信息，请参阅 [托管连接](#)。

主题

- [专用 Direct Connect 连接](#)
- [托管 Direct Connect 连接](#)
- [删除 Direct Connect 连接](#)
- [更新 Direct Connect 连接](#)
- [查看 Direct Connect 连接详情](#)

专用 Direct Connect 连接

要创建 Direct Connect 专用连接，您需要以下信息：

Direct Connect 位置

与合作伙伴计划中的 AWS Direct Connect 合作伙伴合作，帮助您在某个 Direct Connect 地点与您的数据中心、办公室或托管环境之间建立网络回路。他们还可以帮助在与该位置相同的设施内提供托管空间。有关更多信息，请参阅 [APN 合作伙伴支持 Direct Connect](#)。

端口速度

可能的值为 1 Gbps、10 Gbps、100 Gbps 和 400 Gbps。

创建连接请求之后，将无法更改端口速度。要更改端口速度，您必须创建并配置新的连接。

您可以使用连接向导创建连接，也可以创建 Classic 连接。使用连接向导，您可以使用弹性建议来设置连接。如果您是第一次设置连接，建议使用向导。如果您愿意，可以使用 Classic 来创建连接 one-at-

a-time。如果您已有要添加连接的现有设置，建议使用 Classic。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。

在您请求连接后，我们会向您提供《授权和连接设备分配通知函 (LOA-CFA) 》供您下载，或通过电子邮件向您请求更多信息。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 是连接的授权 AWS，您的网络提供商要求您订购交叉连接。如果您在该 Direct Connect 地点没有设备，则无法在那里为自己订购交叉连接。

以下操作可用于专用连接：

- [使用连接向导创建连接](#)
- [创建 Classic 连接](#)
- [the section called “查看 连接详细信息”](#)
- [the section called “更新连接”](#)
- [将 MACsec CKN/CAK 与连接关联](#)
- [the section called “移除 MACsec 密钥和连接之间的关联”](#)
- [the section called “删除连接”](#)

您可以将专用连接添加到链接聚合组 (LAG)，这使您可以将多个连接视为一个连接。有关信息，请参阅[将连接与 LAG 关联](#)。

创建连接后，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[虚拟接口和托管虚拟接口](#)。

如果您在某个 Direct Connect 地点没有设备，请先联系 AWS Direct Connect 合作伙伴计划中的 AWS Direct Connect 合作伙伴。有关更多信息，请参阅[APN 合作伙伴支持 Direct Connect](#)。

如果要创建使用 MAC Security (MACsec) 的连接，请在创建连接之前查看先决条件。有关更多信息，请参阅[the section called “MACsec 专用连接的先决条件”](#)。

《授权和连接设备分配通知函 (LOA-CFA) 》

在我们处理您的连接请求后，您可以下载 LOA-CFA。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信息。

已下载的 LoA 加盖数字签名和水印，以验证 LoA 是由 AWS 签发的真实性。LoA 加盖数字签名和水印。PDF 文档可防止设施提供商在 Direct Connect 站点凭借修改过的或可能存在欺诈性的 LoA 进行操

作。可以通过打开 PDF 并查看签名面板来验证数字签名。有效的文档将显示“签名有效”和“文档自签名以来未经修改”。水印会重复显示在 LoA 正文上指定的配线架和光纤束，作为真实性的直观标识，但并不具备安全性。

在端口处于活动状态或 LOA 签发 90 天后（以先到者为准），将自动开始计费。在激活前或 LOA 签发后 90 天内，您可以删除端口，以避免计费。

如果您的连接在 90 天后仍未建立，且 LOA-CFA 尚未签发，我们将向您发送一封电子邮件，提醒您该端口将在 10 天内被删除。如果您未能在额外的 10 天期限内激活端口，该端口将被自动删除，您需要重新启动端口创建过程。

有关下载连接 LoA-CFA 的步骤，请参阅[下载 LOA-CFA](#)。

Note

有关定价的更多信息，请参阅[Direct Connect 定价](#)。如果您在重新发放 LOA-CFA 之后不再需要连接，必须自行删除此连接。有关更多信息，请参阅[删除 Direct Connect 连接](#)。

主题

- [使用连接向导创建 Direct Connect 专用连接](#)
- [创建 Direct Connect 经典连接](#)
- [下载 Direct Connect LOA-CFA](#)
- [将 MACsec CKN/CAK 与连接关联 Direct Connect](#)
- [移除 MACsec 密钥和 Direct Connect 连接之间的关联](#)

使用连接向导创建 Direct Connect 专用连接

本节介绍如何使用连接向导创建连接。如果您更想创建 Classic 连接，请参阅 [the section called “步骤 2：申请 Direct Connect 专用连接”](#) 中的步骤。

要创建连接向导连接

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择连接，然后选择创建连接。
3. 在创建连接页面上的连接订购类型下，选择连接向导。
4. 为您的网络连接选择弹性级别。弹性级别可以是以下级别之一：

- 最大弹性
- 高弹性
- 开发和测试

有关这些弹性级别的描述和更多详细信息，请参阅 [the section called “AWS Direct Connect 弹性工具包”](#)。

5. 选择下一步。
6. 在配置连接页面上，提供以下详细信息。
 - a. 从带宽下拉列表中，选择连接所需的带宽。可以是 1 Gbps 到 400 Gbps 之间的任何值。
 - b. 在“位置”中，选择相应 Direct Connect 的位置，然后选择第一位置服务提供商，选择在此位置为连接提供连接的服务提供商。
 - c. 对于第二个位置，Direct Connect 在第二个位置选择相应的位置，然后选择第二个位置服务提供商，选择为第二个位置的连接提供连接的服务提供商。
 - d. (可选) 为连接配置 MAC 安全 (MACsec)。在“其他设置”下，选择“请求 MACsec 支持此功能的端口”。

MACsec 仅在专用连接上可用。

- e. (可选) 选择添加标签以添加 key/value 对以进一步帮助识别此连接。
 - 对于 Key (键) ，输入键名称。
 - 对于值，输入键值。

要删除现有标签，请选择该标签，然后选择删除标签。标签不能为空。

7. 选择下一步。
8. 在查看并创建页面上，验证连接。本页面还显示了端口使用的估计成本和额外的数据传输费用。
9. 选择创建。
10. 下载您的授权证书和连接设备分配 (LOA-CFA) ，有关更多信息，请参阅 [the section called “《授权和连接设备分配通知函 \(LOA-CFA \) 》”](#)。

使用以下命令之一。

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

创建 Direct Connect 经典连接

对于专用连接，您可以使用 Direct Connect 控制台提交连接请求。对于托管连接，请与 AWS Direct Connect 合作伙伴合作申请托管连接。确保您具有以下信息：

- 您需要的端口速度。对于专用连接，在创建连接请求后将无法更改端口速度。对于托管连接，您的 AWS Direct Connect 合作伙伴可以更改速度。
- 连接的终止 Direct Connect 位置。

Note

您不能使用 Direct Connect 控制台请求托管连接。相反，请联系 AWS Direct Connect 合作伙伴，合作伙伴可以为您创建托管连接，然后您接受该连接。请跳过以下步骤并转至[接受托管连接](#)。

创建新 Direct Connect 连接

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在 Direct Connect 屏幕上，在 Get started (开始使用) 下，选择 Create a connection (创建连接)。
3. 选择 Classic。
4. 对于 Name (名称)，输入连接的名称。
5. 对于 Location (位置)，选择适当的 Direct Connect 位置。
6. 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。只有当该地点在大楼的多个楼层都有 meet-me 会议室 (MMRs) 时，此选项才可用。
7. 对于 Port Speed (端口速度)，选择连接带宽。
8. 对于本地，当您使用此连接来连接到数据中心时，选择通过 Direct Connect 合作伙伴连接。
9. 对于服务提供商，请选择 AWS Direct Connect 合作伙伴。如果您使用的合作伙伴不在列表中，请选择 Other (其他)。
10. 如果您为服务提供商选择了其他，则对于其他提供商的名称，请输入您使用的合作伙伴的名称。
11. (可选) 选择添加标签以添加 key/value 对以进一步帮助识别此连接。
 - 对于 Key (键) ，输入键名称。
 - 对于值，输入键值。

要删除现有标签，请选择该标签，然后选择删除标签。标签不能为空。

12. 选择创建连接。

最多可能需要 72 个工作小时 AWS 才能审核您的请求并为您的连接配置端口。在此期间，您可能会收到一封电子邮件，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。电子邮件将发送到您注册时使用的电子邮件地址 AWS。您必须在 7 日内回复，否则将删除该连接。

有关更多信息，请参阅 [专用和托管连接](#)。

下载 Direct Connect LOA-CFA

您可以使用 Direct Connect 控制台或命令行下载 LOA-CFA。在您下载了 LOA-CFA 并将其提供给您网络或主机托管提供商后，该提供商就可以为您订购交叉连接。

下载 LOA-CFA

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择连接，然后选择查看详细信息。
4. 选择下载 LOA-CFA。

Note

如果未启用链接，则 LOA-CFA 尚不可供您下载。此操作将创建一个支持案例，请求提供更多信息。在您回复请求并处理请求后，即可下载 LOA-CFA。如果仍然不可用，请联系 [AWS Support](#)。

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 Direct Connect 位置交叉连接](#)。

使用命令行或 API 下载 LOA-CFA

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

将 MACsec CKN/CAK 与连接关联 Direct Connect

创建支持的连接后 MACsec，可以将 CKN/CAK 与该连接关联。您可以使用 Direct Connect 控制台、命令行或 API 创建关联。

Note

将 MACsec 私有密钥与连接关联后，便无法对其进行修改。如果需要修改密钥，请解除密钥与连接的关联，然后将新密钥与连接关联。有关删除关联的信息，请参阅 [移除 MACsec 密钥和连接之间的关联](#)。

将 MACsec 密钥与连接关联

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在左侧窗格中，选择连接。
3. 选择连接，然后选择查看详细信息。
4. 选择关联密钥。
5. 输入密 MACsec 钥。

[使用密钥 CAK/CKN 对] 选择“密钥对”，然后执行以下操作：

- 对于连接关联密钥 (CAK)，输入 CAK。
- 对于连接关联密钥名称 (CKN)，输入 CAK。

[使用密钥] 选择“现有密钥管理器密钥”，然后在“密钥”中，选择 MACsec 密钥。

6. 选择关联密钥。

使用命令行或 API 将 MACsec 密钥与连接关联

- [associate-mac-sec-key](#) (AWS CLI)
- [AssociateMacSecKey](#)(Direct Connect API)

移除 MACsec 密钥和 Direct Connect 连接之间的关联

您可以使用 Direct Connect 控制台、命令行或 API 删除连接和 MACsec 密钥之间的关联。

移除连接和 MACsec 密钥之间的关联

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
- 2.
3. 在左侧窗格中，选择连接。
4. 选择连接，然后选择查看详细信息。
5. 选择要删除的 MACsec 密钥，然后选择“取消关联密钥”。
6. 在确认对话框中，输入 disassociate，然后选择解除关联。

使用命令行或 API 删除连接和 MACsec 密钥之间的关联

- [disassociate-mac-sec-key](#) (AWS CLI)
- [DisassociateMacSecKey](#)(Direct Connect API)

托管 Direct Connect 连接

要创建 Direct Connect 托管连接，您需要以下信息：

Direct Connect 位置

与合作伙伴计划中的 AWS Direct Connect 合作伙伴合作，帮助您在某个 Direct Connect 地点与您的数据中心、办公室或托管环境之间建立网络回路。他们还可以帮助在与该位置相同的设施内提供托管空间。有关更多信息，请参阅 [Direct Connect 交付合作伙伴](#)。

Note

您无法通过 Direct Connect 控制台请求托管连接。但是，AWS Direct Connect 合作伙伴可以为您创建和配置托管连接。配置完成后，连接会出现在控制台中的连接窗格中。您必须接受该托管连接，然后才能使用它。有关更多信息，请参阅 [接受托管连接](#)。

端口速度

对于托管连接，可能的值为 50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps 和 25 Gbps。请注意，只有满足特定要求的 Direct Connect 合作伙伴才能创建 1 Gbps、2 Gbps、5 Gbps、10 Gbps 或 25 Gbps 的托管连接。25 Gbps 连接仅在端口速度为 100 Gbps 的 Direct Connect 位置可用。

注意以下几点：

- 连接端口速度只能由您的 Direct Connect 合作伙伴更改。请咨询您的 AWS Direct Connect 合作伙伴，了解他们是否支持升级或降级现有连接。如果您的合作伙伴支持升级/降级连接，则无需删除连接然后重新创建连接，即可升级或降级现有托管连接的带宽。
- AWS 对托管连接使用流量管制，这意味着当流量速率达到配置的最大速率时，多余的流量将被丢弃。这可能会导致突发流量的吞吐量低于非突发流量。
- 只有最初在 Direct Connect 托管父连接上启用时才能在连接上启用巨型帧。如果在父连接上未启用巨型帧，则在任何连接上都无法启用。

在您请求并接受托管连接后，可以执行以下控制台操作：

- [删除连接](#)
- [更新连接](#)
- [查看 连接详细信息](#)

接受连接后，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 [虚拟接口和托管虚拟接口](#)。

接受 Direct Connect 托管连接

如果您有兴趣购买托管连接，则必须联系 AWS Direct Connect 合作伙伴计划中的 AWS Direct Connect 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 Direct Connect 控制台中的连接窗格中。

在您开始使用托管连接前，必须接受该连接。您可以使用 Direct Connect 控制台、命令行或 API 接受托管连接。

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择托管连接，然后选择查看详细信息。
4. 选中确认复选框，然后选择接受。

使用命令行或 API 接受托管连接

- [confirm-connection](#) (AWS CLI)

- [ConfirmConnection](#)(Direct Connect API)

删除 Direct Connect 连接

只要连接没有连接虚拟接口，您就可以删除该连接。删除您的连接会停止此连接的所有端口小时费用，但您仍可能产生交叉连接或网络电路费用（见下文）。Direct Connect数据传输费用与虚拟接口有关。有关如何删除虚拟接口的详细信息，请参阅 [删除虚拟接口](#)。

删除连接之前，请下载连接（包含跨账户信息）的 LOA，这样您就可以获得有关正在断开的线路的相关信息。有关下载连接 LOA 的步骤，请参阅 [《授权和连接设备分配通知函（LOA-CFA）》](#)。

当您删除连接时，AWS 将指示托管提供商从相应的配线架上拔下光纤交叉连接电缆，从而断开您的网络设备与 Direct Connect 路由器的连接。AWS 但是，您的主机托管或线路提供商仍可能向您收取交叉连接费用或网络线路费用，因为交叉连接线缆可能仍连接到您的网络设备。此类交叉连接费用与 Direct Connect 无关，要向主机托管或线路提供商取消费用，必须使用 LOA 中的信息。

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。

您可以使用 Direct Connect 控制台、命令行或 API 删除连接。

删除连接

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择连接，然后选择 Delete (删除)。
4. 在 Delete (删除) 确认对话框中，选择 Delete (删除)。

使用命令行或 API 删除 连接

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

更新 Direct Connect 连接

您可以使用 Direct Connect 控制台、命令行或 API 更新以下连接属性。

- 连接的名称。
- 连接的 MACsec 加密模式。

Note

虽然您无法直接修改托管连接上的 MACSec 属性，但合作伙伴可以启用 MACSec 自己的互连，为其客户提供安全的托管连接。

有效值为：

- `should_encrypt`
- `must_encrypt`

将加密模式设置为该值后，加密关闭时连接也会中断。

- `no_encrypt`

更新连接

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择连接，然后选择编辑。
4. 修改连接：

[更改名称] 对于 Name (名称)，输入新连接名称。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

5. 选择 Edit connection (编辑连接)。

要使用命令行或 API 更新连接

- [update-connection](#) (AWS CLI)
- [UpdateConnection](#) (Direct Connect API)

查看 Direct Connect 连接详情

您可以使用 Direct Connect 控制台、命令行或 API 查看当前的连接状态。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 LOA-CFA 上的连接 ID 是否匹配。

有关监控连接的信息, 请参阅[监控 Direct Connect 资源](#)。

如何查看连接的详细信息

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在左侧窗格中, 选择连接。
3. 选择连接, 然后选择查看详细信息。

使用命令行或 API 描述连接

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

要求在 Direct Connect 位置交叉连接

在您下载了《授权证书和连接设备分配 (LOA-CFA)》后，您必须完成交叉网络连接（即交叉连接）。如果您在 Direct Connect 位置已经有设备，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。合作伙伴和联系信息按地区整理。要了解具体的交叉连接价格，需直接联系 Direct Connect 合作伙伴。建立交叉连接后，可以使用 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，包括每个位置的可用速度，请参阅 [Direct Connect 位置](#)。

如果您在 Direct Connect 位置还没有设备，您可以与 AWS 合作伙伴网络 (APN) 中的一个合作伙伴合作。他们可帮助您连接到 Direct Connect 位置。有关更多信息，请参阅 [APN 合作伙伴支持 Direct Connect](#)。您必须与您选中的供应商共享 LOA-CFA，以便顺利完成交叉连接。

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 Direct Connect 区域](#)。

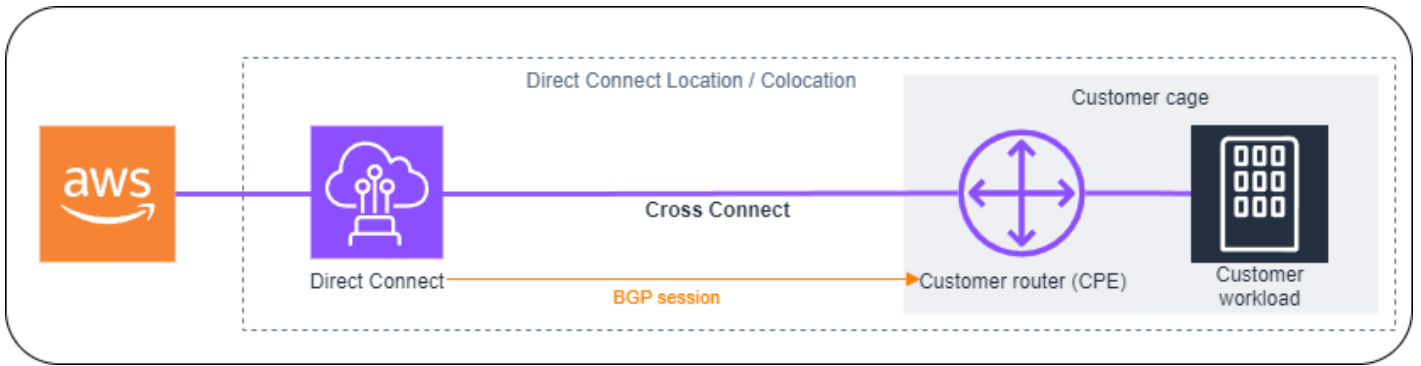
Note

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 Direct Connect 控制台再次下载它。有关更多信息，请参阅 [《授权和连接设备分配通知函 \(LOA-CFA\)》](#)。

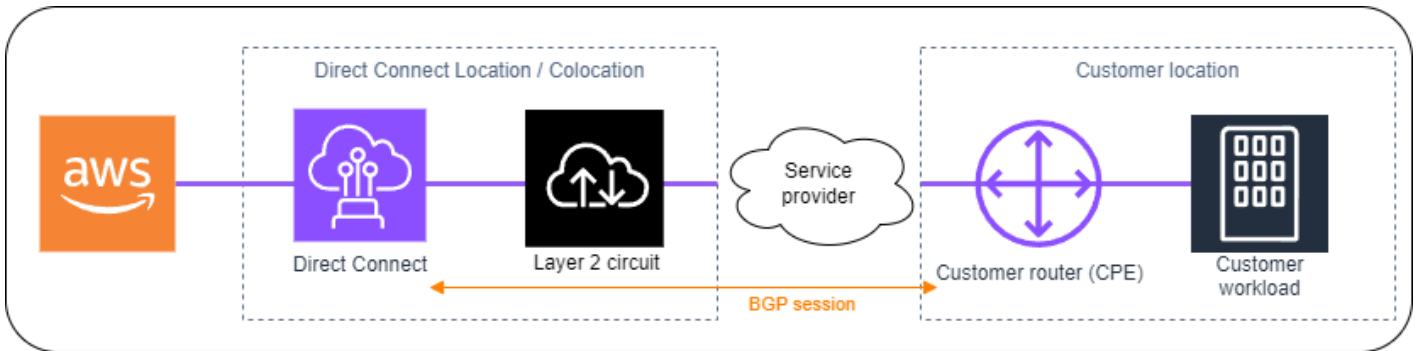
连接选项

连接到 Direct Connect 位置的选项可能因合作伙伴和 AWS 区域而异。您可以与 AWS 合作伙伴网络 (APN) 中可以提供以下一个或多个连接选项的合作伙伴之一合作：

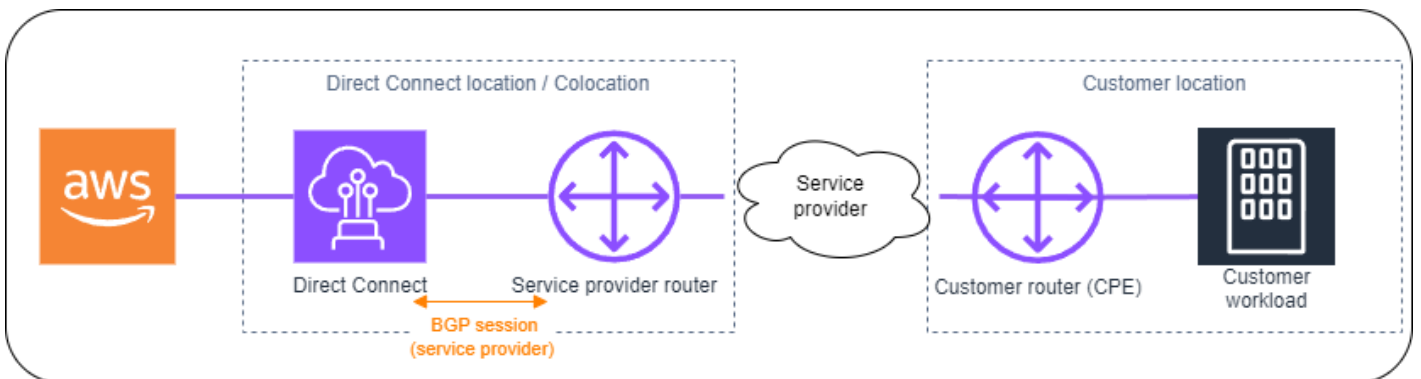
- 如果您将资源部署在与 Direct Connect 位置相同的数据中心/主机托管设施中，则该设施可以在 Direct Connect 设备和您的资源之间提供交叉连接。为此，您必须先向设施提供 LOA-CFA。请参阅 [《授权和连接设备分配通知函 \(LOA-CFA\)》](#) 了解更多信息。下图展示了此 Direct Connect 连接选项的示例：



- 通过与 Direct Connect 合作伙伴合作，通过“线路”将第 2 层（数据链路层）的 Direct Connect 连接从 Direct Connect 位置扩展到客户所在地。安装在客户位置的路由器将直接与 AWS 设备形成 BGP 会话。例如，可以使用的技术包括城域以太网、暗光纤或 Wavelength。下图展示了此 Direct Connect 连接选项的示例。



- 通过与 Direct Connect 合作伙伴合作，将第 3 层（网络层）的 Direct Connect 连接从 Direct Connect 位置扩展到您的位置。对于此连接选项，Direct Connect 合作伙伴在 Direct Connect 位置内提供一台路由器，用于与 AWS 设备形成边界网关协议（BGP）会话。然后，Direct Connect 合作伙伴会与您建立另一个 BGP；例如，可能会通过多协议标签交换 (MLPS) 进行。下图展示了此 Direct Connect 连接选项的示例。



美国东部（俄亥俄州）

| 位置 | 如何申请连接 |
|------------------------------------|---|
| Cologix COL2，哥伦布市 | 联系 Cologix，邮箱为 sales@cologix.com 。 |
| Cologix MIN3，明尼阿波利斯 | 联系 Cologix，邮箱为 sales@cologix.com 。 |
| CyrusOne West III，休斯顿 | 使用 客户联系 表提交申请。 |
| Equinix CH2，芝加哥 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| QTS，芝加哥 | 联系 QTS，邮箱为 AConnect@qtsdatacenters.com 。 |
| Netrality 数据中心，堪萨斯城 格兰大街 1102 号 | 联系 Netrality 数据中心，邮箱为 support@netrality.com 。 |

美国东部（弗吉尼亚州北部）

| 位置 | 如何申请连接 |
|------------------------------------|--|
| 165 Halsey Street，纽瓦克 | 请发送电子邮件至 operations@165halsey.com 。 |
| CoreSite 32k，纽约 | 使用 CoreSite 客户门户网站 下单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| CoreSite VA1-VA2，雷斯顿 | 使用 CoreSite 客户门户网站 下单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| Digital Realty ATL1 &ATL2， 亚特兰大 | 联系 Digital Realty，邮箱为 amazon.orders@digitalrealty.com 。 |
| Digital Realty IAD38，阿什本 | 联系 Digital Realty，邮箱为 amazon.orders@digitalrealty.com 。 |
| Equinix DC1-DC6 和 DC10- D12，阿什本 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

| 位置 | 如何申请连接 |
|----------------------------------|---|
| Equinix DAA1-DC3 和 DC6， 达拉斯 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix MI1，迈阿密 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix NY5，锡考克斯 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| KIO Networks QRO1，墨西哥 克雷塔罗 | 联系“ KIO 网络 ”。 |
| Markley，One Summer Street，波士顿 | 对于当前客户，请使用 客户门户 创建请求。对于新查询，请联系 sales@markleygroup.com 。 |
| Netrality 数据中心，费城 MMR 二楼 | 联系 Netrality 数据中心，邮箱为 support@netrality.com 。 |
| QTS ATL1，亚特兰大 | 联系 QTS，邮箱为 AConnect@qtsdatacenters.com 。 |

美国西部（加利福尼亚北部）

| 位置 | 如何申请连接 |
|--------------------|--|
| CoreSite LA1，洛杉矶 | 使用 CoreSite 客户门户网站 下单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| CoreSite SV2，米尔皮塔斯 | 使用 CoreSite 客户门户网站 下单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| CoreSite SV4，圣克拉拉 | 使用 CoreSite 客户门户网站 下单。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，凤凰城 | 使用 EdgeOS 客户门户网站 下单。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 LA3，埃尔塞贡多 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

| 位置 | 如何申请连接 |
|-----------------------|---|
| Equinix SV1 和 SV5，圣荷西 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| PhoenixNAP，菲尼克斯 | 联系 phoenixNAP Provisioning，邮箱为 provisioning@phoenixnap.com 。 |

美国西部（俄勒冈州）

| 位置 | 如何申请连接 |
|-------------------------------|--|
| CoreSite DE1，丹佛 | 使用 CoreSite 客户门户网站 下单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| Digital Realty SEA10，西雅图威斯汀酒店 | 联系 Digital Realty，邮箱为 amazon.orders@digitalrealty.com 。 |
| EdgeConneX，波特兰 | 使用 EdgeOS 客户门户网站 下单。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 | 联系 Equinix，邮箱为 support@equinix.com 。 |
| Pittock Block，波特兰 | 通过电子邮件发送请求至 crossconnect@pittock.com ，或者致电 +1 503 226 6777。 |
| Switch SUPERNAP 8，拉斯维加斯 | 联系 Switch SUPERNAP，邮箱为 orders@supernap.com 。 |
| TierPoint Seattle | 联系 TierPoint，邮箱为 sales@tierpoint.com 。 |

非洲（开普敦）

| 位置 | 如何申请连接 |
|---------------------------------------|--|
| 开普敦 Internet Exchange/ Teraco 数据中心 | 联系 Teraco，邮箱为 support@teraco.co.za （对于现有 Teraco 客户）或 connect@teraco.co.za （对于新客户）。 |
| Teraco JB1，南非约翰内斯堡 | 联系 Teraco，邮箱为 support@teraco.co.za （对于现有 Teraco 客户）或 connect@teraco.co.za （对于新客户）。 |

