管理员指南

AWS Client VPN

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Client VPN: 管理员指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 AWS Client VPN？ 1
Client VPN 的特性 1
Client VPN 的组件 1
使用 Client VPN 3
Client VPN 的定价 3
规则和最佳实践 4
网络和带宽要求 5
子网和 VPC 配置 5
身份验证和安全 6
连接和 DNS 要求 6
限制和局限性 6
Client VPN 的工作原理 8
场景和示例 9
客户端身份验证 18
Active Directory 身份验证 19
双向身份验证 19
单点登录（基于 SAML 2.0 的联合身份验证） 24
客户端授权 29
安全组 29
基于网络的授权 30
创建端点安全组规则 30
连接授权 31
要求和注意事项 31
Lambda 接口 32
使用客户端连接处理程序进行状况评测 33
启用客户端连接处理程序 34
服务相关角色 34
监控连接授权失败 34
拆分隧道 Client VPN 35
拆分隧道的优势 35
路由注意事项 36
启用拆分隧道 36
连接日志记录 36
连接日志条目 37

扩展注意事项 38
开始使用 Client VPN 40
先决条件 41
步骤 1：生成服务器和客户端证书以及密钥 41
步骤 2：创建 Client VPN 端点 41
步骤 3：关联目标网络 42
步骤 4：添加 VPC 的授权规则 43
步骤 5：提供对 Internet 的访问 44
步骤 6：验证安全组要求 44
步骤 7：下载 Client VPN 端点配置文件 45
步骤 8：连接到 Client VPN 端点 46
使用 Client VPN 47
自助服务门户访问 48
授权规则 48
关键点 49
场景示例 49
添加授权规则 58
删除授权规则 59
查看 授权规则 59
客户端证书吊销列表 60
生成客户端证书吊销列表 60
导入客户端证书吊销列表 62
导出客户端证书吊销列表 63
客户端连接 63
查看 客户端连接 64
终止客户端连接 64
客户端登录横幅 64
横幅创建 65
为现有端点配置客户端登录横幅 65
停用端点的客户端登录横幅 66
修改现有横幅文本 66
查看当前配置的登录横幅 67
使用客户端路由强制执行 67
要求 67
路由冲突 67
注意事项 68

激活客户端路由强制 69
停用客户端路由强制 70
了解如何查看、监控和管理 SageMaker 端点。 70
创建 Client VPN 端点的要求 70
端点修改 71
创建 端点 72
查看端点 75
修改端点 75
删除 端点。 77
连接日志 78
为新端点启用连接日志记录 78
为现有端点启用连接日志记录 79
查看 连接日志 80
关闭 连接日志记录 80
客户端配置文件导出 81
导出 客户端配置文件 82
针对双向身份验证添加客户端证书和密钥信息 82
路线 83
在 Client VPN 端点上使用拆分隧道的注意事项 84
创建端点路由 84
查看端点路由 85
删除端点路由 85
目标网络 86
创建目标网络的要求 86
将目标网络与端点相关联 87
将安全组应用于目标网络 87
查看 目标网络 88
取消目标网络与端点的关联 88
最长 VPN 会话持续时间 89
在创建端点期间配置最长 VPN 会话持续时间 90
查看 当前的最长 VPN 会话持续时间 90
修改最长 VPN 会话持续时间 90
安全性 92
数据保护 92
传输中加密 93
互联网络流量隐私 93

身份和访问管理 94
受众 94
使用身份进行身份验证 95
使用策略管理访问 97
如何 AWS Client VPN 与 IAM 配合使用 99
基于身份的策略示例 104
故障排除 106
使用服务相关角色 108
恢复能力 110
多个目标网络以实现高可用性 111
基础结构安全性 111
最佳实践 111
IPv6 注意事项 112
监控 Client VPN 114
CloudWatch 指标 114
查看 CloudWatch 指标 117
限额 118
客户端 VPN 配额 118
用户和组配额 119
一般注意事项 119
故障排除 120
无法解析 Client VPN 端点 DNS 名称 120
未在子网之间分割流量 121
Active Directory 组的授权规则未按预期运行 122
客户端无法访问对等 VPC、Amazon S3 或 Internet 123
对对等 VPC、Amazon S3 或 Internet 的访问是间歇性的 126
客户端软件返回 TLS 错误 126
客户端软件返回用户名和密码错误（Active Directory 身份验证） 127
客户端软件返回用户名和密码错误（联合身份验证） 128
客户端无法连接（双向身份验证） 128
客户端返回凭证超过最大大小错误 - 联合身份验证 129
客户端不打开浏览器（联合身份验证） 129
客户端返回没有可用端口错误（联合身份验证） 130
由于 IP 不匹配导致 VPN 连接终止 130
无法将流量路由到 LAN 130
验证端点的带宽限制 131

Client VPN 隧道连接 131
网络连接先决条件 132
检查 Client VPN 端点状态 132
验证客户端连接 133
验证客户端身份验证 133
查看授权规则 133
验证 Client VPN 路由 134
验证安全组和网络 ACLs 134
测试客户端连接 135
诊断客户端设备 135
解决 DNS 解析问题 136
排除性能故障 136
监控 Client VPN 指标 137
查看 Client VPN 日志 137
常见问题和解决方案 137
文档历史记录 139
..... cxli

什么是 AWS Client VPN？

AWS Client VPN 是一项基于客户端的托管 VPN 服务，可让您安全地访问本地网络中的 AWS 资源和资源。借助 Client VPN，您可以使用基于 OpenVPN 的 VPN 客户端从任何位置访问您的资源。

主题

- Client VPN 的特性
- Client VPN 的组件
- 使用 Client VPN
- Client VPN 的定价
- 使用 AWS Client VPN的规则和最佳实践

Client VPN 的特性

Client VPN 提供以下特性和功能：

- 安全连接 – 它使用 OpenVPN 客户端从任何位置提供安全的 TLS 连接。
- 托管服务 — 它是一项 AWS 托管服务，因此它消除了部署和管理第三方远程访问 VPN 解决方案的运营负担。
- 高可用性和弹性 — 它会根据连接到您的 AWS 资源和本地资源的用户数量自动扩展。
- 身份验证 – 支持使用 Active Directory、联合身份验证和基于证书的身份验证进行客户端身份验证。
- 精细控制 – 可以让您通过定义基于网络的访问规则来实施自定义安全控制。可以在 Active Directory 组的粒度配置这些规则。您还可以使用安全组实施访问控制。
- 易用性 — 它使您能够使用单个 VPN 隧道访问您的 AWS 资源和本地资源。
- 可管理性 – 它可让您查看连接日志，其中提供有关客户端连接尝试的详细信息。您还可以管理活跃的客户端连接，并且可以终止活跃的客户端连接。
- 深度集成 — 它与现有 AWS 服务（包括 AWS Directory Service 和 Amazon VPC）集成。

Client VPN 的组件

以下是 Client VPN 的主要概念：

Client VPN 端点

Client VPN 终端节点是您创建并配置以用于启用和管理 Client VPN 会话的资源。这是所有 Client VPN 会话的终止点。

目标网络

目标网络是与 Client VPN 端点关联的网络。VPC 中的子网是目标网络。通过将子网与 Client VPN 端点关联，您可以建立 VPN 会话。您可以将多个子网与一个 Client VPN 终端节点关联以实现高可用性。所有子网都必须来自同一 VPC。每个子网都必须属于不同的可用区。

路由

每个 Client VPN 端点都具有一个路由表，用于描述可用的目标网络路由。路由表中的每个路由都指定了到特定资源或网络的途径。

授权规则

授权规则限制可访问网络的用户。对于指定的网络，您可以配置允许访问的 Active Directory 或身份提供商 (IdP) 组。只有属于此组的用户才能访问指定的网络。默认情况下，没有授权规则，您必须配置授权规则来允许用户访问资源和网络。

