aws

用户指南

# AWS Direct Connect

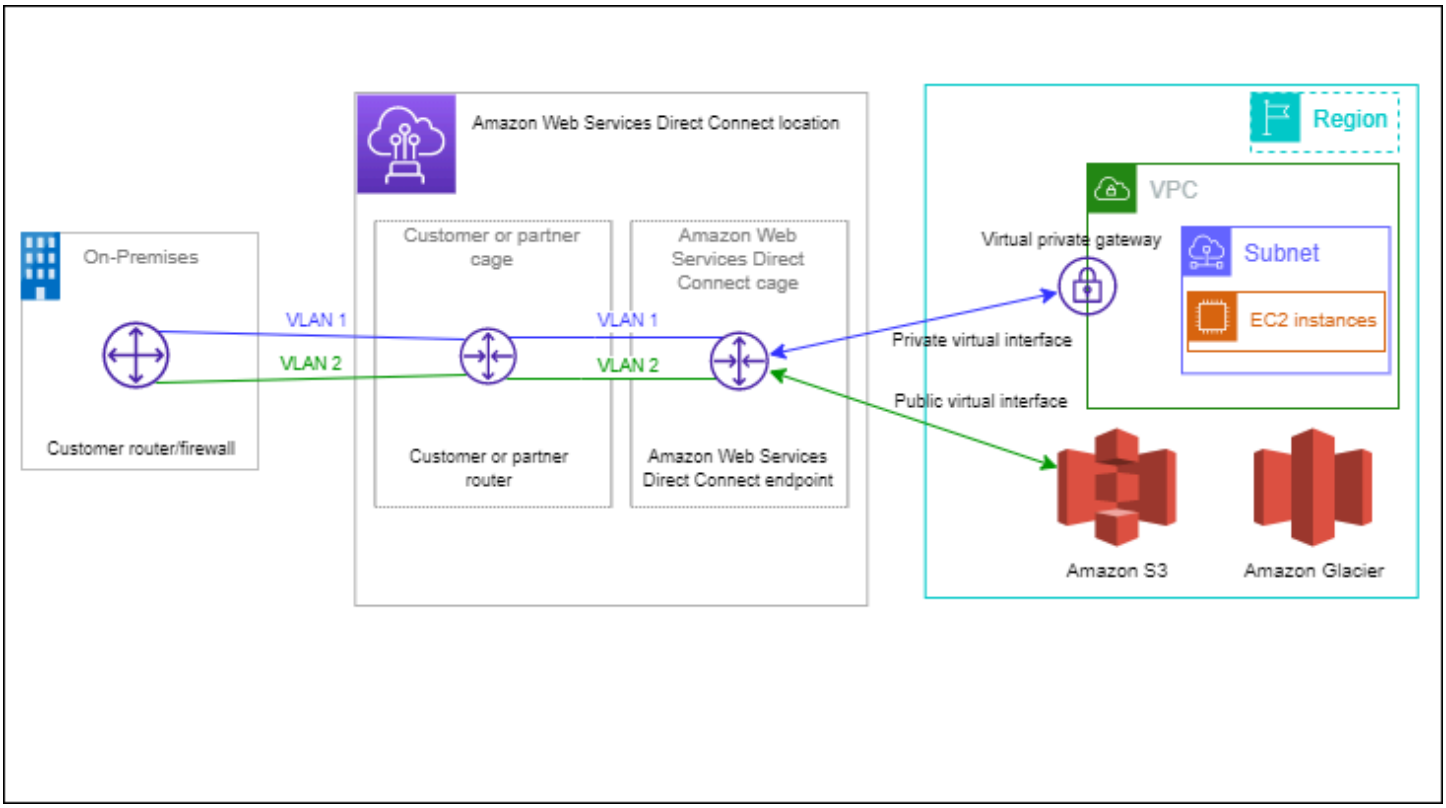
# AWS Direct Connect: 用户指南

# Table of Contents

# 什么是 AWS Direct Connect？

AWS Direct Connect 通过标准以太网光纤电缆将您的内部网络链接到某个 AWS Direct Connect 位置。电缆的一端接到您的路由器，另一端接到 AWS Direct Connect 路由器。通过此连接，您可以绕过网络路径中的互联网服务提供商，直接创建通往公共 AWS 服务（例如 Amazon S3）或 Amazon VPC 的虚拟接口。 AWS Direct Connect 位置提供与其关联 AWS 的区域的访问权限。您可以在公共区域使用单个连接，也可以 AWS GovCloud (US) 访问所有其他公共区域的公共 AWS 服务。

下图简要概述了如何与您的网络 AWS Direct Connect 接口。




内容

# AWS Direct Connect 组件

以下是您使用的关键组件 AWS Direct Connect：

连接

在某个 AWS Direct Connect 位置创建连接，以建立从您的场所到某个 AWS 地区的网络连接。有关更多信息，请参阅 AWS Direct Connect 连接。

虚拟接口

创建虚拟接口以允许访问 AWS 服务。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。有关更多信息，请参阅 AWS Direct Connect 虚拟接口 和 虚拟接口的先决条件。

# 网络要求

要 AWS Direct Connect 在某个 AWS Direct Connect 地点使用，您的网络必须满足以下条件之一：

- 您的网络与现有 AWS Direct Connect 位置处于同一位置。有关可用 AWS Direct Connect 位置的更多信息，请参阅 AWS Direct Connect 产品详情。
- 您正在与 AWS Direct Connect 合作伙伴网络 (APN) 成员的 AWS 合作伙伴合作。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 AWS Direct Connect。

此外，您的网络必须符合以下条件：

- 您的网络必须使用单模光纤，其中 1GB 以太网使用 1000BASE-LX（1310nm）收发器，10GB 以太网使用 10GBASE-LR（1310nm）收发器，或者 100GB 以太网使用 100GBASE-LR4 收发器。
- 对于端口速度超过 1Gbps 的连接，必须禁用端口自动协商。但是，根据为您的连接提供服务的 Di AWS rect Connect 端点，可能需要为 1 Gbps 连接启用或禁用自动协商。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。
- 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）。自动为每个 AWS 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。

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

AWS 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 为私有虚拟接口或中转虚拟接口设置网络 MTU。

## 的定价 AWS Direct Connect

AWS Direct Connect 有两个计费要素：端口时长和出站数据传输。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。

私有接口和传输虚拟接口的数据传输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、经典 EC2 实例或通过 Internet 网关的 EC2 流量），如果出站流量发往同一 AWS 付款人账户拥有的公共前缀并 AWS 通过 AWS Direct Connect 公共虚拟接口主动向其发布广告，则数据传出 (DTO) 使用量按数据传输速率计量给资源所有者。 AWS Direct Connect

有关更多信息，请参阅 AWS Direct Connect 定价。

## AWS Direct Connect 维护

AWS Direct Connect 是一项完全托管的服务，Direct Connect 定期对支持该服务的硬件群组执行维护活动。Direct Connect 连接是在独立的硬件设备上配置的，这使您能够在本地基础设施 Amazon Virtual Private Cloud 之间创建高弹性的网络连接。此功能使您能够以可靠、可扩展且经济实惠的方式访问您的 AWS 资源。有关更多信息，请参阅 AWS Direct Connect 弹性建议。

Direct Connect 维护有两种类型：计划维护和紧急维护：

- 计划维护。计划维护是提前安排的，以提高可用性并交付新功能。此类维护是在维护时段内进行的，我们提供三个通知：14 个日历日、7 个日历日和 1 个日历日。

> **Note**
>
> 日历日包括非工作日和当地节假日。

- 紧急维护。紧急维护是在关键时刻启动的，因为出现了影响服务的故障，需要 AWS 立即采取行动以恢复服务。此类维护不是提前计划的。受影响的客户会在维护前 60 分钟收到紧急维护通知。

我们建议您遵循 AWS Direct Connect 弹性建议，以便在维护期间可以从容、主动地将流量转移到冗余的 Direct Connect 连接。我们还建议您定期主动测试冗余连接的弹性，以验证失效转移是否按预期工作。使用该the section called “AWS Direct Connect 故障转移测试”功能，您可以验证您的流量是否通过其中一个冗余虚拟接口路由。

有关发起取消计划维护请求的资格标准的指南，请参阅如何取消 Direct Connect 维护事件？。

> **Note**
>
> 紧急维护请求无法取消，因为 AWS 必须立即采取行动才能恢复服务。

有关维护事件的更多信息，请参阅AWS Direct Connect 常见问题解答中的维护事件。

# 访问远程 AWS 区域

公有区域或 AWS GovCloud (US) 中的 AWS Direct Connect 位置，可以访问任何其他公有区域 [不包括中国（北京和宁夏）] 中的公有服务。此外，可将公有区域或 AWS GovCloud (US) 中的 AWS Direct Connect 连接配置为：访问您账户中在任何其他公有区域 [不包括中国（北京和宁夏）] 中的 VPC。因此，您可以使用单个 AWS Direct Connect 连接构建多区域服务。无论您是访问公有 AWS 服务还是其他区域中的 VPC，所有网络流量都保留在 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 AWS Direct Connect 连接支持的 BGP 社区的更多信息，请参阅路由策略和 BGP 社区。

## 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AWS Direct Connect 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 AWS Direct Connect 通过私有虚拟接口连接到您账户中位于不同区域的 VPC 或连接到中转网关。有关更多信息，请参阅使用 Direct Connect 网关。

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

## 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 连接性选项

# 路由策略和 BGP 社区

AWS Direct Connect 为公共 AWS 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 AWS Direct Connect 访问公共 AWS 服务，则必须指定要通过 BGP 进行通告的公有 IPv4 前缀或 IPv6 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。
- AWS 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 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。

- AWS 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 AWS 在中国区域中公布。 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。

- AWS Direct Connect 通告前缀的最小路径长度为 3。
- AWS 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 AWS 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 AWS 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。
- AWS 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 AWS Direct Connect 客户
  - 与 AWS 全球网络对等的网络
  - Amazon 中转提供商

## 公有虚拟接口 BGP 社区

AWS Direct Connect 支持 scope BGP 社区标记，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：
  - 北美全境
  - 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。

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

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

- 7224:8100—来自与接入 AWS Direct Connect 点 AWS 关联的同一区域的路由。
- 7224:8200—起源于与入 AWS 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 AWS 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。

AWS Direct Connect 还在宣传的 Amazon 路线上提供 BGP 社区标签。如果您使用 AWS 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 AWS 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。这些前缀可以是公共的，也可以是私有的。

以下出站路由规则基于通告的前缀适用：

- AWS 首先评估最长的前缀长度。 AWS 如果所需的路由路径用于主动/被动连接，则建议使用多个 Direct Connect 虚拟接口发布更具体的路由。有关更多信息，请参阅使用最长前缀匹配影响混合网络上的流量。
- 当所需的路由路径用于主动/被动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。如果本地区域与 Direct Connect 位置没有关联，则将其设置为较低的值。仅当未分配本地首选项社区标签时，这才适用。
- 当前缀长度和本地首选项相同时，AS_PATH 长度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 当前缀具有相同长度和 BGP 属性时，将在多个传输或私有虚拟接口之间进行负载共享。

### 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 会影响使用等价多路径路由 (ECMP) 的能力。 AWS 区域 默认情况下，首选相同关联的 Direct Connec AWS 区域 t 位置。参阅AWS Direct Connect 位置以识别任何 Direct Connect 位置 AWS 区域 的关联位置。

当未应用本地首选项社区标签时，在以下情况下，Direct Connect 支持在两条或更多路径上使用相同长度、AS_PATH 长度和 MED 值的前缀使用私有或传输虚拟接口 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，请参阅如何设置从私有或传输虚拟接口 AWS 到的主动/主动或主动/被动 Direct Connect 连接？

> **Note**
>
> 这对 AWS 区域 从本地位置传送的 ECMP 没有影响。

为了控制路由首选项，Direct Connect 支持私有虚拟接口和传输虚拟接口的本地首选项 BGP 社区标记。

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 AWS 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，则无论其主区域关联如何，都将使用 ECMP 在剩余的活动连接之间进行负载均衡。要支持跨多个 AWS 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。

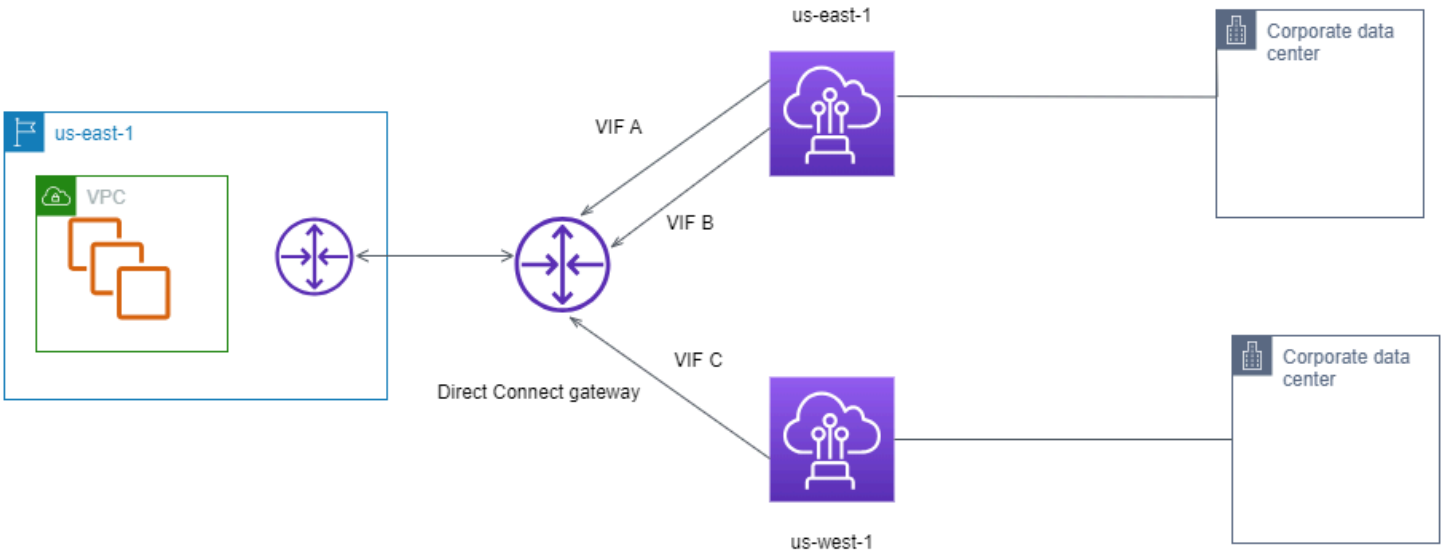
## 私有虚拟接口路由示例

考虑一下 AWS Direct Connect 位置 1 的主区域与 VPC 主区域相同的配置。另一个区域有一个冗余 AWS Direct Connect 位置。从 AWS Direct Connect 位置 1（us-east-1）到 Direct Connect 网关有两个私有 VIF（VIF A 和 VIF B）。从 AWS 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。

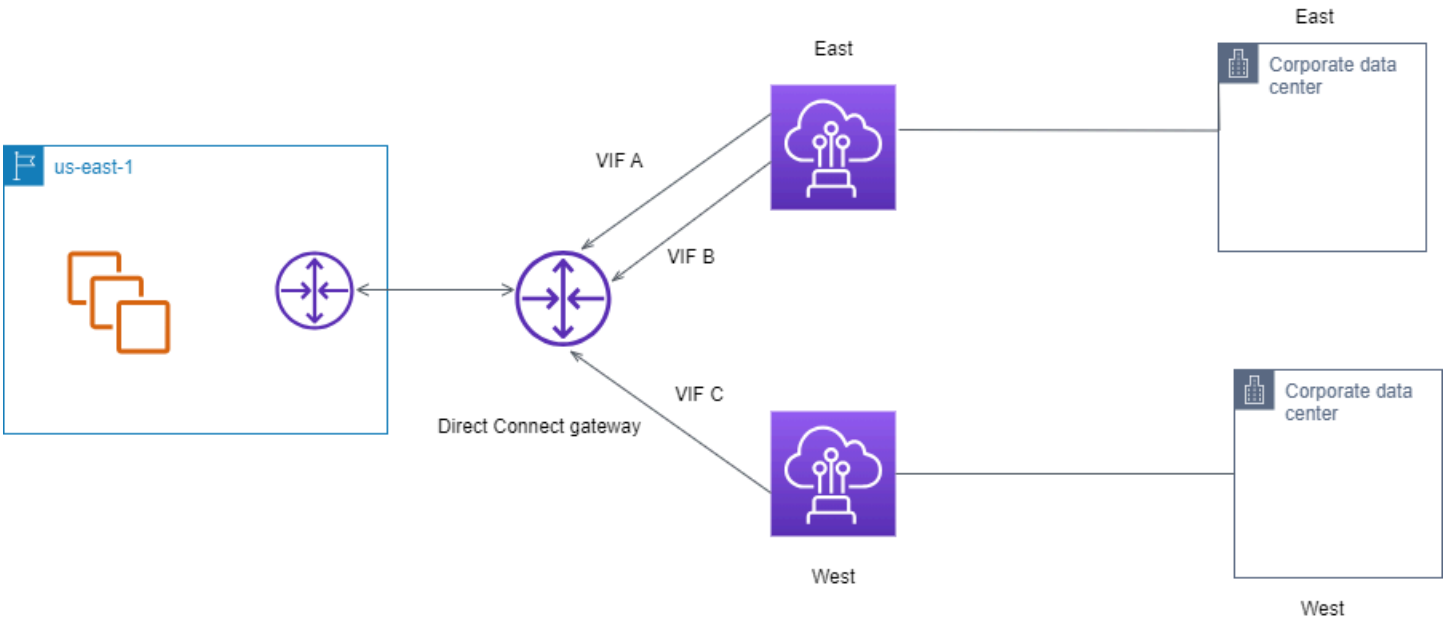
VIF 具有以下配置：

- 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




如果您更改 VIF C 的 CIDR 范围配置，则属于 VIF C CIDR 范围的路由会使用 VIF C，因为它的前缀长度最长。

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


East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

# 使用 AWS Direct Connect 弹性工具包入门

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 AWS 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。
- 当您选择 1Gbps、10Gbps 或 100Gbps 之外的其他速度时，会自动创建链接聚合组（LAG），并向 LAG 添加适当数量的专用连接。
- 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 AWS 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 “AWS Direct Connect 故障转移测试”。
- 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。

弹性工具包中提供了以下 AWS Direct Connect 弹性模型：

- Maximum Resiliency (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 AWS Direct Connect 服务水平协议中指定的实现 SLA 的所有要求。
- High Resiliency (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 AWS 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。
- Classic。此模型面向已有连接且想要添加更多连接的用户。此模型不提供 SLA。

最佳做法是使用 AWS Direct Connect 弹性工具包中的连接向导订购专用连接以实现您的 SLA 目标。

选择弹性模型后，弹 AWS Direct Connect 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

# 先决条件

AWS 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) 收发器或用于 100 千兆以太网的 100GBASE-LR4 收发器。

您可以通过以下方式之一来设置 AWS Direct Connect 连接：

| 模型 | 带宽 | 方法 |
| --- | --- | --- |
| 专用连接 | 1Gbps、10Gbps 和 100Gbps | 与 AWS 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 AWS Direct Connect 位置。网络提供商不必是 AWS Direct Connect 合作伙伴，也可以将您连接到专用连接。 AWS Direct Connect 专用连接通过单模光纤支持以下端口速度： |

| 模型 | 带宽 | 方法 |
| --- | --- | --- |
| | | 1Gbps：1000BASE-LX（1310 nm）、10Gbps：10GBASE-LR（1310 nm）和 100Gbps：100GBASE-LR4。 |
| 托管连接 | 50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps 和 10 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 AWS Direct Connect 地点。<br><br>只有某些合作伙伴提供更高容量的连接。 |