亚太地区（雅加达）

| 位置 | 如何申请连接 |
|----------------|---|
| DCI JK3，雅加达 | 联系印度尼西亚 DCI，邮箱为 awsdx@dc-indonesia.com 。 |
| NTT 2 数据中心，雅加达 | 联系 NTT，邮箱为 tps.cms.presales@global.ntt 。 |

亚太地区（孟买）

| 位置 | 如何申请连接 |
|--------------------------|--|
| Equinix，孟买 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| NetMagic DC2，班加罗尔 | 联系 NetMagic 销售和市场营销，免费电话为 18001033130，邮箱为 marketing@netmagicsolutions.com 。 |
| Sify Rabale，孟买 | 联系 Sify，邮箱为 aws.directconnect@sifycorp.com 。 |
| STT Delhi DC2，德里 | 联系 STT，邮箱为 enquiry.AWSDX@sttelemediagdc.in 。 |
| STT GDC Pvt. Ltd. VSB，钦奈 | 联系 STT，邮箱为 enquiry.AWSDX@sttelemediagdc.in 。 |
| STT Hyderabad DC1，海德拉巴 | 联系 STT，邮箱为 enquiry.AWSDX@sttelemediagdc.in 。 |

亚太地区（首尔）

| 位置 | 如何申请连接 |
|----------------------------------|---|
| Digital Realty ICN1，首尔 | 联系 Digital Realty，邮箱为 amazon.orders@digitalrealty.com 。 |
| KINX Gasan Data Center，首尔 | 联系 KINX，邮箱为 sales@kinx.net 。 |
| LG U+ Pyeong-Chon Mega Center，首尔 | 将 LOA 文档提交至 kidcadmin@lguplus.co.kr 和 center8@kidc.net 。 |

亚太地区（新加坡）

| 位置 | 如何申请连接 |
|----------------------------|--|
| EquinixHK1，香港特别行政区 荃湾新界 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix SG2，新加坡 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Global Switch，新加坡 | 联系 Global Switch，邮箱为 salingsingapore@globalswitch.com 。 |
| GPX，孟买 | 联系 GPX (Equinix)，邮箱为 awsdealreg@equinix.com 。 |
| iAdvantage Mega-i，中国香港 | 联系 iAdvantage，邮箱为 cs@iadvantage.net ，或者使用 iAdvantage 布线订单电子表格 下单。 |
| 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单请求表，请求交叉连接订单。 如果有任何问题联系 service.delivery@aims.com.my 提交请求。 |
| TCC 数据中心，曼谷 | 联系 TCC Technology Co., Ltd，邮箱为 gateway.ne@tcc-technology.com 。 |

亚太地区（悉尼）

| 位置 | 如何申请连接 |
|------------------|---|
| CDC Hume 2，堪培拉 | 登录 CDC 客户门户网站 上的客户门户。 |
| Datacom DH6，奥克兰 | 通过位于 奥克兰的 Datacom Orbit 联系 Datacom。 |
| Equinix ME2，墨尔本 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix SY3，悉尼 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Global Switch，悉尼 | 联系 Global Switch，邮箱为 salesydney@globalswitch.com 。 |
| NEXTDC C1，堪培拉 | 联系 NEXTDC，邮箱为 nxtops@nextdc.com 。 |
| NEXTDC M1，墨尔本 | 联系 NEXTDC，邮箱为 nxtops@nextdc.com 。 |
| NEXTDC P1，珀斯 | 联系 NEXTDC，邮箱为 nxtops@nextdc.com 。 |
| NEXTDC S2，悉尼 | 联系 NEXTDC，邮箱为 nxtops@nextdc.com 。 |

亚太地区（东京）

| 位置 | 如何申请连接 |
|------------------------------|---|
| AT Tokyo Chuo Data Center，东京 | 通过 at-sales@attokyo.co.jp 联系 AT TOKYO。 |
| 是方电讯，台北 | 联系 Chief Telecom，邮箱为 vicky_chan@chief.com.tw 。 |
| Chunghwa Telecom，台北 | 联系 CHT Taipei IDC NOC，邮箱为 taipei_idc@cht.com.tw 。 |
| Equinix OS1，大阪 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix TY2，东京 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| 印西 NEC，印西 | 联系印西 NEC，邮箱为 connection_support@ices.jp.nec.com 。 |

加拿大（中部）

| 位置 | 如何申请连接 |
|------------------------|--|
| Telehouse，多伦多前街西 250 号 | 联系 product@ca.telehouse.com 。 |
| Cologix MTL3，蒙特利尔 | 联系 Cologix，邮箱为 sales@cologix.com 。 |
| Cologix VAN2，温哥华 | 联系 Cologix，邮箱为 sales@cologix.com 。 |
| eStruxture，蒙特利尔 | 联系 eStruxture，邮箱为 directconnect@estrustructure.com 。 |

中国（北京）

| 位置 | 如何申请连接 |
|----------------------------|---|
| CIDS Jiachuang IDC，北京 | 联系 dx-order@sinnnet.com.cn 。 |
| Sinnnet Jiuxianqiao IDC，北京 | 联系 dx-order@sinnnet.com.cn 。 |
| GDS No. 3 数据中心，上海 | 联系 dx@nwcdcloud.cn 。 |
| GDS No. 3 数据中心，深圳 | 联系 dx@nwcdcloud.cn 。 |

中国（宁夏）

| 位置 | 如何申请连接 |
|------------|---|
| 工业园 IDC，宁夏 | 联系 dx@nwcdcloud.cn 。 |
| 沙坡头 IDC，宁夏 | 联系 dx@nwcdcloud.cn 。 |

欧洲地区（法兰克福）

| 位置 | 如何申请连接 |
|-------------------------|---|
| CE Colo，捷克布拉格 | 联系 CE Colo，邮箱为 info@cecolo.com 。 |
| DigiPlex Ulven，挪威奥斯陆 | 联系 DigiPlex，邮箱为 helpme@digiplex.com 。 |
| Equinix AM3，荷兰阿姆斯特丹 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix FR5，法兰克福 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix HE6，赫尔辛基 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix MU1，慕尼黑 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Equinix WA1，华沙 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Interxion AMS7，阿姆斯特丹 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Interxion CPH2，哥本哈根 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Interxion FRA6，法兰克福 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Interxion MAD2，马德里 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Interxion VIE2，维也纳 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Interxion ZUR1，苏黎世 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| IPB，柏林 | 联系 IPB，邮箱为 kontakt@ipb.de 。 |
| Equinix ITConic MD2，马德里 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

欧洲地区（爱尔兰）

| 位置 | 如何申请连接 |
|--------------------------|--|
| Digital Realty (UK), 码头区 | 联系 Digital Realty (UK), 邮箱为 amazon.orders@digitalrealty.com 。 |
| Eircom Clonshaugh | 通过 datacentre@eircom.ie 联系 Eircom。 |
| Equinix DX1, 迪拜 | 联系 Equinix, 邮箱为 awsdealreg@equinix.com 。 |
| Equinix LD5, 伦敦 (Slough) | 联系 Equinix, 邮箱为 awsdealreg@equinix.com 。 |
| Interxion DUB2, 都柏林 | 联系 Interxion, 邮箱为 customer.services@interxion.com 。 |
| Interxion MRS1, 马赛 | 联系 Interxion, 邮箱为 customer.services@interxion.com 。 |

欧洲地区（米兰）

| 位置 | 如何申请连接 |
|----------------------------------|--|
| CDLAN srl Via Caldera 21, Milano | 通过 sales@cdlan.it 与 CDLAN 联系。 |
| Equinix ML2, 意大利米兰 | 联系 Equinix, 邮箱为 awsdealreg@equinix.com 。 |

欧洲地区（伦敦）

| 位置 | 如何申请连接 |
|--------------------------|--|
| Digital Realty (UK), 码头区 | 联系 Digital Realty (UK), 邮箱为 amazon.orders@digitalrealty.com 。 |
| Equinix LD5, 伦敦 (Slough) | 联系 Equinix, 邮箱为 awsdealreg@equinix.com 。 |
| Equinix MA3, 曼彻斯特 | 联系 Equinix, 邮箱为 awsdealreg@equinix.com 。 |

| 位置 | 如何申请连接 |
|-------------------|--|
| Telehouse West，伦敦 | 联系 Telehouse UK，邮箱为 sales.support@uk.telehouse.net 。 |

欧洲地区（巴黎）

| 位置 | 如何申请连接 |
|-----------------------|---|
| Equinix PA3，巴黎 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Interxion PAR7，巴黎 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |
| Telehouse Voltaire，巴黎 | 使用 联系我们 页面联系 Telehouse Paris Voltaire。 |

欧洲地区（斯德哥尔摩）

| 位置 | 如何申请连接 |
|----------------------|---|
| Interxion STO1，斯德哥尔摩 | 联系 Interxion，邮箱为 customer.services@interxion.com 。 |

欧洲（苏黎世）

| 位置 | 如何申请连接 |
|-------------------------|---|
| Equinix ZRH51，瑞士奥伯伦斯特林根 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

以色列（特拉维夫）

| 位置 | 如何申请连接 |
|-----------|---|
| Medone，海法 | 联系 MedOne： support@Medone.co.il |

| 位置 | 如何申请连接 |
|------------------|--|
| EdgeConnex，海尔兹利亚 | 通过 info@edgeconnex.com 联系 EdgeConnect |

中东（巴林）

| 位置 | 如何申请连接 |
|----------------------|--|
| AWS Bahrain DC53，麦纳麦 | 要完成连接，您可以与我们的当地 网络提供商合作伙伴 合作建立连接。然后，您将通过 AWS 支持中心 向 AWS 提供网络提供商授权证书（LOA）。AWS 在该位置完成交叉连接。 |
| AWS Bahrain DC52，麦纳麦 | 要完成连接，您可以与我们的当地 网络提供商合作伙伴 合作建立连接。然后，您将通过 AWS 支持中心 向 AWS 提供网络提供商授权证书（LOA）。AWS 在该位置完成交叉连接。 |

中东（阿联酋）

| 位置 | 如何申请连接 |
|--------------------------------|--|
| Equinix DX1，阿联酋迪拜 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Etisalat SmartHub 数据中心，阿联酋富查伊拉 | 联系 Etisalat SmartHub 数据中心，邮箱为 IntlSales-C&WS@etisalat.ae 。 |

南美洲（圣保罗）

| 位置 | 如何申请连接 |
|-------------------------|--|
| Cirion BNARAGMS，布宜诺斯艾利斯 | 通过 cloud.connect@ciriontechnologies.com 联系 Cirion。 |
| Equinix RJ2，里约热内卢 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

| 位置 | 如何申请连接 |
|-----------------|---|
| Equinix SP4，圣保罗 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |
| Tivit | 联系 Tivit，邮箱为 aws@tivit.com.br 。 |

AWS GovCloud (美国东部)

您无法订购此区域中的连接。

AWS GovCloud (美国西部)

| 位置 | 如何申请连接 |
|-----------------|---|
| Equinix SV5，圣荷西 | 联系 Equinix，邮箱为 awsdealreg@equinix.com 。 |

Direct Connect 虚拟接口和托管虚拟接口

必须创建以下虚拟接口之一 (VIFs) 才能开始使用您的 Direct Connect 连接。

- 私有虚拟接口：应使用私有虚拟接口访问使用私有 IP 地址的 Amazon VPC。
- 公共虚拟接口：公共虚拟接口可以使用公有 IP 地址访问所有 AWS 公共服务。
- 中转虚拟接口：中转虚拟接口用于访问与 Direct Connect 网关关联的一个或多个 Amazon VPC 中转网关。您可以将公共虚拟接口与任何速度的任何 Direct Connect 专用或托管连接一起使用。有关 Direct Connect 网关配置的信息，请参阅[Direct Connect 网关](#)。

要使用 IPv6 地址连接到其他 AWS 服务，请查看服务文档以确认是否支持 IPv6 寻址。

公有虚拟接口前缀公布规则

我们会向您宣传合适的 Amazon 前缀，以便您可以访问您的 AWS 服务 VPCs 和其他服务中工作负载的公有 IP 地址。您可以通过此连接访问所有 AWS 前缀；例如，亚马逊 EC2 实例、Amazon S3、AWS 服务的 API 终端节点和 Amazon.com 使用的公有 IP 地址。您无权访问非 Amazon 前缀。有关使用的前缀的最新列表 AWS，请参阅 Amazon VPC 用户指南中的[AWS IP 地址范围](#)。在此页面上，您可以下载当前已发布 AWS 的 IP 范围的 .json 文件。请注意，对于已发布的 IP 地址范围：

- 与 AWS IP 地址范围列表中列出的前缀相比，通过公共虚拟接口通过 BGP 宣布的前缀可能会被聚合或取消聚合。
- .json 文件中不包含您 AWS 通过自己的 IP 地址 (BYOIP) 带来的任何 IP 地址范围，但 AWS 仍会通过公共虚拟接口通告这些 BYOIP 地址。
- AWS 不会将通过 Direct Connect 公共虚拟接口接收到的客户前缀重新通告到外部的网络。AWS 在公有虚拟接口上通告的前缀将对 AWS 上的所有客户可见。

Note

我们建议您使用防火墙过滤器（基于数据包 source/destination 的地址）来控制进出某些前缀的流量。

有关公有虚拟接口和路由策略的更多信息，请参阅 [the section called “公有虚拟接口路由策略”](#)。

SiteLink

如果您要创建私有或传输虚拟接口，则可以使用 SiteLink。

SiteLink 是专有虚拟接口的可选 Direct Connect 功能，它允许使用 AWS 网络上最短的可用路径在同一 AWS 分区中的任意两个 Direct Connect 接入点 (PoPs) 之间建立连接。这使您可以通过 AWS 全球网络连接本地网络，而无需经过区域路由流量。有关更多信息，SiteLink 请参阅[简介 Direct Connect SiteLink](#)。

Note

- SiteLink 在中国 AWS GovCloud (US) 和中国地区不可用。
- SiteLink 如果本地路由器在多个虚拟接口 AWS 上通告相同的路由，则不起作用。

使用时需要支付单独的定价费 SiteLink。有关更多信息，请参阅[AWS Direct Connect 定价](#)。

SiteLink 不支持所有虚拟接口类型。下表显示了接口类型以及是否受支持。

| 虚拟接口类型 | 支持/不支持 |
|---|--------|
| 中转虚拟接口 | 支持 |
| 连接到具有虚拟网关的 Direct Connect 网关的私有虚拟接口 | 支持 |
| 连接到与虚拟网关或中转网关无关的 Direct Connect 网关的私有虚拟接口 | 支持 |
| 连接到虚拟网关的私有虚拟接口 | 不支持 |
| 公有虚拟接口 | 不支持 |

通过 SiteLink 启用的虚拟接口从 AWS 区域（虚拟或传输网关）到本地位置的流量的流量路由行为与带有 AWS 路径预置的默认 Direct Connect 虚拟接口行为略有不同。启用后 SiteLink，无论关联的区域如何，来自的虚拟接口都 AWS 区域 首选从 Direct Connect 位置的 AS 路径长度较低的 BGP 路径。

例如，系统会为每个 Direct Connect 位置公布关联的区域。如果禁用 SiteLink 则默认情况下，来自虚拟网关或传输网关的流量会优先选择与该网关关联的 Direct Connect 位置 AWS 区域，即使来自与不同区域关联的 Direct Connect 位置的路由器通告的路径长度较短。虚拟或中转网关仍将首选从本地 Direct Connect 位置到关联 AWS 区域的路径。

SiteLink 支持最大巨型帧 MTU 大小为 8500 或 9001，具体取决于虚拟接口类型。有关更多信息，请参阅 [MTUs 用于私有虚拟接口或传输虚拟接口](#)。

虚拟接口的先决条件


在创建虚拟接口之前，请执行以下操作：

- 创建连接。有关更多信息，请参阅 [使用连接向导创建连接](#)。
- 当您有多个您希望将其视为单个连接的连接时，请创建一个链接聚合组 (LAG)。有关信息，请参阅 [将连接与 LAG 关联](#)。

要创建虚拟接口，您需要以下信息：

| 资源 | 所需信息 |
|-----------------|--|
| Connection | 您要为其创建虚拟接口的 Direct Connect 连接或链路聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 虚拟接口所有者 | 如果您要为另一个账户创建虚拟界面，则需要另一个 AWS 账户的账户 ID。 |
| (仅限私有虚拟接口) 连接 | <p>要连接到同一 AWS 区域的 VPC，您需要为自己的 VPC 提供虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关时，您可以指定自己的私有 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 创建虚拟私有网关。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。</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <ul style="list-style-type: none"> • 您不能在虚拟接口上对客户网关和虚拟 gateway/Direct Connect 网关使用相同的 ASN。 </div> |

| 资源 | 所需信息 |
|------|--|
| | <ul style="list-style-type: none"> • 您可以将同一个客户网关 ASN 用于多个虚拟接口。 • 多个虚拟接口可以具有相同的虚拟网关/Direct Connect 网关 ASN 和客户网关 ASN，前提是它们属于不同的 Direct Connect 连接。例如： <p style="margin-left: 20px;">虚拟网关 (ASN 64,496) <---虚拟接口 1 (Direct Connection 连接 1) ---> 客户网关 (ASN 64,511)</p> <p style="margin-left: 20px;">虚拟网关 (ASN 64,496) <---虚拟接口 2 (Direct Connection 连接 2) ---> 客户网关 (ASN 64,511)</p> |
| VLAN | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果您有托管连接，则您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |

| 资源 | 所需信息 |
|----------|--|
| 对等 IP 地址 | <p>虚拟接口可以支持 IPv4、IPv6 或其中一个（双栈）的 BGP 对等会话。请勿使用 Amazon 池中的 Elastic IPs (EIPs) 或自带 IP 地址 (BYOIP) 来创建公共虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> IPv4: <ul style="list-style-type: none"> (仅限公共虚拟接口) 您必须指定自己拥有的唯一公有 IPv4 地址。 <div data-bbox="467 646 1507 1129" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <ul style="list-style-type: none"> 私有和传输虚拟接口 IPs 的对等连接可以来自任何有效的 IP 范围。这也可以包括客户拥有的公有 IP 地址，前提是这些地址仅用于创建 BGP 对等会话，而不是通过虚拟接口通告或用于 NAT。 我们不能保证我们能够满足所有 AWS 提供公共 IPv4 地址的请求。 </div> <p>值可以是以下之一：</p> <ul style="list-style-type: none"> 客户拥有 IPv4 的 CIDR <p>它们可以是任何公用 IPs（客户拥有或由提供 AWS），但是对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /31 范围，例如 203.0.113.0/31，则可以将其 203.0.113.0 用于对等 IP 和 203.0.113.1 对 AWS 等 IP。或者，如果您分配了一个 /24 范围，例如 198.51.100.0/24，则可以将其 198.51.100.10 用于对等 IP 和 198.51.100.20 对 AWS 等 IP。</p> 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权。 |

| 资源 | 所需信息 |
|--------|--|
| | <ul style="list-style-type: none"> • AWS 提供的 /31 CIDR。联系 Su AWS support 申请公共 IPv4 CIDR (并在请求中提供用例) • (仅限私有虚拟接口) Amazon 可以为您生成私有 IPv4 地址。如果您自己指定，请确保 CIDRs 为路由器接口指定私有接口，并且仅为 Direct Connect 接口指定私有接口。例如，请勿指定本地网络中的其他 IP 地址。与公共虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配了一个 /30 范围，例如 192.168.0.0/30，则可以将其 192.168.0.1 用于对等 IP 和 192.168.0.2 对 AWS 等 IP。 • IPv6: 亚马逊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。 |
| 地址系列 | BGP 对等会话是否会结束 IPv4 还是 IPv6 |
| BGP 信息 | <ul style="list-style-type: none"> • 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (ASN)。如果您使用的是公有 ASN，则必须拥有其所有权。如果您使用的是私有 ASN，则可以设置自定义 ASN 值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 1 到 2147483647 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。 • AWS MD5 默认情况下启用。您无法修改此选项。 • MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 |

| 资源 | 所需信息 |
|----------------------|---|
| (仅限公有虚拟接口) 您要公布的前缀 | <p>要通过 BGP 发布的公共 IPv4 IPv6 路由或路由。您必须使用 BGP 至少公布一个前缀，最多 1000 个前缀。</p> <ul style="list-style-type: none"> IPv4: 当以下任一条件为真 Direct Connect 时，IPv4 CIDR IPv4 R 可以与使用宣布的另一个公共 CIDR 重叠： <ul style="list-style-type: none"> CIDRs 他们来自不同 AWS 的地区。确保在公有前缀上应用 BGP 社区标签。 如果配置中有公用 ASN，则可以使用 AS_PATH。 active/passive <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> 通过 Direct Connect 公共虚拟接口，您可以为其指定从 /1 到 /32 以及从 /1 到 /6 IPv4 4 之间的任意前缀长度。 IPv6 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |
| (仅限私有和中转虚拟接口) 巨型帧 | <p>数据包的最大传输单位 (MTU)。 Direct Connect 默认为 1500。将虚拟接口的 MTU 设置为 8500 (巨型帧) 可能会导致底层物理连接更新 (如果之前未更新为支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。 Direct Connect 最多支持 8500 MTU 的巨型帧。在中转网关路由表中配置的静态路由和传播路由将支持巨型帧，包括具有 VPC 静态路由表条目的 EC2 实例和中转网关连接。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口“常规配置”页面上找到支持巨型帧。</p> |

创建虚拟接口时，可以指定拥有虚拟接口的账户。当您选择的 AWS 账户不是您的账户时，以下规则适用：

- 对于私有 VIFs 和传输 VIFs，该账户适用于虚拟接口和虚拟私有 gateway/Direct Connect 网关目标。
- 对于公众 VIFs，该账户用于虚拟接口计费。数据传出 (DTO) 使用量按 Direct Connect 数据传输速率向资源所有者计量。

Note

所有 Direct Connect 虚拟接口类型均支持 31 位前缀。有关更多信息，请参阅 [RFC 3021：在链接上使用 31 位前缀。IPv4 Point-to-Point](#)

MTUs 用于私有虚拟接口或传输虚拟接口

Direct Connect 在链路层支持大小为 1522 或 9023 字节 (14 字节以太网标头 + 4 字节 VLAN 标签 + IP 数据报的字节 + 4 字节 FCS) 的以太网帧大小。

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小 (以字节为单位)。私有虚拟接口的 MTU 可以是 1500 或 9001 (巨型帧)。中转虚拟接口的 MTU 可以是 1500 或 8500 (巨型帧)。您可以在创建接口时指定 MTU，也可以在创建接口后对其进行更新。将虚拟接口的 MTU 设置为 8500 (巨型帧) 或 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在“摘要”选项卡上找到“支持巨型帧”。

为私有虚拟接口或中转虚拟接口启用巨型帧后，您只能将其与支持巨型帧的连接或 LAG 关联。连接到虚拟私有网关或 Direct Connect 网关的私有虚拟接口，或者连接到 Direct Connect 网关的中转虚拟接口支持巨型帧。如果您有两个通告相同路由但使用不同的 MTU 值的私有虚拟接口，或者您的 Site-to-Site VPN 通告相同的路由，则使用 1500 MTU。

Important

巨型帧仅适用于通过中转网关的传播路由 Direct Connect 和通过中转网关的静态路由。中转网关上的巨型帧仅支持 8500 字节。

如果 EC2 实例不支持巨型帧，将从 Direct Connect 中删除巨型帧。除了 C1、T1 和 M1 之外 CC1，所有 EC2 实例类型都支持巨型帧。有关更多信息，请参阅《Amazon EC2 用户指南》中的 [EC2 实例的网络最大传输单位 \(MTU \)](#)。

对于托管连接，只有最初在 Direct Connect 托管父连接上启用时才能启用巨型帧。如果在父连接上未启用巨型帧，则在任何连接上都无法启用。

有关为私有虚拟接口设置 MTU 的步骤，请参阅 [设置私有虚拟接口的 MTU](#)。

Direct Connect 虚拟接口

您可以创建一个中转虚拟接口连接中转网关，创建一个公有虚拟接口连接公有资源（非 VPC 服务），或创建一个私有虚拟接口连接 VPC。

要为 AWS Organizations 或与您不同的 AWS Organizations 内的账户创建虚拟接口，请创建托管的虚拟接口。

要创建虚拟接口，请参阅以下内容：

- [创建公有虚拟接口](#)
- [创建私有虚拟接口](#)
- [创建到 Direct Connect 网关的中转虚拟接口](#)

先决条件

在您开始之前，请确保您阅读了 [虚拟接口的先决条件](#) 中的信息。

将虚拟接口中转到 Direct Connect 网关的先决条件

要将您的 Direct Connect 连接到中转网关，必须为您的连接创建一个中转接口。指定要连接到的 Direct Connect 网关。

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小（以字节为单位）。私有虚拟接口的 MTU 可以是 1500 或 9001（巨型帧）。中转虚拟接口的 MTU 可以是 1500 或 8500（巨型帧）。您可以在创建接口时指定 MTU，也可以在创建接口后对其进行更新。将虚拟接口的 MTU 设置为 8500（巨型帧）或 9001（巨型帧）可能会导致更新底层物理连接（如果它之前未更新以支持巨型帧）。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在摘要选项卡上找到支持巨型帧。

Important

如果您将中转网关与一个或多个 Direct Connect 网关关联，则中转网关和 Direct Connect 网关使用的自治系统号 (ASN) 必须不同。例如，如果您对中转网关和 Direct Connect 网关使用默认的 ASN 64512，则关联请求将失败。

创建 Direct Connect 公有虚拟接口

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

预配置公有虚拟接口

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。
5. 在 Public virtual interface settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - d. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统编号 (ASN)。

有效值为 1 到 4294967294。这包括对 ASN (1-2147483647) 和长 ASN (1-4294967294) 的支持。有关 ASN 和长 ASN 的更多信息，请参阅 [长期支持 ASN Direct Connect](#)。

Note

通过公有虚拟接口与 AWS 建立 BGP 对等会话时，请使用 7224 作为 ASN 在 AWS 侧建立 BGP 会话。您的路由器或客户网关设备上的 ASN 应与该 ASN 不同。

6. 在 Additional settings (其他设置) 下，执行以下操作：
 - a. 要配置 IPv4 BGP 或 IPv6 对等，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等，请选择 IPv4，然后执行下列操作之一：

 - 要自行指定这些 IP 地址，对于 Your router peer IP (您的路由器对等 IP)，输入 Amazon 将流量发送到的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。

[IPv6] 要配置 IPv6 BGP 对等，请选择 IPv6。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。
 - b. 要提供您自己的 BGP 密钥，请输入您的 BGP MD5 密钥。

如果您不输入值，我们将生成一个 BGP 密钥。如果您提供了自己的密钥，或者我们为您生成了密钥，则该值将显示在虚拟接口的虚拟接口详细信息页面上的 BGP 身份验证密钥列中。

- c. 要将前缀公布到 Amazon，对于 Prefixes you want to advertise (您要公布的前缀)，输入通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号分隔)。

Important

您可以向现有的公有 VIF 添加额外的前缀，并联系 [AWS support](#) 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。

- d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

7. 选择 Create virtual interface (创建虚拟接口)。
8. 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](#)。

使用命令行或 API 创建公有虚拟接口

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

创建 Direct Connect 私有虚拟接口

您可以为您的 Direct Connect 连接所在的区域中的虚拟私有网关预置一个私有虚拟接口。有关预置到 Direct Connect 网关的私有虚拟接口的更多信息，请参阅 [Direct Connect 网关](#)。

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](#)。

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小 (以字节为单位)。私有虚拟接口的 MTU 可以是 1500 或 9001 (巨型帧)。中转虚拟接口的 MTU 可以是 1500 或