客户端

连接到 Client VPN 端点以建立 VPN 会话的终端用户。终端用户需要下载 OpenVPN 客户端，并使用您创建的 Client VPN 配置文件来建立 VPN 会话。

客户端 CIDR 范围

从中分配客户端 IP 地址的 IP 地址范围。将从客户端 CIDR 范围中为每个到 Client VPN 端点的连接分配一个唯一的 IP 地址。您可以选择客户端 CIDR 范围，例如 `10.2.0.0/16`。

Client VPN 端口

AWS Client VPN 支持 TCP 和 UDP 的端口 443 和 1194。默认值为端口 443。

Client VPN 网络接口

当您将子网与 Client VPN 端点关联时，我们在该子网中创建 Client VPN 网络接口。从 Client VPN 端点发送到 VPC 的流量将通过 Client VPN 网络接口发送。然后应用源网络地址转换 (SNAT)，将客户端 CIDR 范围内的源 IP 地址转换为 Client VPN 网络接口 IP 地址。

连接日志记录

您可以为 Client VPN 端点启用连接日志记录以记录连接事件。您可以使用此信息运行取证、分析 Client VPN 终端节点的使用方式或调试连接问题。

自助服务门户

Client VPN 为终端用户提供自助服务门户网页，他们可以通过该网页下载最新版 Amazon VPN Desktop Client 和最新版 Client VPN 端点配置文件，该配置文件中包括连接到其端点所需的设置。Client VPN 端点管理员可以为 Client VPN 端点启用或禁用自助服务门户。自助服务门户是一项全球服务，由以下地区的服务堆栈提供支持：美国东部（弗吉尼亚北部）、亚太地区（东京）、欧洲（爱尔兰）和 AWS GovCloud （美国西部）。

使用 Client VPN

您可以通过以下任何方式使用 Client VPN：

AWS Management Console

控制台为 Client VPN 提供基于 Web 的用户界面。如果您已经注册了 AWS 账户，则可以登录 Amazon VPC 控制台，然后在导航窗格中选择 Client VPN。

AWS Command Line Interface (AWS CLI)

AWS CLI 提供对 Client VPN 公共的直接访问 APIs。它在 Windows、macOS 和 Linux 上受支持。有关入门的更多信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》。有关 Client VPN 命令的更多信息，请参阅《亚马逊 EC2 命令行参考》中的EC2 部分。

AWS Tools for Windows PowerShell

AWS 为那些在PowerShell 环境中编写脚本的用户提供了一系列 AWS 产品的命令。有关 AWS Tools for Windows PowerShell入门的更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。如需详细了解 Client VPN 的 cmdlet，请参阅 AWS Tools for Windows PowerShell Cmdlet 参考。

查询 API

Client VPN HTTPS 查询 API 允许你以编程方式访问客户端 VPN 和 AWS。HTTPS 查询 API 可让您直接向服务发布 HTTPS 请求。使用 HTTPS API 时，必须添加代码，才能使用您的凭证对请求进行数字化签名。有关更多信息，请参阅 AWS Client VPN 操作。

Client VPN 的定价

您需要按小时为每个端点关联和每个 VPN 连接付费。有关更多信息，请参阅AWS Client VPN 定价。

您需要支付从 Amazon EC2 向互联网传输数据的费用。有关更多信息，请参阅 Amazon EC2 按需定价页面上的数据传输。

如果您为 Client VPN 终端节点启用连接 CloudWatch 日志，则必须在您的账户中创建日志组。使用日志组需支付费用。有关更多信息，请参阅 Amazon CloudWatch 定价（在 “付费套餐” 下，选择 “日志”）。

如果为 Client VPN 端点启用客户端连接处理程序，则必须创建并调用 Lambda 函数。调用 Lambda 函数需支付费用。有关更多信息，请参阅AWS Lambda 定价。

Client VPN 端点与属于 VPC 中子网的目标网络相关联。如果此 VPC 有 Internet Gateway，我们会将弹性 IP 地址与 Client VPN 弹性网络接口 (ENIs) 关联起来。这些弹性 IP 地址按使用中的公有 IPv4地址收费。有关更多信息，请参阅 VPC 定价页面上的公共 IPv4 地址选项卡。

> **Note**
>
> 客户端 VPN 终端节点在与具有 Internet Gateway 的 VPC 子网关联时需要弹性 IP 地址，因为这些地址 EIPs 可为 VPN 客户端提供直接的互联网连接。通过 Client VPN 端点连接时，他们需要一个公有 IP 地址才能与互联网资源通信。Elastic IPs 通过提供一致的、面向公众的终端节点来实现这一目的。 EIPs 它们连接到 Client VPN 弹性网络接口 (ENIs)，对于维持 VPN 客户端稳定、安全的互联网接入，同时确保流量正确路由至关重要。由于这些弹性 IP 地址已分配并积极用于 Client VPN 服务，因此按照分配和关联 EIPs的标准定价模型，按使用中的公有 IPv4 地址 AWS 收费。

使用 AWS Client VPN的规则和最佳实践

以下各节描述了使用规则和最佳实践 AWS Client VPN：

主题

- 网络和带宽要求
- 子网和 VPC 配置
- 身份验证和安全
- 连接和 DNS 要求
- 限制和局限性

网络和带宽要求

- AWS Client VPN 是一项完全托管的服务，可自动扩展以适应额外的用户连接和带宽需求。每个用户连接的最大基准带宽为 50 Mbps。如果需要，您可以通过 AWS Support 申请加薪。通过 Client VPN 端点连接的用户所体验的实际带宽可能因多种因素而异。这些因素包括数据包大小、流量构成（TCP/UDP 混合）、中间网络上的网络策略（整形或限制）、互联网条件、特定于应用程序的要求以及并发用户连接的总数。
- 客户端 CIDR 范围不能与关联子网所在的 VPC 的本地 CIDR 重叠，也不能与手动添加到 Client VPN 端点的路由表中的任何路由重叠。
- 客户端 CIDR 范围的块大小必须至少为 /22，但不得大于 /12。
- 客户端 CIDR 范围中的一部分地址用于支持 Client VPN 端点的可用性模型，无法分配给客户端。因此，我们建议您分配一个 CIDR 块，其中包含的 IP 地址数量是您计划在 Client VPN 端点上支持的最大并发连接数量所需的 IP 地址数量的两倍。
- 创建 Client VPN 端点后，无法更改客户端 CIDR 范围。
- Client VPN 仅支持 IPv4 流量。有关IPv6 的注意事项 AWS Client VPN详细信息，请参阅 IPv6。
- Client VPN 执行网络地址转换 (NAT)。当客户端通过 Client VPN 连接时：
  - 源 IP 地址将转换为 Client VPN 端点的 IP 地址。
  - 来自客户端的原始源端口号保持不变。
- 仅当并发用户连接到同一目标时，Client VPN 才会执行端口地址转换 (PAT)。端口转换是自动进行的，并且是支持通过同一 VPN 端点进行多个同步连接所必需的。
  - 对于源 IP 转换，源 IP 地址会转换为客户端 VPN 的 IP 地址。
  - 对于单个客户机连接的源端口转换，原始源端口号可能保持不变。
  - 对于连接到同一目的地（相同的目标 IP 地址和端口）的多台客户机的源端口转换，Client VPN 会执行端口转换以确保连接的唯一性。

  例如，当两个客户端（客户端 1 和客户端 2）通过 Client VPN 端点连接到相同的目标服务器和端口时：

  - 客户端 1 的原始端口（例如）可能会转换为其他端口，例如端口4306。9999
  - 客户端 2 的原始端口（例如9999）可能会转换为与客户端 1 不同的唯一端口，例如端口63922。