对于 AWS 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：

- 您的网络必须使用单模光纤，其中 1GB 以太网使用 1000BASE-LX（1310nm）收发器，10GB 以太网使用 10GBASE-LR（1310nm）收发器，或者 100GB 以太网使用 100GBASE-LR4 收发器。
- 对于端口速度超过 1Gbps 的连接，必须禁用端口自动协商。但是，根据为您的连接提供服务的 Di AWS rect Connect 端点，可能需要为 1 Gbps 连接启用或禁用自动协商。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。
- 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）。自动为每个 AWS 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。

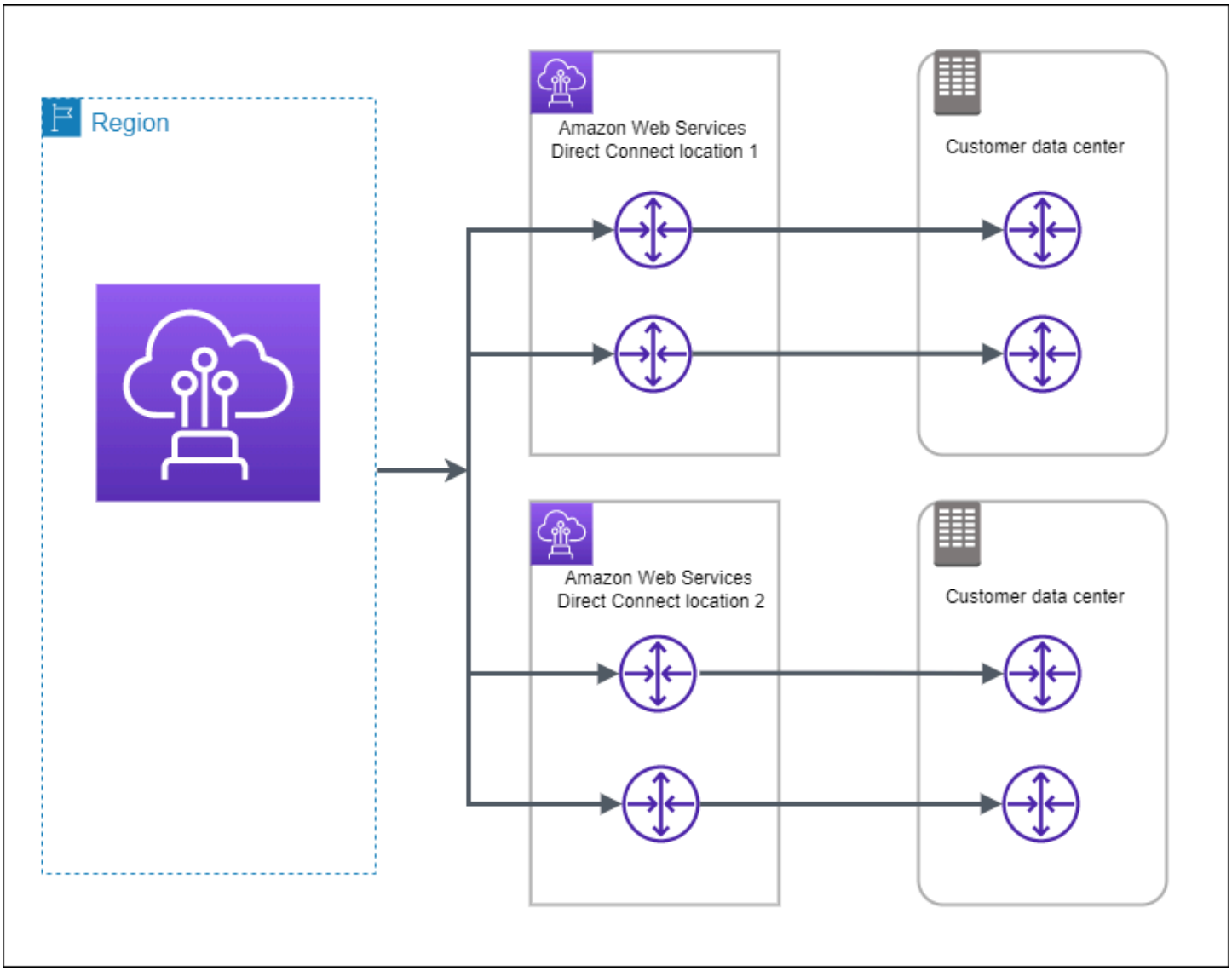
在开始配置之前，请确保您具有以下信息：

- 要使用的弹性模型。
- 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。

# 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 AWS 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。




以下过程演示如何使用 AWS Direct Connect 弹性工具包配置最大弹性模型。

主题

- 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

# 第 1 步：注册 AWS

要使用 AWS 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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 Management Console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》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 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网址。

  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》中的创建权限集。
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》中的添加组。

## 步骤 2：配置弹性模型

配置最大弹性模型

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 对于第一定位服务提供商，请为专用连接选择适当 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

   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 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

   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 Remove tag (删除标签)。

6. 选择下一步。

7. 检查您的连接，然后选择 Continue (继续)。

   如果您的 LOA 已准备就绪，则可选择 Download LOA (下载 LOA)，然后单击 Continue (继续)。

   最多可能需要 72 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连接到三个 VPC。

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 AWS 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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR |

| 资源 | 所需信息 |
| --- | --- |
| | 这些可以是任何公有 IP（客户拥有或由提供 AWS），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。<br>• 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>• 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）<br>**Note**<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>• （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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 |
| --- | --- |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |

| 资源 | 所需信息 |
| --- | --- |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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。 |

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

创建公共虚拟接口时，最多可能需要 72 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。
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。

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）。

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。

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**
>
> 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。
>
> - 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。

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)。

## 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 “AWS Direct Connect 故障转移测试”。

## 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

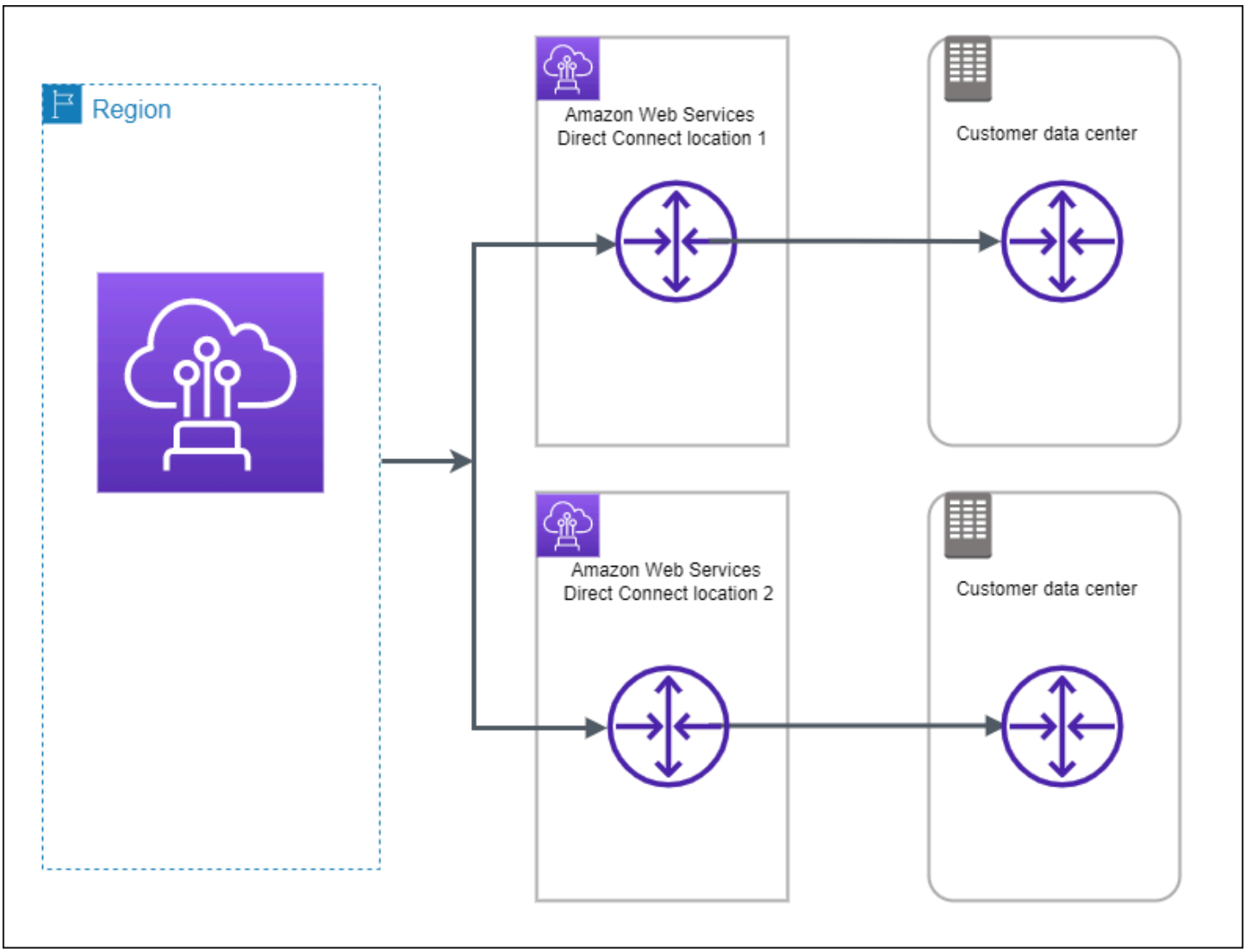
- 运行`traceroute`并验证标 AWS Direct Connect 识符是否在网络跟踪中。

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 Amazon EC2 控制台中使用实例启动向导时，快速启动选项卡中提供 Amazon Linux AMI。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 地址并获得响应。

# 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。




以下过程演示如何使用 AWS Direct Connect 弹性工具包配置高弹性模型。

主题



## 第 1 步：注册 AWS

要使用 AWS 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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 Management Console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》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 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网址。

  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》中的创建权限集。
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》中的添加组。

## 步骤 2：配置弹性模型

配置高弹性模型

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 对于第一定位服务提供商，请选择相应 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

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 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

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 Remove tag (删除标签)。

6. 选择下一步。

7. 检查您的连接，然后选择 Continue (继续)。

如果您的 LOA 已准备就绪，则可选择 Download LOA (下载 LOA)，然后单击 Continue (继续)。

最多可能需要 72 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连接到三个 VPC。

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 AWS Direct Connect 连接或链路聚合组 (LAG)。 |

| 资源 | 所需信息 |
| --- | --- |
| 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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |

| 资源 | 所需信息 |
| --- | --- |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR<br><br>这些可以是任何公有 IP（客户拥有或由提供 AWS），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。<br>  • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>  • 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）<br><br>Note<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>  • （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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。 |

| 资源 | 所需信息 |
| --- | --- |
| 地址系列 | BGP 对等会话是通过 IPv4 还是 IPv6 进行。 |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |

| 资源 | 所需信息 |
| --- | --- |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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 ASN 属于 ISP 或网络运营商， AWS 请您提供更多信息。这可以是使用公司抬头的文档，也可以是来自公司域名的用于验证该网络前缀/ASN 是否可由您使用的电子邮件。

创建公共虚拟接口时，最多可能需要 72 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。

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。

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）。

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。

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**
      >
      > 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。
      >
      > - 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。

   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)。

## 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 “AWS Direct Connect 故障转移测试”。

## 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

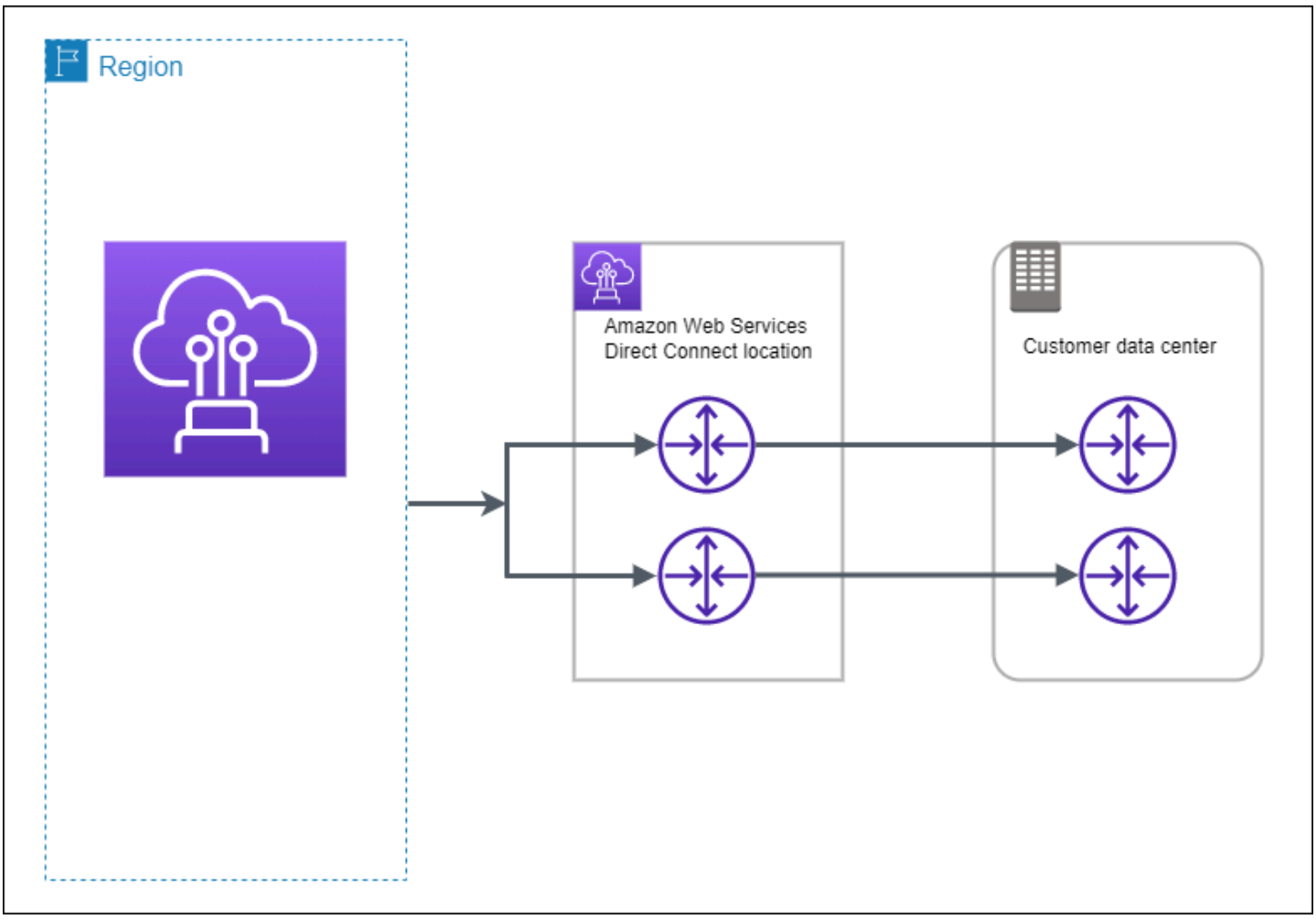
- 运行`traceroute`并验证标 AWS Direct Connect 识符是否在网络跟踪中。

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 Amazon EC2 控制台中使用实例启动向导时，快速启动选项卡中提供 Amazon Linux AMI。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 地址并获得响应。

# 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。




以下过程演示如何使用 AWS Direct Connect 弹性工具包配置开发和测试弹性模型。

主题



## 第 1 步：注册 AWS

要使用 AWS 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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 Management Console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》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 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网址。

  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》中的创建权限集。
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》中的添加组。

## 步骤 2：配置弹性模型

配置弹性模型

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

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 Remove tag (删除标签)。

6. 选择下一步。

7. 检查您的连接，然后选择 Continue (继续)。

如果您的 LOA 已准备就绪，则可选择 Download LOA (下载 LOA)，然后单击 Continue (继续)。

最多可能需要 72 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 AWS 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连接到三个 VPC。

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 AWS 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。 |

| 资源 | 所需信息 |
| --- | --- |
| （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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |

| 资源 | 所需信息 |
| --- | --- |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR<br><br>这些可以是任何公有 IP（客户拥有或由提供 AWS），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。<br>  • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>  • 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）<br><br>Note<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>  • （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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。 |

| 资源 | 所需信息 |
| --- | --- |
| 地址系列 | BGP 对等会话是通过 IPv4 还是 IPv6 进行。 |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |

| 资源 | 所需信息 |
| --- | --- |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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。 |

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

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

配置与非 VPC 服务间的公有虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。

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。

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）。

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。

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**
      >
      > 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。
      >
      > - 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。

   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)。

## 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 “AWS Direct Connect 故障转移测试”。

## 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 AWS 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 Amazon EC2 控制台中使用实例启动向导时，快速启动选项卡中提供 Amazon Linux AMI。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 地址并获得响应。

# Classic

在拥有现有连接时，选择“Classic”。

以下过程演示开始设置 AWS Direct Connect 连接的常见场景。

内容



## 先决条件

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

- 您的网络必须使用单模光纤，其中 1GB 以太网使用 1000BASE-LX（1310nm）收发器，10GB 以太网使用 10GBASE-LR（1310nm）收发器，或者 100GB 以太网使用 100GBASE-LR4 收发器。
- 对于端口速度超过 1Gbps 的连接，必须禁用端口自动协商。但是，根据为您的连接提供服务的 Di AWS rect Connect 端点，可能需要为 1 Gbps 连接启用或禁用自动协商。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。
- 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）。自动为每个 AWS 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。

## 第 1 步：注册 AWS

要使用 AWS 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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 Management Console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》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 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网址。

  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》中的创建权限集。
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》中的添加组。

## 步骤 2：申请 AWS Direct Connect 专用连接

对于专用连接，您可以使用 AWS 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 AWS Direct Connect 位置。

> **Note**
>
> 您不能使用 AWS Direct Connect 控制台请求托管连接。相反，请联系可以为您创建托管连接的 AWS Direct Connect 合作伙伴，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 AWS Direct Connect 连接

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。

   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 AWS 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 Create Connection (创建连接)。

最多可能需要 72 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 AWS Direct Connect 连接。

## 接受托管连接

必须先在 AWS 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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信息。如果仍不可用，或者您在 72 小时后仍未收到电子邮件，请联系 AWS Support。

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。 AWS 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 AWS Direct Connect 地点有设备，请联系托管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。

AWS Direct Connect 列为多个地点的地点（例如 Equinix DC1-DC6 和 DC10-DC11）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 AWS Direct Connect 地点。要实现高可用性，请配置与不同 AWS Direct Connect 位置的连接。

如果您或您的网络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 AWS 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连接到三个 VPC。

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 AWS 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 |

| 资源 | 所需信息 |
| --- | --- |
| | 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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |

| 资源 | 所需信息 |
| --- | --- |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR<br><br>这些可以是任何公有 IP（客户拥有或由提供 AWS），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。<br>  • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>  • 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）<br><br>Note<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>  • （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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。 |

| 资源 | 所需信息 |
| --- | --- |
| 地址系列 | BGP 对等会话是通过 IPv4 还是 IPv6 进行。 |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |

| 资源 | 所需信息 |
| --- | --- |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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。 |