8500 (巨型帧)。您可以在创建接口时指定 MTU，也可以在创建接口后对其进行更新。将虚拟接口的 MTU 设置为 8500 (巨型帧) 或 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧)。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在摘要选项卡上找到支持巨型帧。

配置与 VPC 间的私有虚拟接口

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在虚拟接口类型下，选择私有。
5. 在私有虚拟接口设置下，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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
- c. 对于虚拟接口所有者，如果虚拟接口用于您的 AWS 账户，则选择我的 AWS 账户。
- d. 对于 Direct Connect 网关，选择 Direct Connect 网关。
- e. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
- f. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括对 ASN (1-2147483647) 和长 ASN (1-4294967294) 的支持。有关 ASN 和长 ASN 的更多信息，请参阅 [长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：

- a. 要配置 IPv4 BGP 或 IPv6 对等，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等，请选择 IPv4，然后执行下列操作之一：

- 要自行指定这些 IP 地址，对于 Your router peer IP (您的路由器对等 IP)，输入 Amazon 将流量发送到的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。

Important

配置 AWS Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0/16 IPv4 链路本地范

围分配的 AWS 分配 IPv4 /29 CIDR 地址以实现点对点连接。这些点对点连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等连接。对于 VPC 流量或隧道传输目的，例如 AWS 站点到站点私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是点对点连接。

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等，请选择 IPv6。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。

- 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 8500 (巨型帧)，请选择 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500))。
- (可选) 在启用 SiteLink 下，选择启用以启用 Direct Connect 接入点之间的直接连接。
- (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

- 选择 Create virtual interface (创建虚拟接口)。
- 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](#)。

使用命令行或 API 创建私有虚拟接口

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

为 Direct Connect 网关创建中转虚拟接口

在将中转虚拟接口连接到 Direct Connect 网关之前，请先熟悉[文本](#)。

为 Direct Connect 网关配置中转虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。

创建到 Direct Connect 网关的中转虚拟接口

2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Transit (中转)。
5. 在 Transit virtual interface settings (中转虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，如果虚拟接口适用于您的 AWS 账户，请选择我的 AWS 账户。
 - d. 对于 Direct Connect 网关，选择 Direct Connect 网关。
 - e. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - f. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：

- a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 8500 (巨型帧)，请选择 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500))。
- c. (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。
- d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

创建虚拟接口后，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](#)。

使用命令行或 API 创建中转虚拟接口

- [create-transit-virtual-interface](#) (AWS CLI)
- [CreateTransitVirtualInterface](#) (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-附件](#) () AWS CLI
- [DescribeDirectConnectGatewayAttachments](#) (Direct Connect API)

下载 Direct Connect 路由器配置文件

创建虚拟接口后且接口状态为运行时，您可以下载路由器的路由器配置文件。

如果您将以下任何路由器用于开启 MACsec 的虚拟接口，我们会自动为您的路由器创建配置文件：

- 运行 NX-OS 9.3 或更高版本软件的 Cisco Nexus 9K+ 系列交换机
- 运行 JunOS 9.5 或更高版本软件的 Juniper Networks M/X 系列路由器

下载路由器配置文件

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。
4. 选择 Download router configuration (下载路由器配置)。
5. 对于下载路由器配置，执行以下操作：
 - a. 对于 Vendor (供应商)，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。
6. 选择下载，然后使用适合您的路由器的配置，以确保您可以连接到 Direct Connect。
7. 如果需要为 MACsec 手动配置路由器，请参考下表。

| 参数 | 描述 |
|------------|---|
| CKN 长度 | 这是一个 64 十六进制字符 (0-9 , A-E) 字符串。使用全长可最大限度地提高跨平台兼容性。 |
| CAK 长度 | 这是一个 64 十六进制字符 (0-9 , A-E) 字符串。使用全长可最大限度地提高跨平台兼容性。 |
| 加密算法 | AES_256_CMAC |
| SAK 密码套件 | <ul style="list-style-type: none"> • 对于 100Gbps 连接：GCM_AES_XPN_256 • 对于 10Gbps 连接：GCM_AES_XPN_256 或 GCM_AES_256 |
| 密钥密码套件 | 16 |
| 加密偏移 | 0 |
| ICV 指示符 | 否 |
| SAK 更改密钥时间 | PN 滚动> |


托管式 Direct Connect 虚拟接口

要通过其他账户使用您的 Direct Connect 连接，您可以为该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。

您可以将中转虚拟接口与任何速度的 Direct Connect 专用或托管连接一起使用。托管连接仅支持一个虚拟接口。

要创建虚拟接口，您需要以下信息：

| 资源 | 所需信息 |
|-----------------|---|
| Connection | 要为其创建虚拟接口的 Direct Connect 连接或链接聚合组 (LAG)。 |
| 虚拟接口名称 | 虚拟接口的名称。 |
| 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。 |
| (仅限私有虚拟接口) 连接 | 要连接到同一 AWS 区域中的 VPC，您需要 VPC 的虚拟私有网关。BGP 会话 Amazon 端的 ASN 从虚拟私有网关继承。当您创建虚拟私有网关时，您可以指定自己的私有 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 创建虚拟私有网关 。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 | <p>您的连接上尚未使用的唯一虚拟局域网 (VLAN) 标签。该值必须介于 1 和 4094 之间，并且必须符合以太网 802.1Q 标准。任何经过 Direct Connect 连接的流量都必须有此标签。</p> <p>如果使用托管连接，您的 AWS Direct Connect 合作伙伴会提供此值。创建虚拟接口后，无法修改此值。</p> |
| 对等 IP 地址 | <p>虚拟接口支持 IPv4、IPv6 或其中一个 (双堆栈) 的 BGP 对等会话。请勿使用 Amazon 池中的弹性 IP (EIP) 或自带 IP 地址 (BYOIP) 来创建公有虚拟接口。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 地址范围分配到 BGP 对等会话虚拟接口的每一端。</p> <ul style="list-style-type: none"> IPv4: |

| 资源 | 所需信息 |
|------|--|
| | <ul style="list-style-type: none"> （仅限公有虚拟接口）您必须指定您拥有的唯一公有 IPv4 地址。值可以是以下之一： <ul style="list-style-type: none"> 客户拥有的 IPv4 CIDR <p>这些 IP 可以是任何公有 IP（客户拥有或由 AWS 提供），但对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配一个 /31 范围，比如 203.0.113.0/31，则可以将 203.0.113.0 用于对等 IP，将 203.0.113.1 用于 AWS 对等 IP。或者，如果您分配一个 /24 范围，比如 198.51.100.0/24，则可以将 198.51.100.10 用于对等 IP，将 198.51.100.20 用于 AWS 对等 IP。</p> AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权 AWS 提供的 /31 CIDR。联系 AWS Support，请求一个公有 IPv4 CIDR（并在您的请求中提供一个用例） <div data-bbox="496 919 1507 1138" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>我们无法保证能够满足对 AWS 提供的公有 IPv4 地址的所有请求。</p> </div> <ul style="list-style-type: none"> （仅限私有虚拟接口）Amazon 可以为您生成私有 IPv4 地址。如果您指定自己的 CIDR，请确保仅为路由器接口和 AWS Direct Connect 接口指定私有 CIDR。例如，请勿指定本地网络中的其他 IP 地址。与公有虚拟接口类似，对等 IP 和 AWS 路由器对等 IP 必须使用相同的子网掩码。例如，如果您分配一个 /30 范围，比如 192.168.0.0/30，则可以将 192.168.0.1 用于对等 IP，将 192.168.0.2 用于 AWS 对等 IP。 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。 |
| 地址系列 | BGP 对等会话是通过 IPv4 还是 IPv6 进行。 |

| 资源 | 所需信息 |
|---|--|
| <p>BGP 信息</p> <p>(仅限公有虚拟接口) 您要公布的前缀</p> | <ul style="list-style-type: none"> 您这一端 BGP 会话的公有或私有边界网关协议 (BGP) 自治系统号 (AS N) 。如果您使用的是公有 ASN ，则必须拥有其所有权。如果您使用的是私有 ASN ，则可以设置自定义 ASN 值。对于 16 位 ASN ，该值必须在 64512 到 65534 范围内。对于 32 位 ASN ，该值必须在 1 到 4294967294 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。 AWS 默认启用 MD5。您无法修改此选项。 MD5 BGP 身份验证密钥。您可以提供自己的身份验证密钥，也可以让 Amazon 为您生成一个密钥。 <p>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。</p> <ul style="list-style-type: none"> IPv4：当以下任一项为 true 时，IPv4 CIDR 可能与使用 Direct Connect 公布的另一个公有 IPv4 CIDR 重叠： <ul style="list-style-type: none"> CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。 <p>有关更多信息，请参阅路由策略和 BGP 社区。</p> <ul style="list-style-type: none"> 通过 Direct Connect 公有虚拟接口，您可以为 IPv4 指定从 /1 到 /32 之间的任意前缀长度，为 IPv6 指定从 /1 到 /64 之间的任意前缀长度。 您可以向现有的公有 VIF 添加额外的前缀，并联系 AWS support 来公布这些前缀。在您的支持案例中，请提供您希望添加到公有 VIF 并进行公布的其他 CIDR 前缀列表。 |
| <p>(仅限私有和中转虚拟接口) 巨型帧</p> | <p>Direct Connect 上数据包的最大传输单元 (MTU) 。默认为 1500。将虚拟接口的 MTU 设置为 9001 (巨型帧) 可能会导致更新底层物理连接 (如果它之前未更新以支持巨型帧) 。更新连接会中断与连接关联的所有虚拟接口的网络连接，最长可达 30 秒。巨型帧仅适用于从 Direct Connect 传播的路由。如果在路由表中添加指向虚拟私有网关的静态路由，则通过静态路由传输的流量将使用 1500 MTU 发送。要检查连接或虚拟接口是否支持巨型帧，请在 Direct Connect 控制台中将其选中，然后在虚拟接口常规配置页面上找到支持巨型帧。</p> |

在中创建托管私有虚拟接口 Direct Connect

在您开始之前，请确保您阅读了 [虚拟接口的先决条件](#) 中的信息。

创建托管私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在虚拟接口类型下，对于类型，选择私有。
5. 在私有虚拟接口设置下，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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，选择其他 AWS 账户，对于虚拟接口所有者，输入拥有此虚拟接口的账户 ID。
 - d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - e. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅 [长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对

等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 8500 (巨型帧)，请选择 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500))。
- c. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 在托管虚拟接口被其他 AWS 账户的所有者接受后，就可以下载配置文件。有关更多信息，请参阅[下载路由器配置文件](#)。

使用命令行或 API 创建托管私有虚拟接口

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

在中创建托管的公共虚拟接口 Direct Connect

在您开始之前，请确保您阅读了[虚拟接口的先决条件](#)中的信息。

创建托管公有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Public (公有)。

5. 在 Public Virtual Interface Settings (公有虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，选择其他 AWS 帐户，然后为虚拟接口所有者输入拥有此虚拟接口的帐户的 ID。
 - d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - e. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括对 ASNs (1-2147483647) 和多头 (1-4294967294) 的支持。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

7. 要向 Amazon 宣传前缀，对于要宣传的前缀，请输入应通过虚拟接口将流量路由到的 IPv4 CIDR 目标地址 (用逗号分隔)。
8. 要提供您自己的密钥以验证 BGP 会话，请在 Additional Settings (附加设置) 下，为 BGP authentication key (BGP 验证密钥) 输入该密钥。

如果您不输入值，我们将生成一个 BGP 密钥。

9. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

10. 选择 Create virtual interface (创建虚拟接口)。

11. 在托管虚拟接口被其他 AWS 账户的所有者接受后，就可以下载配置文件。有关更多信息，请参阅 [下载路由器配置文件](#)。

使用命令行或 API 创建托管公有虚拟接口

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

创建 Direct Connect 托管公有虚拟接口

创建托管中转虚拟接口

Important

如果您将中转网关与一个或多个 Direct Connect 网关关联，则中转网关和 Direct Connect 网关使用的自治系统号 (ASN) 必须不同。例如，如果您对中转网关和 Direct Connect 网关使用默认的 ASN 64512，则关联请求将失败。

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Transit (中转)。
5. 在 Transit virtual interface settings (中转虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，选择其他 AWS 帐户，然后为虚拟接口所有者输入拥有此虚拟接口的帐户的 ID。
 - d. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - e. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括对 ASNs (1-2147483647) 和多头 (1-4294967294) 的支持。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅 [长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：

a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

- 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
- 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 8500 (巨型帧)，请选择 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500))。

c. [可选] 添加标签。执行以下操作：

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

8. 在托管虚拟接口被其他 AWS 账户的所有者接受后，就可以为您的设备下载路由器配置文件。有关更多信息，请参阅[下载路由器配置文件](#)。

使用命令行或 API 创建托管中转虚拟接口

- [allocate-transit-virtual-interface](#) (AWS CLI)
- [AllocateTransitVirtualInterface](#)(Direct Connect API)

查看 Direct Connect 虚拟接口详细信息

您可以使用 Direct Connect 控制台或使用命令行或 API 更改虚拟接口的状态。详细信息包括：

- 连接状态
- 名称
- 位置
- VLAN
- BGP 详细信息
- 对等 IP 地址

如何查看有关虚拟接口的详细信息

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在左侧窗格中，选择虚拟接口。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。

使用命令行或 API 描述虚拟接口

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

将 BGP 对等体添加到 Direct Connect 虚拟接口

使用 Direct Connect 控制台或使用命令行或 API 向您的虚拟接口添加或删除 IPv4 或 IPv6 BGP 对等会话。

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。

AWS 默认启用 MD5。您无法修改此选项。

使用以下过程可添加 BGP 对等体。

添加 BGP 对等体

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。
4. 选择添加对等体。
5. (私有虚拟接口) 要添加 IPv4 BGP 对等体，请执行以下操作：
 - 选择 IPv4。
 - 要自行指定这些 IP 地址，对于 Your router peer IP (您的路由器对等 IP)，输入 Amazon 将流量发送到的目标 IPv4 CIDR 地址。对于 Amazon 路由器对等 IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。
6. (公有虚拟接口) 要添加 IPv4 BGP 对等体，请执行以下操作：
 - 对于您的路由器对等 IP，输入应发送流量的 IPv4 CIDR 目标地址。
 - 对于 Amazon 路由器对等 IP，输入用于将流量发送到 AWS 的 IPv4 CIDR 地址。

Important

配置 AWS Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0/16 IPv4 链路本地范围分配的 AWS 分配 IPv4 /29 CIDR 地址以实现点对点连接。这些点对点连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等连接。对于 VPC 流量或隧道传输目的，例如 AWS 站点到站点私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是点对点连接。

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

7. (私有或公有虚拟接口) 要添加 IPv6 BGP 对等体，请选择 IPv6。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。
8. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

对于公有虚拟接口，ASN 必须为私有或已在虚拟接口的允许列表中。

有效值为 1 到 4294967294。这包括对 ASN (1-2147483646) 和长 ASN (1-4294967294) 的支持。有关 ASN 和长 ASN 的更多信息，请参阅 [长期支持 ASN Direct Connect](#)。

请注意，如果您没有输入值，我们会自动分配一个值。

9. 要提供您自己的 BGP 密钥，对于 BGP 身份验证密钥，输入您的 BGP MD5 密钥。
10. 选择添加对等体。

使用命令行或 API 创建 BGP 对等体

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

删除 Direct Connect 虚拟接口 BGP 对等体

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)。您可以使用 Direct Connect 控制台或使用命令行或 API 删除虚拟接口 BGP 对等体。

删除 BGP 对等体

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。
4. 在 Peerings (对等体) 下，选择您要删除的对等体，然后选择 Delete (删除)。
5. 在 Remove peering from virtual interface (从虚拟接口中删除对等体) 对话框中，选择 Delete (删除)。

使用命令行或 API 删除 BGP 对等体

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

设置 Direct Connect 私有虚拟接口的 MTU

如果您的虚拟接口同时具有 IPv4 和 IPv6 BGP 对等会话，则可以删除其中一个 BGP 对等会话（但不能同时删除两个）。有关私有虚拟接口 MTUs 的更多信息，请参阅了解[MTUs 私有虚拟接口或传输虚拟接口](#)。

您可以使用 Direct Connect 控制台、命令行或 API 来设置私有虚拟接口的 MTU。

设置私有虚拟接口的 MTU

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 Edit (编辑)。
4. 在 Jumbo MTU (MTU 大小 8500) 下，选择 已启用。
5. 在 Acknowledge (确认) 下，选择 I understand the selected connection(s) will go down for a brief period (我知道，所选连接将在短时间内断开)。更新完成之前，虚拟接口的状态为 pending。

使用命令行或 API 设置私有虚拟接口的 MTU

- [update-virtual-interface-attributes](#) (AWS CLI)
- [UpdateVirtualInterfaceAttributes](#)(Direct Connect API)

添加或删除 Direct Connect 虚拟接口标签

标签提供一种方法来标识虚拟接口。如果您是虚拟接口的账户所有者，则可以使用 Direct Connect 控制台或使用命令行或 API 添加或删除标签。

添加或删除虚拟接口标签

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 Edit (编辑)。
4. 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。

- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

5. 选择 Edit virtual interface (编辑虚拟接口)。

要使用命令行添加和删除标签

- [tag-resource](#) (AWS CLI)
- [untag-resource](#) (AWS CLI)

删除 Direct Connect 虚拟接口

删除一个或多个虚拟接口。您必须先删除虚拟接口，然后才能删除连接。删除虚拟接口会终止对与虚拟接口相关 Direct Connect 数据传输收费。

您可以使用 Direct Connect 控制台或使用命令行或 API 删除虚拟接口。

删除虚拟接口

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在左侧窗格中，选择虚拟接口。
3. 选择虚拟接口，然后选择 Delete (删除)。
4. 在 Delete (删除) 确认对话框中，选择 Delete (删除)。

使用命令行或 API 删除虚拟接口

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

接受托管 Direct Connect 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私有网关或 Direct Connect 网关。对于中转虚拟接口，您还必须已有中转网关或 Direct Connect 网关。

您可以使用 Direct Connect 控制台、命令行或 API 接受托管虚拟接口。

如何接受托管虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 View details (查看详细信息)。
4. 选择 Accept (接受)。
5. 这适用于私有虚拟接口和中转虚拟接口。

(中转虚拟接口) 在 Accept virtual interface (接受虚拟接口) 对话框中，选择 Direct Connect 网关，然后选择 Accept virtual interface (接受虚拟接口)。

(私有虚拟接口) 在 Accept virtual interface (接受虚拟接口) 对话框中，选择虚拟私有网关或 Direct Connect 网关，然后选择 Accept virtual interface (接受虚拟接口)。

6. 在您接受托管虚拟接口之后，Direct Connect 连接的所有者可下载路由器配置文件。下载路由器配置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](#)(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](#)(Direct Connect API)

使用命令行或 API 接受托管中转虚拟接口

- [confirm-transit-virtual-interface](#) (AWS CLI)
- [ConfirmTransitVirtualInterface](#)(Direct Connect API)

迁移 Direct Connect 虚拟接口

如果要执行以下任一虚拟接口迁移操作，请使用此过程：

- 将与某个连接关联的现有虚拟接口迁移到另一个 LAG。

- 将与某个现有 LAG 关联的现有虚拟接口迁移到新 LAG。
- 将与某个连接关联的现有虚拟接口迁移到另一个连接。

Note

- 您可以将虚拟接口迁移到同一区域内的新连接，但不能将其从一个区域迁移到另一个区域。将现有虚拟接口迁移或关联到新连接时，与这些虚拟接口关联的配置参数是相同的。要解决此问题，您可以在连接上预先设置配置，然后更新 BGP 配置。
- 您无法将 VIF 从一个托管连接迁移到另一个托管连接。VLAN ID 是唯一的；因此，以这种方式迁移 VIF 意味着 VLAN 不匹配。您需要删除连接或 VIF，然后使用连接和 VIF 都相同的 VLAN 重新创建。

Important

虚拟接口会短暂关闭。我们建议您在维护时段执行此过程。

迁移虚拟接口

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择虚拟接口，然后选择 Edit (编辑)。
4. 对于 Connection (连接)，请选择 LAG 或连接。
5. 选择 Edit virtual interface (编辑虚拟接口)。

使用命令行或 API 迁移虚拟接口

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

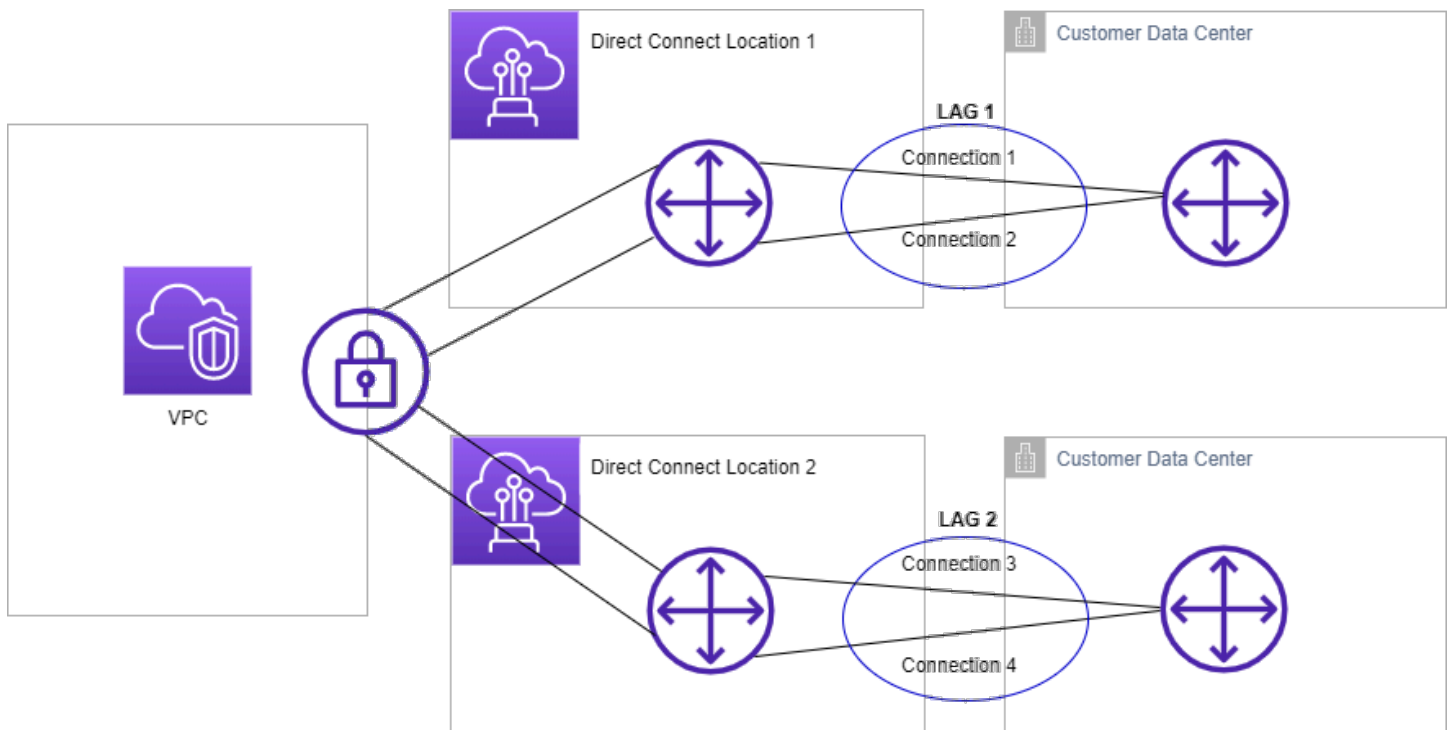
Direct Connect 链接聚合组 (LAG)

您可以使用多个连接来增加可用带宽。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 Direct Connect 终端节点处聚合多个连接，从而允许您将这些连接视为一个托管连接。LAG 简化了配置，因为 LAG 配置适用于组中的所有连接。

Note

AWS 不支持多机箱 LAG (MLAG)。

在下图中，您有四个连接，每个位置有两个连接。您可以为在同一 AWS 设备终止的连接创建一个 LAG，然后使用两个 LAG (而非四个连接) 进行配置和管理。



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：

- 所有连接都必须是专用连接，端口速度为 1 Gbps、10 Gbps、100 Gbps 或 400 Gbps。
- LAG 中的所有连接都必须使用相同的带宽。

- 在 LAG 中，您最多可以有两个 100 Gbps 或 400 Gbps 的连接，或四个端口速度低于 100 Gbps 的连接。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 Direct Connect 终端节点。
- 所有虚拟接口类型（公有、私有和中转）都支持 LAG。

创建 LAG 时，您可以从 Direct Connect 控制台分别为每个新的物理连接下载《授权和连接设备分配通知函（LOA-CFA）》。有关更多信息，请参阅 [《授权和连接设备分配通知函（LOA-CFA）》](#)。

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，如果运行连接数低于此阈值，整个 LAG 将无法运行。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 Direct Connect 终端节点上有足够的可用端口。

主题

- [适用于 Direct Connect 的 MACsec 注意事项](#)
- [在 Direct Connect 端点上创建 LAG](#)
- [查看 Direct Connect 终端节点的 LAG 详细信息](#)
- [更新位于 Direct Connect 端点的 LAG](#)
- [将连接与 Direct Connect 端点中的 LAG 相关联](#)
- [解除连接与位于 Direct Connect 端点的 LAG 的关联](#)
- [将 MACsec CKN/CAK 与 Direct Connect 端点 LAG 关联](#)
- [移除 MACsec 密钥和 Direct Connect 端点 LAG 之间的关联](#)
- [删除 Direct Connect 端点 LAG](#)

适用于 Direct Connect 的 MACsec 注意事项

要在 LAG 上配置 MACsec 时，请考虑以下几点：

- 当您从现有连接创建 LAG 时，我们会解除所有 MACsec 密钥与连接的关联。然后，我们将连接添加到 LAG，并将 LAG MACsec 密钥与这些连接关联。
- 在将现有连接与 LAG 关联时，当前与 LAG 关联的 MACsec 密钥也将与该连接关联。因此，我们将 MACsec 密钥与连接解除关联，将连接添加到 LAG，然后将 LAG MACsec 密钥与连接关联。
- 任何时候在所有 LAG 链路上只能使用一个 MacSec 密钥。支持多个 MACsec 密钥的功能仅用于密钥轮换目的。

在 Direct Connect 端点上创建 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。

要从现有连接创建 LAG，连接必须位于同一 AWS 设备上（在同一 Direct Connect 端点终止）。它们还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。

利用新连接创建 LAG

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择创建 LAG。
4. 在 Lag creation type (Lag 创建类型) 下，选择请求新连接，然后提供以下信息：
 - LAG name (LAG 名称)：LAG 的名称。
 - Location (位置)：LAG 的位置。
 - 端口速度：连接的端口速度。
 - 新连接数：要创建的新连接的数量。当端口速度为 1 G 或 10 G 时，最多可以有四个连接；当端口速度为 100 Gbps 或 400 Gbps 时，最多可以有两个连接。
 - (可选) 为连接配置 MAC 安全 (MACsec)。在其他设置下，选择请求支持 MACsec 的端口。

MACsec 仅在专用连接上可用。

- (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签) ，然后执行以下操作：

- 对于 Key (键) ，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签) 。

5. 选择创建 LAG。

通过现有连接创建 LAG

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择创建 LAG。
4. 在 Lag creation type (Lag 创建类型) 下，选择使用现有连接，然后提供以下信息：
 - LAG name (LAG 名称)：LAG 的名称。
 - 现有连接：用于 LAG 的 Direct Connect 连接。
 - (可选) 新连接数：要创建的新连接数。当端口速度为 1 G 或 10 G 时，最多可以有四个连接；当端口速度为 100 Gbps 或 400 Gbps 时，最多可以有两个连接。
5. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签) ，然后执行以下操作：