子网和 VPC 配置

- 与 Client VPN 端点关联的子网必须位于同一 VPC 中。

- 您无法将同一可用区内的多个子网与一个 Client VPN 终端节点关联。
- Client VPN 端点不支持专用租赁 VPC 中的子网关联。

身份验证和安全

- 自助服务门户不适用于使用双向身份验证进行身份验证的客户端。
- 如果对于 Active Directory 禁用了多重身份验证（MFA），则用户密码不能采用以下格式。

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- AWS Client VPN 中使用的证书必须符合 RFC 5280：Internet X.509 公钥基础设施证书和证书吊销列表 (CRL) 配置文件，包括备忘录第 4.2 节中指定的证书扩展。
- 带有特殊字符的用户名可能会导致连接错误。

连接和 DNS 要求

- 不建议使用 IP 地址连接到 Client VPN 端点。由于 Client VPN 是一种托管服务，因此您偶尔会看到 DNS 名称解析到的 IP 地址发生了变化。此外，您还将在 CloudTrail 日志中看到 Client VPN 网络接口已删除并重新创建。我们建议使用提供的 DNS 名称连接到 Client VPN 端点。
- Client VPN 服务要求客户端连接到的 IP 地址与 Client VPN 端点的 DNS 名称解析到的 IP 相匹配。换句话说，如果您为 Client VPN 终端节点设置了自定义 DNS 记录，然后将流量转发到该端点的 DNS 名称解析到的实际 IP 地址，则此设置将无法使用最近 AWS 提供的客户端。添加此规则是为了缓解服务器IP攻击，如下所述:TunnelCrack.
- 您可以使用 AWS 提供的客户端连接到多个并发 DNS 会话。但是，为了使名称解析正常工作，所有连接的 DNS 服务器都应具有同步记录。
- Client VPN 服务要求客户端设备的局域网（LAN）IP 地址范围位于以下标准私有 IP 地址范围内：`10.0.0.0/8`、`172.16.0.0/12`、`192.168.0.0/16` 或 `169.254.0.0/16`。如果检测到客户端 LAN 地址范围超出上述范围，Client VPN 端点会将 OpenVPN 指令“redirect-gateway block-local”自动推送到客户端，从而强制所有 LAN 流量进入 VPN。因此，如果您需要在 VPN 连接期间访问 LAN，建议您为 LAN 使用上面列出的常规地址范围。强制执行此规则是为了减少本地网络攻击的机会，如下所述:TunnelCrack.

限制和局限性

- 使用 AWS Client VPN 桌面应用程序时，目前不支持 IP 转发。其它客户端支持 IP 转发。

- Client VPN 在 AWS Managed Microsoft AD中不支持多区域复制。Client VPN 终端节点必须与 AWS Managed Microsoft AD 资源位于同一区域。
- 如果有多个用户登录到操作系统，则无法从计算机建立 VPN 连接。

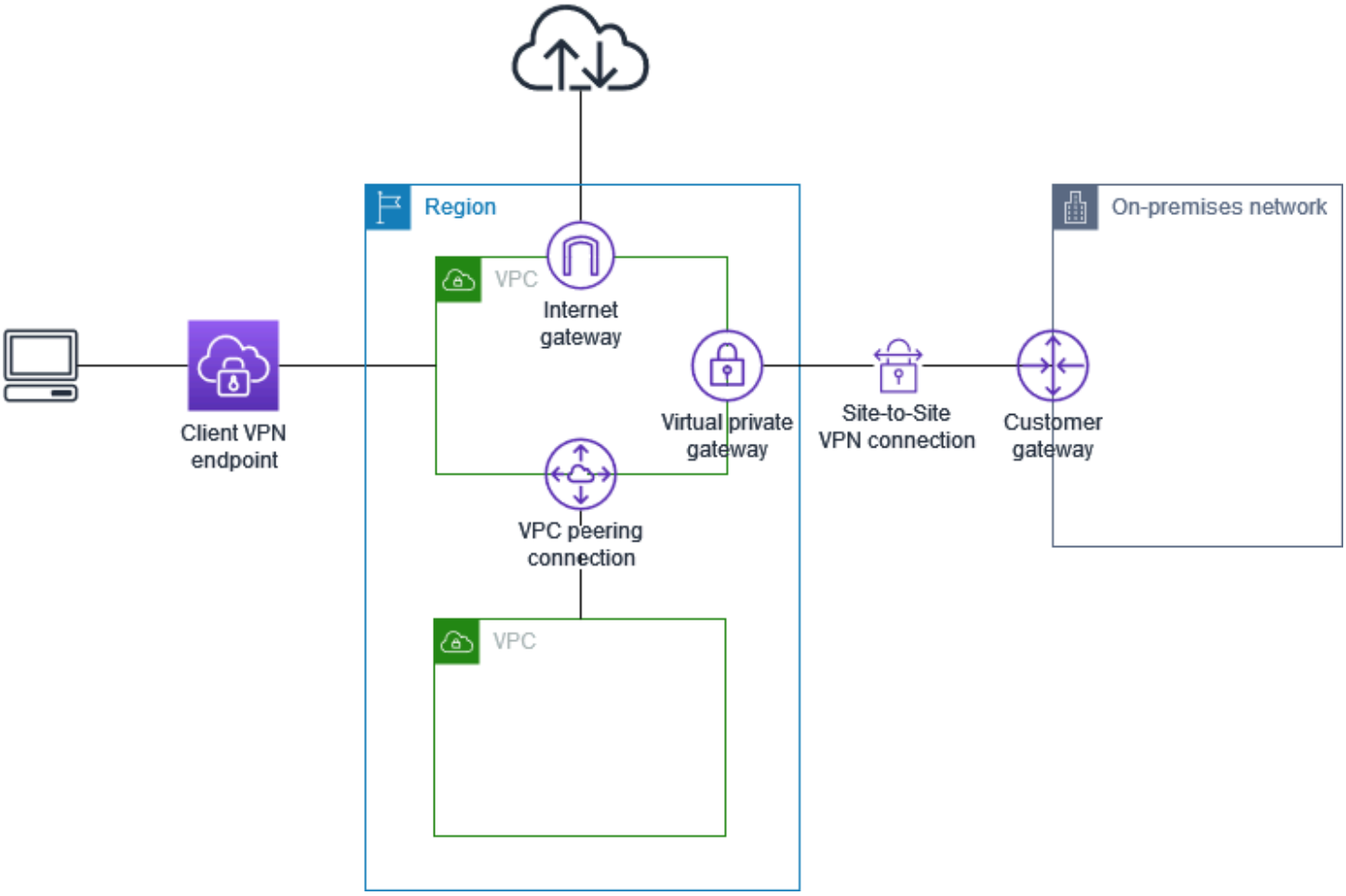
如何 AWS Client VPN 运作

使用 AWS Client VPN，与 Client VPN 端点交互的用户角色有两种：管理员和客户端。

管理员负责设置和配置服务。这包括创建 Client VPN 端点、关联目标网络、配置授权规则，以及设置额外的路由（如果需要）。在设置和配置 Client VPN 端点后，管理员下载 Client VPN 端点配置文件并将其分发给需要访问的客户端。Client VPN 端点配置文件包含 Client VPN 端点的 DNS 名称和建立 VPN 会话所需的身份验证信息。有关设置服务的更多信息，请参阅 开始使用 AWS Client VPN。

客户端 是最终用户。这是连接到 Client VPN 端点以建立 VPN 会话的人。客户端使用基于 OpenVPN 的 VPN 客户端应用程序从其本地计算机或移动设备上建立 VPN 会话。建立 VPN 会话后，它们就可以安全地访问关联子网所在的 VPC 中的资源。如果配置了所需的路由和授权规则，他们还可以访问本地网络或其他客户端中的 AWS其他资源。有关连接到 Client VPN 端点以建立 VPN 会话的更多信息，请参阅《AWS Client VPN 用户指南》中的入门。