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

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）。虚拟私有接口的 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 AWS 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 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。

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 1-2147483647。
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。

   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）。

   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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。
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**
   >
   > 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。
   >
   > - 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。

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 AWS 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 AWS Direct Connect。

有关示例配置文件，请参阅示例路由器配置文件。

在配置您的路由器后，虚拟接口的状态将变为 UP。如果虚拟接口一直处于关闭状态，并且您无法 ping AWS 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

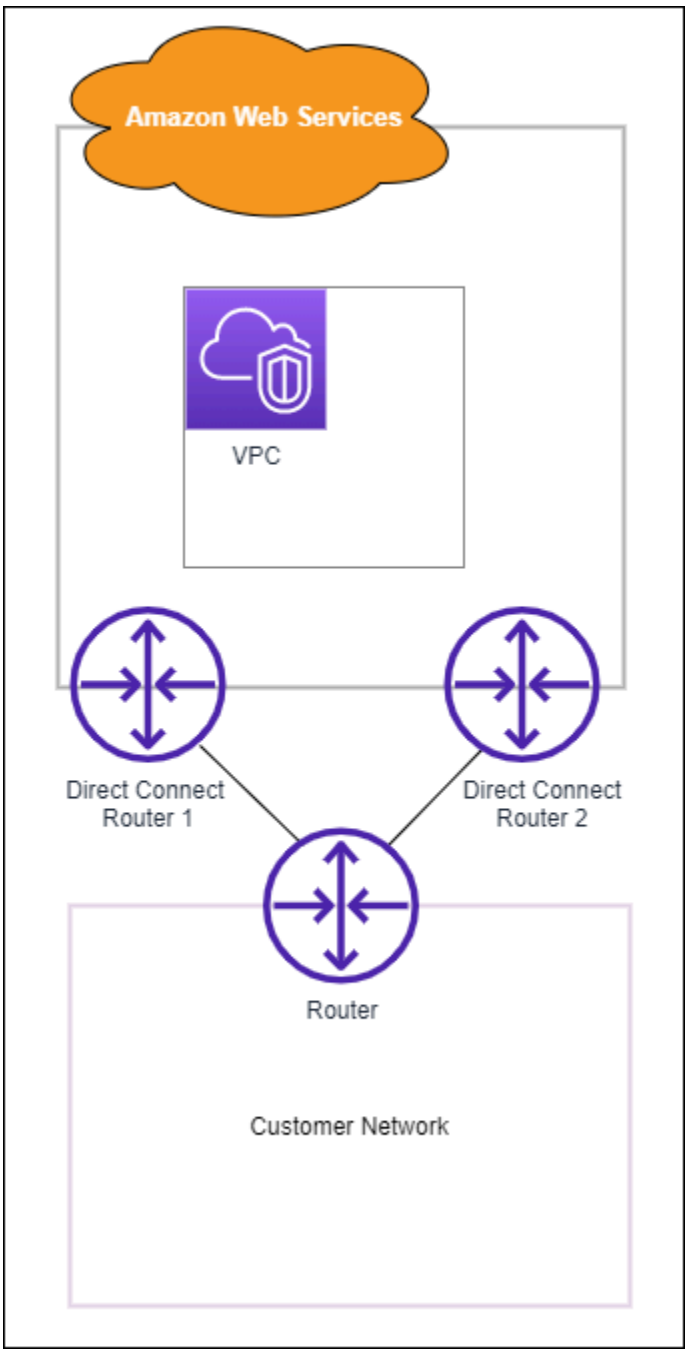
- 运行`traceroute`并验证标 AWS Direct Connect 识符是否在网络跟踪中。

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 Amazon EC2 控制台中使用实例启动向导时，快速启动选项卡中提供 Amazon Linux AMI。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 地址并获得响应。

## （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。 AWS 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 AWS Direct Connect 位置的连接。

有关 AWS Direct Connect 弹性的更多信息，请参阅AWS Direct Connect 弹性建议。

# AWS 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 会话可能会过早恢复。

## 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 BPG 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，请参见 the section called “查看虚拟接口故障转移测试历史记录”。

## 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。账户拥有者通过 AWS CloudTrail 接收已在虚拟接口上运行测试的指示。

## 启动虚拟接口故障转移测试

可以使用 AWS Direct Connect 控制台或 AWS CLI 启动虚拟接口故障转移测试。

从 AWS Direct Connect 控制台启动虚拟接口故障转移测试

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 对于 Peerings to bring down to test (要测试的关闭的对等)，请选择要测试的对等会话，例如 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 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。

使用 AWS CLI 启动虚拟接口故障转移测试

使用StartBgpFailoverTest。

## 查看虚拟接口故障转移测试历史记录

可以使用 AWS Direct Connect 控制台或 AWS CLI 查看虚拟接口故障转移测试历史记录。

从 AWS Direct Connect 控制台查看虚拟接口故障转移测试历史记录

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。

使用 AWS CLI 查看虚拟接口故障转移测试历史记录

使用ListVirtualInterfaceTestHistory。

## 停止虚拟接口故障转移测试

可以使用 AWS Direct Connect 控制台或 AWS CLI 停止虚拟接口故障转移测试。

从 AWS Direct Connect 控制台停止虚拟接口故障转移测试

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 将还原 BGP 对等会话。测试历史记录将显示“已取消”测试。

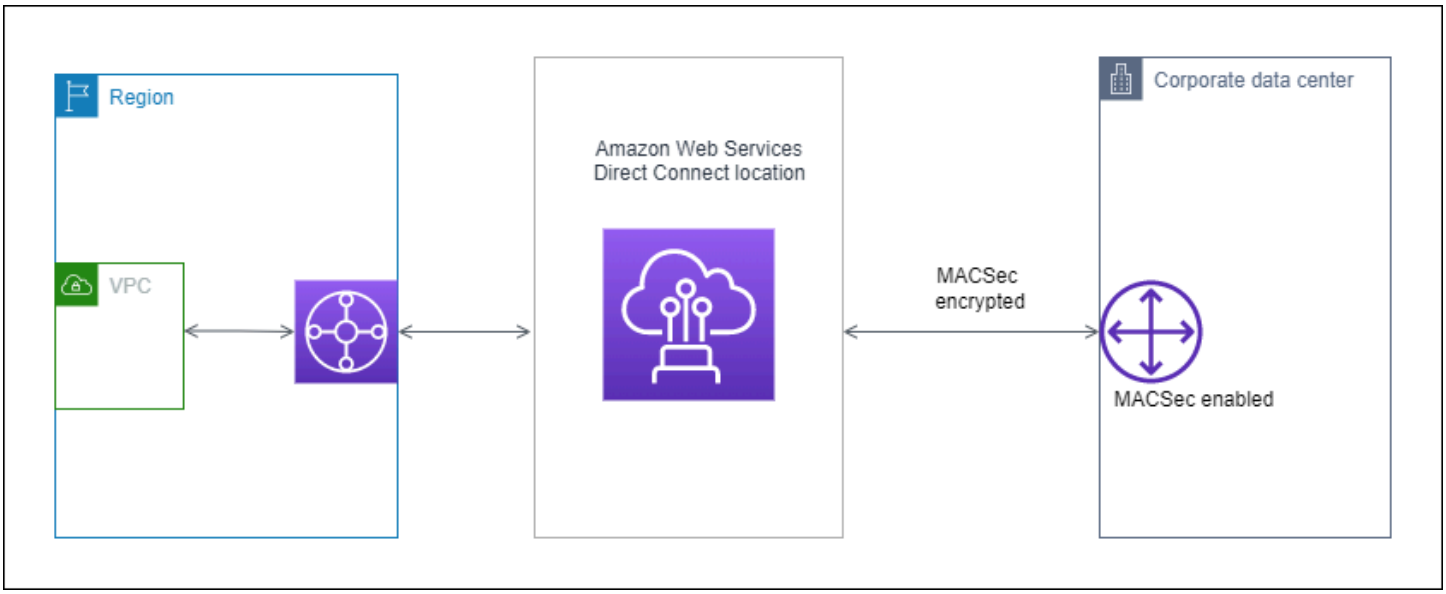
使用 AWS CLI 停止虚拟接口故障转移测试

使用StopBgpFailoverTest。

# MAC 安全

MAC 安全（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 MacSec 在第 2 层运行于两台第 3 层路由器之间，并在第 2 层域上提供加密。流经 AWS 全球网络且与数据中心和区域互连的所有数据在离开数据中心之前都会在物理层自动加密。

在下图中，专用连接和本地资源都必须支持 MACsec。通过专用连接传入或传出数据中心的第 2 层流量都经过加密。




# MACsec 概念

以下是 MACsec 的主要概念：

- MAC 安全（MACsec）：一项 IEEE 802.1 第 2 层标准，可提供数据机密性、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）。
- MacSec 密钥 — 一种预共享密钥，用于在客户本地路由器和该位置的连接端口之间建立 MacSec 连接。 AWS Direct Connect 密钥由连接末端的设备使用 CKN/CAK 对生成，CKN/CAK 对是您提供给设备的 AWS ，也已在设备上配置。
- 连接密钥名称（CKN）和连接关联密钥（CAK）：这对密钥中的值用于生成 MACsec 密钥。您可以生成配对值，将其与 AWS Direct Connect 连接关联，然后在 AWS Direct Connect 连接结束时在边缘设备上进行配置。

# 支持的连接

MACsec 在专用连接上可用。有关如何订购支持 MACsec 的连接的信息，请参阅 AWS Direct Connect。

# 开始在专用连接上使用 MACsec

以下任务可帮助您熟悉 AWS Direct Connect 专用连接上的 MacSec。使用 MacSec 不收取任何额外费用。

在专用连接上配置 MacSec 之前，请注意以下几点：

- 选定入网点的 10Gbps 和 100Gbps 专用 Direct Connect 连接支持 MACsec。对于这些连接，支持以下 MacSec 密码套件：
  - 对于 10Gbps 连接，请使用 GCM-AES-256 和 GCM-AES-XPN-256。
  - 对于 100 Gbps 的连接，请使用 GCM-AES-XPN-256。
- 仅支持 256 位 MacSec 密钥。
- 100Gbps 连接需要使用扩展数据包编号 (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 的专用连接）可能会很快耗尽 MacSec 最初的 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 802.1AEBW-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，必须将其打开。此设置无法调整。
- 不支持 IEEE 802.1Q (dot1q/VLAN) 标签偏移/dot1 q-in-clear 将VLAN标签移出加密有效负载。

有关 Direct Connect 和 MacSec 的更多信息，请参阅常见问题解答的 MacSec 部分。AWS Direct Connect

主题

- 步骤 3：将 CKN/CAK 与连接或 LAG 关联
- 步骤 4：配置本地路由器
- 步骤 5：（可选）删除 CKN/CAK 与连接或 LAG 之间的关联

## MACsec 先决条件

在专用连接上配置 MACsec 之前，请完成以下任务。

- 为 MACsec 密钥创建一个 CKN/CAK 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 “步骤 4：配置本地路由器” 中指定的要求。
- 确保连接端具有支持 MACsec 的设备。
- 必须打开安全通道标识符 (SCI)。
- 仅支持 256 位 MacSec 密钥，提供最新的高级数据保护。

## 服务相关角色

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。 AWS Direct Connect服务相关角色由服务预定义 AWS 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 AWS Direct Connect 更加容易，因为您不必手动添加必要的权限。 AWS Direct Connect 定义其服务相关角色的权限，除非另有定义，否则 AWS 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它 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 使用 AWS 托管 CMK 作为与连接或 LAG 关联的预共享密钥。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》中的 AWS 托管 CMK。

存储的密钥在设计上是只读的，但你可以使用 S AWS ecrets 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。

## 步骤 1：创建连接

要开始使用 MACsec，必须在创建专用连接时开启该功能。有关更多信息，请参阅 the section called “使用连接向导创建连接”。

## （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 MACsec 的 LAG。有关更多信息，请参阅 the section called “MACsec 注意事项” 和 the section called “创建 LAG”。

## 步骤 3：将 CKN/CAK 与连接或 LAG 关联

创建支持 MACsec 的连接或 LAG 后，需要将 CKN/CAK 与连接关联。有关更多信息，请参阅以下章节之一：

- the section called “将 MACsec CKN/CAK 与连接关联”
- the section called “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。本地路由器上和该 AWS Direct Connect 位置的 MacSec 密钥必须匹配。有关更多信息，请参阅 the section called “下载路由器配置文件”。

## 步骤 5：（可选）删除 CKN/CAK 与连接或 LAG 之间的关联

如果您需要删除 MACsec 密钥与连接或 LAG 之间的关联，请参阅以下内容之一：

- the section called “删除 MACsec 密钥和连接之间的关联”
- the section called “删除 MACsec 密钥和 LAG 之间的关联”

# AWS Direct Connect 连接

AWS Direct Connect 使您能够在您的网络和其中一个 AWS 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 AWS Direct Connect 控制台、CLI 或 API 请求专用连接。有关更多信息，请参阅 the section called “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 the section called “托管连接”。

## 专用连接

要创建 AWS Direct Connect 专用连接，您需要以下信息：

AWS 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 AWS 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 AWS Direct Connect。

端口速度

可能的值为 1Gbps、10Gbps 和 100Gbps。

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 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。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 AWS 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：

- the section called “使用连接向导创建连接”
- the section called “创建 Classic 连接”
- the section called “查看您的连接详细信息”
- the section called “更新连接”
- the section called “将 MACsec CKN/CAK 与连接关联”
- the section called “删除 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 AWS Direct Connect 虚拟接口。

如果您在某个 AWS 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 AWS Direct Connect。

如果要创建使用 MAC 安全（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 先决条件 ”。

## 使用连接向导创建连接

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 AWS Direct Connect 专用连接” 中的步骤。

要创建连接向导连接

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 使用 AWS Direct Connect 弹性工具包入门。

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 1Gbps 到 100Gbps 之间的任何值。

   b. 在 “位置” 中，选择相应 AWS 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， AWS 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，选择请求支持 MACsec 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键/值对，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 “下载 LOA-CFA”。

使用以下命令之一。

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

# 创建 Classic 连接

对于专用连接，您可以使用 AWS 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 AWS Direct Connect 位置。

> **Note**
>
> 您不能使用 AWS 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 AWS Direct Connect 连接

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
2. 在 AWS 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 AWS 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。此选项仅在该位置在建筑物的多个楼层中设有汇接机房 (MMR) 时可用。
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 AWS 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键/值对，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 Create Connection (创建连接)。

最多可能需要 72 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 AWS Direct Connect 连接。

## 下载 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。

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。

> **Note**
>
> 有关定价的更多信息，请参阅AWS 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 删除连接。

Console

下载 LOA-CFA

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 在 AWS Direct Connect 各个位置请求交叉连接。

Command line

使用命令行或 API 下载 LOA-CFA

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

## 更新连接

您可以更新以下连接属性：

- 连接的名称。
- 连接的 MACsec 加密模式。

> **Note**
>
> MACsec 仅在专用连接上可用。

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`

Console

更新连接

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 Remove tag (删除标签)。
5. 选择 Edit connection (编辑连接)。

Command line

要使用命令行添加和删除标签

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

要使用命令行或 API 更新连接

- update-connection（AWS CLI）
- UpdateConnection(AWS Direct Connect API)

# 将 MACsec CKN/CAK 与连接关联

创建支持 MACsec 的连接后，您可以将 CKN/CAK 与连接关联。

> **Note**
>
> 将 MACsec 密钥与连接关联后，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 “删除 MACsec 密钥和连接之间的关联”。

Console

要将 MACsec 密钥与连接关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 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。

Command line

要将 MACsec 密钥与连接关联

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

## 删除 MACsec 密钥和连接之间的关联

您可以删除连接和 MACsec 密钥之间的关联。

Console

要删除连接和 MACsec 密钥之间的关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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，然后选择解除密钥关联。
6. 在确认对话框中，输入 disassociate，然后选择解除关联。

Command line

要删除连接和 MACsec 密钥之间的关联

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

# 托管连接

要创建 AWS Direct Connect 托管连接，您需要以下信息：

AWS Direct Connect 位置

与合作伙伴计划中的 AWS Direct Connect AWS Direct Connect 合作伙伴合作，帮助您在某个 AWS 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 AWS Direct Connect 交付合作伙伴。

> **Note**
>
> 您无法通过 AWS 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 the section called “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 AWS 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。

请注意以下几点：

- 连接端口速度只能由您的 AWS Direct Connect 合作伙伴更改。您不再需要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。要更改您的端口速度，请联系管理您的托管连接的 AWS Direct Connect 合作伙伴。
- 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 AWS 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：

- the section called “查看您的连接详细信息”
- the section called “更新连接”
- the section called “删除连接”

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 AWS Direct Connect 虚拟接口。

## 接受托管连接

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 AWS 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。

Console

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。

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。

Command line

使用命令行或 API 接受托管连接

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

# 查看您的连接详细信息

您可以查看您当前的连接状态。您还可以查看连接 ID（例如，dxcon-12nikabc）并验证它与您所接收或下载的 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。

Console

如何查看连接的详细信息

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。

Command line

使用命令行或 API 描述连接

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

# 删除连接

只要连接没有连接虚拟接口，您就可以删除该连接。删除您的连接会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）。 AWS 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。

在删除连接之前，请下载包含跨账户信息的连接的 LOA，这样您就可以获得有关正在断开的电路的相关信息。有关下载连接 LOA 的步骤，请参阅 the section called “下载 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，您的主机托管或电路提供商仍可能向您收取交叉连接费用或网络电路费用，因为交叉连接电缆可能仍连接到您的网络设备。这些交叉连接费用与Direct Connect无关，必须使用LOA中的信息向托管或电路提供商取消这些费用。

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。

Console

删除连接

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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)。

Command line

使用命令行或 API 删除 连接

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

# 在 AWS Direct Connect 各个位置请求交叉连接

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）。如果您已在某个 AWS Direct Connect 地点安装了设备，请联系相应的提供商以完成交叉连接。有关各供应商的具体说明，请参阅下表。有关交叉连接定价，请联系您的供应商。建立交叉连接后，可以使用 AWS Direct Connect 控制台创建虚拟界面。

一些位置设置为园区。有关更多信息，包括每个位置的可用速度，请参阅 AWS Direct Connect 位置。

如果您在某个 AWS Direct Connect 地点还没有设备，则可以与合作伙伴网络 (APN) 中的 AWS 合作伙伴合作。他们可帮助您连接到 AWS Direct Connect 位置。有关更多信息，请参阅 APN 合作伙伴支持 AWS 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。

AWS Direct Connect 连接可以提供对其他区域资源的访问权限。有关更多信息，请参阅访问远程 AWS 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 AWS Direct Connect 控制台再次下载它。有关更多信息，请参阅下载 LOA-CFA。

主机托管

- 美国东部（俄亥俄州）
- 美国东部（弗吉尼亚州北部）
- 美国西部（北加利福尼亚）
- US West（Oregon）
- 非洲（开普敦）
- 亚太地区（雅加达）
- 亚太地区（孟买）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- Asia Pacific（Tokyo）

- Canada（Central）
- 中国（北京）
- 中国（宁夏）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（米兰）
- 欧洲地区（伦敦）
- 欧洲地区（巴黎）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）
- South America（São Paulo）
- AWS GovCloud（美国东部）
- AWS GovCloud（美国西部）