- 对于 Key (键) ，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签) 。

6. 选择创建 LAG。

使用命令行或 API 创建 LAG

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

使用命令行或 API 描述 LAG

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

使用命令行或 API 下载 LOA-CFA

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

创建 LAG 后，您可以将连接与 LAG 关联或解除二者的关联。有关更多信息，请参阅[将连接与 LAG 关联](#)和[解除连接与 LAG 的关联](#)。

查看 Direct Connect 终端节点的 LAG 详细信息

创建 LAG 后，您可以使用 Direct Connect 控制台、命令行或 API 查看其详细信息。

查看有关您的 LAG 的信息

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，请选择 LAGs。
3. 选择 LAG，然后选择 View details (查看详细信息)。
4. 您可以查看有关 LAG 的信息，包括其 ID 和连接终止的终 Direct Connect 端节点。

要使用命令行或 API 查看 LAG 的相关信息

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

更新位于 Direct Connect 端点的 LAG

您可以使用 Direct Connect 控制台或使用命令行或 API 更新以下链接聚合组 (LAG) 属性：

- LAG 的名称。
- 要让 LAG 本身运行而必须运行的最小连接数。

- LAG 的 MACsec 加密模式。

MACsec 仅在专用连接上可用。

AWS 将此值分配给属于 LAG 的每个连接。

有效值为：

- `should_encrypt`
- `must_encrypt`

将加密模式设置为该值后，加密关闭时连接也会中断。

- `no_encrypt`
- 标签。

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. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择 LAG，然后选择编辑。
4. 修改 LAG

[更改名称] 对于 LAG 名称，输入新的 LAG 名称。

[调整最小连接数] 对于最小连接数，输入最小运行连接数。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择 Remove tag (删除标签)。

5. 选择 Edit LAG (编辑 LAG)。

使用命令行或 API 更新 LAG

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

将连接与 Direct Connect 端点中的 LAG 相关联

您可以使用 Direct Connect 控制台或使用命令行或 API 将现有连接与 LAG 相关联。连接可以是独立的，也可以是其他 LAG 的一部分。连接必须位于同一 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期间中断。

将连接与 LAG 关联

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择 LAG，然后选择查看详细信息。
4. 在连接下，选择关联连接。
5. 对于连接，选择要用于 LAG 的 Direct Connect 连接。
6. 选择关联连接。

使用命令行或 API 关联连接

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

解除连接与位于 Direct Connect 端点的 LAG 的关联

使用 Direct Connect 控制台或使用命令行或 API 解除连接与 LAG 的关联，即可将其转换为独立连接。如果解除关联连接将导致 LAG 低于其最小运行连接数的阈值，则无法解除关联。

解除某个连接与 LAG 的关联不会自动解除关联任何虚拟接口。

Important

在解除关联时，您与 AWS 的连接将会中断。

解除连接与 LAG 的关联

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在左侧窗格中，选择 LAG。
3. 选择 LAG，然后选择查看详细信息。
4. 在连接中，从可用连接列表中选择连接，然后选择取消关联。
5. 在确认对话框中，选择 Disassociate (取消关联)。

使用命令行或 API 解除关联连接

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

将 MACsec CKN/CAK 与 Direct Connect 端点 LAG 关联

创建支持 MACsec 的 LAG 后，您可以使用 Direct Connect 控制台或使用命令行或 API 将 CKN/CAK 与连接关联。

Note

将 MACsec 密钥与 LAG 关联后，您无法对其进行修改。如果需要修改密钥，请解除密钥与连接的关联，然后将新密钥与连接关联。有关删除关联的信息，请参阅 [the section called “移除 MACsec 密钥和 LAG 之间的关联”](#)。

要将 MACsec 密钥与 LAG 关联

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择 LAG，然后选择 View details (查看详细信息)。
4. 选择关联密钥。
5. 输入 MACsec 密钥。

[使用 CAK/CKN 对] 选择密钥对，然后执行以下操作：

- 对于连接关联密钥 (CAK)，输入 CAK。
- 对于连接关联密钥名称 (CKN)，输入 CAK。

[使用密钥] 选择现有 Secret Manager 密钥，然后对于密钥，选择 MACsec 密钥。

6. 选择关联密钥。

使用命令行或 API 将 MACsec 密钥与 LAG 相关联

- [associate-mac-sec-key](#) (AWS CLI)
- [AssociateMACsecKey](#) (Direct Connect API)

移除 MACsec 密钥和 Direct Connect 端点 LAG 之间的关联

您可以使用 Direct Connect 控制台、命令行或 API 删除 LAG 和 MACsec 密钥之间的关联。

移除 LAG 和 MACsec 密钥之间的关联

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，请选择 LAGs。
3. 选择 LAG，然后选择 View details (查看详细信息)。
4. 选择要删除的 MACsec 密钥，然后选择“取消关联密钥”。
5. 在确认对话框中，输入 disassociate，然后选择解除关联。

使用命令行或 API 移除 LAG 和 MACsec 密钥之间的关联

- [disassociate-mac-sec-key](#) (AWS CLI)
- [DisassociateMacSecKey](#)(Direct Connect API)

删除 Direct Connect 端点 LAG

如果您不再需要 LAG，可以删除它们。如果 LAG 具有相关联的虚拟接口，则您无法删除它。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；您必须自行删除这些连接。有关更多信息，请参阅 [删除连接](#)。

您可以使用 Direct Connect 控制台或使用命令行或 API 删除 LAG。

删除 LAG

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 LAGs (LAG)。
3. 选择 LAG，然后选择删除。
4. 在确认对话框中，选择删除。

使用命令行或 API 删除 LAG

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

Direct Connect 网关

您可以通过 Amazon VPC 控制台或 AWS CLI 使用 Direct Connect 网关。

- [Direct Connect 网关](#)

使用 Direct Connect 网关，您可以将 Direct Connect 网关与具有多个 VPC 的中转网关、虚拟私有网关或如果您使用 AWS Cloud WAN，与 Cloud WAN 核心网络相关联。

- [虚拟私有网关关联](#)

使用虚拟私有网关，您可以通过私有虚拟接口，将 Direct Connect 网关与位于相同或不同区域的任何账户中的一个或多个 VPC 相关联。

- [中转网关关联](#)

使用 Direct Connect 网关通过中转虚拟接口，将 Direct Connect 连接连到挂载到中转网关的 VPC 或 VPN。

- [Cloud WAN 核心网络关联](#)

使用 Direct Connect 网关将 Direct Connect 网关与 AWS Network Manager 核心网络关联。

- [允许的前缀交互](#)

使用允许的前缀与中转网关和虚拟私有网关交互。

主题

- [Direct Connect 网关](#)
- [Direct Connect 虚拟私有网关关联](#)
- [Direct Connect 网关和中转网关关联](#)
- [Direct Connect 网关和 AWS 云 WAN 核心网络关联](#)
- [Direct Connect 网关允许的前缀交互](#)

Direct Connect 网关

使用 Direct Connect 网关连接您的 VPCs。您可以将 Direct Connect 网关与以下任何一项关联：

- 当您在同一个区域有多个网关时，则为 VPCs 中转网关

- 虚拟私有网关
- AWS 云广域网核心网络

您也可以使用虚拟私有网关来扩展本地区域。此配置允许与本区域关联的 VPC 连接到 Direct Connect 网关。Direct Connect 网关连接到区域中的 Direct Connect 位置。本地数据中心具有与 Direct Connect 位置连接的 Direct Connect 连接。有关更多信息，请参阅《Amazon VPC 用户指南》中的[使用 Direct Connect 网关访问本地区域](#)。

Direct Connect 网关是全球可用资源。您可以使用 Direct Connect 网关连接到全球任何区域。这 AWS GovCloud (US) 包括但不包括 AWS 中国地区。Direct Connect 网关是 Direct Connect 的虚拟组件，旨在充当一组分布式 BGP 路由反射器。由于它在数据流量路径之外运行，因此可以避免造成单点故障或引入对特定 AWS 区域的依赖性。其设计本身就内置了高可用性，因此无需使用多个 Direct Connect 网关。

在当前绕过父可用区的 Direct Connect 上使用 Direct Connect 的客户将无法迁移他们的 Direct Connect 连接或虚拟接口。VPCs

下面描述了可以使用 Direct Connect 网关的场景。

Direct Connect 网关不允许位于同一 Direct Connect 网关上的网关关联相互发送流量（例如，虚拟私有网关发送到另一个虚拟私有网关）。2021 年 11 月实施的该规则的一个例外情况是，超网在两个或更多网络上通告 VPCs，这两个网关的虚拟专用网关 (VGWs) 关联到同一 Direct Connect 网关和同一个虚拟接口。在这种情况下，VPCs 可以通过 Direct Connect 端点相互通信。例如，如果您通告的超网（例如 10.0.0.0/8 或 0.0.0.0/0）与连接 VPCs 到 Direct Connect 网关（例如 10.0.0.0/24 和 10.0.1.0/24）重叠，并且在同一个虚拟接口上，则它们可以从您的本地网络相互通信。VPCs

如果要阻止 Direct Connect 网关内的 VPC-to-VPC 通信，请执行以下操作：

1. 在 VPC 中的实例和其他资源上设置安全组以阻止 VPC 之间的流量 VPCs，也可以将其用作 VPC 中默认安全组的一部分。
2. 避免在本地网络中宣传与您的网络重叠的超网。VPCs 相反，您可以从本地网络发布与您的不重叠的更具体的路由 VPCs。
3. 为要连接到本地网络的每个 VPC 配置一个 Direct Connect 网关，而不是为多个 VPC 使用相同的 Direct Connect 网关 VPCs。例如，与其使用单个 Direct Connect 网关进行开发和生产 VPCs，不如为每个网关使用单独的 Direct Connect 网关 VPCs。

Direct Connect 网关不会阻止流量从一个网关关联发送回同一网关关联（例如，当您有一个本地超网路由包含来自网关关联的前缀时）。如果您的配置中有多个 VPCs 连接到与同一 Direct Connect 网关关

联的中转网关，则 VPCs 可以进行通信。要 VPCs 防止通信，请将路由表与设置了 blackhole 选项的 VPC 附件相关联。

主题

- [场景](#)
- [创建 Direct Connect 网关](#)
- [从虚拟专用网关迁移到网 Direct Connect 关](#)
- [删除网 Direct Connect 关](#)

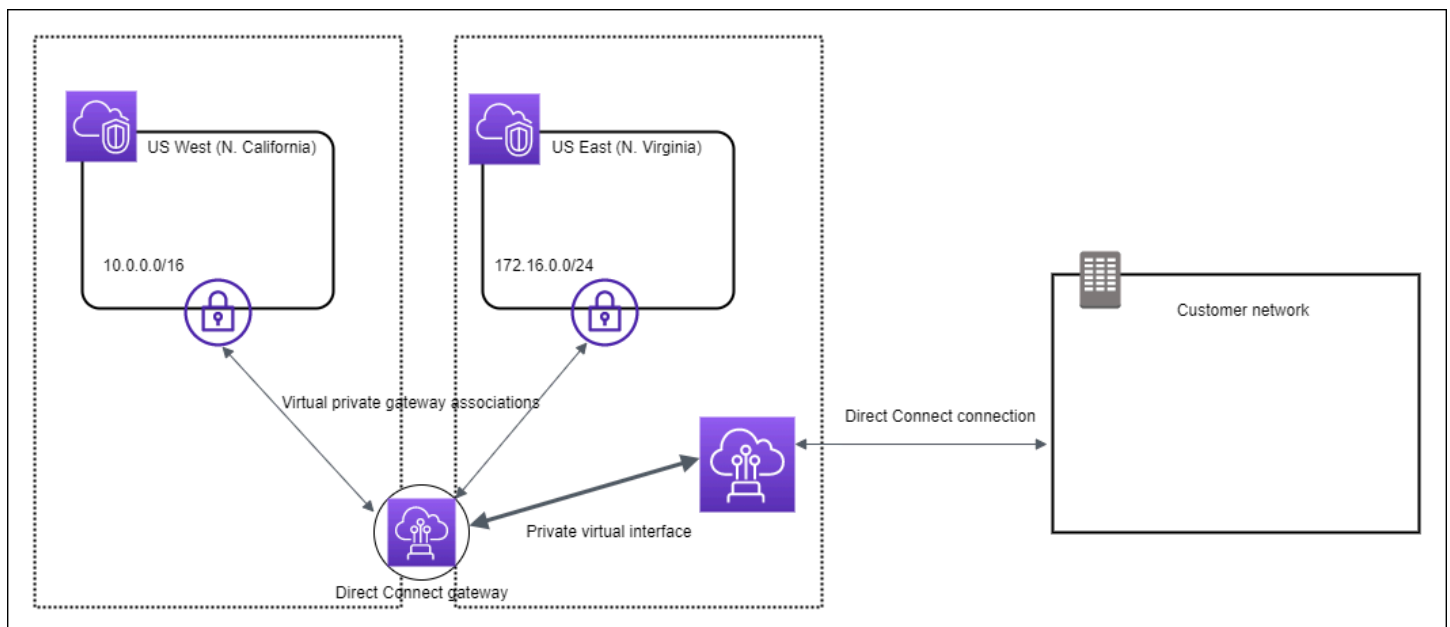
场景

下文仅针对使用 Direct Connect 网关的部分场景进行说明。

场景：虚拟私有网关关联

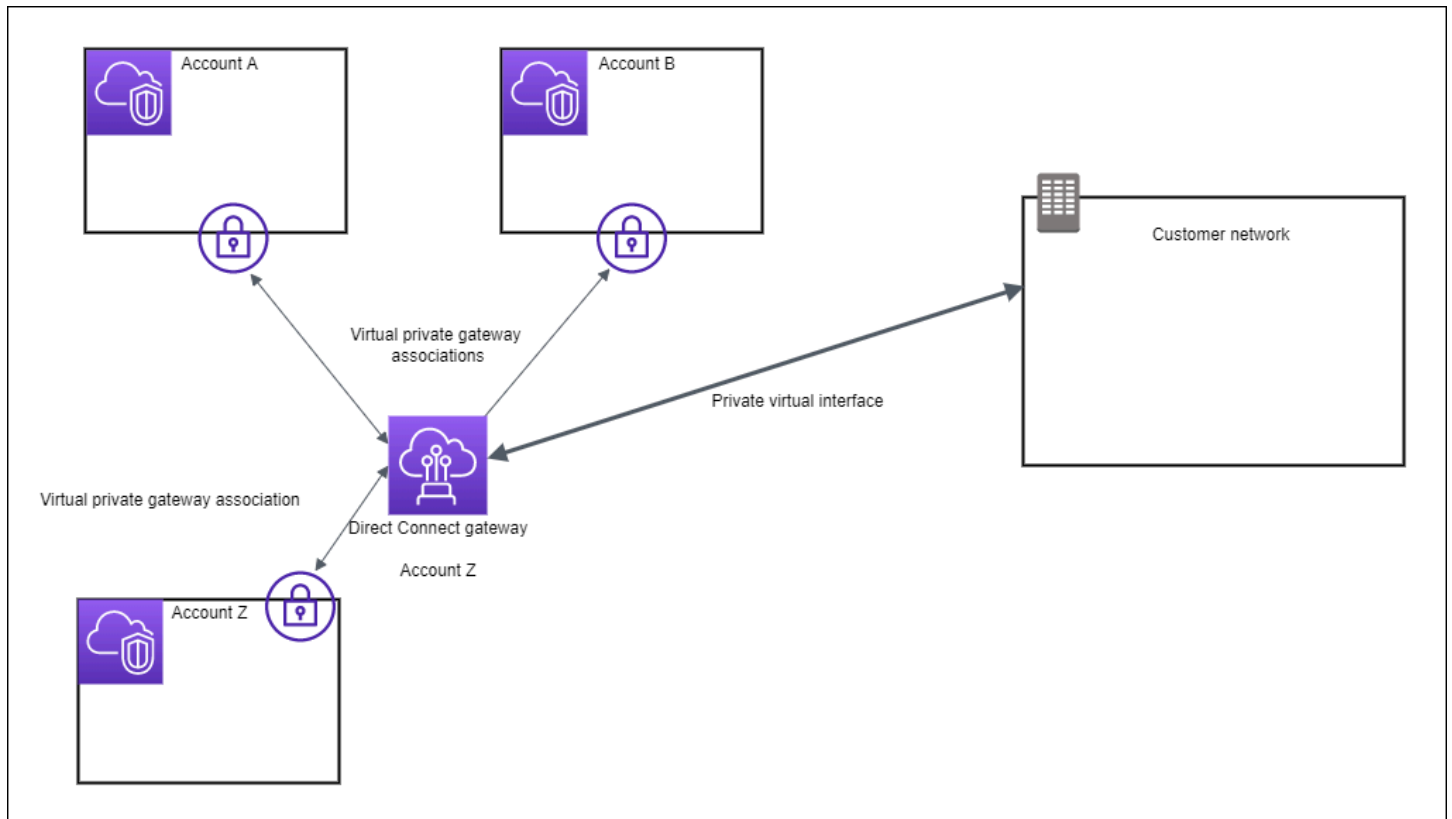
在下图中，Direct Connect 网关允许您使用您在美国东部（弗吉尼亚北部）地区的 Direct Connect 连接，通过您的账户访问 VPCs 美国东部（弗吉尼亚北部）和美国西部（加利福尼亚北部）区域。

每个 VPC 都有一个虚拟私有网关，该网关使用虚拟私有网关关联连接到 Direct Connect 网关。Direct Connect 网关使用私有虚拟接口连接该 Direct Connect 地点。从该位置到客户数据中心有一个 Direct Connect 连接。



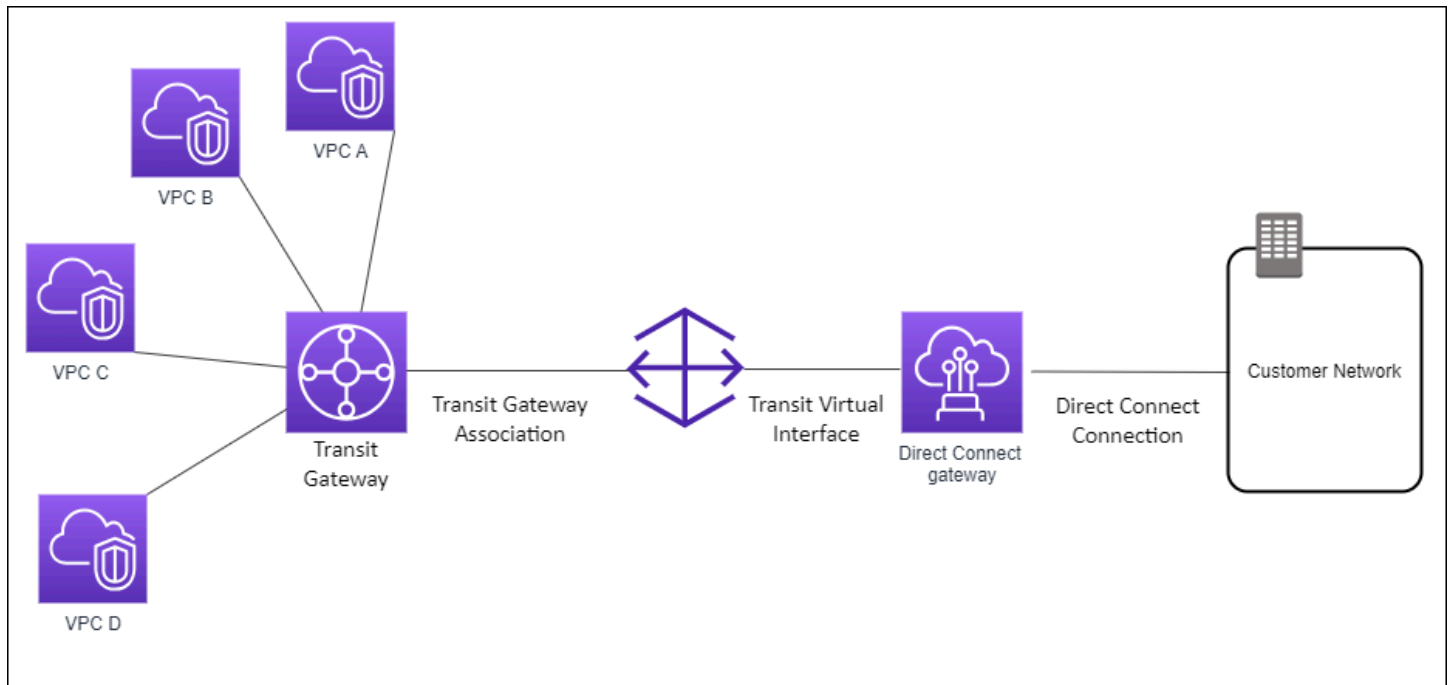
场景：跨账户的虚拟私有网关关联

考虑 Direct Connect 网关所有者（账户 Z）拥有 Direct Connect 网关的此场景。账户 A 和账户 B 想要使用 Direct Connect 网关。账户 A 和账户 B 各自向账户 Z 发送关联提议。账户 Z 接受关联提议，并（可选）更新账户 A 的虚拟私有网关或账户 B 的虚拟私有网关中允许的前缀。账户 Z 接受提议后，账户 A 和账户 B 可以将流量从其虚拟私有网关路由到 Direct Connect 网关。账户 Z 也拥有到客户的路由，因为账户 Z 拥有此网关。



场景：中转网关关联

下图说明了 Direct Connect 网关如何使您能够创建所有人 VPCs 都可以使用的指向 Direct Connect 连接的单个连接。



此解决方案包含以下组件：

- 具有 VPC 挂载的中转网关。
- 一个 Direct Connect 网关。
- Direct Connect 网关与中转网关之间的关联。
- 连接到 Direct Connect 网关的中转虚拟接口。

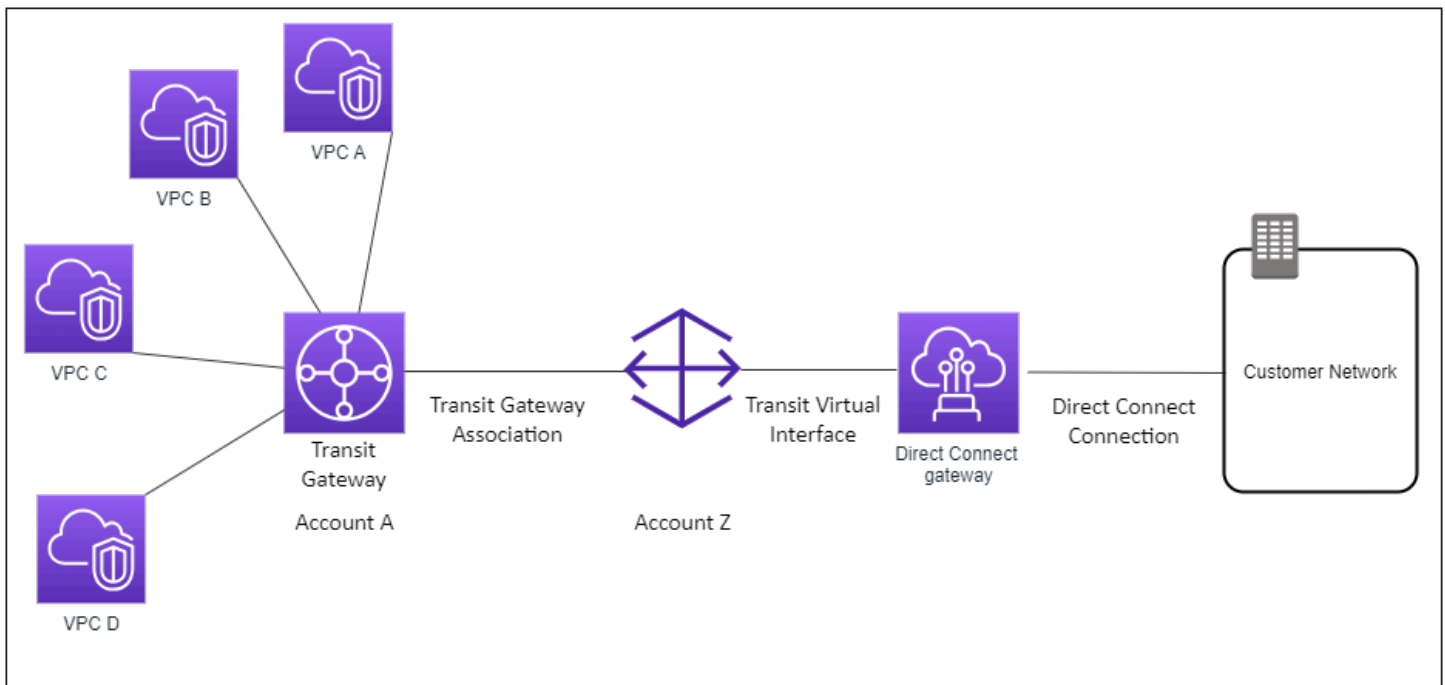
此配置提供以下好处。你可以：

- 管理多个 VPCs 或位于同一区域 VPNs 的单个连接。
- 将前缀从本地广告到本地 AWS 以及从本地广告到本地 AWS 。

有关配置中转网关的信息，请参阅《Amazon VPC 中转网关指南》中的[使用中转网关](#)。

场景：跨账户的中转网关关联

考虑 Direct Connect 网关所有者（账户 Z）拥有 Direct Connect 网关的此场景。账户 A 拥有中转网关，并希望使用 Direct Connect 网关。账户 Z 接受关联提议，并可以选择更新账户 A 的中转网关允许的前缀。账户 Z 接受提案后，VPCs 连接至公交网关的用户可以将流量从公交网关路由到 Direct Connect 网关。账户 Z 也拥有到客户的路由，因为账户 Z 拥有此网关。



创建 Direct Connect 网关

您可以使用 Direct Connect 控制台或使用命令行或 API 在任一受支持地区创建 Direct Connect 网关。

创建 Direct Connect 网关

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Direct Connect Gateways。
3. 选择创建 Direct Connect 网关。
4. 指定以下信息，然后选择创建 Direct Connect 网关。
 - Name (名称)：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 到 4,294,967,294 范围内。

Note

如果您想创建 Direct Connect 网关以用于 AWS Cloud WAN 核心网络。ASN 不能与核心网络的 ASN 位于同一范围内。

使用命令行或 API 创建 Direct Connect 网关

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

从虚拟专用网关迁移到网 Direct Connect 关

您可以将挂载到虚拟接口的虚拟私有网关迁移到 Direct Connect 网关。

如果您在当前绕过父可用区的 Direct Connect 上使用 Direct Connect，则将无法迁移您的 Direct Connect 连接或虚拟接口。VPCs

针对将虚拟私有网关迁移到 Direct Connect 网关的步骤，以下步骤提供了说明。

迁移到 Direct Connect 网关

1. 创建 Direct Connect 网关。

如果 Direct Connect 网关尚未存在，则您需要先创建网关。有关创建 Direct Connect 网关的步骤，请参阅[创建 Direct Connect 网关](#)。

2. 创建 Direct Connect 网关的虚拟接口。

迁移需要虚拟接口。如果接口不存在，则您需要先创建接口。有关创建虚拟接口的步骤，请参阅[虚拟接口](#)。

3. 将虚拟私有网关与 Direct Connect 网关相关联。

Direct Connect 网关和虚拟私有网关都需要关联。有关创建关联的步骤，请参阅[关联虚拟私有网关或解除其关联](#)。

4. 删除与虚拟私有网关相关联的虚拟接口。有关更多信息，请参阅[删除虚拟接口](#)。

删除网 Direct Connect 关

如果您不再需要某一 Direct Connect 网关，可将其删除。您必须先解除关联所有关联的虚拟私有网关并删除附加的私有虚拟接口。取消关联所有关联的虚拟专用网关并删除所有连接的私有虚拟接口后，您可以使用 Direct Connect 控制台、命令行或 API 删除 Direct Connect 网关。

- 有关解除虚拟私有网关关联的步骤，请参阅[关联虚拟私有网关或解除其关联](#)。
- 有关删除虚拟接口的步骤，请参阅[删除虚拟接口](#)。

删除 Direct Connect 网关

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect Gateways。
3. 选择网关，然后选择 Delete (删除)。