下图阐明基本的 Client VPN 架构。



Client VPN 场景和示例

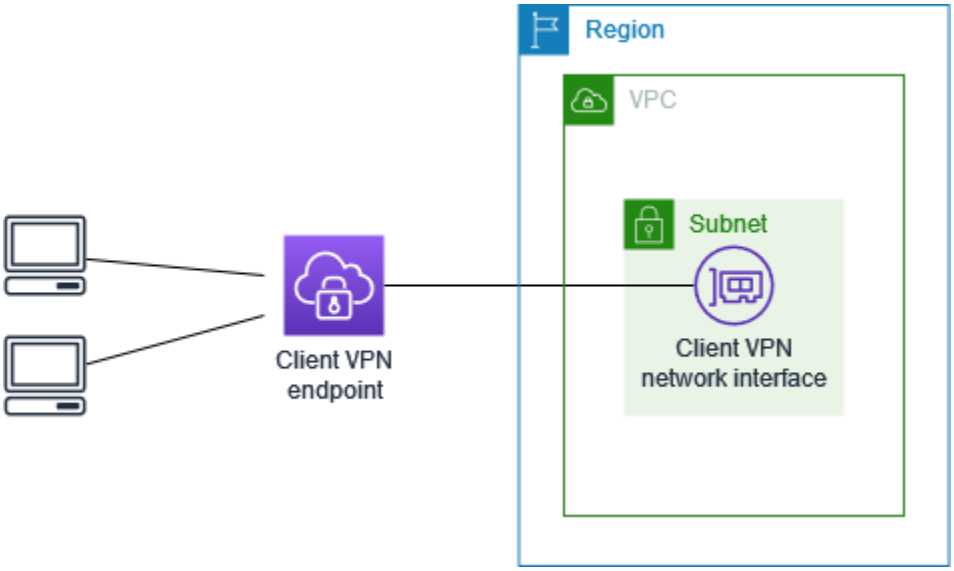
AWS Client VPN 是一种完全托管的远程访问 VPN 解决方案，用于允许客户安全访问本地网络 AWS 和本地网络中的资源。有多个选项可用于配置访问权限。本部分提供为您的客户端创建和配置 Client VPN 访问的示例。

场景

- the section called “访问 VPC”
- the section called “访问对等 VPC”
- the section called “访问本地网络”
- the section called “访问 Internet”
- the section called “C lient-to-client 访问权限”
- the section called “限制对您的网络的访问”

使用 Client VPN 访问 VPC

此场景的 AWS Client VPN 配置包括单个目标 VPC。如果您需要向客户端授予仅对于单个 VPC 中的资源的访问权限，我们建议您采用此配置。



开始之前，请执行以下操作：

- 创建或确定至少具有一个子网的 VPC。确定 VPC 中要与 Client VPN 终端节点关联的子网，并记下其 IPv4 CIDR 范围。
- 为与 VPC CIDR 不重叠的客户端 IP 地址确定合适的 CIDR 范围。

- 查看使用 AWS Client VPN的规则和最佳实践中的 Client VPN 终端节点的规则和限制。

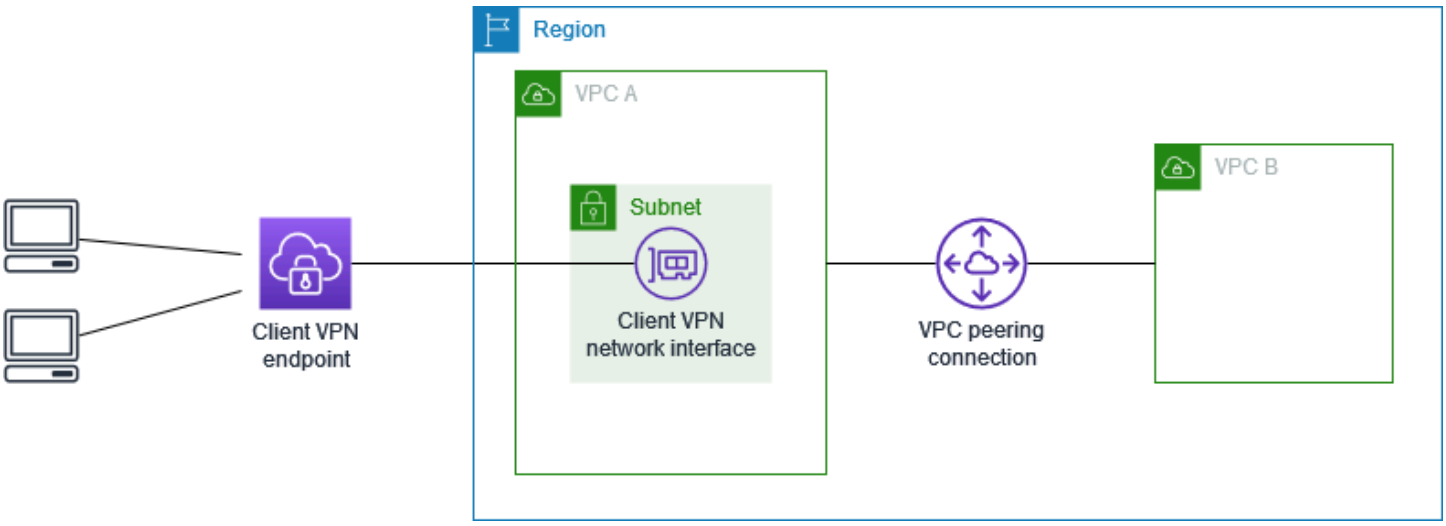
实施此配置

1. 在 VPC 所在的区域中创建 Client VPN 终端节点。要执行此操作，请执行 创建 AWS Client VPN 终端节点 中介绍的步骤。
2. 将子网与 Client VPN 端点相关联。要执行此操作，请执行将目标网络与 AWS Client VPN 端点相关联中介绍的步骤，并选择您之前确定的子网和 VPC。
3. 添加授权规则以向客户端授予访问 VPC 的权限。为此，请执行中描述的步骤添加授权规则，对于目标网络，输入 VPC 的 IPv4 CIDR 范围。
4. 向资源的安全组添加规则，以允许来自在步骤 2 中应用到子网关联的安全组的流量。有关更多信息，请参阅 安全组。

使用 Client VPN 访问对等 VPC

此场景的 AWS Client VPN 配置包括与其他 VPC (VPC B) 对等的目标 VPC (VPC A)。如果您需要允许客户端访问目标 VPC 内部的资源以及与之对等的其他资源（例如 VPC B） VPCs ，我们建议您使用此配置。

> **Note**
>
> 仅当在拆分隧道模式下配置 Client VPN 端点时，才需要执行允许访问对等 VPC 的过程（在网络图后概述）。在全隧道模式下，原定设置情况下允许访问对等 VPC。