# 美国东部（俄亥俄州）

| 位置 | 如何申请连接 |
| --- | --- |
| Cologix COL2，哥伦布市 | 通过 sales@cologix.com 联系 Cologix。 |
| Cologix MIN3，明尼阿波利斯 | 通过 sales@cologix.com 联系 Cologix。 |
| CyrusOne West III，休斯顿 | 使用客户门户网站提交申请。 |
| 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 客户门户下订单。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，Reston | 在CoreSite 客户门户下订单。完成表单后，请检查订单的准确性，然后使用网站审批订单。 |
| 数字房地产 ATL1 和 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，Ashburn | 联系 Equinix，邮箱为 awsdealreg@equinix.com。 |
| 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，Seacaucus | 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。 |
| 费城 MMR 二楼 Netrality 数据中心 | 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（北加利福尼亚）

| 位置 | 如何申请连接 |
| --- | --- |
| CoreSite，LA1，洛杉矶 | 使用CoreSite 客户门户下订单。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，Milpitas | 使用CoreSite客户门户下订单。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 客户门户下订单。填写完表格后，请检查订单的准确性，然后使用 MyCoreSite 网站进行批准。 |
| EdgeConneX，菲尼克斯 | 使用 EdgeOS 客户门户网站下单。在您提交表格后，EdgeConneX 将提供一份服务订单表以供批准。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。 |
| Equinix SV1 和 SV5，圣何塞 | 联系 Equinix，邮箱为 awsdealreg@equinix.com。 |
| PhoenixNAP，菲尼克斯 | 联系 phoenixNAP Provisioning，邮箱为 provisioning@phoenixnap.com。 |

# US West（Oregon）

| 位置 | 如何申请连接 |
| --- | --- |
| CoreSite DE1，丹佛 | 使用CoreSite 客户门户下订单。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，西雅图威斯汀大厦 | 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。在您提交表格后，EdgeConneX 将提供一份服务订单表以供批准。您可以将问题发送到 cloudaccess@edgeconnex.com。 |

| 位置 | 如何申请连接 |
| --- | --- |
| 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 西雅图 | 请通过 TierPoint sales@tierpoint.com 联系。 |

## 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 jessie.w@dci-indonesia.com.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 | 请拨打 18001033130 或 marketing@netmagicsolutions.com 免费联系 NetMagic 销售和营销部门。 |
| Sify Rabale，孟买 | 联系 Sify，邮箱为 aws.directconnect@sifycorp.com。 |
| STT Delhi DC2，德里 | 如有疑问，请联系 STT。 AWSDX@sttelemediagdc .in。 |
| STT GDC Pvt. Ltd. VSB，钦奈 | 如有疑问，请联系 STT。 AWSDX@sttelemediagdc .in。 |
| STT Hyderabad DC1，海德拉巴 | 如有疑问，请联系 STT。 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。 |

| 位置 | 如何申请连接 |
| --- | --- |
| 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 salessingapore@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 Datacom O rbit —奥克兰联系数据通信。 |
| 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 salessydney@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。 |

| 位置 | 如何申请连接 |
| --- | --- |
| NEXTDC S2，悉尼 | 联系 NEXTDC，邮箱为 nxtops@nextdc.com。 |

## Asia Pacific（Tokyo）

| 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。 |

## Canada（Central）

| 位置 | 如何申请连接 |
| --- | --- |
| Allied 250 Front St W，多伦多 | 联系 driches@alliedreit.com。 |
| Cologix MTL3，蒙特利尔 | 通过 sales@cologix.com 联系 Cologix。 |
| Cologix VAN2，温哥华 | 通过 sales@cologix.com 联系 Cologix。 |
| eStruxture，蒙特利尔 | 联系 eStruxture，邮箱为 directconnect@estruxture.com。 |

## 中国（北京）

| 位置 | 如何申请连接 |
| --- | --- |
| CIDS Jiachuang IDC，北京 | 联系 dx-order@sinnet.com.cn。 |
| Sinnet Jiuxianqiao IDC，北京 | 联系 dx-order@sinnet.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，奥斯陆，挪威 | 请通过 DigiPlex helpme@digiplex.com 联系。 |
| 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。 |

| 位置 | 如何申请连接 |
| --- | --- |
| 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 | 联系 Eircom，邮箱为 awsorders@eircom.ie。 |
| 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。 |
| 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 Pari s 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 | 请通过 MedOne support@Medone.co.il 联系我们 |
| EdgeConnex，荷兹利亚 | 请通过 EdgeConnect info@edgeconnecx.com 联系我们 |

## 中东（巴林）

| 位置 | 如何申请连接 |
| --- | --- |
| AWS 巴林 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 AWS 通过 Support Cent er 提供网络提供商的授权书 (LOA)。AWS AWS 在此位置完成交叉连接。 |
| AWS 巴林 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 AWS 通过 Support Cent er 提供网络提供商的授权书 (LOA)。AWS AWS 在此位置完成交叉连接。 |

## 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。 |
| 阿联酋富查伊拉阿联酋阿提萨拉特 SmartHub 数据中心 | 请通过 IntlSales- C& WS@etisalat.ae 联系阿提萨拉特 SmartHub 数据中心。 |

## South America（São Paulo）

| 位置 | 如何申请连接 |
| --- | --- |
| Equinix RJ2，里约热内卢 | 联系 Equinix，邮箱为 awsdealreg@equinix.com。 |
| 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。 |

# AWS Direct Connect 虚拟接口

必须创建以下虚拟接口 (VIF) 之一才能开始使用您的 AWS 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。您可以将公交虚拟接口与任何速度的任何 AWS 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the section called “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，以便您可以访问自己的 VPC 或其他 AWS 服务。您可以通过此连接访问所有 AWS 前缀；例如 Amazon EC2、Amazon S3 和 Amazon.com。您无权访问非 Amazon 前缀。有关发布的前缀的最新列表 AWS，请参阅中的 AWS IP 地址范围。Amazon Web Services 一般参考 AWS 不会将通过 Direc AWS t Connect 公共虚拟接口接收的客户前缀重新通告给其他客户。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”。

> **Note**
>
> 我们建议您使用防火墙筛选条件 (根据数据包的源/目标地址) 来控制流量传入和传出某些前缀。如果您使用前缀筛选条件 (路由映射)，请确保它接受精确匹配或更长的前缀。广告来源的前缀 AWS Direct Connect 可能会被汇总，并且可能与前缀过滤器中定义的前缀不同。

## 托管的虚拟接口

要使用与其他账户的 AWS 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。

您可以将传输虚拟接口与 Direct Connect 专用连接或任何速度的托管连接配合使用。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 | 您要为其创建虚拟接口的 AWS 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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR<br><br>这些可以是任何公有 IP（客户拥有或由提供 AWS），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。 |

| 资源 | 所需信息 |
| --- | --- |
| | • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>• 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）<br>**Note**<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>• （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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。 |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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。 |

# SiteLink

如果您要创建私有或传输虚拟接口，则可以使用 SiteLink。

SiteLink 是虚拟专用接口的可选 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 AWS Direct Connect SiteLink。

> **Note**
>
> SiteLink 在中国 AWS GovCloud (US) 和中国地区不可用。

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联的 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 the section called “为私有虚拟接口或中转虚拟接口设置网络 MTU”。

## 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 the section called “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 AWS 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 | 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 AWS Direct Connect 连接的流量都必须有此标签。<br><br>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。 |

| 资源 | 所需信息 |
| --- | --- |
| 对等 IP 地址 | 虚拟接口支持 IPv4、IPv6 或其中一个（双堆栈）的 BGP 对等会话。请勿使用弹性 IP (EIP) 或从 Amazon Pool 中自带 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。<br><br>• IPv4:<br>  • （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：<br>  • 客户拥有的 IPv4 CIDR<br><br>这些可以是任何公有 IP（客户拥有或由提供 AWS），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。<br>  • 您的 AWS Direct Connect 合作伙伴或 ISP 拥有的 IP 范围，以及 LOA-CFA 授权<br>  • 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）<br><br>Note<br>我们不能保证我们能够满足对 AWS提供的公有 IPv4 地址的所有请求。<br>  • （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，请确保仅为路由器接口和 Di AWS rect 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。<br>• 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。 |

| 资源 | 所需信息 |
| --- | --- |
| 地址系列 | BGP 对等会话是通过 IPv4 还是 IPv6 进行。 |
| BGP 信息 | • 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。<br>• AWS 默认情况下启用 MD5。您无法修改此选项。<br>• 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 | 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。<br>• IPv4：当以下任一条件为真 AWS Direct Connect 时，IPv4 CIDR 可以与使用宣布的另一个公有 IPv4 CIDR 重叠：<br>  • CIDR 来自不同的 AWS 区域。确保在公有前缀上应用 BGP 社区标签。<br>  • 当您在主动/被动配置中拥有公有 ASN 时，可以使用 AS_PATH。<br>  有关更多信息，请参阅路由策略和 BGP 社区。<br>• IPv6：指定 /64 或更短的前缀长度。<br>• 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。<br>• 您可以通过 Direct Connect 公有虚拟接口指定任何前缀长度。IPv4 应支持 /1 - /32 之间的任何值，而 IPv6 应支持 /1 - /64 之间的任何值。 |

| 资源 | 所需信息 |
| --- | --- |
| （仅限私有虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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。 AWS 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 AWS 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。 |
| （仅限中转虚拟接口）巨型帧 | 数据包的最大传输单位 (MTU)。 AWS 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 AWS 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。 |

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 VIF 和传输 VIF，该账户适用于虚拟接口和虚拟私有网关/Direct Connect 网关目标。
- 对于公有 VIF，该账户用于虚拟接口计费。数据传出 (DTO) 使用量按 AWS 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 IPv4 点对点链路上使用 31 位前缀。

# 创建虚拟接口

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。

要为你内部的账户或 AWS Organizations 与你的 AWS Organizations账户不同的账户创建虚拟界面，请创建一个托管虚拟接口。有关更多信息，请参阅 the section called “创建托管虚拟接口”。

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。

## 创建公有虚拟接口

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

预配置公有虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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号。

      有效值为 1-2147483647。
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(AWS Direct Connect API)

## 创建私有虚拟接口

您可以为与您的 AWS Direct Connect 连接位于同一区域的虚拟专用网关配置私有虚拟接口。有关为 AWS Direct Connect 网关配置私有虚拟接口的更多信息，请参阅使用 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）。虚拟私有接口的 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 AWS 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。
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**
>
> 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。相反，你应该使用 RFC 1918 或其他寻址（非 RFC 1918），然后自己指定地址。
>
> - 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。

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. 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(AWS Direct Connect API)

## 创建到 Direct Connect 网关的中转虚拟接口

要将 AWS 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。

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）。虚拟私有接口的 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 AWS 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。

为 Direct Connect 网关配置中转虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。
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**
>
> 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。相反，你应该使用 RFC 1918 或其他寻址（非 RFC 1918），然后自己指定地址。
>
> - 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。

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 Remove tag (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(AWS Direct Connect API)

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

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

## 下载路由器配置文件

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

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 AWS Direct Connect。

### MACsec 注意事项

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。 |

| 参数 | 描述 |
| --- | --- |
| 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 | • 对于 100Gbps 连接：GCM_AES_XPN_256<br>• 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> |

# 查看虚拟接口详细信息

您可以查看虚拟接口的当前状态。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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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)
- DescribeVirtual接口 (AWS Direct Connect API)

# 添加或删除 BGP 对等体

对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 默认情况下启用 MD5。您无法修改此选项。

## 添加 BGP 对等体

使用以下过程可添加 BGP 对等体。

添加 BGP 对等体

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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**
   >
   > 如果您允许 AWS 自动分配 IP 地址，则将从 169.254.0.0/16 分配 /29 CIDR。 AWS 如果您打算使用客户路由器对等 IP 地址作为流量的源和目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。有关 RFC 1918 的更多信息，请参阅私有互联网的地址分配。

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 1-2147483647。

   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 (API)AWS Direct Connect

## 删除 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)。

删除 BGP 对等体

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 (API)AWS Direct Connect

# 为私有虚拟接口或中转虚拟接口设置网络 MTU

AWS 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）。虚拟私有接口的 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 AWS 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。如果您有两个公布相同路由但使用不同 MTU 值的私有虚拟接口，或者如果您有公布相同路由的站点到站点 VPN，则使用 1500 MTU。

> **Important**
>
> 巨型帧仅适用于通过中转网关的传播路由 AWS 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 C1、CC1、T1 和 M1 外，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。

设置私有虚拟接口的 MTU

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 size 9001) (巨型帧 (MTU 大小 9001)) 或 Jumbo MTU (MTU size 8500) (巨型帧 MTU (MTU 大小 8500)) 下，选择 Enabled (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(AWS Direct Connect API)

## 添加或删除虚拟接口标签

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，则可以添加或删除标签。

添加或删除虚拟接口标签

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。删除虚拟接口会停止与该虚拟接口相关的 AWS Direct Connect 数据传输费用。

删除虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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)
- DeleteVirtual接口 (AWS Direct Connect API)

# 创建托管虚拟接口

您可以创建公有、中转或私有托管虚拟接口。在您开始之前，请确保您阅读了 虚拟接口的先决条件中的信息。

# 创建托管私有虚拟接口

创建托管私有虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。
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**
   >
   > 如果您允许 AWS 自动分配 IP 地址，则将从 169.254.0.0/16 分配 /29 CIDR。 AWS 如果您打算使用客户路由器对等 IP 地址作为流量的源和目的地，则不建议使用此选项。相反，你应该使用 RFC 1918 或其他寻址（非 RFC 1918），然后自己指定地址。有关 RFC 1918 的更多信息，请参阅私有互联网的地址分配。

[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）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. 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(AWS Direct Connect API)

## 创建托管公有虚拟接口

创建托管公有虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。

6. 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**
>
> 如果您允许 AWS 自动分配 IP 地址，则将从 169.254.0.0/16 分配 /29 CIDR。 AWS 如果您打算使用客户路由器对等 IP 地址作为流量的源和目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。有关 RFC 1918 的更多信息，请参阅私有互联网的地址分配。

[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。

7. 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）。
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 Remove tag (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(AWS Direct Connect API)

## 创建托管中转虚拟接口

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1-2147483647。
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**
>
> 如果您允许 AWS 自动分配 IP 地址，则将从 169.254.0.0/16 分配 /29 CIDR。 AWS 如果您打算使用客户路由器对等 IP 地址作为流量的源和目的地，则不建议使用此选项。您应该使用 RFC 1918 或其他寻址，并自行指定地址。有关 RFC 1918 的更多信息，请参阅私有互联网的地址分配。

[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 Remove tag (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(AWS Direct Connect API)

# 接受托管虚拟接口

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

如何接受托管虚拟接口

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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， AWS 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(AWS Direct Connect API)

使用命令行或 API 接受托管公有虚拟接口

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

使用命令行或 API 接受托管中转虚拟接口

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

# 迁移虚拟接口

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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

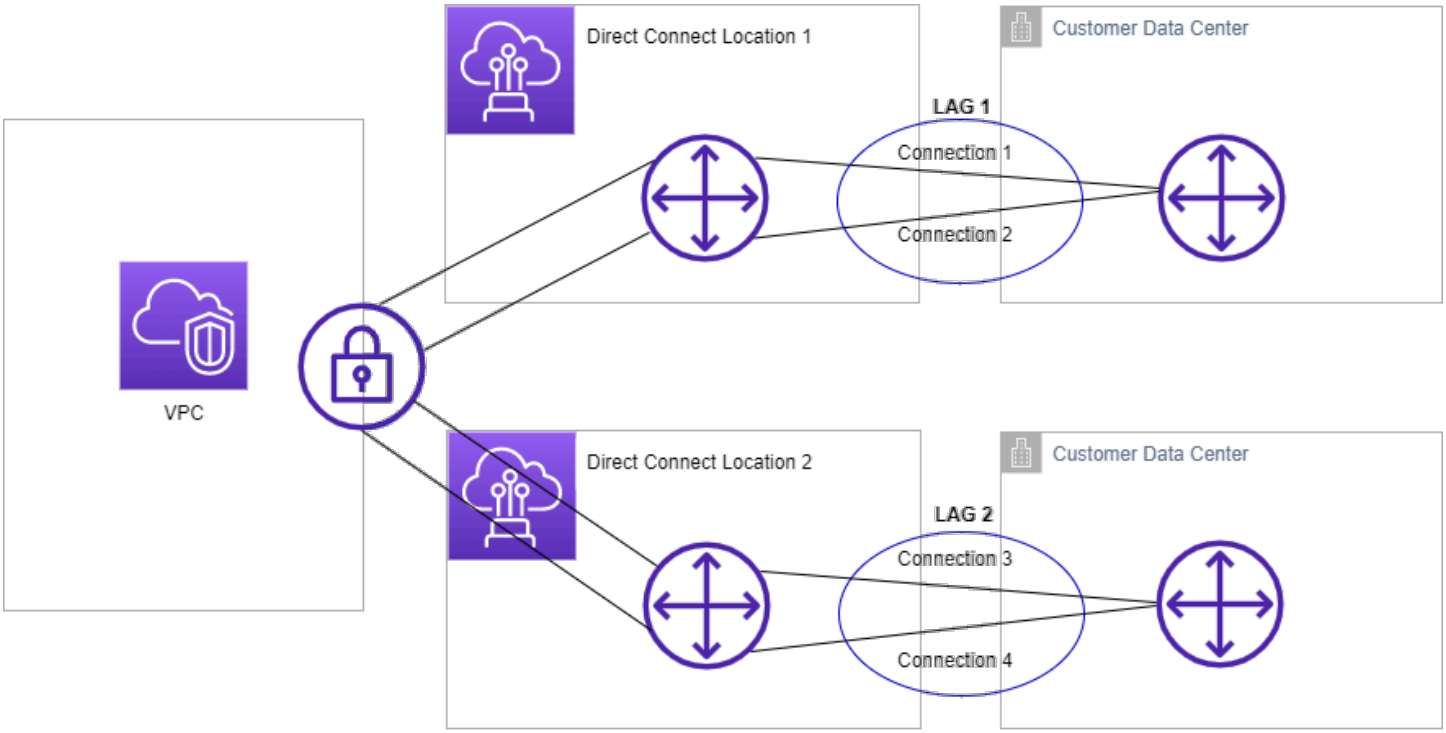
- associate-virtual-interface (AWS CLI)
- AssociateVirtual接口 (AWS Direct Connect API)

# 链接聚合组

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 AWS 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。您可以为终止在同一AWS设备和相同位置的连接创建 LAG，然后使用两个 LAG 而不是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 1Gbps、10Gbps 或 100Gbps。
- 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 100G 连接，或四个端口速度低于 100G 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 AWS 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 AWS Direct Connect 控制台分别为每个新的物理连接下载《授权证书和连接设备分配 (LOA-CFA)》。有关更多信息，请参见 下载 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 AWS Direct Connect 终端节点上有足够的可用端口。

## 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。

## 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 AWS 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。

Create a LAG with new connections using the console

利用新连接创建 LAG

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1G 或 10G 时，最多可以有四个连接；当端口速度为 100G 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。

Create a LAG with existing connections using the console

通过现有连接创建 LAG

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 1G 或 10G 时，最多可以有四个连接；当端口速度为 100G 时，最多可以有两个连接。
   - 最小连接数：要让 LAG 本身运行而必须运行的连接的最小数量。如果您未指定值，我们将分配默认值 0。
5. （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。

Command line

使用命令行或 API 创建 LAG

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

使用命令行或 API 描述 LAG

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

使用命令行或 API 下载 LOA-CFA

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

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 LAG 详细信息

创建 LAG 后，您可以查看其详细信息。

Console

查看有关您的 LAG 的信息

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 您可以查看 LAG 的相关信息，包括其 ID 和连接终止的 AWS Direct Connect 端点。