使用命令行或 API 删除 Direct Connect 网关

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

Direct Connect 虚拟私有网关关联

您可以将虚拟私有网关与 Direct Connect 网关关联，以便跨不同账户和区域的 Direct Connect 连接与 VPC 之间建立连接。每个 VPC 都需要虚拟私有网关，您将此网关与 Direct Connect 网关关联。建立这些关联后，您就可以在与 Direct Connect 网关的 Direct Connect 连接上创建私有虚拟接口，从而允许多个 VPC 通过各自的虚拟私有网关关联共享同一个 Direct Connect 连接。

以下规则适用于虚拟私有网关关联：

- 在将虚拟网关与 Direct Connect 网关关联之前，请勿启用路由传播。如果在关联网关之前启用路由传播，则可能无法正确传播路由。
- 创建和使用 Direct Connect 网关是有限制的。有关更多信息，请参阅 [Direct Connect 的配额](#)。
- 当 Direct Connect 网关已与中转网关关联时，您无法将 Direct Connect 网关连接到虚拟私有网关。
- 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 网关仅支持连接的私有虚拟接口和关联的虚拟私有网关之间的通信，并且可以启用到另一个私有网关的虚拟私有网关。以下流量不受支持：
 - 与单个 Direct Connect 网关相关联的多个 VPC 之间的直接通信。包括在本地网络中经由单个 Direct Connect 网关使用发夹，从一个 VPC 到另一个 VPC 的流量。
 - 附加到单个 Direct Connect 网关的虚拟接口之间的直接通信。
 - 附加到单个 Direct Connect 网关的虚拟接口和与同一 Direct Connect 网关关联的虚拟私有网关上的 VPN 连接之间的直接通信。

- 您不能将一个虚拟私有网关与多个 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 网关关联的虚拟私有网关必须附加到 VPC。
- 虚拟私有网关关联提议将在创建的 7 天后过期。
- 接受的虚拟私有网关提议或删除的虚拟私有网关提议将在 3 天内保持可见。
- 虚拟私有网关可以与 Direct Connect 网关相关联，也可以附加到虚拟接口。
- 从 VPC 分离虚拟私有网关也会解除虚拟私有网关与 Direct Connect 网关的关联。
- 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。

要将您的 Direct Connect 仅连接到相同区域中的 VPC，您可以创建一个 Direct Connect 网关。或者，您可以创建一个私有虚拟接口，并将其附加到 VPC 的虚拟私有网关。有关更多信息，请参阅[创建私有虚拟接口](#)和[VPN CloudHub](#)。

要通过其他账户中的 VPC 使用您的 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私有网关或 Direct Connect 网关。有关更多信息，请参阅[虚拟接口和托管虚拟接口](#)。

主题

- [创建 Direct Connect 虚拟私有网关](#)
- [关联或取消关联 Direct Connect 虚拟专用网关](#)
- [为 Direct Connect 网关创建私有虚拟接口](#)
- [跨账户关联 Direct Connect 虚拟私有网关](#)

创建 Direct Connect 虚拟私有网关

虚拟私有网关必须附加到您要连接到的 VPC。您可以使用 Direct Connect 控制台或使用命令行或 API 创建虚拟私有网关，并将其挂载到 VPC。

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。

创建虚拟专用网关后，必须将其连接到您的 VPC。

创建虚拟专用网关并将其连接到您的 VPC

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择虚拟私有网关，然后选择创建虚拟私有网关。
3. (可选) 为虚拟私有网关输入名称。这样做可创建具有 Name 键以及您指定的值的标签。
4. 对于 ASN，保留默认选择以使用默认的 Amazon ASN。否则，选择自定义 ASN 并输入一个值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 4200000000 到 4294967294 范围内。
5. 选择 Create Virtual Private Gateway。
6. 选择您已创建的虚拟专用网关，然后依次选择 Actions、Attach to VPC。
7. 从列表中选择您的 VPC，然后选择 Yes, Attach。

使用命令行或 API 创建虚拟专用网关

- [CreateVpnGateway](#) (Amazon EC2 查询 API)
- [create-vpn-gateway](#) (AWS CLI)
- [New-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

使用命令行或 API 将虚拟专用网关连接到 VPC

- [AttachVpnGateway](#) (Amazon EC2 查询 API)
- [attach-vpn-gateway](#) (AWS CLI)
- [Add-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

关联或取消关联 Direct Connect 虚拟专用网关

您可以使用 Direct Connect 控制台、命令行或 API 关联或取消关联虚拟专用网关和 Direct Connect 网关。虚拟私有网关的账户所有者执行这些操作。

关联虚拟私有网关

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect 网关，然后选择 Direct Connect 网关。

3. 请选择查看详细信息。
4. 选择网关关联，然后选择关联网关。
5. 对于 Gateways (网关)，选择要关联的虚拟私有网关，然后选择 Associate gateway (关联网关)。

您可以通过选择 Gateway associations (网关关联) 查看与 Direct Connect 网关关联的所有虚拟私有网关。

取消关联虚拟私有网关

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect 网关，然后选择 Direct Connect 网关。
3. 请选择查看详细信息。
4. 选择 Gateway associations (网关关联)，然后选择虚拟私有网关。
5. 选择取消关联。

使用命令行或 API 关联虚拟私有网关

- [create-direct-connect-gateway-协会](#) (AWS CLI)
- [CreateDirectConnectGatewayAssociation](#) (Direct Connect API)

使用命令行或 API 查看与 Direct Connect 网关关联的虚拟私有网关

- [describe-direct-connect-gateway-协会](#) (AWS CLI)
- [DescribeDirectConnectGatewayAssociations](#) (Direct Connect API)

使用命令行或 API 取消关联虚拟私有网关

- [delete-direct-connect-gateway-协会](#) (AWS CLI)
- [DeleteDirectConnectGatewayAssociation](#) (Direct Connect API)

为 Direct Connect 网关创建私有虚拟接口

要将您的 Direct Connect 连接连接到远程 VPC，您必须为连接创建私有虚拟接口。指定要连接到的 Direct Connect 网关。您可以使用 Direct Connect 控制台、命令行或 API 创建私有虚拟接口。

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](#)。

为 Direct Connect 网关配置私有虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。
3. 选择 Create virtual interface (创建虚拟接口)。
4. 在虚拟接口类型下，选择私有。
5. 在私有虚拟接口设置下，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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，如果虚拟接口适用于您的 AWS 账户，请选择我的 AWS 账户。
 - d. 对于 Direct Connect 网关，选择 Direct Connect 网关。
 - e. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - f. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

⚠ Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 9001 (巨型帧)，请选择巨型帧 MTU (MTU 大小 9001)。
- (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。
- (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

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](#)。

使用命令行或 API 创建私有虚拟接口

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

跨账户关联 Direct Connect 虚拟私有网关

您可以将 Direct Connect 网关与任何 AWS 账户拥有的虚拟私有网关关联。Direct Connect 网关可以是现有网关，您也可以创建新网关。虚拟私有网关的所有者创建关联提议，而 Direct Connect 网关的所有者必须接受此关联提议。

关联提议可以包含虚拟私有网关中将允许的前缀。Direct Connect 网关的所有者可以选择覆盖关联提议中的任何请求的前缀。

允许的前缀

当您为虚拟私有网关与 Direct Connect 网关关联时，您可以指定一个要公布到 Direct Connect 网关的 Amazon VPC 前缀的列表。该前缀列表用作筛选器，以允许相同的 CIDR 或更小的 CIDR 公布到 Direct Connect 网关。您必须将 Allowed prefixes (允许的前缀) 设置为等于或大于 VPC CIDR 的范围，因为我们在虚拟私有网关上预配置整个 VPC CIDR。

考虑以下情况：VPC CIDR 为 10.0.0.0/16。您可以将 Allowed prefixes (允许的前缀) 设置为 10.0.0.0/16 (VPC CIDR 值) 或 10.0.0.0/15 (大于 VPC CIDR 的值)。

任何通过 Direct Connect 通告的网络前缀内部的虚拟接口只能传播到跨区域的中转网关，但不能传播到同一区域内的中转网关。有关允许的前缀如何与虚拟私有网关和中转网关交互的更多信息，请参阅 [允许的前缀交互](#)。

Direct Connect 网关和中转网关关联

您可以使用 Direct Connect 网关，将 Direct Connect 连接通过中转虚拟接口连接到与挂载到中转网关的 VPC 或 VPN。将 Direct Connect 网关与中转网关关联。然后，创建一个中转虚拟接口以将 Direct Connect 连接到 Direct Connect 网关。

以下规则适用于中转网关关联：

- 当 Direct Connect 网关已与虚拟私有网关关联或已连接到私有虚拟接口时，您无法将 Direct Connect 网关连接到中转网关。

- 创建和使用 Direct Connect 网关是有限制的。有关更多信息，请参阅 [Direct Connect 的配额](#)。
- Direct Connect 网关支持挂载的中转虚拟接口与关联的中转网关之间的通信。
- 如果连接到位于不同区域的多个中转网关，请为每个中转网关使用唯一的 ASN。
- 任何使用 /30 范围的点对点连接地址（例如 192.168.0.0/30）都不会传播到中转网关。

跨账户关联中转网关

您可以将现有 Direct Connect 网关或新的 Direct Connect 网关与任何 AWS 账户拥有的中转网关关联。中转网关的所有者创建关联提议，Direct Connect 网关的所有者必须接受此关联提议。

关联提议可以包含中转网关允许的前缀。Direct Connect 网关的所有者可以选择覆盖关联提议中的任何请求的前缀。

允许的前缀

对于中转网关关联，您可以在 Direct Connect 网关上预置允许的前缀列表。此列表用于将流量从本地路由到 AWS 进入中转网关，即使连接到中转网关的 VPC 未分配 CIDR。Direct Connect 网关允许前缀列表中的前缀源自 Direct Connect 网关，并公布到本地网络。有关允许的前缀如何与中转网关和虚拟私有网关交互的更多信息，请参阅 [允许的前缀交互](#)。

主题

- [关联或取消 Direct Connect 与传输网关的关联](#)
- [为 Direct Connect 网关创建中转虚拟接口](#)
- [创建公交网关和 Direct Connect 关联提案](#)
- [接受或拒绝中转网关和 Direct Connect 关联提议](#)
- [更新公交网关和 Direct Connect 关联允许的前缀](#)
- [删除公交网关和 Direct Connect 关联提案](#)

关联或取消 Direct Connect 与传输网关的关联

使用 Direct Connect 控制台、命令行或 API 关联或取消关联公交网关。

要关联中转网关

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。

2. 在导航窗格中，选择 Direct Connect 网关，然后选择 Direct Connect 网关。
3. 请选择查看详细信息。
4. 选择 Gateways associations (网关关联)，然后选择 Associate gateway (关联网关)。
5. 对于网关，选择要关联的中转网关。
6. 在允许的前缀中，输入 Direct Connect 网关向本地数据中心公布的前缀（用逗号分隔或换行）。有关允许的前缀的更多信息，请参阅 [允许的前缀交互](#)。
7. 选择关联网关

您可以通过选择 Gateway associations (网关关联) 查看与 Direct Connect 网关关联的所有网关。

要解除关联中转网关

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect 网关，然后选择 Direct Connect 网关。
3. 请选择查看详细信息。
4. 选择 Gateway associations (网关关联)，然后选择中转网关。
5. 选择取消关联。

更新中转网关允许的前缀

您可以向中转网关添加或删除允许的前缀。

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect 网关，然后选择您想为其添加或删除允许的前缀的 Direct Connect 网关。
3. 选择网关关联选项卡。
4. 选择要修改其允许前缀的网关，然后选择编辑。
5. 在允许的前缀中，输入 Direct Connect 网关向本地数据中心公布的前缀。对于多个前缀，请用逗号分隔每个前缀，或将每个前缀放在新的一行。您添加的前缀应与所有虚拟私有网关的 Amazon VPC CIDRs 相匹配。有关允许的前缀的更多信息，请参阅 [允许的前缀交互](#)。
6. 选择编辑关联。

在网关关联部分，状态显示正在更新。完成后，状态将变为已关联。这可能需要几分钟或更长时间才能完成。

要使用命令行或 API 关联中转网关

- [create-direct-connect-gateway-协会](#) ()AWS CLI
- [CreateDirectConnectGatewayAssociation](#)(Direct Connect API)

要使用命令行或 API 查看与 Direct Connect 网关关联的中转网关

- [describe-direct-connect-gateway-协会](#) ()AWS CLI
- [DescribeDirectConnectGatewayAssociations](#)(Direct Connect API)

要使用命令行或 API 解除关联中转网关

- [delete-direct-connect-gateway-协会](#) ()AWS CLI
- [DeleteDirectConnectGatewayAssociation](#)(Direct Connect API)

要使用命令行或 API 更新中转网关允许的前缀

- [update-direct-connect-gateway-协会](#) ()AWS CLI
- [UpdateDirectConnectGatewayAssociation](#)(Direct Connect API)

为 Direct Connect 网关创建中转虚拟接口

要将 Direct Connect 连接连接到传输网关，必须为连接创建传输接口。指定要连接到的 Direct Connect 网关。您可以使用 Direct Connect 控制台，也可以使用命令行或 API。

Important

如果您将中转网关与一个或多个 Direct Connect 网关关联，则中转网关和 Direct Connect 网关使用的自治系统号 (ASN) 必须不同。例如，如果您对中转网关和 Direct Connect 网关使用默认的 ASN 64512，则关联请求将失败。

为 Direct Connect 网关配置中转虚拟接口

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Virtual Interfaces。

3. 选择 Create virtual interface (创建虚拟接口)。
4. 在 Virtual interface type (虚拟接口类型) 下，对于 Type (类型)，选择 Transit (中转)。
5. 在 Transit virtual interface settings (中转虚拟接口设置) 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 Connection (连接)，选择要用于此接口的 Direct Connect 连接。
 - c. 对于虚拟接口所有者，如果虚拟接口适用于您的 AWS 账户，请选择我的 AWS 账户。
 - d. 对于 Direct Connect 网关，选择 Direct Connect 网关。
 - e. 对于 VLAN，输入您的虚拟局域网 (VLAN) 的 ID 号。
 - f. 对于 BGP ASN，输入新虚拟接口的本地对等路由器的边界网关协议自治系统号。

有效值为 1 到 4294967294。这包括同时支持 ASNs (1-2147483647) 和多头 (1-4294967294)。ASNs 有关 ASNs 和详细内容的更多信息，ASNs 请参阅[长期支持 ASN Direct Connect](#)。

6. 在附加设置下，执行以下操作：
 - a. 要配置 IPv4 BGP 或对 IPv6 等体，请执行以下操作：

[IPv4] 要配置 IPv4 BGP 对等体，请选择 IPv4 并执行以下任一操作：

 - 要自己指定这些 IP 地址，请在您的路由器对等 IP 中，输入 Amazon 应向其发送流量的目标 IPv4 CIDR 地址。
 - 对于 Amazon 路由器对等 IP，请输入用于向其发送流量的 IPv4 CIDR 地址。AWS

Important

配置 Direct Connect 虚拟接口时，您可以使用 RFC 1918 指定自己的 IP 地址，使用其他寻址方案，或者选择从 RFC 3927 169.254.0.0 IPv4 /16 Link-Local 范围 AWS 分配的分配的 /29 CIDR 地址进行连接。IPv4 point-to-point 这些 point-to-point 连接应专门用于您的客户网关路由器和 Direct Connect 端点之间的 eBGP 对等。对于 VPC 流量或隧道传输目的，例如 AWS Site-to-Site 私有 IP VPN 或 Transit Gateway Connect，AWS 建议使用客户网关路由器上的环回或局域网接口作为源地址或目标地址，而不是连接。point-to-point

- 有关 RFC 1918 的更多信息，请参阅[私有互联网的地址分配](#)。
- 有关 RFC 3927 的更多信息，请参阅[IPv4 链路本地地址的动态配置](#)。

[IPv6] 要配置 IPv6 BGP 对等体，请选择 IPv6。对等 IPv6 地址是从亚马逊的地址池中自动分配 IPv6 的。您不能指定自定义 IPv6 地址。

- b. 要将最大传输单元 (MTU) 从 1500 (默认) 更改为 8500 (巨型帧)，请选择 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500))。
- c. (可选) 在“启用”下 SiteLink，选择“启用”以启用 Direct Connect 接入点之间的直接连接。
- d. (可选) 添加或删除标签。

[添加标签] 选择 Add tag (添加标签)，然后执行以下操作：

- 对于 Key (键)，输入键名称。
- 对于值，输入键值。

[删除标签] 在标签旁，选择删除标签。

7. 选择 Create virtual interface (创建虚拟接口)。

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](#)。

使用命令行或 API 创建中转虚拟接口

- [create-transit-virtual-interface](#) (AWS CLI)
- [CreateTransitVirtualInterface](#) (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-附件](#) ()AWS CLI
- [DescribeDirectConnectGatewayAttachments](#)(Direct Connect API)

创建公交网关和 Direct Connect 关联提案

如果您拥有中转网关，则必须创建关联提议。传输网关必须连接到您 AWS 账户中的 VPC 或 VPN。Direct Connect 网关的所有者必须共享 Direct Connect 网关的 ID 及其 AWS 账户的 ID。在创建提议后，Direct Connect 网关的所有者必须接受此提议，以便您能够通过 Direct Connect 访问本地网络。您可以使用 Direct Connect 控制台、命令行或 API 创建关联提案。

创建关联提议

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。

2. 在导航窗格中，选择中转网关，然后选择中转网关。
3. 请选择查看详细信息。
4. 选择 Direct Connect gateway associations (Direct Connect 网关关联)，然后选择 Associate Direct Connect gateway (关联 Direct Connect 网关)。
5. 在 Association account type (关联账户类型) 下，对于 Account owner (账户所有者)，选择 Another account (其他账户)。
6. 对于 Direct Connect 网关所有者，输入拥有 Direct Connect 网关的账户 ID。
7. 在 Association settings (关联设置) 下，执行以下操作：
 - a. 对于 Direct Connect gateway ID (Direct Connect 网关 ID)，输入 Direct Connect 网关的 ID。
 - b. 对于虚拟接口所有者，输入拥有虚拟接口以进行关联的账户 ID。
 - c. (可选) 要指定中转网关允许的前缀列表，请将前缀添加到允许的前缀中，并用逗号分隔，或者在新行中输入。
8. 选择 Associate Direct Connect gateway (关联 Direct Connect 网关)。

使用命令行或 API 创建关联提议

- [create-direct-connect-gateway-协会提案](#) (AWS CLI)
- [CreateDirectConnectGatewayAssociationProposal](#) (Direct Connect API)

接受或拒绝中转网关和 Direct Connect 关联提议

如果您拥有 Direct Connect 网关，您必须接受关联提议才能创建关联。您也可以选择拒绝关联提议。您可以使用 Direct Connect 控制台或使用命令行或 API 接受或拒绝关联提议。

接受关联提议

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Direct Connect 网关。
3. 选择具有待定提议的 Direct Connect 网关，然后选择 View details (查看详细信息)。
4. 在 Pending proposals (待定提议) 选项卡上，选择提议，然后选择 Accept proposal (接受提议)。
5. (可选) 要指定中转网关允许的前缀列表，请将前缀添加到允许的前缀中，并用逗号分隔，或者在新行中输入。
6. 选择 Accept proposal (接受提议)。

拒绝关联提议

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Direct Connect 网关。
3. 选择具有待定提议的 Direct Connect 网关，然后选择 View details (查看详细信息)。
4. 在 Pending proposals (待定提议) 选项卡中，选择中转网关，然后选择 Reject proposal (拒绝提议)。
5. 在 Reject proposal (拒绝提议) 对话框中，输入 Delete，然后选择 Reject proposal (拒绝提议)。

使用命令行或 API 查看关联提议

- [describe-direct-connect-gateway-association-proposals](#) (AWS CLI)
- [DescribeDirectConnectGatewayAssociationProposals](#) (Direct Connect API)

使用命令行或 API 接受关联提议

- [accept-direct-connect-gateway-association-proposal](#) (AWS CLI)
- [AcceptDirectConnectGatewayAssociationProposal](#) (Direct Connect API)

使用命令行或 API 拒绝关联提议

- [delete-direct-connect-gateway-association-proposal](#) (AWS CLI)
- [DeleteDirectConnectGatewayAssociationProposal](#) (Direct Connect API)

更新公交网关和 Direct Connect 关联允许的前缀

您可以使用 Direct Connect 控制台、命令行或 API 更新允许通过公交网关通过 Direct Connect 网关访问的前缀。要使用 Direct Connect 控制台更新公交网关和 Direct Connect 关联允许的前缀，

- 如果您是中转网关的所有者，您需要为该 Direct Connect 网关创建新关联提议，并指定允许的前缀。有关创建新关联提议的步骤，请参阅[创建中转网关关联提议](#)。
- 如果您是 Direct Connect 网关的所有者，您可以在接受关联提议或者为现有关联更新允许的前缀时更新允许的前缀。有关在接受关联时更新允许的前缀的步骤，请参阅[接受或拒绝中转网关关联提议](#)。

使用命令行或 API 为现有关联更新允许的前缀

- [update-direct-connect-gateway-协会](#) (AWS CLI)
- [UpdateDirectConnectGatewayAssociation](#)(Direct Connect API)

删除网关和 Direct Connect 关联提案

如果 Direct Connect 网关关联提案仍处于待定状态，则网关的所有者可以删除该提案。接受提案后，您无法将其删除，但您可以解除网关与 Direct Connect 网关之间的关联。有关更多信息，请参阅 [创建网关关联提案](#)。

您可以使用 Direct Connect 控制台、命令行或 API 删除网关和 Direct Connect 关联提案。

删除关联提案

1. 在 <https://console.aws.amazon.com/directconnect/v2/> home 中打开 Direct Connect 主机。
2. 在导航窗格中，选择网关，然后选择网关。
3. 请选择查看详细信息。
4. 选择 Pending gateway associations (待定的网关关联)，选择此关联并选择 Delete association (删除关联)。
5. 在 Delete association proposal (删除关联提案) 对话框中，输入 Delete，然后选择 Delete (删除)。

使用命令行或 API 删除待定的关联提案

- [delete-direct-connect-gateway-协会提案](#) (AWS CLI)
- [DeleteDirectConnectGatewayAssociationProposal](#)(Direct Connect API)

Direct Connect 网关和 AWS 云 WAN 核心网络关联

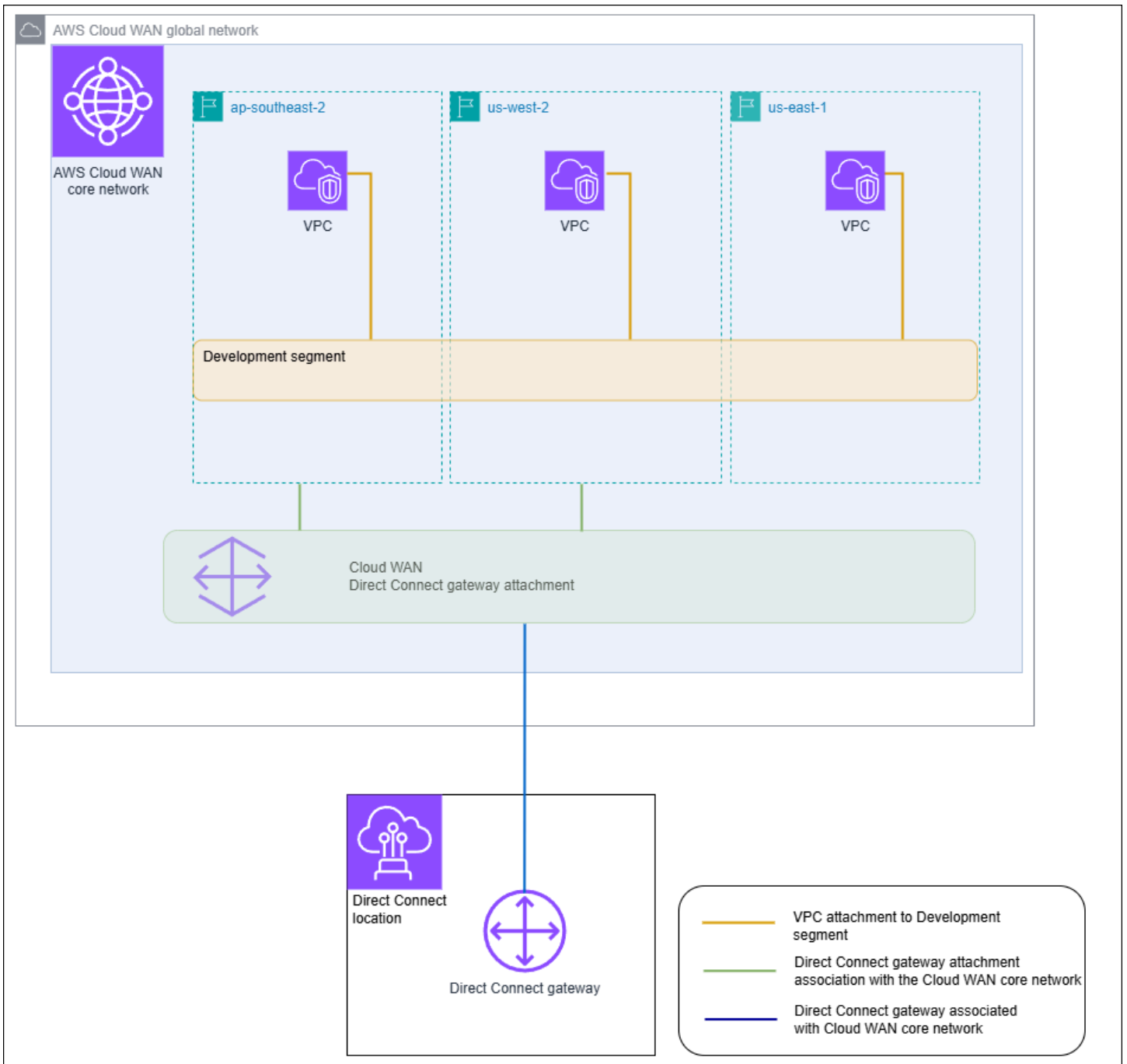
使用 AWS Cloud WAN 中的 Direct Connect 连接类型将 Direct Connect 网关关联到云广域网核心网络。这种直接关联使用最短可用路径在核心网络的选定边缘站点和您的 Direct Connect 连接之间路由流量。

Direct Connect 网关连接类型支持 BGP (边界网关协议)，用于在核心网络和本地位置之间自动传播路由信息。Direct Connect 连接还支持标准的 Cloud WAN 功能，例如基于中央策略的管理、基于标签的连接自动化以及用于高级安全配置的分段。

Note

核心网络和 Direct Connect 网关之间的关联是通过 Network Manager 中的 Cloud WAN 控制台创建、删除和管理的。在云广域网中使用 Direct Connect 网关时，Direct Connect 控制台 APIs 和 CLI 将反映关联，但不能用于对其进行修改。但是，您可以使用 Direct Connect API 或命令行来验证关联是否已创建。

以下示例显示了在 Cloud WAN 核心网络中包含三个区域的 Cloud WAN 全球网络。每个区域都有自己的 VPC，连接到这三个区域共享的核心网络开发分段。使用 Cloud WAN，通过 Direct Connect 网关在 Cloud WAN 中创建 Direct Connect 网关连接，该网关是使用 Direct Connect 创建的。该连接与三个区域中的两个（ap-southeast-2 和 us-west-2）相关联，并且允许访问开发分段。尽管 us-east-1 共享相同的开发分段，但 Direct Connect 网关连接未与该区域共享，因此不可用。



主题

- [先决条件](#)
- [注意事项](#)
- [Direct Connect 网关与 Cloud WAN 核心网络关联](#)
- [验证 Direct Connect 网关与 AWS Cloud WAN 核心网络的关联](#)