开始之前，请执行以下操作：

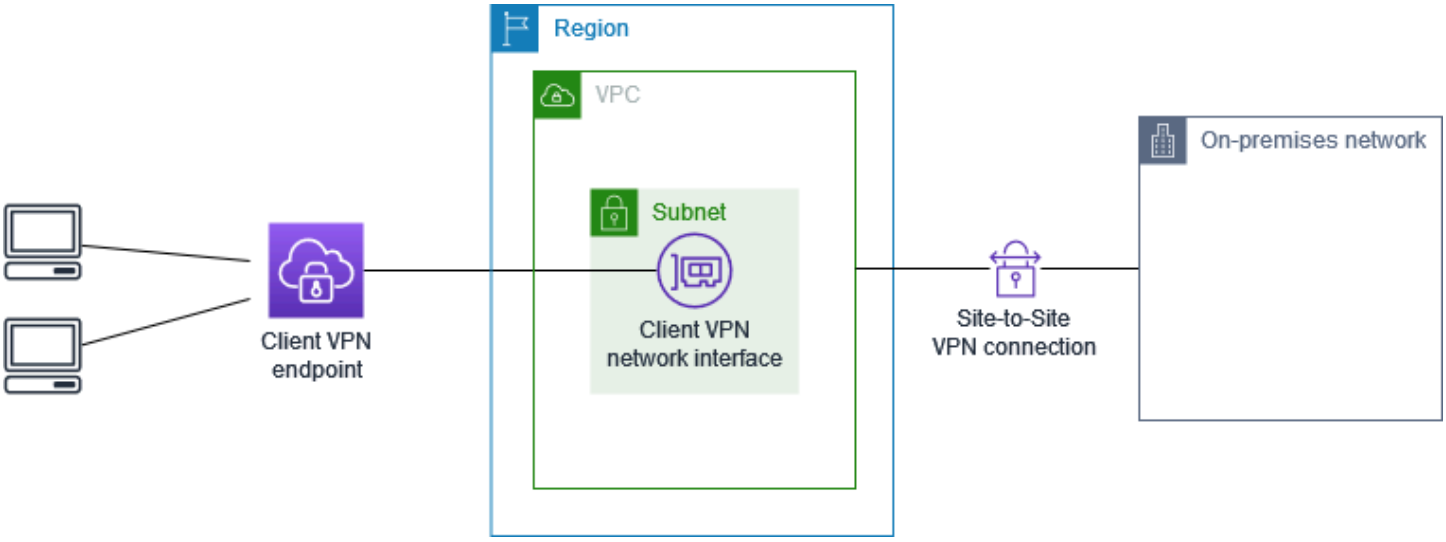
- 创建或确定至少具有一个子网的 VPC。确定 VPC 中要与 Client VPN 终端节点关联的子网，并记下其 IPv4 CIDR 范围。
- 为与 VPC CIDR 不重叠的客户端 IP 地址确定合适的 CIDR 范围。
- 查看使用 AWS Client VPN的规则和最佳实践中的 Client VPN 终端节点的规则和限制。

实施此配置

1. 在之间建立 VPC 对等连接。 VPCs按照 Amazon VPC 对等指南 中的创建并接受 VPC 对等连接的步骤进行操作。确认 VPC A 中的实例可以使用对等连接与 VPC B 中的实例通信。
2. 在目标 VPC 所在的同一个区域中创建 Client VPN 端点。在图中，这是 VPC A。执行创建 AWS Client VPN 终端节点中介绍的步骤。
3. 将您确定的子网与您创建的 Client VPN 端点关联。要执行此操作，请执行将目标网络与 AWS Client VPN 端点相关联中介绍的步骤，同时选择 VPC 和子网。原定设置情况下，我们将 VPC 的原定设置安全组与 Client VPN 端点相关联。您可以使用the section called “将安全组应用于目标网络”中所述的步骤关联不同的安全组。
4. 添加授权规则以向客户端授予访问目标 VPC 的权限。要执行此操作，请执行 添加授权规则 中介绍的步骤。要启用目标网络，请输入 VPC 的 IPv4 CIDR 范围。
5. 添加路由以将流量定向到对等 VPC。在图中，这是 VPC B。要执行此操作，请执行创建 AWS Client VPN 终端节点路由中介绍的步骤。在路由目标中，输入对等互连 VPC 的 IPv4 CIDR 范围。对于目标 VPC 子网 ID，选择与 Client VPN 端点关联的子网。
6. 添加授权规则以向客户端授予访问对等 VPC 的权限。要执行此操作，请执行 添加授权规则 中介绍的步骤。对于目标网络，请输入对等互连 VPC 的 IPv4 CIDR 范围。
7. 向 VPC A 和 VPC B 中实例的安全组添加规则，以允许来自在步骤 3 中应用了Client VPN 端点的安全组的流量。有关更多信息，请参阅 安全组。

使用 Client VPN 访问本地网络

此场景的 AWS Client VPN 配置仅包括对本地网络的访问。如果您需要向客户端授予仅对于本地网络中资源的访问权限，我们建议您采用此配置。



开始之前，请执行以下操作：

- 创建或确定至少具有一个子网的 VPC。确定 VPC 中要与 Client VPN 终端节点关联的子网，并记下其 IPv4 CIDR 范围。
- 为与 VPC CIDR 不重叠的客户端 IP 地址确定合适的 CIDR 范围。
- 查看使用 AWS Client VPN的规则和最佳实践中的 Client VPN 终端节点的规则和限制。

实施此配置

1. 通过 VP AWS Site-to-Site N 连接启用 VPC 和您自己的本地网络之间的通信。要执行此操作，请执行 AWS Site-to-Site VPN 用户指南中的使用入门中描述的步骤。

   > **Note**
   >
   > 或者，您可以通过使用您的 VPC 和本地网络之间的 AWS Direct Connect 连接来实现此场景。有关更多信息，请参阅 用户指南。AWS Direct Connect

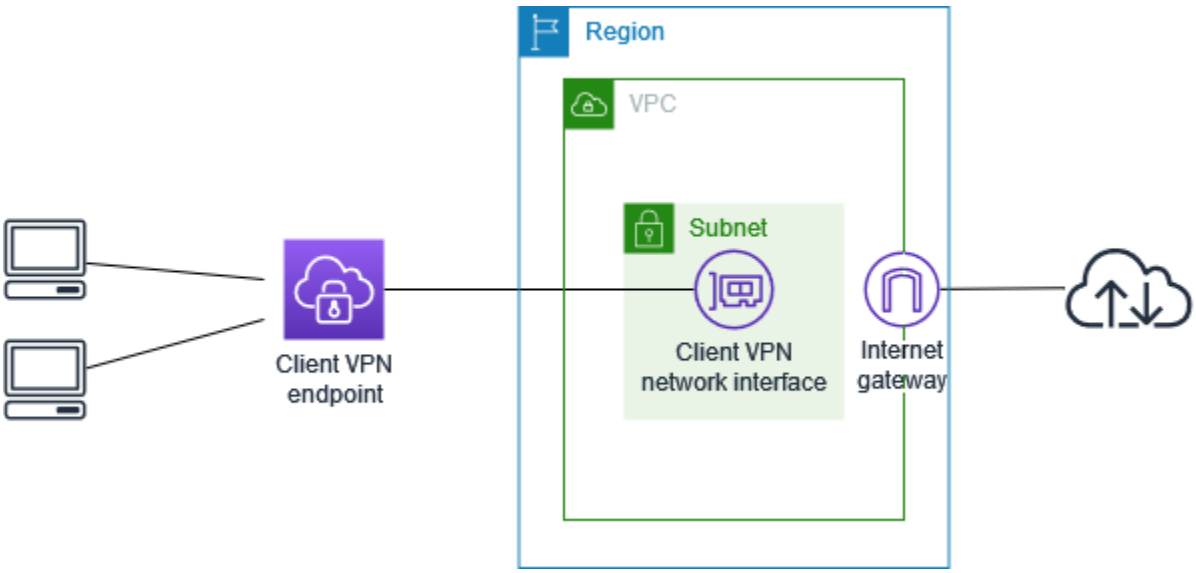
2. 测试您在上一步中创建的 AWS Site-to-Site VPN 连接。为此，请执行AWS Site-to-Site VPN 用户指南中测试 Site-to-Site VPN 连接中描述的步骤。如果 VPN 连接按预期正常工作，则继续执行下一步。
3. 在 VPC 所在的区域中创建 Client VPN 终端节点。要执行此操作，请执行 创建 AWS Client VPN 终端节点 中介绍的步骤。
4. 将先前确定的子网与 Client VPN 终端节点关联。要执行此操作，请执行 将目标网络与 AWS Client VPN 端点相关联 中介绍的步骤，并选择 VPC 和子网。