Command line

要使用命令行或 API 查看 LAG 的相关信息

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

# 更新 LAG

您可以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。

Console

更新 LAG

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 )。

Command line

使用命令行或 API 更新 LAG

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

要使用命令行添加和删除标签

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

# 将连接与 LAG 关联

您可将现有连接与 LAG 关联。连接可以是独立的，也可以是其他 LAG 的一部分。连接必须位于同一 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。

Console

将连接与 LAG 关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。

Command line

使用命令行或 API 关联连接

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

# 解除连接与 LAG 的关联

解除某个连接与 LAG 之间的关联，可将该连接转换为独立连接。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。

Console

解除连接与 LAG 的关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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)。

Command line

使用命令行或 API 解除关联连接

- disassociate-connection-from-lag (AWS CLI)

- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

# 将 MACsec CKN/CAK 与 LAG 关联

创建支持 MACsec 的 LAG 后，您可以将 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 “删除 MACsec 密钥和 LAG 之间的关联”。

Console

要将 MACsec 密钥与 LAG 关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。

Command line

要将 MACsec 密钥与 LAG 关联

- associate-mac-sec-key (AWS CLI)

- AssociateMacSecKey(AWS Direct ConnectAPI)

# 删除 MACsec 密钥和 LAG 之间的关联

您可以删除 LAG 和 MACsec 密钥之间的关联。

Console

要删除 LAG 和 MACsec 密钥之间的关联

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 选择要删除的 MACsec 密钥，然后选择解除密钥关联。
5. 在确认对话框中，输入 disassociate，然后选择解除关联。

Command line

要删除 LAG 和 MACsec 密钥之间的关联

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

# 删除 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，请参见 删除连接。

Console

删除 LAG

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。

### Command line

使用命令行或 API 删除 LAG

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

# 使用 Direct Connect 网关

您可以使用 Amazon VPC 控制台或使用 AWS Direct Connect 网关 AWS CLI。

内容



## Direct Connect 网关

使用 AWS Direct Connect 网关连接您的 VPC。将 AWS Direct Connect 网关与以下任一网关关联：

- 当您在同一区域有多个 VPC 时的中转网关
- 虚拟私有网关

您也可以使用虚拟私有网关来扩展本地区域。此配置允许与本地区域关联的 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。这包括 AWS GovCloud (US) 但不包括 AWS 中国区域。

对于使用 Direct Connect 且 VPC 当前绕过父级可用区的客户，将无法迁移其 Direct Connect 连接或虚拟接口。

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 月实施的这一规则有一种例外情况，即在两个或多个 VPC 上公布超网，这些 VPC 连接的虚拟私有网关（VGW）关联到同一 Direct Connect 网关并位于同一虚拟接口上。在这种情况下，VPC 可通过 Direct Connect 端点相互通信。例如，如果您公布的超网（例如 10.0.0.0/8 或 0.0.0.0/0）与连接到 Direct Connect 网关（例如 10.0.0.0/24 和 10.0.1.0/24）的 VPC 重叠，并位于同一虚拟接口上，则这些 VPC 可以从您的本地网络相互通信。

如果您想在 Direct Connect 网关内阻止 VPC 到 VPC 的通信，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，也可以将其用作 VPC 中默认安全组的一部分。
2. 避免从与 VPC 重叠的本地网络公布超网。相反，您可以从不与 VPC 重叠的本地网络公布特定的路由。
3. 为要连接到本地网络的每个 VPC 预置一个 Direct Connect 网关，而不是为多个 VPC 使用同一 Direct Connect 网关。例如，不要为开发和生产 VPC 使用单个 Direct Connect 网关，而是为每个 VPC 使用单独的 Direct Connect 网关。

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 VPC 连接到与同一 Direct Connect 网关关联的中转网关，则这些 VPC 可以进行通信。要防止 VPC 通信，请将路由表与设置了黑洞选项的 VPC 附件相关联。

下面描述了可以使用 Direct Connect 网关的场景。

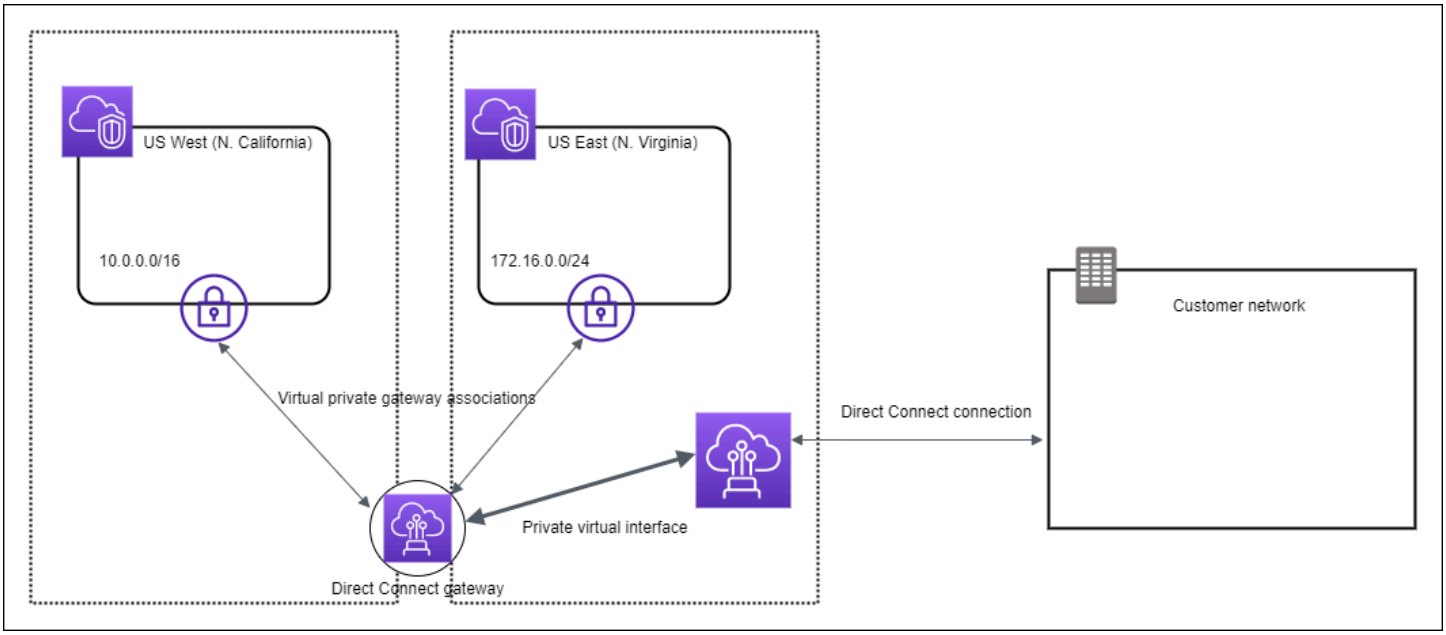
场景

- 虚拟私有网关关联
- 跨账户的虚拟私有网关关联
- 中转网关关联
- 跨账户的中转网关关联
- 创建 Direct Connect 网关
- 删除 Direct Connect 网关
- 从虚拟私有网关迁移到 Direct Connect 网关

## 虚拟私有网关关联

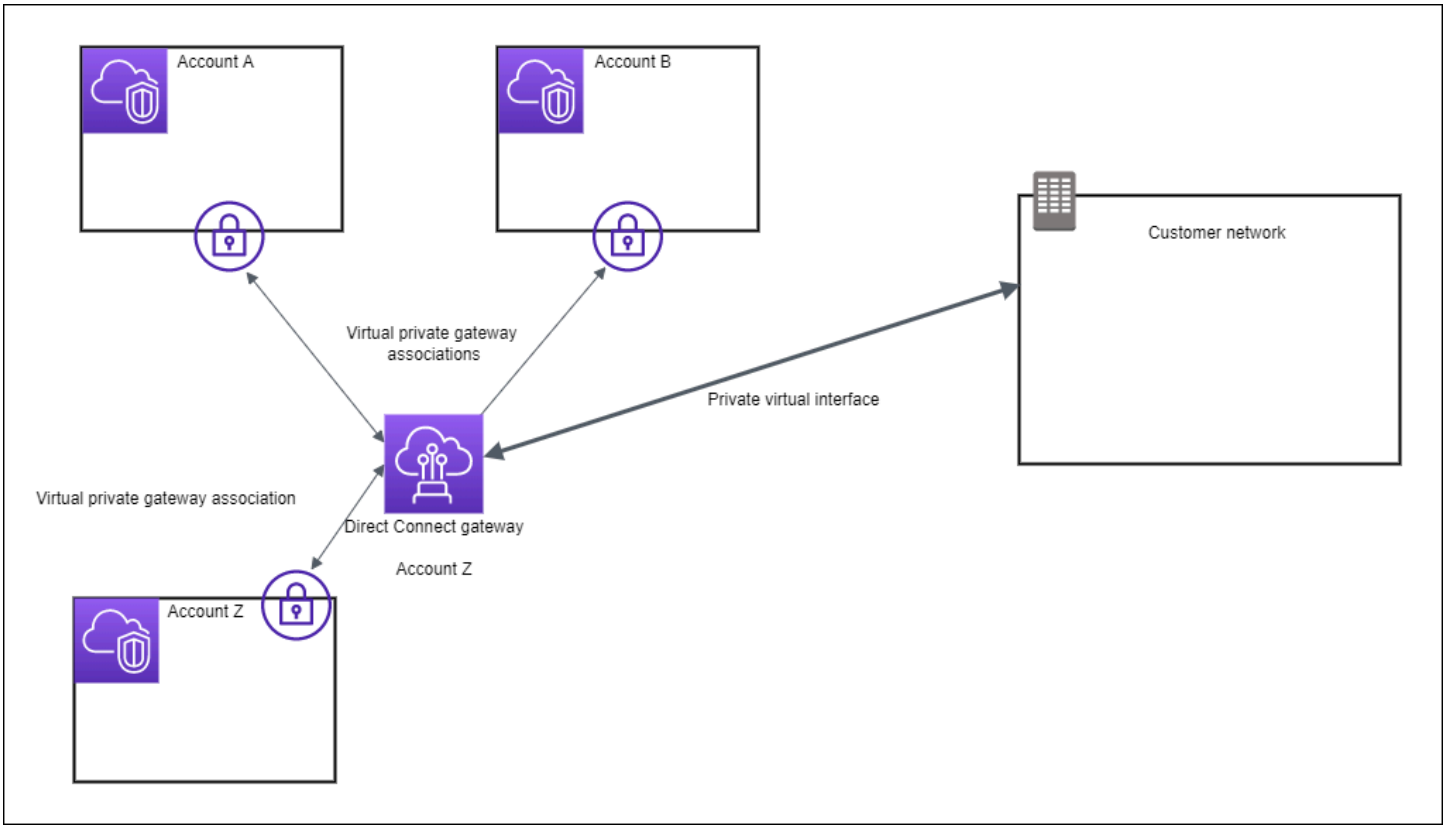
在下图中，Direct Connect 网关允许您使用美国东部（弗吉尼亚州北部）区域的 AWS Direct Connect 连接，访问您账户中位于美国东部（弗吉尼亚州北部）和美国西部（北加利福尼亚）区域的 VPC。

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 AWS Direct Connect 地点。从该位置到客户数据中心有一个 AWS Direct Connect 连接。



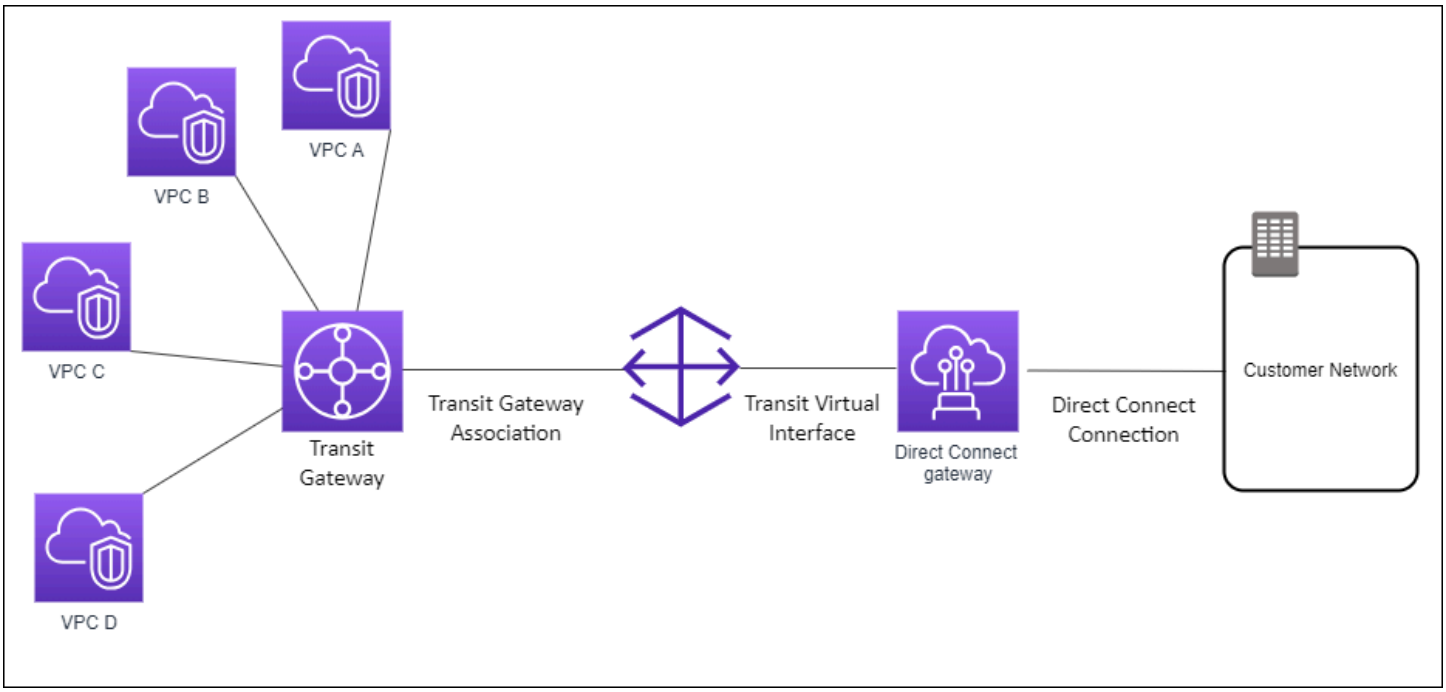

# 跨账户的虚拟私有网关关联

考虑 Direct Connect 网关拥有者（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。




## 中转网关关联

下图说明如何通过 Direct Connect 网关创建一条可供您的所有 VPC 使用的到 Direct Connect 连接的单一连接。



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。

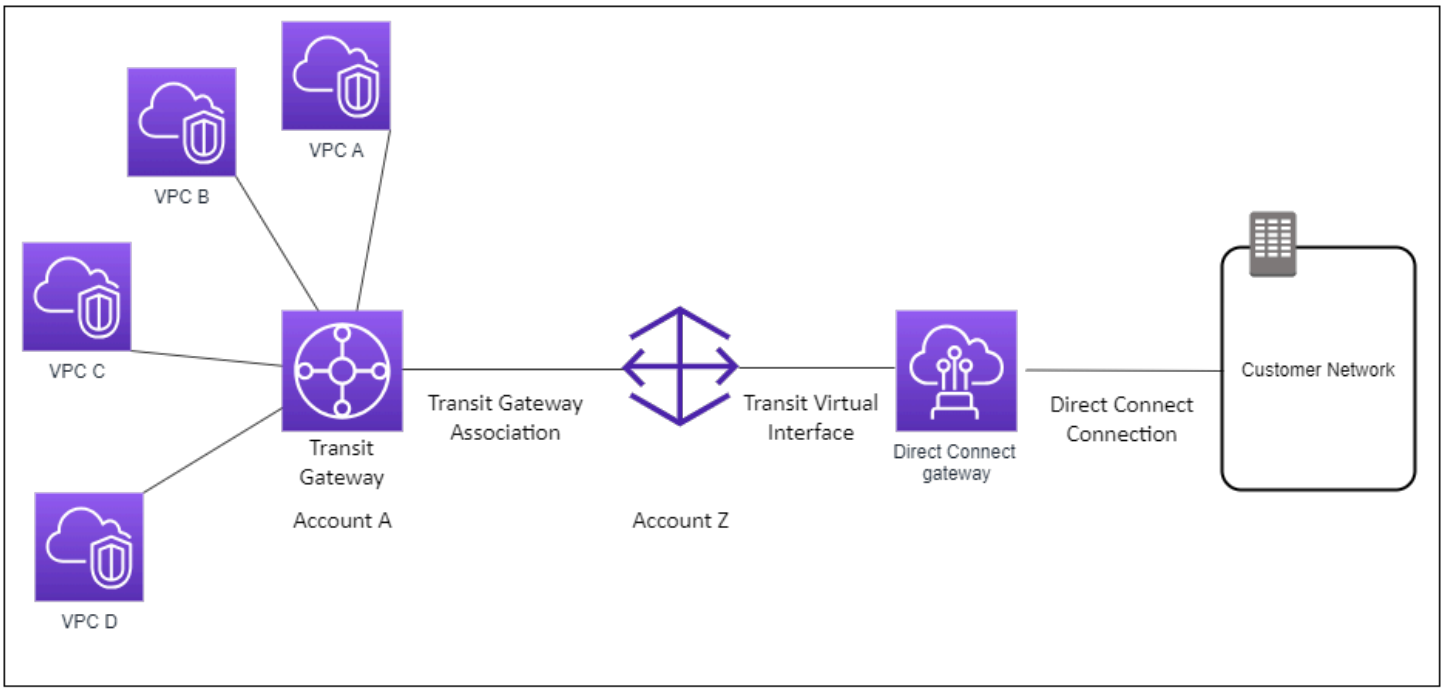
此配置提供以下好处。您可以：

- 对于同一区域中的多个 VPC 或 VPN，只需管理一个连接。
- 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。

## 跨账户的中转网关关联

考虑 Direct Connect 网关拥有者（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 接受提议后，连接到中转网关的 VPC 可以将流量从中转网关路由到 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。




内容

- 创建 Direct Connect 网关
- 删除 Direct Connect 网关
- 从虚拟私有网关迁移到 Direct Connect 网关

## 创建 Direct Connect 网关

您可以在任何受支持的区域创建 Direct Connect 网关。

创建 Direct Connect 网关

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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。
   - 虚拟私有网关：要关联虚拟私有网关，请选择虚拟私有网关。

使用命令行或 API 创建 Direct Connect 网关

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

## 删除 Direct Connect 网关

如果您不再需要某一 Direct Connect 网关，可将其删除。您必须先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。

删除 Direct Connect 网关

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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(AWS Direct Connect API)

## 从虚拟私有网关迁移到 Direct Connect 网关

如果您有一个虚拟私有网关附加到虚拟接口，并且您想要迁移到 Direct Connect 网关，请执行以下步骤：

迁移到 Direct Connect 网关

1. 创建 Direct Connect 网关。有关更多信息，请参阅 the section called “创建 Direct Connect 网关”。
2. 创建 Direct Connect 网关的虚拟接口。有关更多信息，请参阅 the section called “创建虚拟接口”。
3. 将虚拟私有网关与 Direct Connect 网关相关联。有关更多信息，请参阅 the section called “关联和取消关联虚拟私有网关”。
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 the section called “删除虚拟接口”。