先决条件

Direct Connect 网关与 Cloud WAN 核心网络的关联需要满足以下条件：

- 现有的 Direct Connect 网关。有关创建 Direct Connect 网关的步骤，请参阅[创建 Direct Connect 网关](#)。
- AWS 云广域网核心网络。有关 Cloud WAN 的信息，请参阅[AWS Cloud WAN 用户指南](#)。

注意事项

以下限制适用于 Direct Connect 网关与 Cloud WAN 核心网络的关联：

- Direct Connect 网关可以与单个 Cloud WAN 核心网络以及该核心网络的单个分段相关联。一旦创建了关联，该网关就无法与 AWS 区域中的其他资源相关联。如果您取消网关与核心网络的关联，就可以将该网关用于其他关联类型。
- Cloud WAN Direct Connect 网关连接使用中转虚拟接口类型进行连接。
- Cloud WAN 连接不支持允许的前缀列表。核心网络分段中的所有前缀都将通告到与该分段关联的 Direct Connect 网关。
- 可以通过中转虚拟接口从本地向 AWS 通告的最大前缀配额与从 Cloud WAN 核心网络向本地通告的前缀配额不同。用于 Cloud WAN 关联的其他 Direct Connect 资源的配额也适用。请参阅[Direct Connect 的配额](#)。
- AS-PATH BGP 属性将在核心网络、Direct Connect 网关和虚拟接口中保留。
- Direct Connect 网关的 ASN 必须超出为 Cloud WAN 核心网络配置的 ASN 范围。例如，如果您的核心网络的 ASN 范围为 64512-65534，则 Direct Connect 网关的 ASN 必须使用该范围之外的 ASN。
- Cloud WAN 可能不支持使用 Direct Connect 连接类型进行传输的特定连接类型。有关云广域网核心网络的 Direct Connect 网关附件的更多信息，请参阅《[云广域网用户指南](#)》中的[AWS Cloud WAN 中的 Direct AWS Connect 网关附件](#)。
- CloudWatch 与 Cloud WAN Direct Connect 网关连接类型一起使用时，网络监控器支持延迟和丢包指标。不支持网络运行状况指标功能。有关更多信息，请参阅《[Amazon CloudWatch 用户指南](#)》中的[使用 Amazon CloudWatch 网络监测仪](#)。

Direct Connect 网关与 Cloud WAN 核心网络关联

使用 Cloud WAN 控制台、AWS Cloud WAN APIs 或命令行将 Direct AWS Connect 网关与云广域网核心网络关联起来。

要将现有的 Direct Connect 网关与 Cloud WAN 核心网络相关联，请在 Cloud WAN 控制台中创建新的 Direct Connect 连接。创建 Direct Connect 连接后，关联就已建立。默认情况下，在创建关联时，您可以选择默认值，将所选核心网络分段中的所有核心网络边缘站点都包括在内。或者，您可以指定各个边缘站点。

有关云广域网核心网络的 Direct Connect 网关附件的更多信息，请参阅《云广域网用户指南》中的 [AWS Cloud WAN 中的 Direct Connect 网关附件](#)。

验证 Direct Connect 网关与 AWS Cloud WAN 核心网络的关联

您可以使用 Direct Connect 控制台、Direct Connect API 或命令行来验证 Direct Connect 网关与 Cloud WAN 核心网络的关联。

使用控制台验证 Direct Connect 网关与 Cloud WAN 核心网络的关联

1. 在 <https://console.aws.amazon.com/directconnect/v2/home> 中打开 Direct Connect 主机。
2. 在导航窗格中，选择 Direct Connect 网关。
3. 选择要查看关联的 Direct Connect 网关连接。
4. 选择网关关联选项卡。
 - ID 列显示 Direct Connect 网关关联的核心网络 ID。
 - 状态列显示已关联。
 - 关联类型列显示 Cloud WAN 核心网络。

使用命令行或 API 验证 Direct Connect 网关与 Cloud WAN 核心网络的关联

- [DescribeDirectConnectGatewayAssociations](#) (Direct Connect API)
- [describe-direct-connect-gateway-协会](#) () AWS CLI

Direct Connect 网关允许的前缀交互

了解允许的前缀如何与中转网关和虚拟私有网关交互。有关更多信息，请参阅 [Routing policies and BGP communities](#)。

虚拟私有网关关联

前缀列表 (IPv4 和 IPv6) 作为筛选器，允许相同的 CIDR 或更小范围的 CIDR 公布到 Direct Connect 网关。您必须将前缀设置为与 VPC CIDR 块相同或比此块更宽的范围。

Note

允许的列表仅起到筛选器的作用，并且只有关联的 VPC CIDR 才会公布到客户网关。

请考虑以下情况：将具有 CIDR 10.0.0.0/16 的 VPC 附加到虚拟私有网关。

- 当允许的前缀列表设置为 22.0.0.0/24 时，您不会收到任何路由，因为 22.0.0.0/24 与 10.0.0.0/16 不同，或者比后者更宽。
- 当允许的前缀列表设置为 10.0.0.0/24 时，您不会收到任何路由，因为 10.0.0.0/24 与 10.0.0.0/16 不同。
- 当允许的前缀列表设置为 10.0.0.0/15 时，您会收到 10.0.0.0/16，因为此 IP 地址比 10.0.0.0/16 更宽。

删除或添加允许的前缀时，不使用该前缀的流量不会受到影响。在更新过程中，状态从 `associated` 变为 `updating`。修改现有前缀只能延迟或丢弃使用该前缀的流量。

中转网关关联

对于中转网关关联，您可以在 Direct Connect 网关上预置允许的前缀列表。此列表将往返于 Direct Connect 网关的本地流量路由到中转网关，即使连接到中转网关的 VPC 未分配 CIDR。允许的前缀工作方式不同，具体取决于网关类型：

- 对于中转网关关联，只有输入的允许前缀才会公布到本地。这些前缀将显示为来自 Direct Connect 网关 ASN。
- 对于虚拟私有网关，输入的允许前缀充当筛选器，允许相同或更小的 CIDR。

请考虑这样的场景：将一个 CIDR 为 10.0.0.0/16 的 VPC 连接到中转网关。

- 当允许的前缀列表设置为 22.0.0.0/24 时，您在中转虚拟接口上通过 BGP 收到 22.0.0.0/24。您不会收到 10.0.0.0/16，因为我们直接配置允许的前缀列表中的前缀。
- 当允许的前缀列表设置为 10.0.0.0/24 时，您在中转虚拟接口上通过 BGP 收到 10.0.0.0/24。您不会收到 10.0.0.0/16，因为我们直接配置允许的前缀列表中的前缀。
- 当允许的前缀列表设置为 10.0.0.0/8 时，您在中转虚拟接口上通过 BGP 收到 10.0.0.0/8。

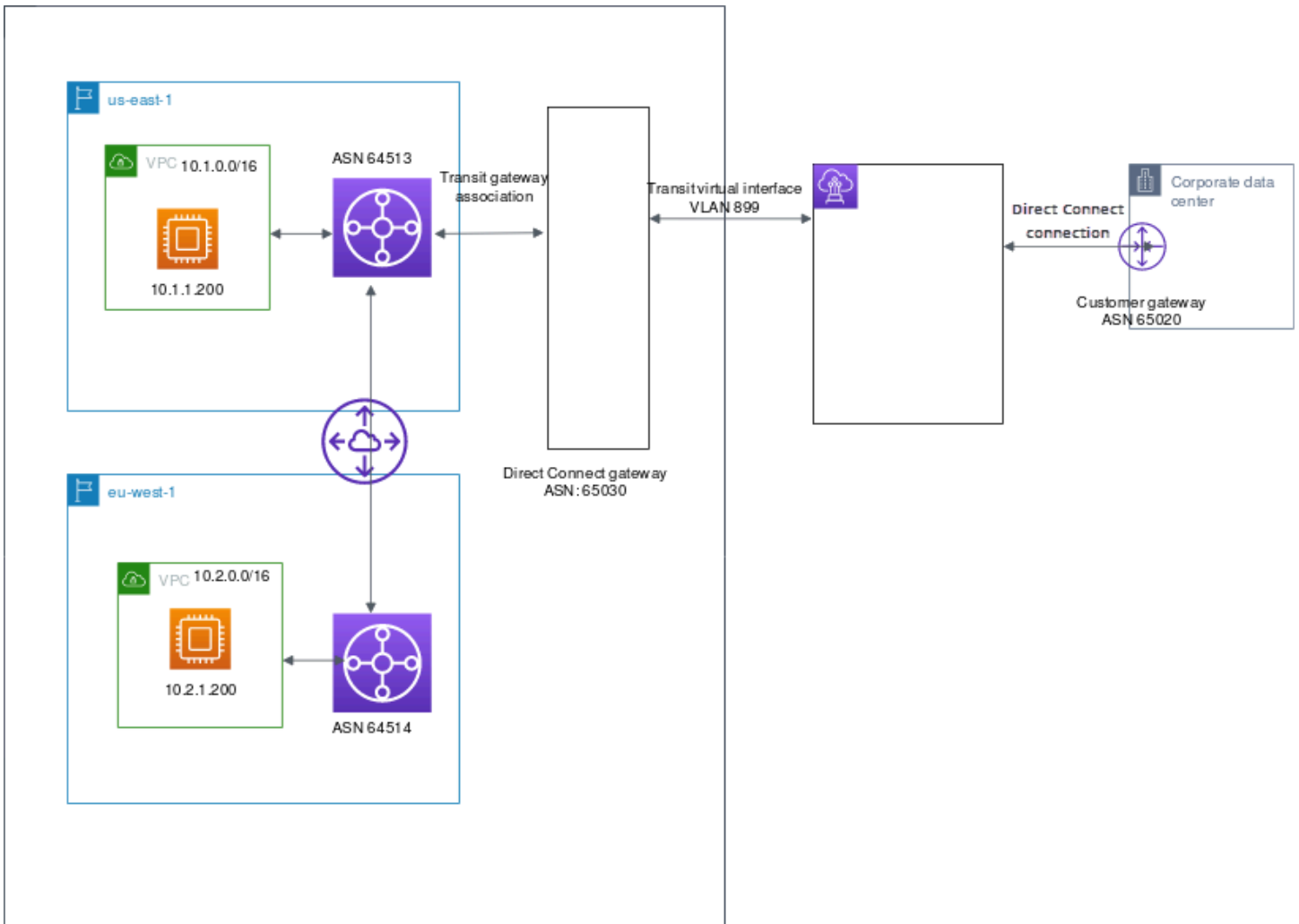
当多个中转网关与 Direct Connect 网关关联时，不允许出现允许的前缀重叠。例如，如果您有一个中转网关的允许前缀列表包含 10.1.0.0/16，而第二个中转网关的允许前缀列表包含 10.2.0.0/16 和 0.0.0.0/0，则您不能将第二个中转网关的关联设置为 0.0.0.0/0。由于 0.0.0.0/0 包括所有 IPv4 网络，因此如果多个中转网关与 Direct Connect 网关关联，则无法配置 0.0.0.0/0。系统将返回错误消息，表示允许的路由与 Direct Connect 网关上的一个或多个现有的允许路由重叠。

删除或添加允许的前缀时，不使用该前缀的流量不会受到影响。在更新过程中，状态从 `associated` 变为 `updating`。修改现有前缀只能延迟或丢弃使用该前缀的流量。

示例：允许在中转网关配置中添加前缀

考虑以下配置：在两个不同的 AWS 区域拥有需要访问公司数据中心的实例。对于此配置，可以使用以下资源：

- 每个区域的中转网关。
- 中转网关对等连接。
- Direct Connect 网关。
- 其中一个中转网关（us-east-1 中的网关）与 Direct Connect 网关之间的中转网关关联。
- 来自本地位置和 Direct Connect 位置的中转虚拟接口。



为资源配置以下选项：

- Direct Connect 网关：将 ASN 设置为 65030。有关更多信息，请参阅 [创建 Direct Connect 网关](#)。
- 中转虚拟接口：将 VLAN 设置为 899，将客户路由器对等 ASN 设置为 65020。有关更多信息，请参阅 [创建到 Direct Connect 网关的中转虚拟接口](#)。
- Direct Connect 网关与中转网关关联：将允许的前缀设置为 10.0.0.0/8。

此 CIDR 数据块包含两个 VPC CIDR 数据块 (10.0.0.0/16 和 10.2.0.0/16)。有关更多信息，请参阅 [将中转网关与 Direct Connect 关联或解除其关联](#)。

- VPC 路由：要路由来自 10.2.0.0/16 VPC 的流量，请在 VPC 路由表中创建一个目的地为 0.0.0.0/0，目标为中转网关 ID 的路由。这使来自 VPC 的流量可以到达 Direct Connect 网关。有关路由到中转网关的更多信息，请参阅《Amazon VPC 用户指南》中的 [中转网关路由](#)。

标记 AWS Direct Connect 资源

标签是资源所有者分配给其 Direct Connect 资源的签条。每个标签都包含定义的一个键和一个可选值。标签可让资源所有者按不同方式（例如，按用途或环境）对 Direct Connect 资源进行分类。这在您拥有许多同类型资源时很有用 - 您可以根据分配给资源的标签快速识别特定资源。

例如，在一个区域中有两个 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 of 连接和虚拟接口添加标签来进行区分：

| Resource ID | 标签密钥 | 标签值 |
|----------------|------|-------|
| dxcon-11aa22bb | 用途 | 生产 |
| | 位置 | 阿姆斯特丹 |
| dxvif-33cc44dd | 用途 | 生产 |
| dxcon-abcabcab | 用途 | 备份 |
| | 位置 | 法兰克福 |
| dxvif-12312312 | 用途 | 备份 |

我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理资源时会更加轻松。标签对 Direct Connect 没有任何语义意义，应严格按字符串进行解析。同时，标签不会自动分配至您的资源。您可以修改标签的密钥和值，还可以随时删除资源的标签。您可以将标签的值设为空的字符串，但是不能将其设为空值。如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。如果删除资源，资源的所有标签也会被删除。

您可以使用 Direct Connect 控制台、Direct Connect API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS SDK 标记以下 Direct Connect 资源。当您使用这些工具管理标签时，您必须为资源指定 Amazon 资源名称 (ARN)。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 [Amazon 资源名称 \(ARN\)](#)。

| 资源 | 支持标签 | 支持在创建时标记 | 支持通过标签控制访问和资源分配 | 支持成本分配 |
|-------------------|------|----------|-----------------|--------|
| 连接 | 支持 | 是 | 是 | 是 |
| 虚拟接口 | 支持 | 是 | 是 | 否 |
| 链接聚合组 (LAG) | 支持 | 是 | 是 | 是 |
| 互连 | 支持 | 是 | 是 | 是 |
| Direct Connect 网关 | 支持 | 是 | 是 | 否 |

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
- 标签键和值区分大小写。
- aws：前缀专门预留供 AWS 使用。当标签具有带 aws：前缀的标签键时，您将无法编辑或删除标签的键或值。具有带 aws：前缀的标签键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：+ - = . _ : / @
- 只有资源所有者可以添加或删除标签。例如，如果有一个托管连接，合作伙伴将无法添加、删除或查看标签。
- 仅对于连接、互连和 LAG 才支持成本分配标签。有关如何在成本管理中使用标签的信息，请参阅《AWS 账单与成本管理 用户指南》中的[使用成本分配标签](#)。

通过 CLI 或 API 使用标签

使用以下命令添加、更新、列出和删除资源标签。

| 任务 | API | CLI |
|---------------|-------------------------------|----------------------------------|
| 添加或覆盖一个或多个标签。 | TagResource | - tag-resource |
| 删除一个或多个标签。 | UntagResource | - untag-resource |
| 描述一个或多个标签。 | DescribeTags | describe-tags |

示例

使用 [tag-resource](#) 命令标记连接 dxcon-11aa22bb。

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

使用 [describe-tags](#) 命令描述连接 dxcon-11aa22bb 标签。

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

使用 [untag-resource](#) 命令删除连接 dxcon-11aa22bb 中的标签。

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

安全性 AWS Direct Connect

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。[责任共担模式](#)将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。AWS 还为您提供可以安全使用的服务。作为 [AWS 合规性计划](#) 的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 AWS Direct Connect，请参阅[按合规计划划分的范围内的AWS 服务](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 Direct Connect。以下主题向您介绍如何进行配置 Direct Connect 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Direct Connect 资源。

主题

- [AWS Direct Connect 中的数据保护](#)
- [适用于 Direct Connect 的 Identity and Access Management](#)
- [AWS Direct Connect 中的日志记录和监控](#)
- [的合规性验证 AWS Direct Connect](#)
- [AWS Direct Connect 中的故障恢复能力](#)
- [Direct Connect 中的基础结构安全性](#)

AWS Direct Connect 中的数据保护

AWS [责任共担模式](#)适用于 Direct Connect 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础架构。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题](#)。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 [AWS Shared Responsibility Model and GDPR](#) 博客文章。

出于数据保护目的，建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日记账记录。有关使用 CloudTrail 跟踪来捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用 CloudTrail 跟踪](#)。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅[《美国联邦信息处理标准 \(FIPS \) 第 140-3 版》](#)。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理 Direct Connect 或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

有关数据保护的更多信息，请参阅 AWS 安全性博客 上的[AWS 责任共担模式和 GDPR](#) 博客文章。

主题

- [网际流量隐私 AWS Direct Connect](#)
- [加密 AWS Direct Connect](#)

网际流量隐私 AWS Direct Connect

服务与本地客户端和应用之间的流量

您的专用网络和以下两种连接方式可供选择 AWS：

- 与 AWS Site-to-Site VPN 的关联。有关更多信息，请参阅[基础结构安全性](#)。
- 与... 的关联 VPCs。有关更多信息，请参阅[虚拟私有网关关联](#)和[中转网关关联](#)。

同一区域内 AWS 资源之间的流量

您有两个连接选项：

- 与 AWS Site-to-Site VPN 的关联。有关更多信息，请参阅 [基础结构安全性](#)。
- 与... 的关联 VPCs。有关更多信息，请参阅 [虚拟私有网关关联](#) 和 [中转网关关联](#)。

加密 AWS Direct Connect

AWS Direct Connect 默认情况下，不会对传输中的流量进行加密。要对传输中的数据进行加密 AWS Direct Connect，必须使用该服务的传输加密选项。有关 EC2 实例流量加密的信息，请参阅《Amazon EC2 用户指南》中的 [传输中加密](#)。

使用 AWS Direct Connect 和 AWS Site-to-Site VPN，您可以将一个或多个 AWS Direct Connect 专用网络连接与 Amazon VPC VPN 结合使用。这种组合提供了 IPsec 加密的私有连接，与基于互联网的 VPN 连接相比，还可以降低网络成本，增加带宽吞吐量，并提供更稳定的网络体验。有关更多信息，请参阅 [Amazon VPC-to-Amazon VPC 连接选项](#)。

MAC Security (MACsec) 是一项 IEEE 标准，可提供数据机密性、数据完整性和数据来源真实性。您可以使用支持 MACsec 加密从公司数据中心到该 Direct Connect 位置的数据的 Direct Connect 连接。有关更多信息，请参阅 [MAC 安全 \(MACsec\)](#)。

适用于 Direct Connect 的 Identity and Access Management

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 Direct Connect 资源。您可以使用 IAM AWS 服务，无需支付额外费用。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [Direct Connect 如何与 IAM 结合使用](#)
- [Direct Connect 基于身份的策略示例](#)
- [的服务相关角色 Direct Connect](#)
- [AWS 的托管策略 AWS Direct Connect](#)

- [Direct Connect 身份和访问问题排查](#)

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅[Direct Connect 身份和访问问题排查](#)）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅[Direct Connect 如何与 IAM 结合使用](#)）
- IAM 管理员：编写用于管理访问权限的策略（请参阅[Direct Connect 基于身份的策略示例](#)）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center））、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的[如何登录您的 AWS 账户](#)。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的[适用于 API 请求的 AWS 签名版本 4](#)。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。AWS IAM Identity Center 有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[什么是 IAM Identity Center？](#)。

IAM 用户和群组

[IAM 用户](#)是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的[要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问](#)。

[IAM 组](#)指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的[IAM 用户使用案例](#)。

IAM 角色

[IAM 角色](#)是具有特定权限的身份，可提供临时凭证。您可以通过[从用户切换到 IAM 角色（控制台）](#)或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的[担任角色的方法](#)。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的[JSON 策略概述](#)。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的[在托管策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中[指定主体](#)。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM 实体的权限边界](#)。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的[资源控制策略 \(RCPs\)](#)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

Direct Connect 如何与 IAM 结合使用

在使用 IAM 管理对 Direct Connect 的访问之前，了解哪些 IAM 功能可用于 Direct Connect。

可与 Direct Connect 结合使用的 IAM 功能

| IAM 功能 | Direct Connect 支持 |
|-------------------------|-------------------|
| 基于身份的策略 | 是 |
| 基于资源的策略 | 否 |
| 策略操作 | 是 |

| IAM 功能 | Direct Connect 支持 |
|---------------------------------|-------------------|
| 策略资源 | 是 |
| 策略条件键 (特定于服务) | 是 |
| ACLs | 否 |
| ABAC (策略中的标签) | 部分 |
| 临时凭证 | 是 |
| 主体权限 | 是 |
| 服务角色 | 是 |
| 服务关联角色 | 否 |

要全面了解 Direct Connect 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 [IAM 用户指南中与 IAM 配合使用的 AWS 服务](#)。

Direct Connect 基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

Direct Connect 基于身份的策略示例

要查看 Direct Connect 基于身份的策略示例，请参阅 [Direct Connect 基于身份的策略示例](#)。

Direct Connect 基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

Direct Connect 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 Direct Connect 操作列表，请参阅《Service Authorization Reference》中的[Actions Defined by Direct Connect](#)。

Direct Connect 的策略操作在操作前使用以下前缀：

```
Direct Connect
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [  
    "directconnect:action1",  
    "directconnectaction2"  
]
```

Direct Connect 的策略资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其[Amazon 资源名称 \(ARN\)](#) 指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Direct Connect 资源类型及其列表 ARNs，请参阅《AWS Direct Connect API 参考》中的 [Direct Connect 定义的资源](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Direct Connect 定义的操作](#)。

要查看 Direct Connect 基于身份的策略示例，请参阅 [Direct Connect 基于身份的策略示例](#)。

要查看 Direct Connect 基于资源的策略示例，请参阅 [Direct Connect 基于身份的策略示例 \(使用基于标签的条件\)](#)。

Direct Connect 的条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用 [条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的 [AWS 全局条件上下文密钥](#)。

要查看 Direct Connect 条件键列表，请参阅 AWS Direct Connect API 参考中的 [Direct Connect 的条件键](#)。要了解可以为条件键使用的操作和资源，请参阅《Service Authorization Reference》中的 [Actions, Resources, and Condition Keys for Direct Connect](#)。

要查看 Direct Connect 基于身份的策略示例，请参阅 [Direct Connect 基于身份的策略示例](#)。

ACLs 在直接连接中

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Direct Connect 的 ABAC

支持 ABAC（策略中的标签）：部分支持

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的 [使用 ABAC 授权定义权限](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的 [使用基于属性的访问权限控制 \(ABAC\)](#)。

对 Direct Connect 使用临时凭证

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 中的临时安全凭证](#) 和 [使用 IAM 的 AWS 服务](#)

Direct Connect 的跨服务主体权限

支持转发访问会话 (FAS)：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅 [转发访问会话](#)。

Direct Connect 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 [创建向 AWS 服务委派权限的角色](#)。

Warning

更改服务角色的权限可能会破坏 Direct Connect 的功能。仅当 Direct Connect 提供相关指导时才编辑服务角色。

Direct Connect 的服务相关角色

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅[能够与 IAM 搭配使用的AWS 服务](#)。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Direct Connect 基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Direct Connect 资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM 策略 \(控制台 \)](#)。

有关 Direct Connect 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 [Direct Connect 的操作、资源和条件密钥](#)。ARNs

主题

- [策略最佳实践](#)
- [Direct Connect 的操作、资源和条件](#)
- [使用 Direct Connect 控制台](#)
- [允许用户查看他们自己的权限](#)
- [只读访问权限 Direct Connect](#)
- [完全访问权限 Direct Connect](#)
- [Direct Connect 基于身份的策略示例 \(使用基于标签的条件 \)](#)

策略最佳实践

基于身份的策略决定某人是否可以在您的账户中创建、访问或删除 Direct Connect 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [AWS 托管策略](#)或[工作职能的AWS 托管策略](#)。

- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [使用 IAM Access Analyzer 验证策略](#)。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 [使用 MFA 保护 API 访问](#)。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

Direct Connect 的操作、资源和条件

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。Direct Connect 支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素参考](#)。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

Direct Connect 的策略操作在操作前使用以下前缀：directconnect:。例如，要授予某人使用 Amazon EC2 DescribeVpnGateways API 操作运行 Amazon EC2 实例的权限，您应将 ec2:DescribeVpnGateways 操作纳入其策略。策略语句必须包含 Action 或 NotAction 元素。Direct Connect 定义了一组自己的操作，来描述您可以使用该服务执行的任务。

以下示例策略授予对的读取权限 Direct Connect。

JSON

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

以下示例策略授予对的完全访问权限 Direct Connect。

JSON

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

要查看 Direct Connect 操作列表，请参阅《IAM 用户指南》中的 [Direct Connect 定义的操作](#)。

资源

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"

```

Direct Connect 使用以下内容 ARNs：

直接连接资源 ARNs

| 资源类型 | 进行筛选 |
|------------|---|
| dxcon | arn:\${Partition}:directconnect:\${Region}:\${Account}:dxcon/\${ConnectionId} |
| dxlag | arn:\${Partition}:directconnect:\${Region}:\${Account}:dxlag/\${LagId} |
| dx-vif | arn:\${Partition}:directconnect:\${Region}:\${Account}:dxvif/\${VirtualInterfaceId} |
| dx-gateway | arn:\${Partition}:directconnect::\${Account}:dx-gateway/\${DirectConnectGatewayId} |

有关格式的更多信息 ARNs，请参阅 [Amazon 资源名称 \(ARNs\)](#) 和 [AWS 服务命名空间](#)。

例如，要在语句中指定 dxcon-11aa22bb 接口，请使用以下 ARN：

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb

```

要指定属于特定账户的所有虚拟接口，请使用通配符 (*)：

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

无法对特定资源执行某些 Direct Connect 操作，例如，创建资源的操作。在这些情况下，您必须使用通配符 (*)。

```
"Resource": "*"
```

要查看 Direct Connect 资源类型及其列表 ARNs，请参阅 IAM 用户指南 Direct Connect 中[定义的资源类型](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Direct Connect 定义的操作](#)。

如果在、或 IAM 策略声明的 Resource 字段中指定了资源 ARN 或资源 ARN 模式以外的 * 资源 ARN 模式 DescribeConnections DescribeVirtualInterfaces DescribeDirectConnectGateways DescribeInterconnects DescribeLags，则除非在 API 调用中还传递了匹配的资源 ID，否则指定的内容 Effect 不会出现。但是，如果您在 IAM 策略声明中提供 * 作为资源而不是特定的资源 ID，则指定的 Effect 将起作用。

在以下示例中，如果在请求中未传递 connectionId 的情况下调用 DescribeConnections 操作，则两个指定的 Effect 都不会成功。

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "directconnect:DescribeConnections"
    ],
    "Resource": [
      "arn:aws:directconnect:*:123456789012:dxcon/*"
    ]
  },
  {
    "Effect": "Deny",
    "Action": [
      "directconnect:DescribeConnections"
    ],
    "Resource": [
      "arn:aws:directconnect:*:123456789012:dxcon/example1"
    ]
  }
]
```

但是，在以下示例中，无论在请求中是否指定了 `connectionId`，`DescribeConnections` 操作的 `"Effect": "Allow"` 都将成功，这是由于为 IAM 策略声明的 `Resource` 字段提供了 `*`。

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

条件键

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

Direct Connect 定义了一组自己的条件键，还支持使用一些全局条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

您可以将条件键与标签资源一起使用。有关更多信息，请参阅[示例：限制对特定区域的访问](#)。

要查看 Direct Connect 条件键列表，请参阅《IAM 用户指南》中的[Direct Connect 条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅[Direct Connect 定义的操作](#)。

使用 Direct Connect 控制台

要访问 Direct Connect 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 AWS 账户中 Direct Connect 资源的详细信息。如果创建的基于身份的策略比最低权限要求更严格，则对于具有该策略的实体（用户或角色），控制台将无法按预期工作。

为确保这些实体仍然可以使用 Direct Connect 控制台，还需要将以下 AWS 托管策略附加到这些实体。有关更多信息，请参阅《IAM 用户指南》中的[为用户添加权限](#)：