5. 添加允许访问 AWS Site-to-Site VPN 连接的路由。为此，请执行中描述的步骤创建 AWS Client VPN 终端节点路由；在路由目标中，输入 AWS Site-to-Site VPN 连接的 IPv4 CIDR 范围，在目标 VPC 子网 ID 中，选择与 Client VPN 终端节点关联的子网。
6. 添加授权规则以允许客户端访问 AWS Site-to-Site VPN 连接。为此，请执行中描述的步骤向 AWS Client VPN 端点添加授权规则；对于目标网络，输入 AWS Site-to-Site VPN 连接 IPv4 CIDR 范围。

使用 Client VPN 访问 Internet

此场景的 AWS Client VPN 配置包括单个目标 VPC 和互联网访问权限。如果您需要向客户端授予对单一目标 VPC 中资源的访问权限并另外允许访问 Internet，建议您采用此配置。

如果您完成了 开始使用 AWS Client VPN教程，则您已实现了本场景。



开始之前，请执行以下操作：

- 创建或确定至少具有一个子网的 VPC。确定 VPC 中要与 Client VPN 终端节点关联的子网，并记下其 IPv4 CIDR 范围。
- 为与 VPC CIDR 不重叠的客户端 IP 地址确定合适的 CIDR 范围。
- 查看使用 AWS Client VPN的规则和最佳实践中的 Client VPN 终端节点的规则和限制。

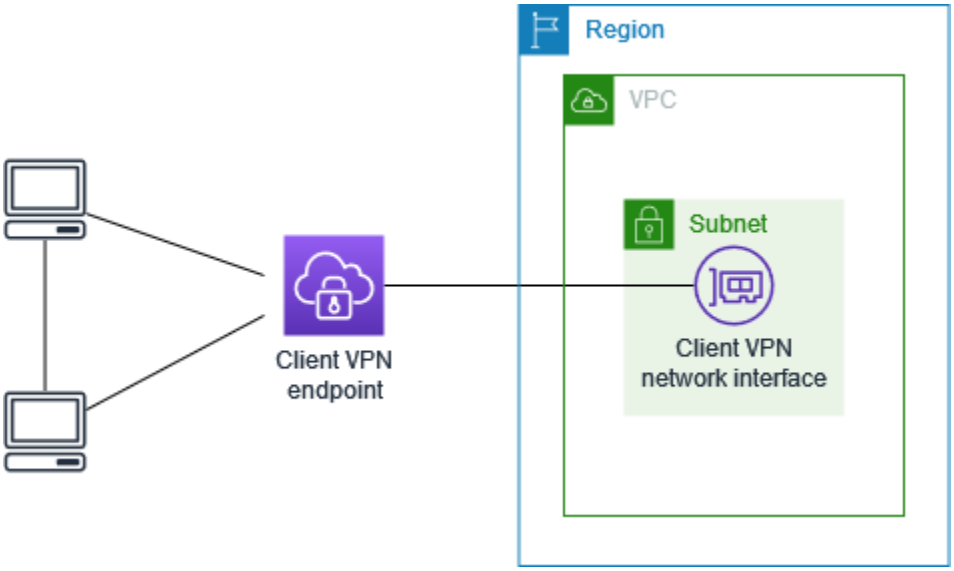
实施此配置

1. 确保您将用于 Client VPN 端点的安全组允许发送到 Internet 的出站流量。为此，请添加允许发送到 0.0.0.0/0 的 HTTP 和 HTTPS 流量的出站规则。

2. 创建 Internet 网关并将其附加到 VPC。有关更多信息，请参阅 Amazon VPC 用户指南 中的创建并附加 Internet 网关。
3. 通过将通向 Internet 网关的路由添加到路由表，使子网成为公用子网。在 VPC 控制台中，选择 Subnets（子网），选择要与 Client VPN 端点关联的子网，选择 Route Table（路由表），然后选择路由表 ID。选择操作，选择 Edit routes (编辑路由)，然后选择添加路由。对于 Destination (目的地)，输入 `0.0.0.0/0`，然后为 Target (目标) 选择上一步中的 Internet 网关。
4. 在 VPC 所在的区域中创建 Client VPN 终端节点。要执行此操作，请执行 创建 AWS Client VPN 终端节点 中介绍的步骤。
5. 将先前确定的子网与 Client VPN 终端节点关联。要执行此操作，请执行 将目标网络与 AWS Client VPN 端点相关联 中介绍的步骤，并选择 VPC 和子网。
6. 添加授权规则以向客户端授予访问 VPC 的权限。为此，请执行中描述的步骤添加授权规则；要启用目标网络，请输入 VPC 的 IPv4 CIDR 范围。
7. 添加允许进入 Internet 的流量的路由。要执行此操作，请执行创建 AWS Client VPN 终端节点路由中介绍的步骤；对于 Route destination（路由目标），输入 `0.0.0.0/0`，对于 Target VPC Subnet ID（目标 VPC 子网 ID），选择与 Client VPN 端点关联的子网。
8. 添加授权规则以向客户端授予访问 Internet 的权限。要执行此操作，请执行添加授权规则中介绍的步骤，而对于目标网络，输入 `0.0.0.0/0`。
9. 确保 VPC 中资源的安全组具有一条规则，该规则允许从与 Client VPN 端点关联的安全组进行访问。这将允许您的客户端访问 VPC 中的资源。

Client-to-client 使用 Client VPN 进行访问

此场景的 AWS Client VPN 配置使客户端能够访问单个 VPC，并使客户端能够将流量路由到彼此。如果连接到同一 Client VPN 端点的客户端也需要相互通信，我们建议使用此配置。当客户端连接到 Client VPN 端点时，客户端可以使用从客户端 CIDR 范围分配给它们的唯一 IP 地址相互通信。



开始之前，请执行以下操作：

- 创建或确定至少具有一个子网的 VPC。确定 VPC 中要与 Client VPN 终端节点关联的子网，并记下其 IPv4 CIDR 范围。
- 为与 VPC CIDR 不重叠的客户端 IP 地址确定合适的 CIDR 范围。
- 查看使用 AWS Client VPN的规则和最佳实践中的 Client VPN 终端节点的规则和限制。

> **Note**
>
> 此方案不支持使用 Active Directory 组或基于 SAML 的 IdP 组的基于网络的授权规则。

实施此配置

1. 在 VPC 所在的区域中创建 Client VPN 终端节点。要执行此操作，请执行 创建 AWS Client VPN 终端节点 中介绍的步骤。
2. 将先前确定的子网与 Client VPN 终端节点关联。要执行此操作，请执行 将目标网络与 AWS Client VPN 端点相关联 中介绍的步骤，并选择 VPC 和子网。
3. 将路由添加到路由表中的本地网络。要执行此操作，请执行 创建 AWS Client VPN 终端节点路由 中介绍的步骤。对于路由目标，输入客户端 CIDR 范围；对于目标 VPC 子网 ID，指定 `local`。
4. 添加授权规则以向客户端授予访问 VPC 的权限。要执行此操作，请执行 添加授权规则 中介绍的步骤。要启用目标网络，请输入 VPC 的 IPv4 CIDR 范围。

5. 添加授权规则以向客户端授予访问客户端 CIDR 范围的权限。要执行此操作，请执行 添加授权规则 中介绍的步骤。对于要启用的目标网络，输入客户端 CIDR 范围。