# 虚拟私有网关关联

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

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 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。

要将您的 AWS Direct Connect 连接仅连接到同一区域的 VPC，您可以创建 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。

要使用您与其他账户中的 VPC 的 AWS Direct Connect 连接，您可以为该账户创建托管私有虚拟接口。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 AWS Direct Connect 虚拟接口。

内容

# 创建虚拟私有网关

虚拟私有网关必须附加到您要连接到的 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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（亚马逊 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（亚马逊 EC2 查询 API）
- attach-vpn-gateway (AWS CLI)

- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

## 关联和取消关联虚拟私有网关

您可以关联或解除关联虚拟私有网关和 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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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(AWS 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(AWS 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(AWS Direct Connect API)

## 创建到 Direct Connect 网关的私有虚拟接口

要将您的 AWS 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。

> **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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。

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**
   >
   > 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。相反，你应该使用 RFC 1918 或其他寻址（非 RFC 1918），然后自己指定地址。
   >
   > - 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。

   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)。

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(AWS Direct Connect API)

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

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

## 跨账户关联虚拟私有网关

您可以将 Direct Connect 网关与任何 AWS 账户拥有的虚拟专用网关相关联。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

当您将虚拟私有网关与 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 通告的网络内部前缀的虚拟接口都只能传播到跨区域的中转网关，而不是在同一区域内。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 the section called “允许的前缀交互”。

任务

- 创建关联提议
- 接受或拒绝关联提议
- 为关联更新允许的前缀
- 删除关联提议

## 创建关联提议

如果您拥有虚拟私有网关，您必须创建一个关联提议。虚拟私有网关必须连接到您 AWS 账户中的 VPC。Direct Connect 网关的所有者必须共享 Direct Connect 网关的 ID 及其 AWS 账户 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 AWS Direct Connect访问本地网络。

创建关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
2. 在导航窗格中，选择虚拟私有网关，然后选择虚拟私有网关。
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 AWS 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 Direct Connect 网关所有者，请输入拥有该关联的 Direct Connect 网关的 AWS 账户 ID。
   c. （可选）要指定虚拟私有网关中允许的前缀列表，请将前缀添加到 Allowed prefixes (允许的前缀) 中，并用逗号将它们分隔开。
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(AWS Direct Connect API)

## 接受或拒绝关联提议

如果您拥有 Direct Connect 网关，您必须接受关联提议才能创建关联。否则，您可以拒绝关联提议。

### 接受关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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）要指定虚拟私有网关中允许的前缀列表，请将前缀添加到 Allowed prefixes (允许的前缀) 中，并用逗号将它们分隔开。
6. 选择 Accept proposal (接受提议)。

### 拒绝关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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，选择虚拟私有网关，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-协会提案 ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

### 使用命令行或 API 接受关联提议

- accept-direct-connect-gateway-协会提案 ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

### 使用命令行或 API 拒绝关联提议

- delete-direct-connect-gateway-协会提案 ()AWS CLI

- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

## 为关联更新允许的前缀

您可以通过 Direct Connect 网关更新虚拟私有网关中允许的前缀。

如果您是虚拟私有网关的所有者，请为相同的 Direct Connect 网关和虚拟私有网关创建一个新的关联提议，同时指定允许的前缀。

如果您是 Direct Connect 网关的所有者，请在您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，如下所示。

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(AWS Direct Connect API)

## 删除关联提议

如果 Direct Connect 网关关联提议仍处于待定状态，则虚拟私有网关的所有者可以删除关联提议。接受提议后，您无法将其删除，但您可以解除虚拟私有网关与 Direct Connect 网关之间的关联。有关更多信息，请参阅 the section called “关联和取消关联虚拟私有网关”。

删除关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
2. 在导航窗格中，选择虚拟私有网关，然后选择虚拟私有网关。
3. 请选择查看详细信息。
4. 选择 Pending Direct Connect gateway associations (待定的 Direct Connect 网关关联)，选择此关联并选择 Delete association (删除关联)。
5. 在 Delete association proposal (删除关联提议) 对话框中，输入 Delete，然后选择 Delete (删除)。

使用命令行或 API 删除待定的关联提议

- delete-direct-connect-gateway-协会提案 ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

# 中转网关关联

您可以使用 AWS Direct Connect 网关，将 AWS 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，为您与 Direct Connect 网关的 AWS Direct Connect 连接创建一个中转虚拟接口。

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 配额。
- Direct Connect 网关支持连接的传输虚拟接口和关联的传输网关之间的通信。
- 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。
- 通过 Direct Connect 通告的网络内部任何虚拟接口都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传输网关

## 关联和解除关联中转网关

要关联中转网关

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 the section called “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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。

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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 CIDR 匹配。有关允许的前缀的更多信息，请参阅 the section called “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。
7. 选择取消关联。
8. 再次选择解除关联以确认您要解除关联网关。

   在网关关联部分，状态显示正在解除关联。完成后，将显示一条确认消息，网关将从该部分删除。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(AWS 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(AWS 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(AWS 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(AWS Direct Connect API)

## 创建到 Direct Connect 网关的中转虚拟接口

要将 AWS 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。

> **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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 2147483647。

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**
>
> 如果您允许 AWS 自动分配 IPv4 地址，则将根据 RFC 3927 从 169.254.0.0/16 IPv4 Link-Local 中分配 /29 CIDR 以进行连接。 point-to-point AWS 如果您打算使用客户路由器对等 IP 地址作为 VPC 流量的源和/或目的地，则不建议使用此选项。相反，你应该使用 RFC 1918 或其他寻址（非 RFC 1918），然后自己指定地址。
>
> - 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。

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 Remove tag (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(AWS Direct Connect API)

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

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

## 跨账户关联中转网关

您可以将现有的 Direct Connect 网关或新的 Direct Connect 网关与任何 AWS 账户拥有的传输网关相关联。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。该列表用于将流量从本地路由 AWS 到传输网关，即使连接到传输网关的 VPC 没有分配 CIDR 也是如此。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 the section called “允许的前缀交互”。

任务

- 创建中转网关关联提议
- 接受或拒绝中转网关关联提议
- 为中转网关关联更新允许的前缀
- 删除中转网关关联提议

## 创建中转网关关联提议

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 AWS Direct Connect访问本地网络。

创建关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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(AWS Direct Connect API)

## 接受或拒绝中转网关关联提议

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。

接受关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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-协会提案 ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

使用命令行或 API 接受关联提议

- accept-direct-connect-gateway-协会提案 ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

使用命令行或 API 拒绝关联提议

- delete-direct-connect-gateway-协会提案 ()AWS CLI

- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

## 为中转网关关联更新允许的前缀

您可以通过 Direct Connect 网关更新中转网关允许的前缀。

如果您是中转网关的所有者，请为同一 Direct Connect 网关和虚拟私有网关创建新的关联提议，并指定允许的前缀。

如果您是 Direct Connect 网关的所有者，请在您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，如下所示。

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(AWS Direct Connect API)

## 删除中转网关关联提议

如果 Direct Connect 网关关联提议仍处于待定状态，则中转网关的所有者可以删除该提议。接受提议后，您无法将其删除，但您可以解除中转网关与 Direct Connect 网关之间的关联。有关更多信息，请参阅 the section called “创建中转网关关联提议”。

删除关联提议

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
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 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 (删除关联提议) 对话框中，输入 Delete，然后选择 Delete (删除)。

使用命令行或 API 删除待定的关联提议

- delete-direct-connect-gateway-协会提案 ()AWS CLI

- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

# 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 the section called “路由策略和 BGP 社区”。

## 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。

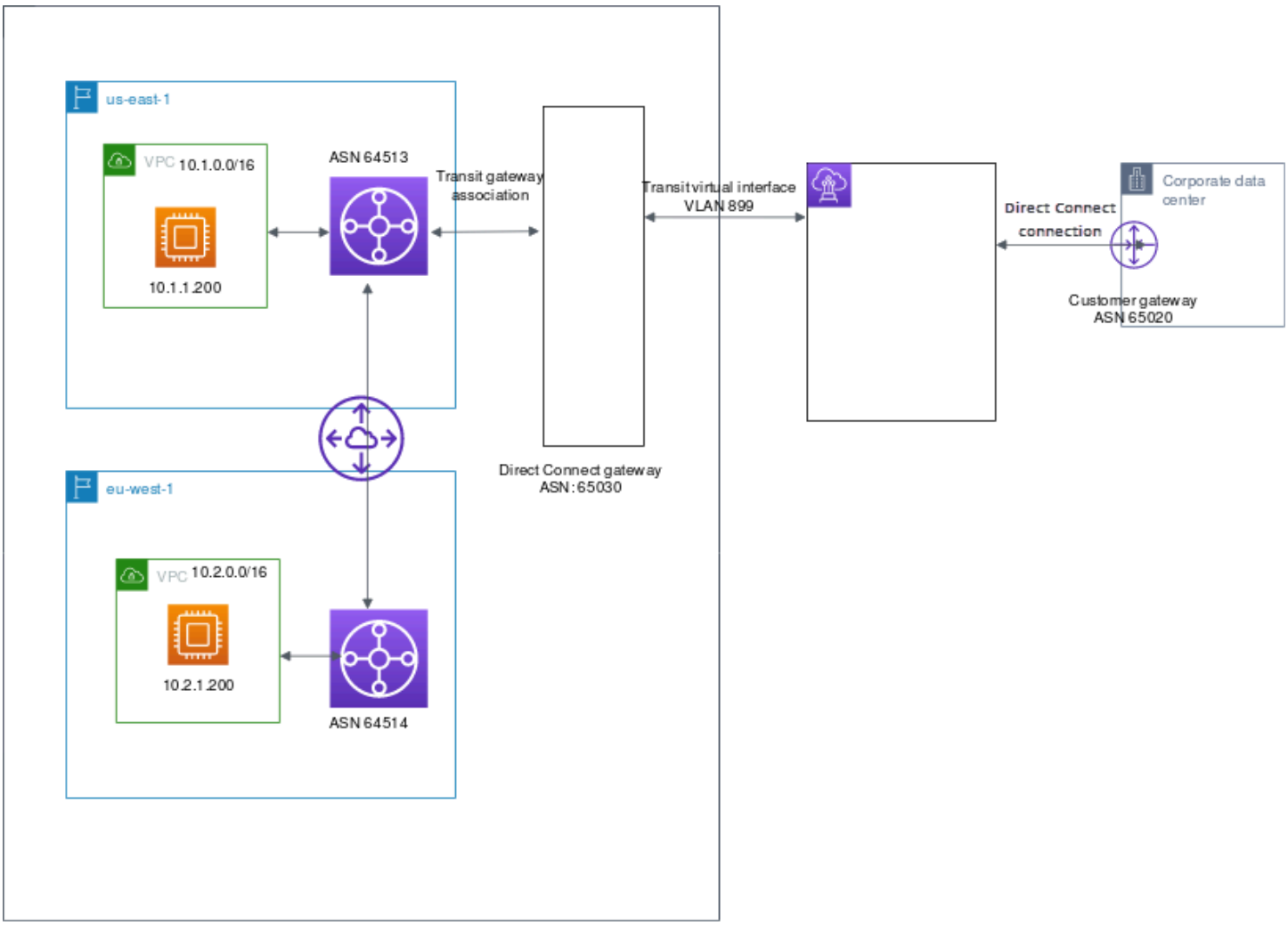
当多个中转网关与 Direct Connect 网关关联时，不允许出现允许的前缀重叠。例如，如果您有一个中转网关的允许前缀列表包含 10.1.0.0/16，而第二个中转网关的允许前缀列表包含 10.2.0.0/16 和 0.0.0.0/0，则您不能将第二个中转网关的关联设置为 0.0.0.0/0。由于 0.0.0.0/0 包括所有 IPv4 网络，因此如果多个中转网关与 Direct Connect 网关关联，则无法配置 0.0.0.0/0。系统将返回错误消息，表示允许的路由与 Direct Connect 网关上的一个或多个现有的允许路由重叠。

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 AWS 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the section called “创建 Direct Connect 网关”：
- 中转虚拟接口： 将 VLAN 设置为 899，将 ASN 设置为 65020。有关更多信息，请参阅the section called “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 块涵盖两个 VPC CIDR 块。有关更多信息，请参阅the section called “关联和解除关联中转网关”：
- VPC 路由：要路由来自 10.2.0.0 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。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。

# 为 AWS Direct Connect 资源添加标签

标签是资源拥有者分配给其 AWS Direct Connect 资源的签条。每个标签都包含您定义的一个键和一个可选值。标签可让资源拥有者按不同方式（例如，按用途或环境）对 AWS 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 AWS Direct Connect 连接，每个连接处于不同的位置。连接 dxcon-11aa22bb 是服务生产流量的连接，与虚拟接口 dxvif-33cc44dd 相关联。连接 dxcon-abcabcab 是冗余（备份）连接，与虚拟接口 dxvif-12312312 相关联。您可以选择用以下方式为连接和虚拟接口添加标签来进行区分：

| 资源 ID | 标记密钥 | 标记值 |
| --- | --- | --- |
| dxcon-11aa22bb | 目的 | 生产 |
| | 位置 | 阿姆斯特丹 |
| dxvif-33cc44dd | 目的 | 生产 |
| dxcon-abcabcab | 目的 | 备份 |
| | 位置 | 法兰克福 |
| dxvif-12312312 | 目的 | 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 AWS 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 AWS Direct Connect 控制台、AWS Direct Connect API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS SDK 标记以下 AWS 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 | 是 | 是 | 是 | 是 |
| 虚拟接口 | 是 | 是 | 是 | 否 |
| 链接聚合组 (LAG) | 是 | 是 | 是 | 是 |
| 互连 | 是 | 是 | 是 | 是 |
| Direct Connect 网关 | 否 | 否 | 否 | 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：+ - = . _ : / @
- 只有资源拥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 Billing and Cost Management 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
```

# AWS Direct Connect 中的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS负责保护在AWS云中运行AWS服务的基础设施。AWS还向您提供可安全使用的服务。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。要了解适用于 AWS Direct Connect 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 AWS Direct Connect 时应用责任共担模型 以下主题说明如何配置 AWS Direct Connect 以实现您的安全性和合规性目标。您还会了解如何使用其它 AWS 服务以帮助您监控和保护 AWS Direct Connect 资源。

主题



## AWS Direct Connect 中的数据保护

AWS 责任共担模式适用于 AWS 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 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。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 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 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。我们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 和用户活动日志记录。
- 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。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 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 140-2 版》。

我们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 AWS 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，我们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

- AWS Direct Connect 中的互联网络流量隐私
- 传输过程中加密 AWS Direct Connect

# AWS Direct Connect 中的互联网络流量隐私

## 服务与本地客户端和应用之间的流量

私有网络和 AWS 之间有两种连接方式：

- 与 AWS Site-to-Site VPN 的关联。有关更多信息，请参阅the section called “基础设施安全性”。
- 与 VPC 的关联。有关更多信息，请参阅 the section called “虚拟私有网关关联” 和 the section called “中转网关关联”：

### 同一区域中 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the section called “基础设施安全性”。
- 与 VPC 的关联。有关更多信息，请参阅 the section called “虚拟私有网关关联” 和 the section called “中转网关关联”：

## 传输过程中加密 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。要了解有关 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，并提供更一致的网络体验。有关更多信息，请参阅 Amazon VPC 到 Amazon VPC 连接选项。

MAC 安全（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 的 AWS Direct Connect 连接来加密从公司数据中心到该 AWS Direct Connect 位置的数据。有关更多信息，请参阅 MAC 安全。

# 适用于 Direct Connect 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。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。IAM 是一项无需额外费用即可使用的 AWS 服务。

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
- AWS Direct Connect 的服务相关角色

- 适用于 AWS Direct Connect 的 AWS 托管式策略
- Direct Connect 身份和访问问题排查

## 受众

使用 AWS Identity and Access Management（IAM）的方式因您可以在 Direct Connect 中执行的操作而异。

服务用户：如果您使用 Direct Connect 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Direct Connect 功能来完成工作时，您可能需要更多权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Direct Connect 中的功能，请参阅 Direct Connect 身份和访问问题排查。

服务管理员：如果您在公司负责管理 Direct Connect 资源，您可能拥有对 Direct Connect 全部访问权限。您有责任确定您的服务用户应访问哪些 Direct Connect 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Direct Connect 结合使用的更多信息，请参阅 Direct Connect 如何与 IAM 结合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望详细了解如何编写策略来管理对 Direct Connect 的访问。要查看可在 IAM 中使用的 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。

## 使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过担任 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center(IAM Identity Center) 用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接担任角色。

根据用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的如何登录到 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS 中使用多重身份验证 (MFA)。

### AWS 账户 根用户

创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

### 联合身份

作为最佳实操，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、网络身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份源提供的凭证来访问 AWS 服务 的用户。当联合身份访问 AWS 账户时，他们担任角色，而角色提供临时凭证。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到自己的身份源中的一组用户和组以跨所有 AWS 账户 和应用程序使用。有关 IAM Identity Center 的信息，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 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用群组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用群组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人担任。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

## IAM 角色

IAM 角色是 AWS 账户 中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时担任 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义网址以代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为座席）。要了解用于跨账户存取的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 - 某些 AWS 服务使用其他 AWS 服务中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的政策详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而担任的 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。
  - 服务相关角色 - 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 - 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文

件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

## 使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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。

默认情况下，用户和角色没有权限。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。然后，管理员可以向角色添加 IAM 策略，并且用户可以担任角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

### 基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户群组或角色）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》中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、群组或角色中。托管策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户管理型策略。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。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。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

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来自 IAM 的 AWS 托管策略。

### 访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表 (ACL) 概览。

### 其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可以为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 - 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。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 AWS 如何确定在涉及多种策略类型时是否允许请求，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 特征 | 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 |
| 策略资源 | 可以 |
| 策略条件键（特定于服务） | 可以 |
| ACL | 否 |
| ABAC（策略中的标签） | 部分 |
| 临时凭证 | 是 |
| 主体权限 | 可以 |
| 服务角色 | 可以 |
| 服务相关角色 | 不可以 |

要大致了解 Direct Connect 和其他 AWS 服务如何与大多数 IAM 功能结合使用，请参阅《IAM 用户指南》中的与 IAM 结合使用的 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》中的创建 IAM 策略。

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。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。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。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，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。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 AWS 账户 中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

## 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内容。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。策略操作通常与相关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

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《服务授权参考》中的 Direct Connect 定义的操作。

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": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

## 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内容。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。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN)指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），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 ARN 列表，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 | 可以 |

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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。

在 Condition 元素（或 Condition 块）中，您可以指定语句生效的条件。Condition 元素是可选的。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。

如果在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个密钥，则 AWS 使用逻辑 AND 运算评估它们。如果您要为单个条件密钥指定多个值，则 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

您也可以在指定条件时使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

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。要了解可以使用条件键的操作和资源，请参阅《服务授权参考》中的 Direct Connect 的操作、资源和条件密钥。

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 中的 ACL

| | |
|---|---|
| 支持 ACL | 否 |

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 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 |

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 AWS 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件密钥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密钥，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密钥，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的什么是 ABAC？。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 | 可以 |

某些 AWS 服务 在使用临时凭证登录时无法正常工作。有关更多信息，包括 AWS 服务 与临时凭证配合使用，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。

如果您不使用用户名和密码而用其他方法登录到AWS Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

## Direct Connect 的跨服务主体权限

| | |
|---|---|
| 支持转发访问会话（FAS） | 可以 |

当您使用 IAM 用户或角色在AWS中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求

的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的政策详情，请参阅转发访问会话。

### Direct Connect 的服务角色

| | |
|---|---|
| 支持服务角色 | 可以 |

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 | 不可以 |

服务相关角色是一种与 AWS 服务相关的服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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 Yes 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。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。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 policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

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 policy。

有关 Direct Connect 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 Direct Connect 的操作、资源和条件键。

主题

- 策略最佳实操
- 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
- 对 AWS Direct Connect 的只读访问权限
- 对 AWS Direct Connect 的完全访问权限
- Direct Connect 基于身份的策略示例（使用基于标签的条件）

## 策略最佳实操

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，请遵循以下准则和建议：

- AWS 托管式策略及转向最低权限许可入门——要开始向用户和工作负载授予权限，请使用 AWS 托管式策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。建议通过定义特定于您的使用场景的 AWS 客户管理型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 托管式策略或工作职能的 AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 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 policy 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。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。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 policy，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 policy 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，有助于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 IAM Access Analyzer 策略验证。
- 需要多重身份验证 (MFA) – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，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内容。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。策略操作通常与相关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

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。

以下示例策略授予针对 AWS Direct Connect 的读取权限。

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

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