```
directconnect
```

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

只读访问权限 Direct Connect

以下示例策略授予对的读取权限 Direct Connect。

JSON

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

完全访问权限 Direct Connect

以下示例策略授予对的完全访问权限 Direct Connect。

JSON

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

Direct Connect 基于身份的策略示例 (使用基于标签的条件)

您可以使用标签键条件控制对资源和请求的访问。您还可以在 IAM policy 中使用条件来控制是否可以在资源或请求中使用特定标签键。

有关如何在 IAM 策略中使用标签的信息，请参阅《IAM 用户指南》中的[使用标签控制访问](#)。

基于标签关联 Direct Connect 虚拟接口

以下示例显示您可以如何创建此类策略：仅当标签包含环境键和预生产或生产值时，才允许关联虚拟接口。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "directconnect:AssociateVirtualInterface"
      ],
      "Resource": "arn:aws:directconnect:*:*:dxvif/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/environment": [
            "preprod",
            "production"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "directconnect:DescribeVirtualInterfaces",
      "Resource": "*"
    }
  ]
}
```

基于标签控制对请求的访问

您可以使用 IAM 策略中的条件来控制可以在为资源添加标签的请求中传递哪些标签键值对。AWS 以下示例显示了如何创建策略，该策略仅在标签包含环境密钥以及预生产值或生产值时才允许使用 Direct Connect TagResource 操作将标签附加到虚拟接口。作为最佳实践，请将 ForAllValues 修饰符与 aws:TagKeys 条件键配合使用，以指示只允许在请求中使用键环境。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "arn:aws:directconnect:*:*:dxvif/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/environment": [
          "preprod",
          "production"
        ]
      },
      "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
    }
  }
}
```

控制标签键

您可以在 IAM policy 中使用条件来控制是否可以在资源或请求中使用特定标签键。

以下示例显示如何可以创建一个策略，让您能够标记资源但仅限于标签键环境

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
```

```
"Action": "directconnect:TagResource",
"Resource": "*",
"Condition": {
  "ForAllValues:StringEquals": {
    "aws:TagKeys": [
      "environment"
    ]
  }
}
```

的服务相关角色 Direct Connect

AWS Direct Connect 使用 AWS Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。Direct Connect 服务相关角色由服务预定义 Direct Connect，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 Direct Connect 更加容易，因为您不必手动添加必要的权限。Direct Connect 定义其服务相关角色的权限，除非另有定义，否则 Direct Connect 只能担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务关联角色。这可以保护您的 Direct Connect 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅[使用 IAM 的 AWS 服务](#)并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务关联角色文档。

的服务相关角色权限 Direct Connect

Direct Connect 使用名 `AWSServiceRoleForDirectConnect` 为的服务相关角色。这样 Direct Connect 就可以代表您检索存储 AWS Secrets Manager 在中的 MACSec 密钥。

`AWSServiceRoleForDirectConnect` 服务相关角色信任以下服务代入该角色：

- `directconnect.amazonaws.com`

`AWSServiceRoleForDirectConnect` 服务相关角色使用托管策略 `AWSDirectConnectServiceRolePolicy`。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。为了成功创建 `AWSServiceRoleForDirectConnect` 服务相关角色，用于 Direct Connect 的 IAM 身份必须具有所需的权限。要授予所需的权限，请将以下策略附加到 IAM 身份。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "iam:CreateServiceLinkedRole",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "directconnect.amazonaws.com"
        }
      },
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": "iam:GetRole",
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的[服务关联角色权限](#)。

为创建服务相关角色 Direct Connect

您无需手动创建服务相关角色。AWS Direct Connect 为您创建服务相关角色。运行 `associate-mac-sec-key` 命令时，AWS 会创建一个服务相关角色，该角色 Direct Connect 允许在 AWS 管理控制台 AWS CLI、或 AWS API 中 AWS Secrets Manager 代表您检索存储在中的 MACsec 机密。

Important

如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务关联角色可以出现在您的账户中。要了解更多信息，请参阅[我的 IAM 账户中的新角色](#)。

如果您删除了此服务相关角色，然后需要重新创建它，则可以使用相同的过程在您的账户中重新创建该角色。Direct Connect 再次为您创建服务相关角色。

您也可以使用 IAM 控制台为 AWS Direct Connect 用例创建服务相关角色。在 AWS CLI 或 AWS API 中，使用服务名称创建服务相关角色。directconnect.amazonaws.com 有关更多信息，请参阅 IAM 用户指南 中的 [创建服务相关角色](#)。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

编辑的服务相关角色 Direct Connect

Direct Connect 不允许您编辑 `AWSServiceRoleForDirectConnect` 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的 [编辑服务关联角色](#)。

删除的服务相关角色 Direct Connect

无需手动删除 `AWSServiceRoleForDirectConnect` 角色。删除服务关联角色时，必须删除存储在 AWS Secrets Manager Web 服务中的所有关联资源。AWS 管理控制台 AWS CLI、或 AWS API 会 Direct Connect 清理资源并为您删除服务相关角色。

您还可以使用 IAM 控制台删除服务相关角色。为此，必须先手动清理服务相关角色的资源，然后才能将其删除。

Note

如果您尝试删除资源时 Direct Connect 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟，然后再次尝试操作。

删除使用的 Direct Connect 资源 `AWSServiceRoleForDirectConnect`

1. 移除所有 MACsec 按键和连接之间的关联。有关更多信息，请参阅 [the section called “移除 MACsec 密钥和连接之间的关联”](#)。
2. 移除所有 MACsec 密钥和之间的关联 LAGs。有关更多信息，请参阅 [the section called “移除 MACsec 密钥和 LAG 之间的关联”](#)。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 `AWSServiceRoleForDirectConnect` 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的 [删除服务关联角色](#)。

Direct Connect 服务相关角色支持的区域

Direct Connect 支持在所有提供 MAC 安全功能 AWS 区域 的地方使用服务相关角色。有关更多信息，请参阅 [AWS Direct Connect 地点](#)。

AWS 的托管策略 AWS Direct Connect

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的 [客户管理型策略](#) 来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 [AWS 托管策略](#)。

AWS 托管策略：AWSDirectConnectFullAccess

您可以将 AWSDirectConnectFullAccess 策略附加到 IAM 身份。此策略授予允许完全访问的权限 Direct Connect。

要查看此策略的权限，请参阅 AWS 管理控制台中的 [AWSDirectConnectFullAccess](#)。

AWS 托管策略：AWSDirectConnectReadOnlyAccess

您可以将 AWSDirectConnectReadOnlyAccess 策略附加到 IAM 身份。此策略授予允许只读访问的权限 Direct Connect。

要查看此策略的权限，请参阅 AWS 管理控制台中的 [AWSDirectConnectReadOnlyAccess](#)。

AWS 托管策略：AWSDirectConnectServiceRolePolicy

此策略附加到名为的服务相关角色，AWSServiceRoleForDirectConnect 允许 Direct Connect 代表您检索 MAC Security 机密。有关更多信息，请参阅 [the section called “服务关联角色”](#)。

要查看此策略的权限，请参阅 AWS 管理控制台中的 [AWSDirectConnectServiceRolePolicy](#)。

Direct Connect AWS 托管策略的更新

查看 Direct Connect 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅“Direct Connect 文档历史记录”页面上的 RSS feed。

| 更改 | 描述 | 日期 |
|---|--|-----------------|
| AWSDirectConnectServiceRolePolicy : 新策略 | 为了支持 MAC 安全，添加了AWSServiceRoleForDirectConnect服务相关角色。 | 2021 年 3 月 31 日 |
| Direct Connect 开始跟踪更改 | Direct Connect 开始跟踪其托管 AWS 策略的更改。 | 2021 年 3 月 31 日 |

Direct Connect 身份和访问问题排查

以下信息可帮助您诊断和修复在使用 Direct Connect 和 IAM 时可能遇到的常见问题。

主题

- [我没有在 Direct Connect 中执行操作的权限](#)
- [我无权执行 iam : PassRole](#)
- [我想允许我以外的人访问我的 Direct Connect 资源](#)

我没有在 Direct Connect 中执行操作的权限

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 `directconnect:GetWidget` 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
directconnect:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 `directconnect:GetWidget` 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Direct Connect。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Direct Connect 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 Direct Connect 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Direct Connect 是否支持这些功能，请参阅 [Direct Connect 如何与 IAM 结合使用](#)。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户，请参阅 [IAM 用户指南中的向您拥有 AWS 账户的另一个 IAM 用户提供访问权限](#)。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 [IAM 用户指南中的向第三方提供访问权限。AWS 账户](#)。
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的 [为经过外部身份验证的用户（身份联合验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

AWS Direct Connect 中的日志记录和监控

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

- Amazon CloudWatch 警报：在指定时间段内监控某个指标。在多个时间段内根据相对于给定阈值的指标值，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 进行监控 CloudWatch](#)。
- AWS CloudTrail 日志监控：在账户之间共享日志文件，并通过将日志文件发送到 CloudWatch Logs 来实时监控 CloudTrail 日志文件。您还可以使用 Java 编写日志处理应用程序，并验证您的日志文件在 CloudTrail 交付后未发生更改。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 [使用记录 Direct Connect API 调用 AWS CloudTrail](#) 和 [使用 CloudTrail 日志文件](#)。

有关更多信息，请参阅 [监控 Direct Connect 资源](#)。

的合规性验证 AWS Direct Connect

要了解某个 AWS 服务是否在特定合规性计划范围内，请参阅[合规性计划范围内的 AWS 服务](#)，然后选择您感兴趣的合规性计划。有关常规信息，请参阅 [AWS 合规性计划](#)、。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅[在 AWS Artifact 中下载报告](#)、。

您在使用 AWS 服务时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。有关您在使用 AWS 服务时的合规责任的更多信息，请参阅 [AWS 安全性文档](#)。

AWS Direct Connect 中的故障恢复能力

AWS全球基础架构围绕AWS区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 [AWS全球基础设施](#)。

除了 AWS 全球基础设施之外，Direct Connect 还提供了多种功能，以帮助支持您的数据弹性和备份需求。

有关如何将 VPN 与 AWS Direct Connect 一起使用的更多信息，请参阅 [AWS Direct Connect Plus VPN](#)。

失效转移

AWS Direct Connect 弹性工具包提供了一个具有多个弹性模型的连接向导，可帮助您订购专用连接以实现 SLA 目标。您可以选择一个弹性模型，然后 AWS Direct Connect 弹性工具包将引导您完成专用连接订购过程。这些弹性模型旨在确保您在多个位置具有适当数量的专用连接。

- **最大弹性**：通过使用在多个位置的不同设备上终止的单独连接，您可以实现关键工作负载的最大弹性。该模型针对设备、连接性和完整位置故障均提供了弹性。
- **高弹性**：通过使用到多个位置的单一连接，您可以实现关键工作负载的高弹性。此模型可针对因光纤切断或设备故障而导致的连接故障提供弹性。它还有助于防止完整位置故障。
- **开发和测试**：通过使用在一个位置的不同设备上终止的单独连接，您可以实现非关键工作负载的开发和测试弹性。此模型提供了针对设备故障的弹性，但没有提供针对位置故障的弹性。

有关更多信息，请参阅 [the section called “AWS Direct Connect 弹性工具包”](#)。

Direct Connect 中的基础结构安全性

作为一项托管式服务，AWS Direct Connect 受 AWS 全球网络安全程序的保护。您可以使用 AWS 发布的 API 调用通过网络访问 Direct Connect。客户端必须支持传输层安全性 (TLS) 1.2 或更高版本。我们建议使用 TLS 1.3。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

您可以从任何网络位置调用这些 API 操作，但 Direct Connect 支持基于资源的访问策略，其中可以包含基于源 IP 地址的限制。您还可以使用 Direct Connect 策略来控制来自特定 Amazon Virtual Private Cloud (Amazon VPC) 端点或特定 VPC 的访问。事实上，这隔离了在 Direct Connect 网络中仅从特定 VPC 到给定 AWS 资源的网络访问。有关示例，请查看 [the section called “Direct Connect 基于身份的策略示例”](#)。

边界网关协议 (BGP) 安全

互联网在很大程度上依赖于 BGP 来获取网络系统之间的路由信息。BGP 路由有时容易受到恶意攻击或 BGP 劫持。要了解 AWS 如何保护您的网络免受 BGP 劫持，请参阅 [AWS 如何帮助保护互联网路由](#)。

使用 Direct Connect CLI

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

以下示例使用 AWS CLI 命令创建 Direct Connect 连接。您也可以下载《授权证书和连接设备分配 (LOA-CFA)》或预置一个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

- [步骤 1：创建连接](#)
- [步骤 2：下载 LOA-CFA](#)
- [步骤 3：创建虚拟接口，获取路由器配置](#)

步骤 1：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 Direct Connect 位置。有关更多信息，请参阅 [专用和托管连接](#)。

创建连接请求

1. 描述您当前区域中的 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": "City 1, United States",
      "locationCode": "Example Location 1"
    },
    {
      "locationName": "City 2, United States",
      "locationCode": "Example location"
    }
  ]
}
```

```
}
```

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 Example location --bandwidth 1Gbps
--connection-name "Connection to AWS"
```

```
{
  "ownerAccount": "123456789012",
  "connectionId": "dxcon-EXAMPLE",
  "connectionState": "requested",
  "bandwidth": "1Gbps",
  "location": "Example location",
  "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 macOS 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 directconnect 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 Direct Connect 连接以后，您必须创建虚拟接口以开始使用。您可以创建一个私有虚拟接口来连接到您的 VPC。或者，您也可以创建一个公有虚拟接口，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 [the section called “虚拟接口的先决条件”](#) 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。要创建特定于您的设备的路由器配置，请使用 Direct Connect 控制台。有关更多信息，请参阅 [下载路由器配置文件](#)。

创建私有虚拟接口

1. 获取附加到您 VPC 的虚拟私有网关的 ID (vgw-xxxxxxx)。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-ffhkh74f",
  "authKey": "asdf34example",
  "routeFilterPrefixes": [],
  "location": "Example location",
  "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-ffhkh74f\">\n  <vlan>101</
  vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
  <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
  \n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
  amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
  logical_connection>\n",
  "amazonAddress": "192.168.1.1/30",
  "virtualInterfaceType": "private",
  "virtualInterfaceName": "PrivateVirtualInterface"
```

```
}

```

要创建支持 IPv6 流量的私有虚拟接口，请使用上述命令并为 `ipv6` 参数指定 `addressFamily`。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。

- 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-ffhkh74f
--query virtualInterfaces[*].customerRouterConfig --output text

```

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

```

创建公有虚拟接口

- 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
{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": "Example location",
"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,routeFilterId=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>
```

使用记录 Direct Connect API 调用 AWS CloudTrail

Direct Connect 与 AWS CloudTrail 一项服务集成，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 Direct Connect。CloudTrail 将所有 API 调用捕获 Direct Connect 为事件。捕获的调用包括来自 Direct Connect 控制台的调用和对 Direct Connect API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 Direct Connect。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 Direct Connect、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关更多信息，请参阅 [AWS CloudTrail 《用户指南》](#)。

Direct Connect 信息在 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当活动发生在中时 Direct Connect，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 [使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您 AWS 账户中的事件，包括的事件 Direct Connect，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- [创建跟踪概述](#)
- [CloudTrail 支持的服务和集成](#)
- [配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件](#)

所有 Direct Connect 操作均由《API 参考》记录 CloudTrail 并记录在《[Direct Connect API 参考](#)》中。例如，调用 `CreateConnection` 和 `CreatePrivateVirtualInterface` 操作会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM 用户) 凭证发出。

- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

了解 Direct Connect 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下是的 CloudTrail 日志记录示例 Direct Connect。

Example 例如：CreateConnection

```
{
  "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"
    }
},
...
]
}

```

Example例如 : CreatePrivateVirtualInterface

```

{
  "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"
    }
  },
  ...
]
}

```

Example 例如 : DescribeConnections

```

{
  "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
},
...
]
}

```

Example 例如：DescribeVirtualInterfaces