使用 Client VPN 限制对网络的访问

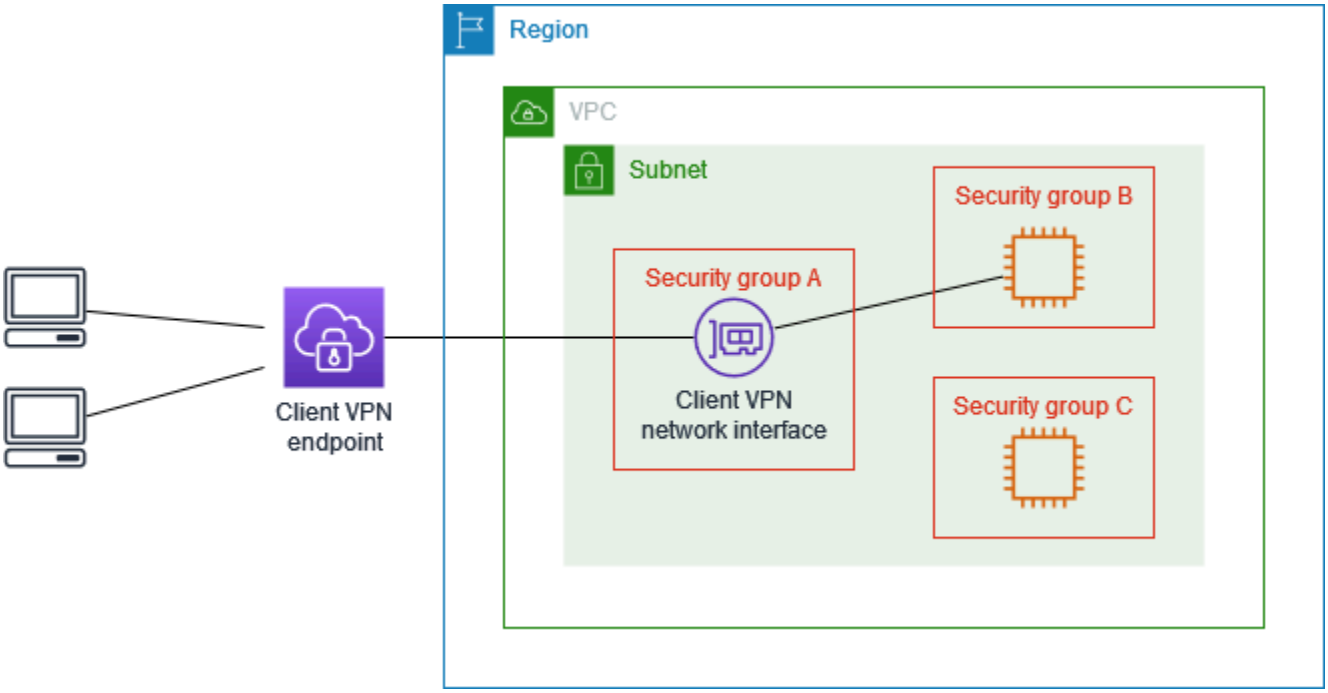
您可以将 AWS Client VPN 终端节点配置为限制对您的 VPC 中特定资源的访问。对于基于用户的身份验证，您还可以根据访问 Client VPN 终端节点的用户组限制对网络各部分的访问。

使用安全组限制访问

您可以通过添加或删除引用了安全组（应用到目标网络关联的安全组，即 Client VPN 安全组）的安全组规则，授予或拒绝对您 VPC 中特定资源的访问权限。此配置在使用 Client VPN 访问 VPC 中介绍的场景基础之上进行了扩展。除了该情景中配置的授权规则之外，还应用此配置。

要授予对特定资源的访问权限，请确定与运行资源的实例相关联的安全组。然后，创建允许来自 Client VPN 安全组的流量的规则。

在下图中，安全组 A 是 Client VPN 安全组，安全组 B 与 EC2 实例关联，安全组 C 与 EC2 实例关联。如果您向安全组 B 添加允许从安全组 A 进行访问的规则，则客户端可以访问与安全组 B 关联的实例。如果安全组 C 没有允许从安全组 A 进行访问的规则，则客户端无法访问与安全组 C 关联的实例。



在开始之前，请检查 Client VPN 安全组是否与 VPC 中的其他资源相关联。如果您添加或删除引用 Client VPN 安全组的规则，则可能还会授予或拒绝对其他关联资源的访问权限。为防止出现这种情况，请使用专门为与 Client VPN 端点一起使用而创建的安全组。

创建安全组规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择安全组。
3. 选择与运行您资源的实例相关联的安全组。
4. 选择 Actions (操作)、Edit inbound rules (编辑入站规则)。
5. 选择 Add Rule (添加规则)，然后执行以下操作：
   - 对于 Type (类型)，选择 All traffic (所有流量) 或要允许的特定流量类型。
   - 对于源，请选择自定义，然后输入或选择 Client VPN 安全组的 ID。
6. 选择 Save rules (保存规则)。

要删除对特定资源的访问权限，请检查与运行资源的实例相关联的安全组。如果存在允许来自 Client VPN 安全组的流量的规则，请将其删除。

检查安全组规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择安全组。
3. 选择 Inbound Rules (入站规则)。
4. 查看规则列表。如果有一个规则，其中 Source（源）是 Client VPN 安全组，请选择 Edit Rules（编辑规则），然后为该规则选择 Delete（删除）（x 图标）。选择保存规则。

根据用户组限制访问

如果您的 Client VPN 端点配置为进行基于用户的身份验证，则可以授予特定用户组访问网络特定部分的权限。为此，请完成以下步骤：

1. 在 AWS Directory Service 或您的 IdP 中配置用户和群组。有关更多信息，请参阅以下主题：
   - Client VPN 中的 Active Directory 身份验证
   - 基于 SAML 的联合身份验证的要求和注意事项
2. 为 Client VPN 端点创建授权规则，以允许指定的组访问网络的全部或某个部分。有关更多信息，请参阅 AWS Client VPN 授权规则。

如果您的 Client VPN 端点配置为进行双向身份验证，则无法配置用户组。创建授权规则时，必须向所有用户授予访问权限。要允许特定用户组访问网络的特定部分，您可以创建多个 Client VPN 端点。例如，对于访问网络的每个用户组，请执行以下操作：

1. 为该用户组创建一组服务器以及客户端证书和密钥。有关更多信息，请参阅 双向认证 AWS Client VPN。
2. 创建 Client VPN 终端节点。有关更多信息，请参阅 创建 AWS Client VPN 终端节点。
3. 创建授权规则，以授予对网络全部或某个部分的访问权限。例如，对于管理员使用的 Client VPN 端点，您可以创建授权规则，以授予对整个网络的访问权限。有关更多信息，请参阅 添加授权规则。

中的客户端身份验证 AWS Client VPN

客户端身份验证是在 AWS 云端的第一个入口点实施的。它用于确定是否允许客户端连接到客户端 VPN 终端节点。如果身份验证获得成功，客户端连接到客户端 VPN 终端节点并建立 VPN 会话。如果身份验证失败，连接被拒绝，客户端无法建立 VPN 会话。

客户端 VPN 提供以下类型的客户端身份验证：

- Active Directory 身份验证（基于用户）
- 双向身份验证额（基于证书）
- 单点登录（基于 SAML 的联合身份验证）（基于用户）

您可以单独使用上面的方法之一，也可以将双向身份验证与基于用户的方法结合使用，如下所示：

- 双向身份验证和联合身份验证
- 双向身份验证和 Active Directory 身份验证

> **Important**
>
> - 要创建 Client VPN 端点，无论您使用何种身份验证，都必须在 AWS Certificate Manager 中预置服务器证书。有关创建和预置服务器证书的更多信息，请参阅双向认证 AWS Client VPN中的步骤。
> - 如果将相互身份验证和基于用户的身份验证结合使用，则必须使用这两种方法在 VPN 中正确进行身份验证。