```
{
```

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

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内容。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。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN)指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Direct Connect 使用以下 ARN：

Direct Connect 资源 ARN

| 资源类型 | ARN |
| --- | --- |
| dxcon | `arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}` |
| dxlag | `arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}` |

| 资源类型 | ARN |
| --- | --- |
| dx-vif | `arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}` |
| dx-gateway | `arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}` |

有关 ARN 格式的更多信息，请参阅 Amazon 资源名称 (ARN) 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 ARN 列表，请参阅《IAM 用户指南》中的 AWS Direct Connect 定义的资源类型。要了解您可以使用哪些操作指定每个资源的 ARN，请参阅 SERVICE-ACTIONS-URL。

条件键

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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。

在 Condition 元素（或 Condition 块）中，您可以指定语句生效的条件。Condition 元素是可选的。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。

如果在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个密钥，则 AWS 使用逻辑 AND 运算评估它们。如果您要为单个条件密钥指定多个值，则 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

您也可以在指定条件时使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

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 全局条件上下文键。

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 SERVICE-ACTIONS-URL。

## 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 Direct Connect 资源（位于您的 AWS 账户中）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。

要确保这些实体仍可使用 Direct Connect 控制台，也可向实体附加以下 AWS 托管式策略。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

```
directconnect
```

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。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策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "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": "*"
        }
    ]
}
```

## 对 AWS Direct Connect 的只读访问权限

以下示例策略授予针对 AWS Direct Connect 的读取权限。

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

```
            "Resource": "*"
        }
    ]
}
```

## 对 AWS Direct Connect 的完全访问权限

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

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

## 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。

```
       {
      "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

您可以在 IAM 策略中使用条件，来控制可以在标记 AWS 资源的请求中传递哪些标记键值对。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AWS 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。

```
    {
        "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

```
    {
     "Version": "2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "directconnect:TagResource",
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringEquals": {
           "aws:TagKeys": [
             "environment"
           ]
         }
       }
     }
   }
```

## AWS Direct Connect 的服务相关角色

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独特类型的 IAM 角色，它与 AWS Direct Connect 直接相关。服务相关角色由 AWS Direct Connect 预定义，并包含该服务代表您调用其他 AWS 服务所需的一切权限。

服务相关角色使 AWS Direct Connect 的设置更轻松，因为您不必手动添加必要的权限。AWS Direct Connect 定义其服务相关角色的权限，除非另行定义，否则仅 AWS Direct Connect 可以代入其角色。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它 IAM 实体的权限策略。

只有在首先删除相关资源后，才能删除服务相关角色。这将保护您的 AWS Direct Connect 资源，因为您不会无意中删除对资源的访问权限。

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 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

## AWS Direct Connect 的服务相关角色权限

AWS Direct Connect 使用名为 AWSServiceRoleForDirectConnect 的服务相关角色。这允许 AWS Direct Connect 代表您检索存储在 AWS Secrets Manager 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。

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。为了成功创建 AWSServiceRoleForDirectConnect 服务相关角色，用于 AWS 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。

```
{
    "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 用户指南中的服务相关角色权限。

## 为 AWS Direct Connect 创建服务相关角色

您无需手动创建服务相关角色。AWS Direct Connect 会为您创建服务相关角色。运行 `associate-mac-sec-key` 命令时，AWS 将创建一个服务相关角色，该角色允许 AWS Direct Connect 代表您在 AWS Management Console、AWS CLI 或 AWS API 中检索存储在 AWS Secrets Manager 中的 MACsec 密钥。

> **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，此服务相关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 账户中出现新角色。

如果您删除此服务相关角色，然后需要再次进行创建，则可以使用相同的过程在您的账户中重新创建此角色。AWS Direct Connect 将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 `directconnect.amazonaws.com` 服务名称创建服务相关角色。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，则可以使用此相同过程再次创建角色。

## 为 AWS Direct Connect 编辑服务相关角色

AWS 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相关角色。

## 删除 AWS Direct Connect 的服务相关角色

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。在 AWS Management Console、AWS CLI 或 AWS API 中，AWS Direct Connect 会为您清理资源并删除服务相关角色。

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**
>
> 如果在您尝试删除资源时，AWS Direct Connect 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟，然后再次尝试操作。

删除 **AWSServiceRoleForDirectConnect** 所用的 AWS Direct Connect 资源

1. 删除所有 MACSec 密钥和连接之间的关联。有关更多信息，请参阅the section called “删除 MACsec 密钥和连接之间的关联”。
2. 删除所有 MACSec 密钥和 LAG 之间的关联。有关更多信息，请参阅the section called “删除 MACsec 密钥和 LAG 之间的关联”。

使用 IAM 手动删除 服务相关角色

使用 IAM 控制台，即 AWS CLI 或 AWS API 来删除 `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相关角色。

### AWS Direct Connect 服务相关角色的受支持区域

AWS Direct Connect 支持在 MAC 安全功能可用的所有 AWS 区域 使用服务相关角色。有关更多信息，请参阅 AWS Direct Connect 地点。

## 适用于 AWS Direct Connect 的 AWS 托管式策略

AWS 托管策略是由 AWS 创建和管理的独立策略。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使用场景授予最低权限，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 托管式策略中定义的权限。如果 AWS 更新在 AWS 托管策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

### 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 AWS Direct Connect 的权限。

要查看此策略的权限，请参阅 AWS Management Console 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 AWS Direct Connect 的权限。

要查看此策略的权限，请参阅 AWS Management Console 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AWS Direct Connect代表您检索 MAC Security 机密。有关更多信息，请参阅the section called “服务相关角色”：

要查看此策略的权限，请参阅 AWS Management Console 中的 AWSDirectConnectServiceRolePolicy。

### AWS Direct Connect 更新了 AWS 托管策略

查看有关 AWS Direct Connect 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 AWS Direct Connect 文档历史记录页面上的 RSS 源。

| 更改 | 说明 | 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 |
| AWS Direct Connect 开启了跟踪更改 | AWS Direct Connect 对其 AWS 托管式策略开启了跟踪更改。 | 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
- 我希望允许我的 AWS 账户 以外的人员访问我的 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，表明您无权执行某个操作，则您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 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 允许将现有角色传递到该服务，而不是创建新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 AWS 管理员。您的管理员是提供登录凭证的人。

## 我希望允许我的 AWS 账户 以外的人员访问我的 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 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

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。
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅《IAM 用户指南》中的为您拥有的另一个 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 账户 提供您的资源的访问权限，请参阅《IAM 用户指南》中的为第三方拥有的 AWS 账户 提供访问权限。
- 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 角色与基于资源的策略有何不同。

# 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 AWS 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 AWS CloudTrail 记录 AWS Direct Connect API 调用 和使用 CloudTrail 日志文件。

有关更多信息，请参阅监控。

# 合规性验证 AWS Direct Connect

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

# AWS Direct Connect 中的故障恢复能力

AWS全球基础设施围绕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设施相比，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，AWS 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，请参阅使用 AWS Direct Connect 弹性工具包入门。

## AWS Direct Connect 中的基础设施安全性

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 AWS 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 委托人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 AWS 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 AWS 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 AWS 网络中仅从特定 VPC 到给定 AWS Direct Connect 资源的网络访问。有关示例，请查看 the section called “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 AWS CLI

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

以下示例使用 AWS CLI 命令创建 AWS Direct Connect 连接。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。

目录



## 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 AWS Direct Connect 位置。有关更多信息，请参阅AWS Direct Connect 连接。

创建连接请求

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

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "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 directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

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

下载 LOA-CFA 之后，将其发送到网络提供商或主机托管提供商。

# 步骤 3：创建虚拟接口，获取路由器配置

订购 AWS Direct Connect 连接以后，您必须创建虚拟接口以开始使用。您可以创建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 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 AWS 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-xxxxxxxx)。您需要该 ID 在下一步创建虚拟接口。

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

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

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

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

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

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