```

{
  "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-fhajollyy"
  },
  "responseElements": null
},
...
]
}
```

监控 Direct Connect 资源

监控指标是维护 Direct Connect 资源的可靠性、可用性和性能的重要环节。您应该从 AWS 解决方案的所有部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。不过，在开始监控 Direct Connect 连接之前，您应制定监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 应监控哪些资源？
- 监控这些资源的频率应如何？
- 您可以使用哪些监控工具？
- 谁执行监控任务？
- 出现错误时应通知谁？

下一步，通过在不同时间和不同负载条件下测量性能，在您的环境中建立正常 Direct Connect 性能的基准。在监控 Direct Connect 时，存储历史监控数据。这样，您可以将历史监控数据与当前性能数据进行比较，确定性能的正常模式和性能异常，并找出解决问题的方法。

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

内容

- [监控工具](#)
- [使用 Amazon 进行监控 CloudWatch](#)

监控工具

AWS 提供了可用于监视 Direct Connect 连接的各种工具。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 Direct Connect 连接并在出现错误时报告：

- Amazon CloudWatch 警报 — 在您指定的时间段内观察单个指标。在多个时间段内根据相对于给定阈值的指标值，执行一项或多项操作。该操作是发送给 Amazon SNS 主题的通知。CloudWatch 警

报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关可用指标和维度的信息，请参阅 [使用 Amazon 进行监控 CloudWatch](#)。

- AWS CloudTrail 日志监控-在账户之间共享日志文件，并通过将 CloudTrail 日志文件发送到“日志”来实时监控 CloudWatch 日志文件。您还可以使用 Java 编写日志处理应用程序并确认您的日志文件在 CloudTrail 传送后未发生更改。有关更多信息，请参阅AWS CloudTrail 用户指南中的[记录 API 调用](#)和[使用 CloudTrail 日志文件](#)。

手动监控工具

监控 Direct Connect 连接的另一个重要部分是手动监控 CloudWatch 警报未涵盖的项目。Direct Connect 和 CloudWatch 控制台控制面板提供了 AWS 环境状态的 at-a-glance 视图。

- 控制 Direct Connect 台显示：
 - 连接状态 (请参阅 State 列)
 - 虚拟接口状态 (请参阅 State 列)
- CloudWatch 主页显示：
 - 当前告警和状态
 - 告警和资源图表
 - 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。
- 搜索并浏览您的所有 AWS 资源指标。
- 创建和编辑告警接收有关问题的通知。

使用 Amazon 进行监控 CloudWatch

您可以使用监控物理 Direct Connect 连接和虚拟接口 CloudWatch。CloudWatch 从 Direct Connect 收集原始数据，并将其处理为可读的指标。默认情况下，以 5 分钟为间隔 CloudWatch 提供 Direct Connect 指标数据。每个间隔中的指标数据是对该间隔内收集的至少两个样本的聚合。

有关详细信息 CloudWatch，请参阅 [Amazon CloudWatch 用户指南](#)。您还可以监控您的服务 CloudWatch，以了解哪些服务正在使用资源。有关更多信息，请参阅[发布 CloudWatch 指标的AWS 服务](#)。

内容

- [Direct Connect 指标和维度](#)
- [查看 Direct Connect CloudWatch 指标](#)
- [创建 Amazon CloudWatch 警报以监控 Direct Connect 连接](#)

Direct Connect 指标和维度


Direct Connect 物理连接和虚拟接口的指标可用。

Direct Connect 连接指标

Direct Connect 专用连接中包含以下指标。

| 指标 | 说明 |
|----------------------|---|
| ConnectionState | <p>连接的状态。1 表示运行，0 表示关闭。</p> <p>此指标适用于专用连接和托管连接。</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>除了连接所有者账户外，该指标还适用于托管虚拟接口所有者账户。</p> </div> <p>单位：此指标没有返回任何单位。</p> |
| ConnectionBpsEgress | <p>来自连接 AWS 端的出站数据的比特率。</p> <p>报告的数量是指定时间段（默认为 5 分钟，最短 1 分钟）内的聚合（平均值）。您可以更改默认聚合。</p> <p>对于新连接或当设备重新启动时，此衡量指标可能不适用。在连接用于发送或接收流量时，该指标启动。</p> <p>单位：每秒比特数</p> |
| ConnectionBpsIngress | <p>连接 AWS 侧进站数据的比特率。</p> |

| 指标 | 说明 |
|-------------------------|---|
| | <p>对于新连接或当设备重新启动时，此衡量指标可能不适用。在连接用于发送或接收流量时，该指标启动。</p> <p>单位：每秒比特数</p> |
| ConnectionPpsEgress | <p>来自连接 AWS 端的出站数据的数据包速率。</p> <p>报告的数量是指定时间段（默认为 5 分钟，最短 1 分钟）内的聚合（平均值）。您可以更改默认聚合。</p> <p>对于新连接或当设备重新启动时，此衡量指标可能不适用。在连接用于发送或接收流量时，该指标启动。</p> <p>单位：每秒数据包数</p> |
| ConnectionPpsIngress | <p>连接 AWS 侧入站数据的数据包速率。</p> <p>报告的数量是指定时间段（默认为 5 分钟，最短 1 分钟）内的聚合（平均值）。您可以更改默认聚合。</p> <p>对于新连接或当设备重新启动时，此衡量指标可能不适用。在连接用于发送或接收流量时，该指标启动。</p> <p>单位：每秒数据包数</p> |
| ConnectionCRCErrorCount | <p>此计数不再使用。请改用 ConnectionErrorCount 。</p> |

| 指标 | 说明 |
|------------------------|---|
| ConnectionErrorCount | <p>AWS 设备记录的所有 MAC 级别错误的总错误数。总数包括循环冗余检查 (CRC) 错误。这些错误的根本原因可能是客户方面，也可能是客户 AWS 方面。</p> <p>此指标是自上次报告数据点以来发生的错误计数。当接口出现错误时，指标会报告非零值。要获取所选时间间隔（例如 5 分钟）内 CloudWatch 所有错误的总数，请应用“sum”统计数据。</p> <p>当接口上的错误停止时，指标值设置为 0。</p> <div data-bbox="748 699 1508 919" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px;"><p> Note 此指标会替换 ConnectionCRCError Count，不再使用。</p></div> <p>单位：计数</p> |
| ConnectionLightLevelTx | <p>指示来自连接 AWS 侧的出站（出口）流量的光纤连接的运行状况。</p> <p>此指标有两个维度。有关更多信息，请参阅 Direct Connect 可用维度。</p> <p>单位：dBm</p> |
| ConnectionLightLevelRx | <p>指示流向连接 AWS 侧的进站（入口）流量的光纤连接的运行状况。</p> <p>此指标有两个维度。有关更多信息，请参阅 Direct Connect 可用维度。</p> <p>单位：dBm</p> |

| 指标 | 说明 |
|-----------------------------|---|
| ConnectionEncryptionState | 表示连接加密状态。1 表示连接加密为 up，0 表示连接加密为 down。将此指标应用于 LAG 时，1 表示 LAG 中的所有连接加密均为 up。0 表示至少一个 LAG 连接加密为 down。 |
| ConnectionDiscardsPpsEgress | <p>连接 AWS 端出站数据的数据包丢弃率。该指标跟踪由于缓冲区溢出、接口拥塞或其他网络状况而丢弃的数据包。</p> <p>报告的数量是指定时间段（默认为 5 分钟，最短 1 分钟）内的聚合（平均值）。您可以更改默认聚合。</p> <p>单位：每秒数据包数</p> |

Direct Connect 虚拟接口指标

以下指标可从 Direct Connect 虚拟接口获得。

| 指标 | 说明 |
|----------------------------|---|
| VirtualInterfaceBpsEgress | <p>来自虚拟接口 AWS 一侧的出站数据的比特率。</p> <p>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。</p> <p>单位：每秒比特数</p> |
| VirtualInterfaceBpsIngress | <p>虚拟接口 AWS 一侧的进站数据的比特率。</p> <p>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。</p> <p>单位：每秒比特数</p> |
| VirtualInterfacePpsEgress | 来自虚拟接口 AWS 一侧的出站数据的数据包速率。 |

| 指标 | 说明 |
|----------------------------|---|
| | 报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。 单位：每秒数据包数 |
| VirtualInterfacePpsIngress | 虚拟接口 AWS 一侧的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）内的聚合（平均值）。 单位：每秒数据包数 |

Direct Connect 可用尺寸

您可以使用以下维度筛选 Direct Connect 数据。

| 维度 | 说明 |
|--------------------|--|
| ConnectionId | Direct Connect 连接和虚拟接口的指标中提供此维度。此维度按连接筛选数据。 |
| OpticalLaneNumber | 此维度筛选 ConnectionLightLevelTx 数据和 ConnectionLightLevelRx 数据，并按照 Direct Connect 连接的光纤通道编号筛选数据。 |
| VirtualInterfaceId | Direct Connect 虚拟接口的指标中提供此维度，并按虚拟接口筛选数据。 |

主题

- [查看 Direct Connect CloudWatch 指标](#)
- [创建 Amazon CloudWatch 警报以监控 Direct Connect 连接](#)

查看 Direct Connect CloudWatch 指标

Direct Connect 会发送有关 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。默认情况下，系统每隔 5 分钟都会将 Direct Connect 指标数据写入 CloudWatch。

Note

通过 CloudWatch 监控 Direct Connect 时，您可以按 1 分钟的时间间隔请求指标。但是，实际的更新频率由 CloudWatch 控制。由于 CloudWatch 控制间隔，因此 Direct Connect 不能始终保证间隔短于五分钟。

您可以按照以下步骤查看 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。有关使用 Amazon CloudWatch 查看 Direct Connect 指标（包括添加数学函数或预建查询）的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[使用 Amazon CloudWatch 指标](#)。

1. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Metrics（指标），然后选择 All metrics（所有指标）。
3. 在指标部分，选择 DX。
4. 选择 ConnectionId 或指标名称，然后选择以下任一选项来进一步定义指标：
 - 添加到搜索：将此指标添加到您的搜索结果。
 - 仅搜索此指标：仅搜索此指标。
 - 从图表中移除：从图表中移除此指标。
 - 仅绘制此指标的图表：仅绘制此指标的图表。
 - 绘制所有搜索结果的图表：绘制所有指标的图表。
 - 使用 SQL 查询绘制图表：打开 Metric Insights 查询生成器，允许您通过创建 SQL 查询来选择要绘制图表的内容。有关使用 Metric Insights 的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[使用 CloudWatch Metrics Insights 查询您的指标](#)。

使用 Direct Connect 控制台查看指标

1. 访问 <https://console.aws.amazon.com/directconnect/v2/home> 并打开 Direct Connect 控制台。
2. 在导航窗格中，选择 Connections (连接)。
3. 选择连接。
4. 选择监控选项卡以显示连接的指标。

使用 查看指标AWS CLI

在命令提示符处，使用以下命令。

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

创建 Amazon CloudWatch 警报以监控 Direct Connect 连接

您可以创建在警报改变状态时发送 Amazon SNS 消息的 CloudWatch 警报。警报会监控您指定的时间段内的某个指标。它将根据指标值在多个时间段内相对于给定阈值的情况向 Amazon SNS 主题发送通知。

例如，您可以创建一个监控 Direct Connect 连接状态的警报。它会在连接状态在连续五个 1 分钟时间段内都为关闭时发送通知。有关创建警报的须知信息以及创建警报的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[使用 Amazon CloudWatch 警报](#)。

要创建 CloudWatch 警报。

1. 通过 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Alarms (告警)，然后选择 All alarms (所有告警)。
3. 选择创建警报。
4. 选择选择指标，然后选择 DX。
5. 选择连接指标指标。
6. 选择 Direct Connect 连接，然后选择选择指标指标。
7. 在指定指标和条件页面上，配置警报的参数。有关指定指标和条件的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[使用 Amazon CloudWatch 警报](#)。
8. 选择下一步。
9. 在配置操作页面上配置警报操作。有关配置警报操作的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[警报操作](#)。

10. 选择下一步。
11. 在添加名称和描述页面上，输入名称和可选的警报描述来描述该警报，然后选择下一步。
12. 在预览和创建页面上验证建议的警报。
13. 如果需要，请选择编辑以更改任何信息，然后选择创建警报。

警报页面将显示一个新行，其中包含有关新警报的信息。操作状态显示操作已启用，表示警报处于活动状态。

Direct Connect 限额

下表列出了与 Direct Connect 相关的配额。

| 组件 | 配额 | 评论 |
|--|----|---|
| 每个 Direct Connect 私有连接的私有或公有虚拟接口 | 50 | 不能提高此限制。 |
| 每个 Direct Connect 专用连接的中转虚拟接口。 中转虚拟接口可用于连接到中转网关或 AWS Cloud WAN 核心网络。有关更多信息，请参阅 网关 。 | 4 | 如需进一步帮助，请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| 每个 Direct Connect 专用连接的私有或公有虚拟接口，以及每个 Direct Connect 专用连接的中转虚拟接口 | 51 | 启动对 Amazon VPC 中转网关的 AWS Direct Connect 支持后，每个专用连接的 50 个私有或公有虚拟接口的配额中增加了一 (1) 个中转虚拟接口的配额。现在，允许的中转虚拟接口数量为四 (4) 个，并计入每个专用连接的 51 个虚拟接口上限。不能提高此限制。 |
| 每个 Direct Connect 托管连接的私有、公有或中转虚拟接口 | 1 | 不能提高该限制。 |
| 每个账户每个区域每个 Direct Connect 位置的活动 Direct Connect 连接数 | 10 | 如需进一步帮助，请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| 每个链接聚合组 (LAG) 的虚拟接口数 | 51 | 启动对 Amazon VPC 中转网关的 AWS Direct Connect 支持后，每个 LAG 的 50 个私有或公有虚拟接口配额中增加了一 (1) 个中转虚拟接口的配额。现在，允许的中转虚拟接口数量为四 (4) 个，并计入每个 LAG 的 51 个虚拟接口上限。不能提高此限制。 |

| 组件 | 配额 | 评论 |
|---|---|--|
| 私有虚拟接口或中转虚拟接口 (从本地到 AWS) 上的每个边界网关协议 (BGP) 会话的路由。 如果通过 BGP 会话为 IPv4 和 IPv6 各公布超过 100 个路由, 则 BGP 会话将进入空闲状态, 并且 BGP 会话将会关闭。 | IPv4 和 IPv6 各 100 个 | 如需进一步帮助, 请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| 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) 的专用连接数 | 端口速度低于 100G 时 4 个 端口速度为 100G 时 2 个 | |
| 每个区域的链接聚合组 (LAG) 数 | 10 | 如需进一步帮助, 请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| Direct Connect 每个账户的 网关数 | 200 | 如需进一步帮助, 请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| 每个 Direct Connect 网关的虚拟私有网关数 | 20 | 不能提高此限制。 |
| 每个 Direct Connect 网关的中转网关 | 6 | 不能提高此限制。 |

| 组件 | 配额 | 评论 |
|--|---------------------|---|
| 从 AWS Cloud WAN 核心网络 Direct Connect 网关连接到本地的通告路由前缀的最大数量。 | 5000 | 如需进一步帮助，请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p>Note</p> <p>连接到该 Direct Connect 网关的所有中转虚拟接口都将接收核心网络通告的所有路由前缀。</p> </div> | | |
| 每个 Direct Connect 网关的虚拟接口 (私有或中转) | 30 | 不能提高此限制。 |
| 中转虚拟接口上从 AWS 到本地每个 AWS Transit Gateway 的前缀数 | IPv4 和 IPv6 共 200 个 | 如需进一步帮助，请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |
| 每个虚拟私有网关的虚拟接口数 | 没有限制。 | |
| 与中转网关关联的 Direct Connect 网关数 | 20 | 不能提高此限制。 |
| SiteLink 前缀限制 | 100 | 如需进一步帮助，请联系您的解决方案架构师 (SA) 或者技术客户经理 (TAM)。 |

Direct Connect 支持通过单模光纤的以下端口速度：1Gbps：1000BASE-LX (1310 nm)、10 Gbps：10GBASE-LR (1310 nm)、100Gbps：100GBASE-LR4 和 400 Gbps：400GBASE-LR4。

BGP 配额

以下是 BGP 配额。BGP 计时器在路由器之间协商降至最低值。BFD 间隔由最慢的设备定义。

- 默认保持计时器：90 秒
- 最短保持计时器：3 秒

不支持将保持值设为 0。

- 默认保持连接计时器：30 秒
- 最短保持连接计时器：1 秒
- 安全重启计时器：120 秒

建议您不要同时配置安全重启和 BFD。

- BFD 活性检测最小间隔：300 毫秒
- BFD 最小倍数：3

ASN 限制

以下限制适用于 Direct Connect 使用的自治系统编号 (ASN)：

- 客户端 ASN 范围：1 至 4,294,967,294
 - ASN：1 至 2147483647
 - 长 ASN：1 至 4294967294
- Amazon 端 ASN：由 AWS 分配的固定值（对于公有虚拟接口，通常为 7224）
- 私有 ASN 范围：
 - 私有 ASN：64,512 至 65,534
 - 私有长 ASN：4,200,000,000 至 4,294,967,294

Note

对于公有虚拟接口，您的 ASN 必须是私有 ASN，或者已经注册并允许用于虚拟接口。

负载均衡注意事项

如果要对多个公有 VIF 使用负载均衡，则所有 VIF 必须位于同一个区域中。

Direct Connect 问题排查

以下问题排查信息可以帮助您诊断和解决 Direct Connect 连接问题。

目录

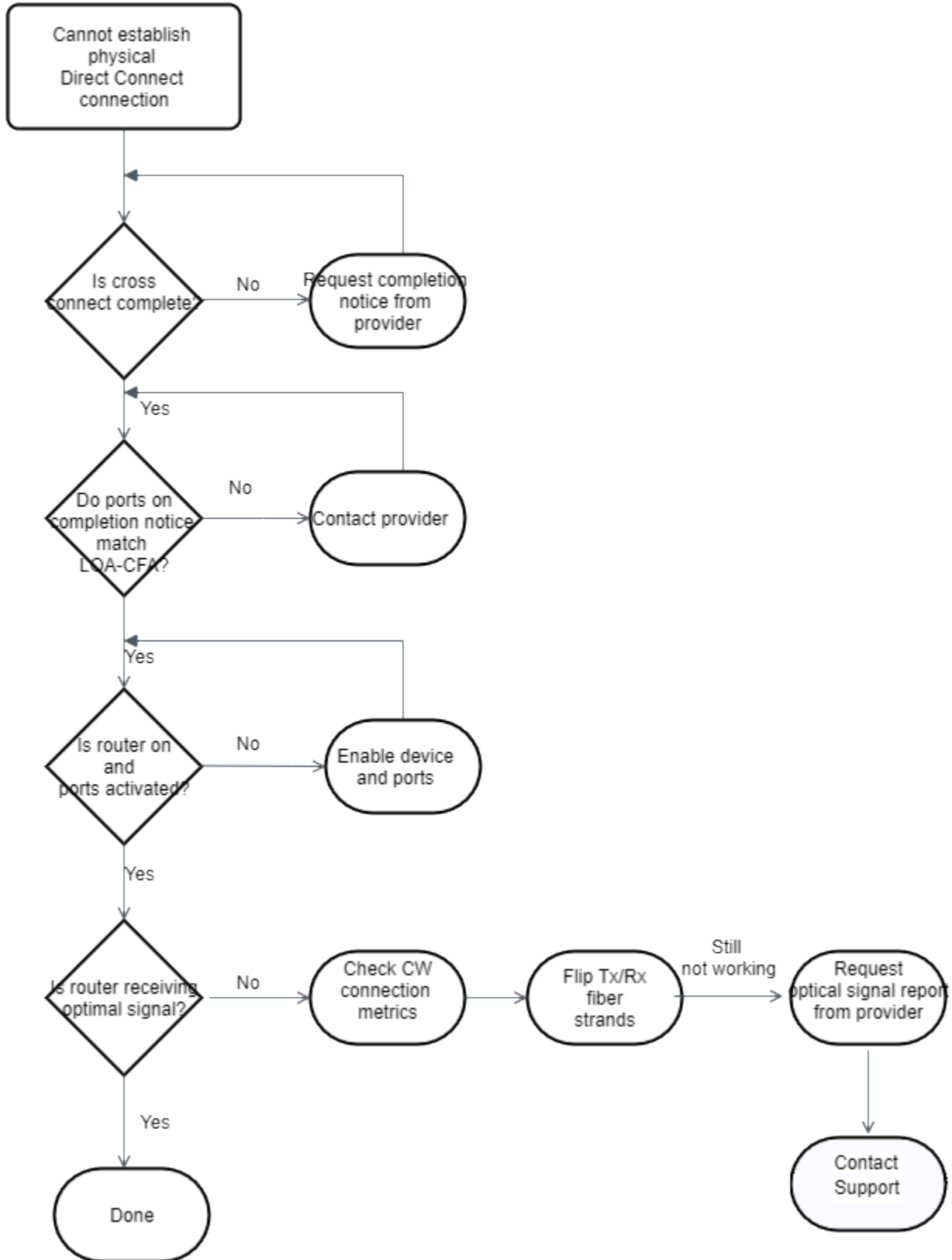
- [排查第 1 层 \(物理 \) 问题](#)
- [排查第 2 层 \(数据链路 \) 问题](#)
- [排查第 3/4 层 \(网络/传输 \) 问题](#)
- [排查长 ASN 问题](#)
- [排查路由问题](#)

排查第 1 层 (物理) 问题

如果您或您的网络提供商在建立与 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. 确保路由器使用正确的光学收发器。如果连接端口速度超过 1Gbps，则必须禁用端口自动协商。但是，根据为连接提供服务的 AWS Direct Connect 端点，可能需要为 1Gbps 连接启用或禁用自动协商。如果需要为连接禁用自动协商，则必须手动配置端口速度和全双工模式。如果虚拟接口仍处于关闭状态，请参阅 [排查第 2 层 \(数据链路 \) 问题](#)。根据为连接终端提供服务的 Direct Connect 端点，可能需要相应地启用或禁用自动协商。
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 Direct Connect 的 Amazon CloudWatch 指标。您可以验证 Direct Connect 设备的 Tx/Rx 光学读数 (1 Gbps 和 10 Gbps)、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 支持](#) 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。

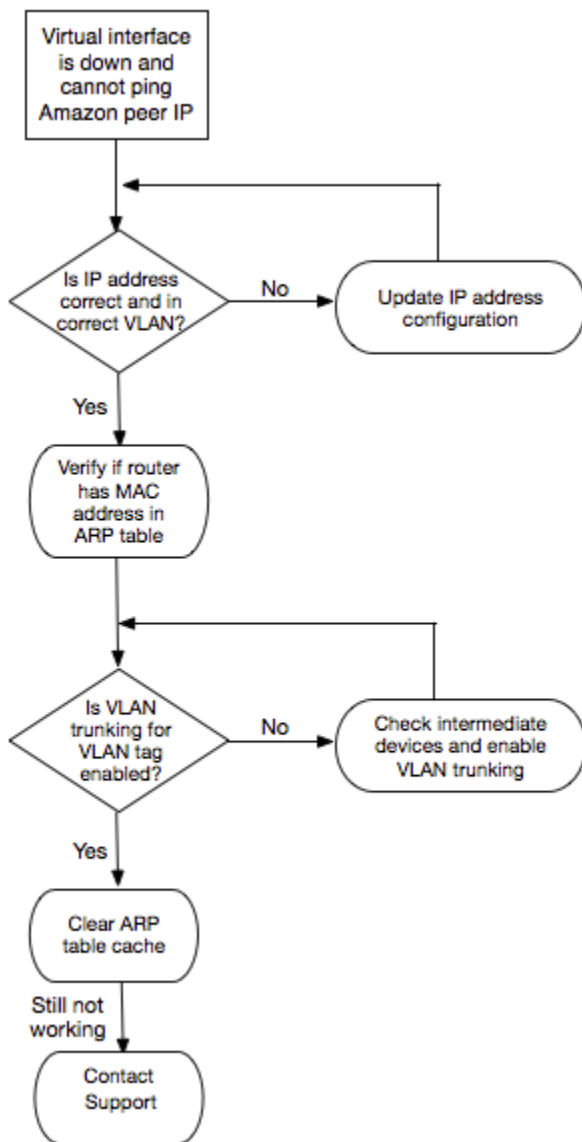


排查第 2 层 (数据链路) 问题

如果您的 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. 验证路由器的地址解析协议 (ARP) 表中是否有来自 AWS 端点的 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 接收标记的流量之前，无法在 AWS 端建立 ARP。
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](#)。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](#)。

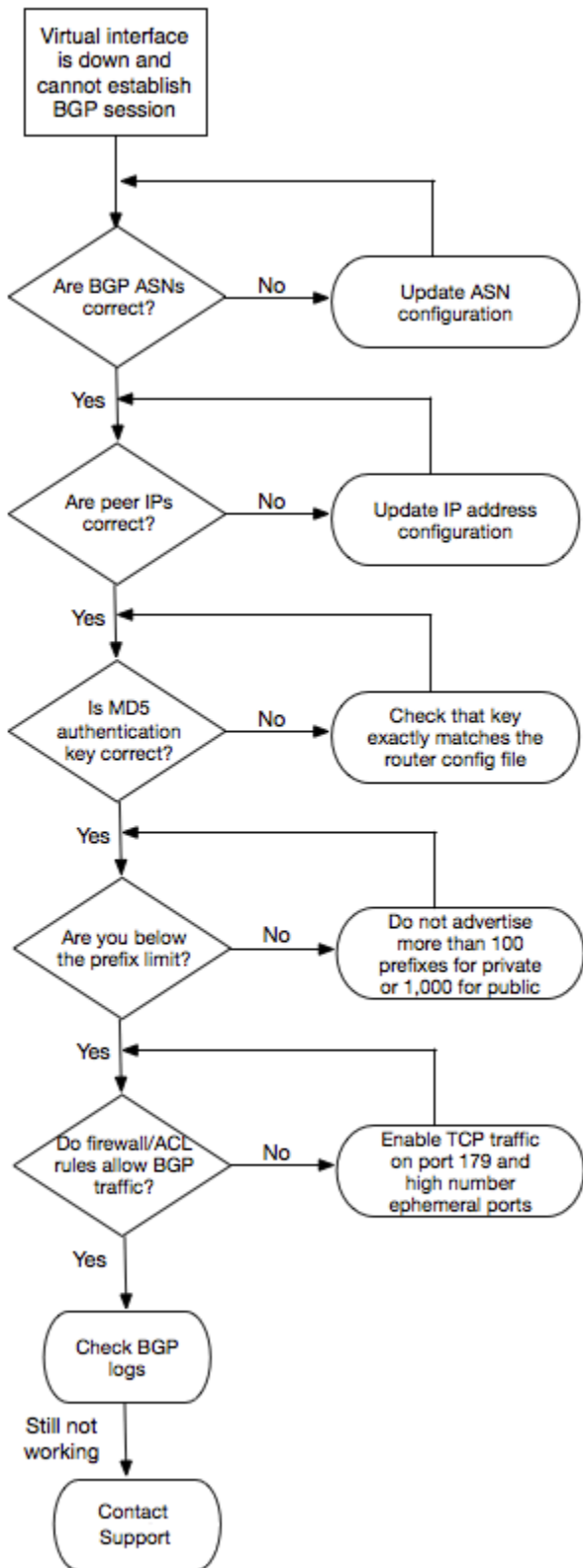
排查第 3/4 层（网络/传输）问题

考虑以下情况：您的 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。如果您的虚拟接口已开启且 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 个前缀或为公有虚拟接口公布超过 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。



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](#)。

排查长 ASN 问题

如果您遇到长 ASN 配置的问题，请执行以下步骤进行排查：

BGP 会话因长 ASN 而失败

症状：配置长 ASN 后无法建立 BGP 会话

原因：本地路由器可能不支持长 ASN 功能

解决方案：

- 验证您的路由器是否支持 RFC 6793
- 检查 BGP 配置以获得一致的 ASN 格式
- 查看 BGP 日志中是否存在能力协商错误

API 响应显示 ASN 为 0

症状：API 响应将 asn 字段显示为 0

原因：当实际 ASN 超过 2,147,483,647 时这是预期的行为

解决方案：使用 API 响应中的 asnLong 字段获取正确的 ASN 值

从 ASN 迁移到长 ASN 问题

症状：ASN 迁移期间连接丢失

原因：更改 ASN 需要重新建立 BGP 会话

解决方案：

- 在维护时段内规划迁移
- 一次更新一个虚拟接口
- 在更改期间监控 BGP 会话状态
- 迁移后验证路由表的收敛性

如果您在执行这些排查步骤后仍然遇到长 ASN 配置的问题，[请联系 AWS 支持](#)并提供以下信息：

- 虚拟接口 ID 或 BGP 对等体 ID

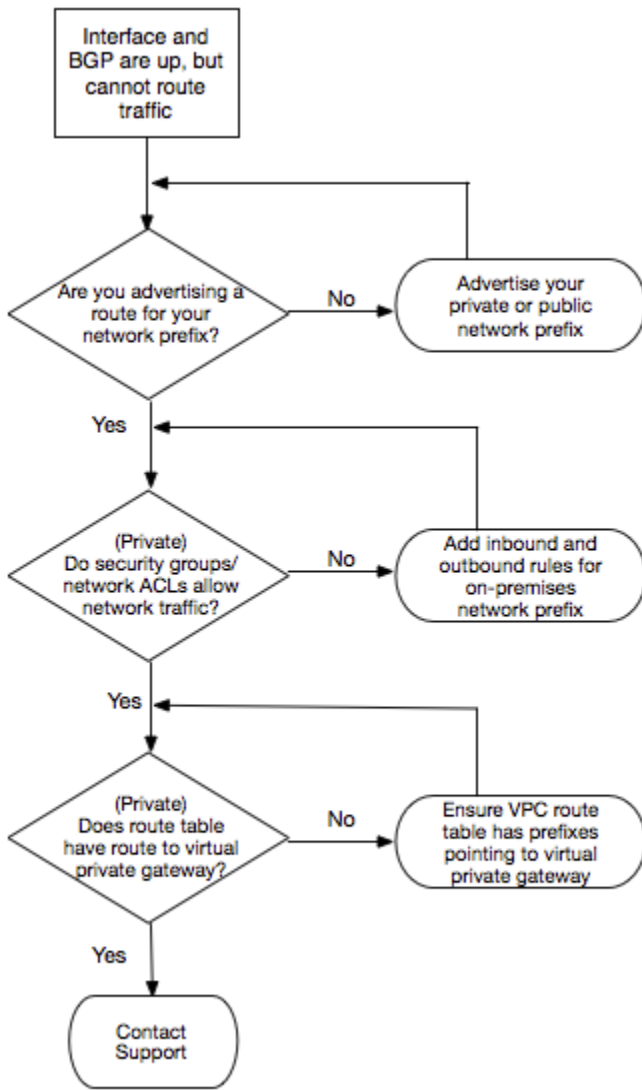
- 已配置的 ASN 值 (ASN 和长 ASN)
- 路由器型号和软件版本
- BGP 配置和日志
- 错误消息或观察到的症状

排查路由问题

考虑以下情况：您的虚拟接口已开启并且您已建立 BGP 对等会话。如果您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私有网关的前缀。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 或 ::/0)，同时将该虚拟私有网关作为您的 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。



文档历史记录

下表介绍了 AWS Direct Connect 的版本。要获得本文档的更新通知，您可以订阅 RSS 源。

| 变更 | 说明 | 日期 |
|---|--|------------------|
| 支持长 ASN | 现在，您可以对带有 Direct Connect 虚拟接口的 BGP 会话使用长 ASN 值。 | 2025 年 7 月 24 日 |
| 在 Direct Connect 网关和 AWS Network Manager 核心网络之间创建关联 | 现在，您可以直接在 Direct Connect 和 AWS Cloud WAN 核心网络之间创建 Direct Connect 网关关联。 | 2024 年 11 月 25 日 |
| 支持 400G | 更新了主题，以涵盖对 400G 连接的支持。 | 2024 年 7 月 18 日 |
| 添加了 SiteLink 前缀限制 | SiteLink 的前缀限制已添加到配额和限制主题中。 | 2023 年 6 月 15 日 |
| 支持 SiteLink | 您可以创建一个私有虚拟接口，以实现同一 AWS 区域中两个 Direct Connect 入网点 (PoP) 之间的连接。 | 2021 年 12 月 1 日 |
| 支持 MAC 安全 | 您可以使用支持 MACsec 的 Direct Connect 连接，来加密从公司数据中心到 Direct Connect 位置的数据。 | 2021 年 3 月 31 日 |
| 支持 100G | 更新了主题，涵盖对 100G 专用连接的支持。 | 2021 年 2 月 12 日 |
| 意大利的新增位置 | 更新了主题，包含意大利的新增位置。 | 2021 年 1 月 22 日 |

| | | |
|---|--|------------------|
| 以色列的新增位置 | 更新了主题，包含以色列的新增位置。 | 2020 年 7 月 7 日 |
| 弹性工具包故障转移测试支持 | 使用弹性工具包失效转移测试功能可以测试连接的弹性。 | 2020 年 6 月 3 日 |
| CloudWatch VIF 指标支持 | 您可以使用 CloudWatch 监控物理 Direct Connect 连接和虚拟接口。 | 2020 年 5 月 11 日 |
| AWS Direct Connect 弹性工具包 | AWS Direct Connect 弹性工具包提供了一个具有多个弹性模型的连接向导，可帮助您订购专用连接以实现 SLA 目标。 | 2019 年 10 月 7 日 |
| 针对账户之间的 AWS Transit Gateway 的额外区域支持 | 针对账户之间的 AWS Transit Gateway 的额外区域支持。 | 2019 年 9 月 30 日 |
| AWS Direct Connect 支持 AWS Transit Gateway | 您可以使用 Direct Connect 网关将 Direct Connect 连接通过中转虚拟接口连接到与您的中转网关连接的 VPC 或 VPN。将 Direct Connect 网关与中转网关关联。然后，创建一个中转虚拟接口以将 Direct Connect 连接到 Direct Connect 网关。 | 2019 年 3 月 27 日 |
| 巨型帧支持 | 您可以通过 Direct Connect 发送巨型帧 (9001 MTU)。 | 2018 年 11 月 10 日 |
| 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。 | 2018 年 2 月 6 日 |
| Direct Connect 网关 | 您可以使用 Direct Connect 网关将您的 Direct Connect 连接到远程区域中的 VPC。 | 2017 年 11 月 1 日 |

| | | |
|---------------------------------------|---|-----------------|
| Amazon CloudWatch 指标。 | 您可以查看 Direct Connect 连接的 CloudWatch 指标。 | 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 Direct Connect 连接。 | 2017 年 2 月 13 日 |
| IPv6 支持 | 您的虚拟接口现在可以支持 IPv6 BGP 对等会话。 | 2016 年 12 月 1 日 |
| 标记支持 | 现在您可以标记您的 Direct Connect 资源。 | 2016 年 11 月 4 日 |
| 自助服务 LOA-CFA | 现在，您可以使用 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 年 6 月 22 日 |
| 硅谷新增节点 | 更新了主题，包含美国西部（北加利福尼亚）区域新增的硅谷位置。 | 2016 年 6 月 3 日 |
| 阿姆斯特丹新增节点 | 更新了主题，包含欧洲地区（法兰克福）区域新增的阿姆斯特丹位置。 | 2016 年 5 月 19 日 |
| 俄勒冈州波特兰和新加坡新增了位置 | 更新了主题，包含美国西部（俄勒冈州）和亚太地区（新加坡）区域新增的波特兰、俄勒冈州和新加坡位置。 | 2016 年 4 月 27 日 |
| 巴西圣保罗新增节点 | 更新了主题，包含南美洲（圣保罗）区域新增的巴西圣保罗位置。 | 2015 年 12 月 9 日 |

| | | |
|---|---|------------------|
| 达拉斯、伦敦、硅谷和孟买新增节点 | 更新了主题，包含达拉斯 [美国东部 (弗吉尼亚州北部) 区域]、伦敦 [欧洲地区 (爱尔兰) 区域]、硅谷 [AWS GovCloud (美国西部) 区域] 和孟买 [亚太地区 (新加坡) 区域] 和孟买 [亚太地区 (新加坡) 区域] 新增的位置。 | 2015 年 11 月 27 日 |
| 中国 (北京) 区域新增的位置 | 更新了主题，包含中国 (北京) 区域新增的北京位置。 | 2015 年 4 月 14 日 |
| 美国西部 (俄勒冈) 区域中新增拉斯维加斯位置 | 更新了主题，增加了位于美国西部 (俄勒冈) 区域的新的 Direct Connect 拉斯维加斯地点。 | 2014 年 11 月 10 日 |
| 新增欧洲 (法兰克福) 区域 | 更新了主题，增加了为欧洲 (法兰克福) 区域提供服务的新 Direct Connect 地点。 | 2014 年 10 月 23 日 |
| 亚太地区 (悉尼) 区域中新增位置 | 更新了主题，增加了为亚太地区 (悉尼) 区域提供服务的新 Direct Connect 地点。 | 2014 年 7 月 14 日 |
| 支持 AWS CloudTrail | 添加了新的主题，说明如何在 Direct Connect 中使用 CloudTrail 记录活动。 | 2014 年 4 月 4 日 |
| 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。 | 2013 年 12 月 19 日 |
| 支持托管连接 | 更新主题，以涵盖对托管连接的支持。 | 2013 年 10 月 22 日 |

| | | |
|--|--|------------------|
| 欧洲（爱尔兰）区域中新增位置 | 更新了主题，添加了为欧洲（爱尔兰）区域提供服务的新 Direct Connect 位置。 | 2013 年 6 月 24 日 |
| 美国西部（俄勒冈）区域中新增西雅图位置 | 更新了主题，添加了位于西雅图的为美国西部（俄勒冈）区域提供服务的新 Direct Connect 位置。 | 2013 年 5 月 8 日 |
| 支持 IAM 与 Direct Connect 一起使用 | 添加了关于通过 AWS Identity and Access Management 使用 Direct Connect 的主题。 | 2012 年 12 月 21 日 |
| 新增亚太地区（悉尼）区域 | 更新了主题，添加了为亚太地区（悉尼）区域提供服务的新 Direct Connect 位置。 | 2012 年 12 月 14 日 |
| 新的 AWS Direct Connect 控制台和美国东部（弗吉尼亚州北部）和南美洲（圣保罗）区域 | 使用“Direct Connect User Guide”取代了“Direct Connect Getting Started Guide”。添加了新主题，以涵盖新的 Direct Connect 控制台；添加了计费主题；添加了路由器配置信息；更新了主题以涵盖为美国东部（弗吉尼亚北部）和南美洲（圣保罗）区域提供服务的两个新增 Direct Connect 位置。 | 2012 年 8 月 13 日 |
| 支持欧洲（爱尔兰）、亚太地区（新加坡）和亚太地区（东京）区域 | 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的 Direct Connect 位置。 | 2012 年 1 月 10 日 |

[支持美国西部 \(加利福尼亚北部 \) 区域](#)

更新了主题，以包含添加的美国西部 (加利福尼亚北部) 区域。

2011 年 9 月 8 日

[公开发布](#)

首次发布 Direct Connect。

2011 年 8 月 3 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。