```
}
```

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

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

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

创建公有虚拟接口

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

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

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{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,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

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

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

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

# 使用 AWS CloudTrail 记录 AWS Direct Connect API 调用

AWS Direct Connect 与 AWS CloudTrail 集成，后者是在 AWS 中记录用户、角色或 AWS Direct Connect 服务所执行操作的服务。CloudTrail 将 AWS Direct Connect 的所有 API 调用作为事件捕获。捕获的调用包含来自 AWS Direct Connect 控制台和代码的 AWS Direct Connect API 操作调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 AWS Direct Connect 的事件）。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 AWS Direct Connect 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

有关更多信息，请参阅 AWS CloudTrail 用户指南。

## CloudTrail 中的 AWS Direct Connect 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 AWS Direct Connect 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在 Event history (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 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 AWS Direct Connect 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 AWS Direct Connect 操作，AWS Direct Connect API 参考中介绍了这些操作。例如，对 `CreateConnection` 和 `CreatePrivateVirtualInterface` 操作的调用会在 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。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM 用户）凭证发出的。

- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail `userIdentity` 元素。

# 了解 AWS Direct Connect 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下是 AWS Direct Connect 的 CloudTrail 日志记录示例。

Example 示例：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 示例：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 示例：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 示例：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-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

# 监控 AWS Direct Connect 资源

监控是维护 Direct Connect 资源的可靠性、可用性和性能的重要组成部分。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对其进行调试。但是，在开始监控 Direct Connect 之前，您应该创建一个包含以下问题答案的监控计划：

- 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？

下一步是通过测量不同时间和不同负载条件下的性能，为环境中的正常 Direct Connect 性能建立基准。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，您应该监控物理 Direct Connect 连接的使用情况、状态和运行状况。

内容



## 监控工具

AWS 提供了可用于监控 AWS 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监控工具来监视 Direct Connect 并在出现问题时进行报告：

- 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 用户指南中的使用 AWS CloudTrail 记录 AWS Direct Connect API 调用和使用 CloudTrail 日志文件。

## 手动监控工具

监控 AWS 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 AWS 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 AWS 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。

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



# AWS Direct Connect 指标和维度

AWS Direct Connect 物理连接和虚拟接口的指标可用。

## AWS Direct Connect 连接指标

Direct Connect 专用连接提供了以下指标。

| 指标 | 描述 |
| --- | --- |
| ConnectionState | 连接的状态。1 表示运行，0 表示关闭。<br><br>此指标适用于专用连接和托管连接。<br><br>**Note**<br>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。<br><br>单位：布尔值 |
| ConnectionBpsEgress | 来自连接 AWS 端的出站数据的比特率。<br><br>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。<br><br>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。<br><br>单位：每秒比特数 |
| ConnectionBpsIngress | 连接 AWS 侧入站数据的比特率。 |

| 指标 | 描述 |
| --- | --- |
| | 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。<br><br>单位：每秒比特数 |
| ConnectionPpsEgress | 来自连接 AWS 端的出站数据的数据包速率。<br><br>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。<br><br>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。<br><br>单位：每秒数据包数 |
| ConnectionPpsIngress | 连接 AWS 侧入站数据的数据包速率。<br><br>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。<br><br>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。<br><br>单位：每秒数据包数 |
| ConnectionCRCErrorCount | 此计数不再使用。请改用 ConnectionErrorCount 。 |

| 指标 | 描述 |
| --- | --- |
| ConnectionErrorCount | AWS 设备上所有类型的 MAC 级别错误的总错误计数。总数包括循环冗余检查 (CRC) 错误。<br><br>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。有关获取总和统计数据的更多信息，请参阅 Amazon CloudWatch 用户指南中的获取指标的统计数据。<br><br>当接口上的错误停止时，指标值设置为 0。<br><br>**Note**<br>此指标会替换 ConnectionCRCError Count ，不再使用。<br><br>单位：计数 |
| ConnectionLightLevelTx | 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。<br><br>此指标有两个维度。有关更多信息，请参阅the section called “AWS Direct Connect 可用尺寸”。<br><br>单位：dBm |
| ConnectionLightLevelRx | 指示流向连接 AWS 侧的入站（入口）流量的光纤连接的运行状况。<br><br>此指标有两个维度。有关更多信息，请参阅the section called “AWS Direct Connect 可用尺寸”。<br><br>单位：dBm |

| 指标 | 描述 |
| --- | --- |
| 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。 |

## AWS Direct Connect 虚拟接口指标

以下指标可从 AWS Direct Connect 虚拟接口获得。

| 指标 | 描述 |
| --- | --- |
| VirtualInterfaceBpsEgress | 来自虚拟接口 AWS 一侧的出站数据的比特率。<br><br>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。<br><br>单位：每秒比特数 |
| VirtualInterfaceBpsIngress | 虚拟接口 AWS 一侧的入站数据的比特率。<br><br>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。<br><br>单位：每秒比特数 |
| VirtualInterfacePpsEgress | 来自虚拟接口 AWS 一侧的出站数据的数据包速率。<br><br>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。<br><br>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。<br><br>报告的数量是指定时间段（默认为 5 分钟）内的聚合（平均值）。 |

| 指标 | 描述 |
| --- | --- |
| | 单位：每秒数据包数 |

### AWS Direct Connect 可用尺寸

您可以使用以下维度筛选 AWS Direct Connect 数据。

| 维度 | 描述 |
| --- | --- |
| ConnectionId | 此维度在 Direct Connect 连接和虚拟接口的指标中可用。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 Direct Connect 连接的光纤通道号筛选数据。 |
| VirtualInterfaceId | 此维度在 Direct Connect 虚拟接口的指标中可用，并按虚拟接口筛选数据。 |

## 查看 AWS Direct Connect CloudWatch 指标

AWS Direct Connect 发送有关您的 Direct Connect 连接的以下指标。 CloudWatch然后，Amazon 将这些数据点聚合为 1 分钟或 5 分钟的时间间隔。默认情况下，Direct Connect 指标数据每隔 5 分钟写入 CloudWatch 一次。

> **Note**
>
> 如果您设置了 1 分钟的时间间隔，Direct Connect 将尽最大努力 CloudWatch 使用此间隔写入指标，但不能始终保证。

您可以使用以下过程查看 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《亚马逊 CloudWatch 用户指南》中的使用 Amazon CloudWatch 指标。

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
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该指标：
   - 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 指标见解查询您的指标。

使用 AWS Direct Connect 控制台查看指标

1. 打开AWS Direct Connect控制台，网址为 https://console.aws.amazon.com/directconnect/v2/home。
2. 在导航窗格中，选择 Connections (站点到站点 VPN 连接)。
3. 选择连接。
4. 选择监控选项卡以显示连接的指标。

要查看指标，请使用 AWS CLI

在命令提示符处，使用以下命令。

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

# 创建 CloudWatch 警报以监控 AWS Direct Connect 连接

您可以创建一个 CloudWatch 警报，在警报状态发生变化时发送 Amazon SNS 消息。告警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 AWS 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。要详细了解如何创建警报以及有关创建警报的更多信息，请参阅《亚马逊 CloudWatch 用户指南》中的 “使用亚马逊 CloudWatch 警报”。

创建 CloudWatch 警报。

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
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 AWS 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，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 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。

# AWS Direct Connect 配额

下表列出了与相关的配额 AWS Direct Connect。

| 组件 | 限额 | 注释 |
| --- | --- | --- |
| 每个 AWS Direct Connect 专用连接的私有或公有虚拟接口 | 50 | 不能提高此限制。 |
| 每个 AWS Direct Connect 专用连接的传输虚拟接口 | 4 | 不能提高此限制。 |
| 每个专用连接的私有或公有虚拟接口以及每个 AWS Direct Connect AWS Direct Connect 专用连接的传输虚拟接口 | 51 | 启动对 Amazon VPC Transit Gateways 的 AWS Direct Connect 支持时，在每个专用连接 50 个私有或公有虚拟接口的配额中，增加了一 (1) 个传输虚拟接口的配额。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 AWS Direct Connect 托管连接的私有、公共或传输虚拟接口 | 1 | 不能提高该限制。 |
| 每个账户每个地区每个 Direct Connect 位置的活跃 AWS 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 传输网关的 AWS Direct Connect 支持时，在每个 LAG 的 50 个私有或公有虚拟接口的配额中，增加了一 (1) 个传输虚拟接口的配额。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。 |
| 私有虚拟接口上每个边界网关协议 (BGP) 会话的路由，或者从本地到 AWS的中转虚拟接口。 | IPv4 和 IPv6 各 100 个 | 不能提高此限制。 |

| 组件 | 限额 | 注释 |
| --- | --- | --- |
| 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。 | | |
| 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<br><br>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)。 |
| AWS Direct Connect 每个账户的网关 | 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)。 |
| 每个网关的虚拟专用 AWS Direct Connect 网关 | 20 | 不能提高此限制。 |
| 每个网关的中转 AWS Direct Connect 网关 | 6 | 不能提高此限制。 |
| 每个 AWS Direct Connect 网关的虚拟接口（私有接口或传输接口） | 30 | 不能提高此限制。 |
| 在传输虚拟接口上，每个 AWS Transit Gateway 从 AWS 到本地的前缀数量 | IPv4 和 IPv6 共 200 个 | 不能提高此限制。 |

| 组件 | 限额 | 注释 |
| --- | --- | --- |
| 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)。 |

AWS Direct Connect 通过单模光纤支持以下端口速度：1 Gbps：1000BASE-LX（1310 nm）、10 Gbps：10Gbase-LR（1310 nm）和 100Gbps：100GBASE-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

# 负载平衡注意事项

如果要对多个公有 VIF 使用负载平衡，则所有 VIF 必须位于同一个区域中。

# 故障排除 AWS Direct Connect

以下问题排查信息可以帮助您诊断和解决 AWS Direct Connect 连接问题。

目录

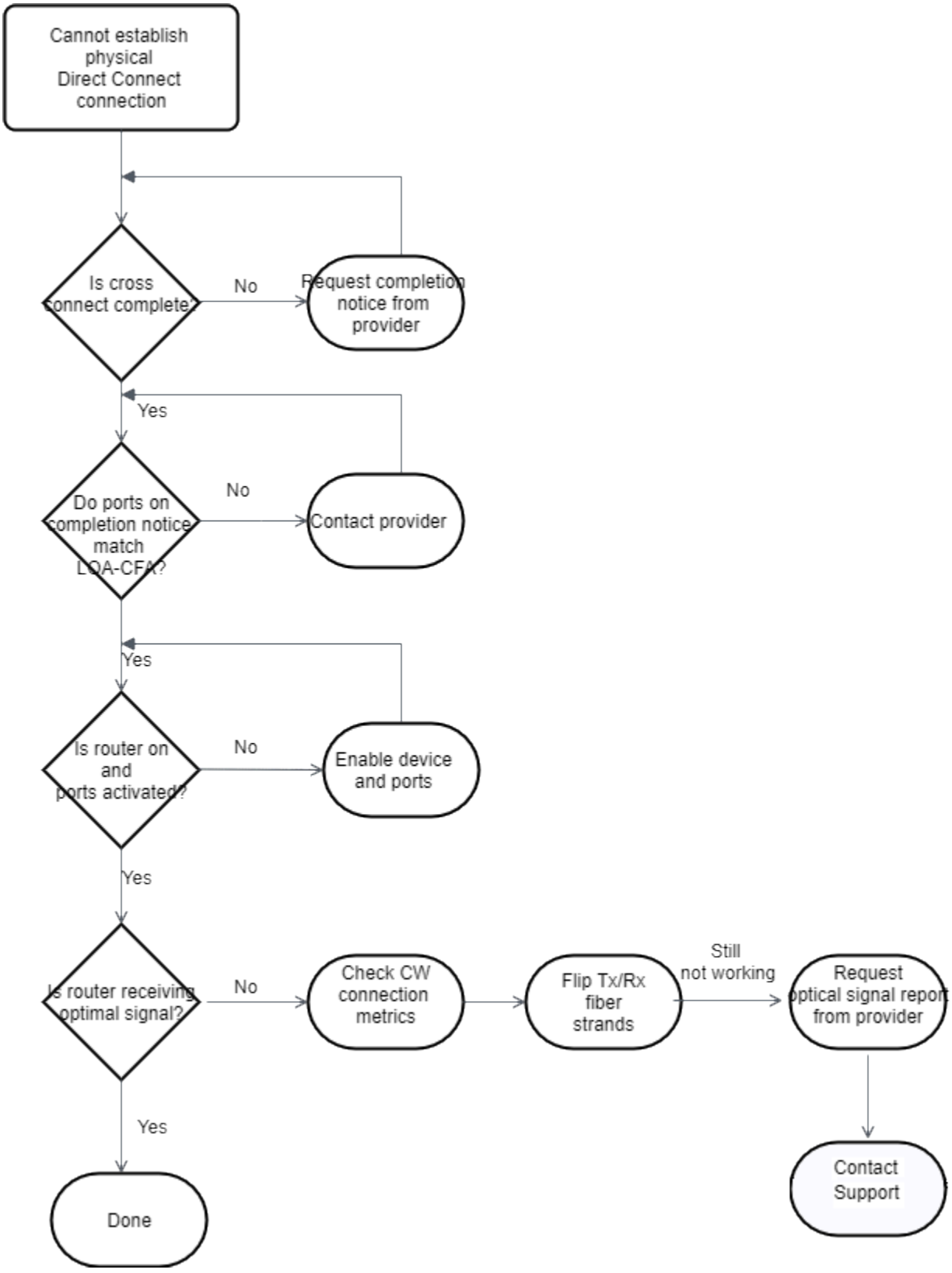


## 排查第 1 层（物理）问题

如果您或您的网络提供商在与 AWS Direct Connect 设备建立物理连接时遇到困难，请使用以下步骤对问题进行故障排除。

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，根据为您的连接提供服务的 Di AWS rect Connect 端点，可能需要为 1 Gbps 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。
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. 请查看 Amazon 的 CloudWatch 指标 AWS Direct Connect。您可以验证 AWS 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 进行监控 CloudWatch。
7. 联系主机托管提供商并请求跨交叉连接的 Tx/Rx 光信号的书面报告。
8. 如果上述步骤未解决物理连接问题，请联系 AWS Support 并提供来自主机托管提供商的交叉连接完成通知和光信号报告。

以下流程图包含诊断物理连接问题的步骤。

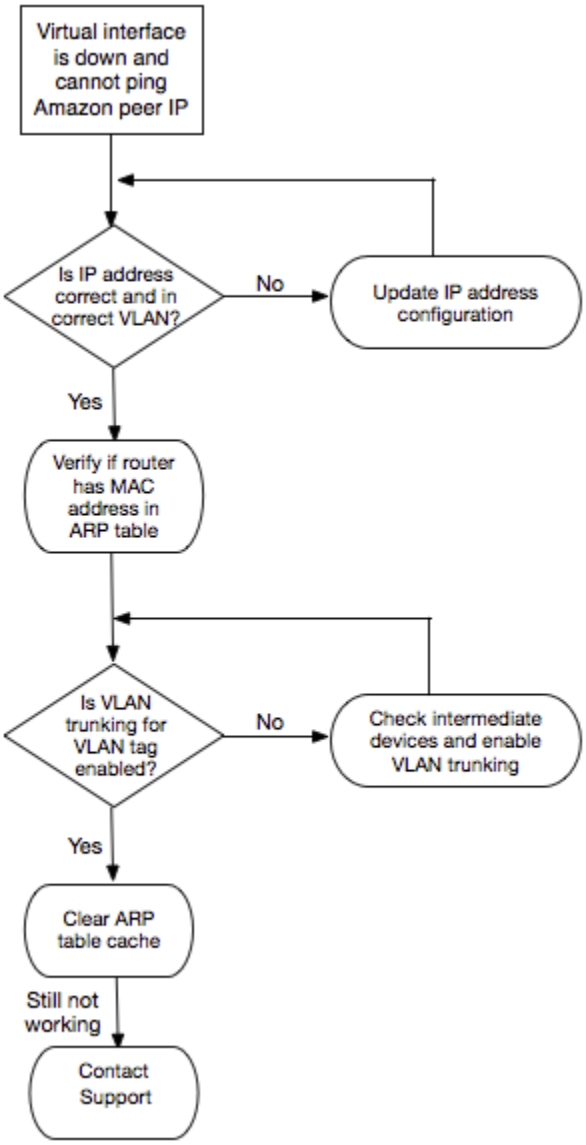

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

# 排查第 2 层（数据链路）问题

如果您的 AWS Direct Connect 物理连接已开启，但虚拟接口已关闭，请使用以下步骤来解决问题。

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中配置 IP 地址（例如，使用 GigabitEthernet 0/0.123 而不是 0/0）。 GigabitEthernet
2. 验证路由器在地址解析协议 (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 收到标记流量之前，无法在 AWS 侧面建立 ARP。
4. 清除您或您的提供商的 ARP 表缓存。
5. 如果上述步骤无法建立 ARP，或者您仍然无法 ping 亚马逊对等 IP，请联系 Su AWS pp ort。

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。

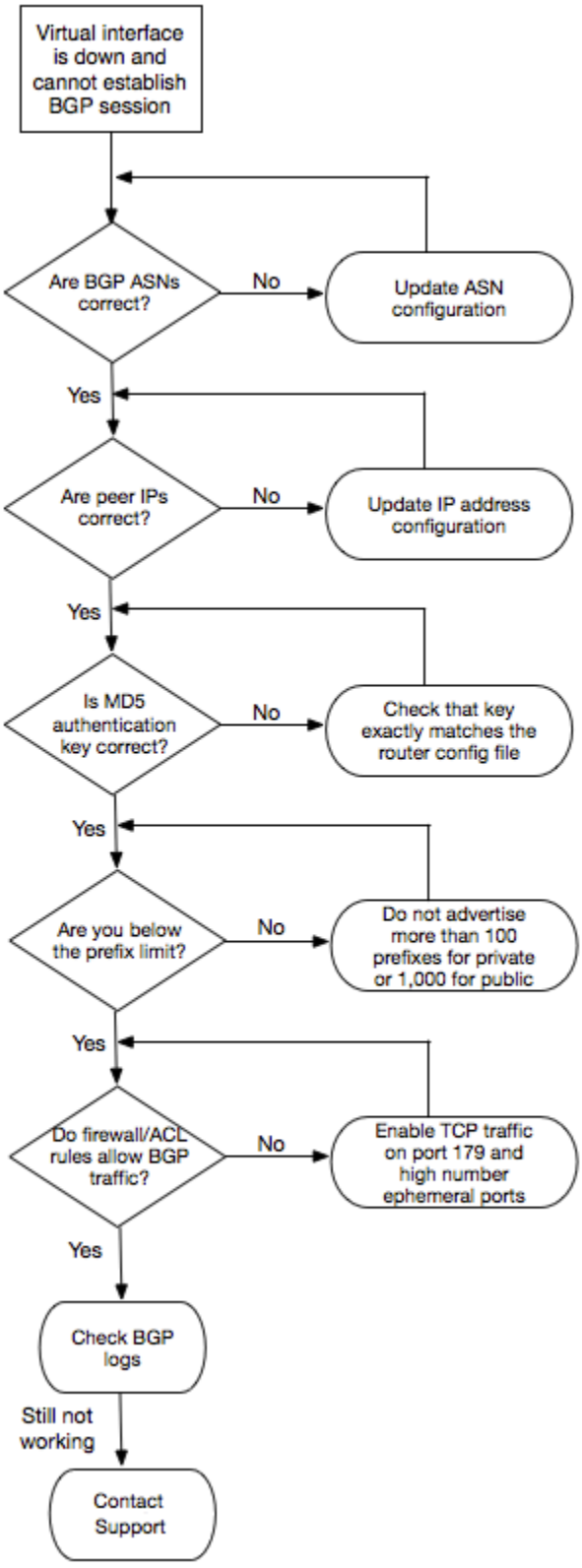
# 排查第 3/4 层（网络/传输）问题

考虑一下这样的情况：您的 AWS Direct Connect 物理连接已开启，您可以 ping 亚马逊对等 IP 地址。如果您的虚拟接口已关闭且 BGP 对等会话无法建立，请使用以下步骤排查该问题：

1. 确保您的 BGP 本地自治系统编号 (ASN) 和 Amazon 的 ASN 已正确配置。
2. 确保 BGP 对等会话两端的对等 IP 已正确配置。

3. 确保您的 MD5 身份验证密钥已配置且与下载的路由器配置文件中的密钥完全匹配。检查是否有多余的空格或字符。
4. 验证您或您的提供商是否没有为私有虚拟接口公布超过 100 个前缀或为公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. 如果上述步骤未能建立 BGP 对等会话，请联系 Su pp AWS ort。

以下流程图包含诊断 BGP 对等会话问题的步骤。



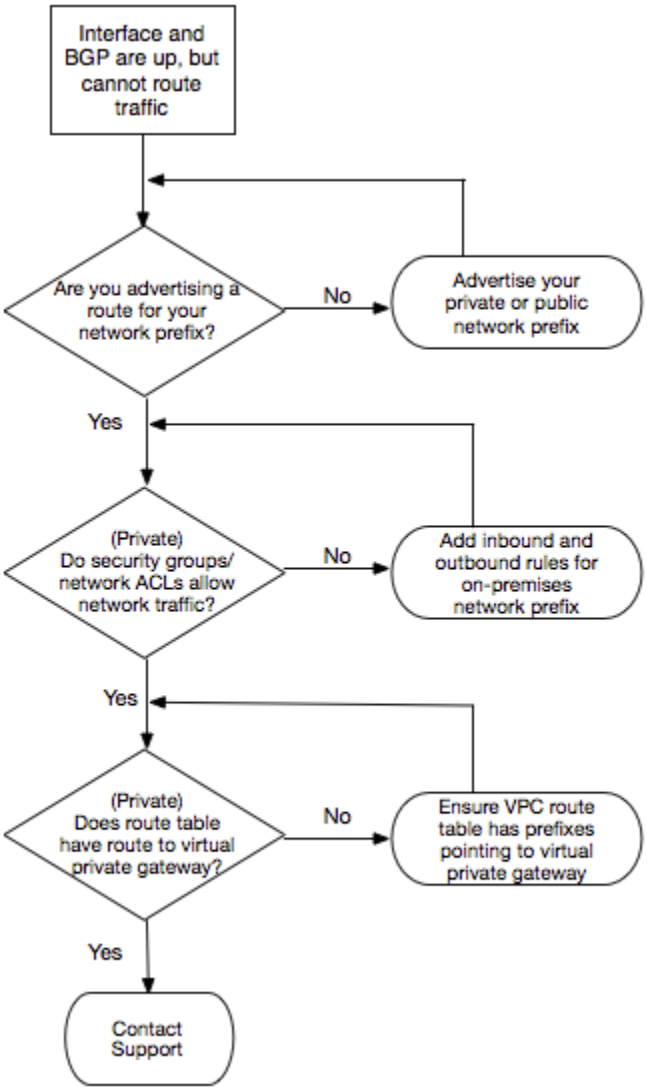

如果已建立 BGP 对等会话但您遇到了路由问题，请参阅排查路由问题。

# 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. 如果上述步骤不能解决您的路由问题，请联系 Su AWS pport。

以下流程图包含诊断路由问题的步骤。


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

# 文档历史记录

下表介绍了 AWS Direct Connect 的版本。

| 功能 | 说明 | 日期 |
| --- | --- | --- |
| Support SiteLink | 您可以创建一个虚拟专用接口，以便在同一AWS区域的两个 Direct Connect 接入点 (PoPs) 之间实现连接。有关更多信息，请参阅 托管的虚拟接口。 | 2021-12-01 |
| 支持 MAC 安全 | 您可以使用支持 MACsec 的 AWS Direct Connect 连接，来加密从公司数据中心到 AWS Direct Connect 位置的数据。有关更多信息，请参阅MAC 安全： | 2021-03-31 |
| 支持 100G | 更新了主题，涵盖对 100G 专用连接的支持。 | 2021-02-12 |
| 意大利的新增位置 | 更新了主题，包含意大利的新增位置。有关更多信息，请参阅the section called “欧洲地区（米兰）”： | 2021-01-22 |
| 以色列的新增位置 | 更新了主题，包含以色列的新增位置。有关更多信息，请参阅the section called “以色列（特拉维夫）”： | 2020-07-07 |
| 弹性工具包故障转移测试支持 | 使用弹性工具包故障转移测试功能可以测试连接的弹性。有关更多信息，请参阅the section called “AWS Direct Connect 故障转移测试”： | 2020-06-03 |
| CloudWatch VIF 指标支持 | 您可以使用监控物理AWS Direct Connect连接和虚拟接口 CloudWatch。有关更多信息，请参阅the section called “使用 Amazon 进行监控 CloudWatch”： | 2020-05-11 |
| 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。有关更多信息，请参阅使用 AWS Direct Connect 弹性工具包入门： | 2019-10-07 |
| 针对账户之间的 AWS Transit | 有关信息，请参阅 the section called “中转网关关联”。 | 2019-09-30 |

| 功能 | 说明 | 日期 |
| --- | --- | --- |
| Gateway 的额外区域支持 | | |
| AWS Direct Connect 对于 AWS Transit Gateway的支持 | 您可以使用 AWS Direct Connect 网关 将 AWS Direct Connect 连接通过中转虚拟接口连接到已附加到中转网关的 VPC 或 VPN。首先，您将 Direct Connect 网关与中转网关关联。然后，为 AWS Direct Connect 连接创建到 Direct Connect 网关的中转虚拟接口。有关信息，请参阅 the section called “中转网关关联”。 | 2019-03-27 |
| 巨型帧支持 | 您可以通过 AWS Direct Connect 发送巨型帧 (9001 MTU)。有关更多信息，请参阅为私有虚拟接口或中转虚拟接口设置网络 MTU： | 2018-10-11 |
| 本地首选项 BGP 社区 | 您可以使用本地首选项 BGP 社区标签来实现网络传入通信的负载平衡和路由首选项。有关更多信息，请参阅本地首选项 BGP 社区： | 2018-02-06 |
| AWS Direct Connect 网关 | 您可以使用 Direct Connect 网关将您的 AWS Direct Connect 连接到远程区域中的 VPC。有关更多信息，请参阅使用 Direct Connect 网关： | 2017-11-01 |
| 亚马逊 CloudWatch 指标 | 您可以查看AWS Direct Connect连接 CloudWatch 指标。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch： | 2017-06-29 |
| 链接聚合组 | 您可创建一个链接聚合组 (LAG) 来聚合多个 AWS Direct Connect 连接。有关更多信息，请参阅链接聚合组： | 2017-02-13 |
| IPv6 支持 | 您的虚拟接口现在可以支持 IPv6 BGP 对等会话。有关更多信息，请参阅添加或删除 BGP 对等体： | 2016-12-01 |
| 标记支持 | 现在您可以标记您的 AWS Direct Connect 资源。有关更多信息，请参阅为 AWS Direct Connect 资源添加标签： | 2016-11-04 |
| 自助服务 LOA-CFA | 现在，您可以使用 AWS Direct Connect 控制台或 API 下载《授权证书和连接设备分配 (LOA-CFA) 通知函》。 | 2016-06-22 |

| 功能 | 说明 | 日期 |
| --- | --- | --- |
| 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。 | 2016-06-03 |
| 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。 | 2016-05-19 |
| 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。 | 2016-04-27 |
| 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。 | 2015-12-09 |
| 达拉斯、伦敦、硅谷和孟买新增节点 | 更新了主题，增加了在达拉斯（美国东部（弗吉尼亚北部）区域）、伦敦（欧洲（爱尔兰）区域）、硅谷（（美国西部）地区）和孟买 AWS GovCloud （亚太地区（新加坡）区域）和孟买（亚太地区（新加坡）区域）的新增地点。 | 2015-11-27 |
| 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。 | 2015-04-14 |
| 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 AWS Direct Connect 拉斯维加斯地点。 | 2014-11-10 |
| 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 AWS Direct Connect 地点。 | 2014-10-23 |
| 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 AWS Direct Connect 地点。 | 2014-07-14 |
| 支持 AWS CloudTrail | 添加了一个新主题来解释 CloudTrail 如何使用登录活动AWS Direct Connect。有关更多信息，请参阅使用 AWS CloudTrail 记录 AWS Direct Connect API 调用： | 2014-04-04 |

| 功能 | 说明 | 日期 |
| --- | --- | --- |
| 支持访问远程 AWS 区域 | 添加了一个新主题，用于说明如何访问远程区域中的公有资源。有关更多信息，请参阅访问远程 AWS 区域： | 2013-12-19 |
| 支持托管连接 | 更新主题，以涵盖对托管连接的支持。 | 2013-10-22 |
| 欧洲（爱尔兰）区域中新增位置 | 更新了主题，添加了为欧洲（爱尔兰）区域提供服务的新 AWS Direct Connect 位置。 | 2013-06-24 |
| 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 AWS Direct Connect 位置。 | 2013-05-08 |
| 支持 IAM 与 AWS Direct Connect 一起使用 | 添加了关于通过 AWS Direct Connect 使用 AWS Identity and Access Management 的主题。有关更多信息，请参阅the section called “身份和访问管理”： | 2012-12-21 |
| 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 AWS Direct Connect 位置。 | 2012-12-14 |
| 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“AWS Direct Connect User Guide”取代了“AWS Direct Connect Getting Started Guide”。添加了新主题，以涵盖新的 AWS Direct Connect 控制台；添加了计费主题；添加了路由器配置信息；更新了主题以涵盖为美国东部（弗吉尼亚北部）和南美洲（圣保罗）区域提供服务的两个新增 AWS Direct Connect 位置。 | 2012-08-13 |
| 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 AWS Direct Connect 位置。 | 2012-01-10 |

| 功能 | 说明 | 日期 |
| --- | --- | --- |
| 支持美国西部（加利福利亚北部）区域 | 更新了主题，以包含添加的美国西部（加利福利亚北部）区域。 | 2011-09-08 |
| 公开发行 | 首次发布 AWS Direct Connect。 | 2011-08-03 |

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。