Client VPN 中的 Active Directory 身份验证

Client VPN 通过与集成来提供活动目录支持 AWS Directory Service。借助 Active Directory 身份验证，客户端可对照现有 Active Directory 组进行身份验证。使用 AWS Directory Service，Client VPN 可以连接到本地网络中 AWS 或内部网络中配置的现有活动目录。这样，您就可以使用您的现有客户端身份验证基础结构。如果您使用的是本地 Active Directory，并且没有现有的 AWS 托管 Microsoft AD，则必须配置 Active Directory 连接器（AD Connector）。您可以使用一个 Active Directory 服务器对用户进行身份验证。有关 Active Directory 集成的更多信息，请参阅 AWS Directory Service 管理指南。

为 AWS 托管的 Microsoft AD 或 AD Connector 启用多重身份验证（MFA）后，Client VPN 支持多重身份验证（MFA）。如果启用了 MFA，客户端在连接到 Client VPN 端点时必须输入用户名、密码和 MFA 代码。有关启用 MFA 的更多信息，请参阅 AWS Directory Service 管理指南中的为 AWS 托管的 Microsoft AD 启用多重身份验证和为 AD Connector 启用多重身份验证。

有关在 Active Directory 中配置用户和组的配额和规则，请参阅用户和组配额。

双向认证 AWS Client VPN

借助双向身份验证，Client VPN 使用证书在客户端和服务器之间执行身份验证。证书是由证书颁发机构（CA）颁发的数字化身份。当客户端尝试连接到 Client VPN 端点时，服务器使用客户端证书对客户端进行身份验证。您必须创建服务器证书和密钥，以及至少一个客户端证书和密钥。

您必须将服务器证书上传到 AWS Certificate Manager (ACM)，并在创建 Client VPN 端点时指定该证书。将服务器证书上载到 ACM 时，还需要指定证书颁发机构 (CA)。如果客户端证书的 CA 与服务器证书的 CA 不同，您只需将客户端证书上传到 ACM。有关 ACM 的更多信息，请参阅 AWS Certificate Manager 用户指南。

您可以为将连接到 Client VPN 端点的每个客户端创建单独的客户端证书和密钥。这使您能够在用户退出组织时撤销特定的客户端证书。在这种情况下，当您创建 Client VPN 端点时，可以为客户端证书指定服务器证书 ARN，前提是客户端证书与服务器证书是由相同 CA 颁发的。

AWS Client VPN 中使用的证书必须符合 RFC 5280：Internet X.509 公钥基础设施证书和证书吊销列表 (CRL) 配置文件，包括备忘录第 4.2 节中指定的证书扩展。

> **Note**
>
> Client VPN 端点仅支持 1024 位和 2048 位 RSA 密钥大小。此外，客户端证书的“主题”字段中必须具有 CN 属性。

当与 Client VPN 服务一起使用的证书更新时，无论是通过 ACM 自动轮换、手动导入新证书，还是通过 IAM Identity Center 的元数据更新，Client VPN 服务都将使用较新的证书自动更新 Client VPN 终端节点。这是一个自动化流程，最多可能需要 5 个小时。

任务

- 启用双向认证 AWS Client VPN
- 续订您的服务器证书 AWS Client VPN

启用双向认证 AWS Client VPN

您可以在 Linux/macOS 或 Windows 的 Client VPN 中启用双向身份验证。

Linux/macOS

以下过程使用 OpenVPN easy-rsa 生成服务器和客户端证书和密钥，然后将服务器证书和密钥上传到 ACM。有关更多信息，请参阅 Easy-RSA 3 快速入门自述文件。

生成服务器和客户端证书和密钥并将其上传到 ACM

1. 将 OpenVPN easy-rsa 存储库克隆到本地计算机并导航到 `easy-rsa/easyrsa3` 文件夹。

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. 初始化一个新的 PKI 环境。

```
$ ./easyrsa init-pki
```

3. 要构建新的证书颁发机构（CA），请运行此命令并按照提示进行操作。

```
$ ./easyrsa build-ca nopass
```

4. 生成服务器证书和密钥。

```
$ ./easyrsa --san=DNS:server build-server-full server nopass
```

5. 生成客户端证书和密钥。

请务必保存客户端证书和客户端私有密钥，因为您配置客户端时需要这些信息。

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

您可以选择为需要客户端证书和密钥的每个客户端（最终用户）重复此步骤。

6. 将服务器证书和密钥和客户端证书和密钥复制到自定义文件夹，然后导航到此自定义文件夹。

   复制证书和密钥之前，请使用 `mkdir` 命令创建自定义文件夹。以下示例在您的主目录中创建自定义文件夹。

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. 将服务器证书和密钥以及客户端证书和密钥上传到 ACM。请确保在您打算在其中创建客户端 VPN 终端节点的同一区域中上传证书。以下命令使用 AWS CLI 上传证书。要改为使用 ACM 控制台上传证书，请参阅 AWS Certificate Manager 用户指南中的导入证书。

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

   您不必将客户端证书上传到 ACM。如果服务器证书和客户端证书是由相同证书颁发机构 (CA) 颁发，则您可以在创建客户端 VPN 端点时在服务器和客户端中使用服务器证书 ARN。在上述步骤中，使用了相同 CA 来创建两个证书。但是，为了完整起见，其中包括上传客户端证书的步骤。

Windows

以下过程安装 Easy-RSA 3.x 软件，并使用它生成服务器和客户端证书和密钥。

生成服务器和客户端证书和密钥并将它们上载到 ACM

1. 打开 EasyRSA 版本页面，然后下载适用于您的 Windows 版本的 ZIP 文件并对它进行解压缩。
2. 打开命令提示符，然后导航到 `EasyRSA-3.x` 文件夹解压缩到的位置。
3. 运行以下命令以打开 EasyRSA 3 shell。

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. 初始化一个新的 PKI 环境。

```
# ./easyrsa init-pki
```

5. 要构建新的证书颁发机构（CA），请运行此命令并按照提示进行操作。

```
# ./easyrsa build-ca nopass
```

6. 生成服务器证书和密钥。

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. 生成客户端证书和密钥。

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

   您可以选择为需要客户端证书和密钥的每个客户端（最终用户）重复此步骤。

8. 退出 EasyRSA 3 shell。

```
# exit
```

9. 将服务器证书和密钥和客户端证书和密钥复制到自定义文件夹，然后导航到此自定义文件夹。

   复制证书和密钥之前，请使用 `mkdir` 命令创建自定义文件夹。以下示例在您的 C:\ 驱动器中创建自定义文件夹。

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
```

```
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. 将服务器证书和密钥以及客户端证书和密钥上传到 ACM。请确保在您打算在其中创建客户端 VPN 终端节点的同一区域中上传证书。以下命令 AWS CLI 使用上传证书。要改为使用 ACM 控制台上传证书，请参阅 AWS Certificate Manager 用户指南中的导入证书。

```
aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate \
    --certificate fileb://client1.domain.tld.crt \
    --private-key fileb://client1.domain.tld.key \
    --certificate-chain fileb://ca.crt
```

您不必将客户端证书上传到 ACM。如果服务器证书和客户端证书是由相同证书颁发机构 (CA) 颁发，则您可以在创建客户端 VPN 端点时在服务器和客户端中使用服务器证书 ARN。在上述步骤中，使用了相同 CA 来创建两个证书。但是，为了完整起见，其中包括上传客户端证书的步骤。

续订您的服务器证书 AWS Client VPN

您可以续订并重新导入已过期的 Client VPN 服务器证书。根据您使用的 OpenVPN easy-rsa 版本，过程会有所不同。有关更多详细信息，请参阅 Easy-RSA 3 证书续订和吊销文档。

续订服务器证书

1. 请执行以下操作之一：
   - Easy-RSA 版本 3.1.x
     - 运行证书续订命令。

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA 版本 3.2.x

a. 运行过期命令。

```
$ ./easyrsa expire server
```

b. 签署新证书。

```
$ ./easyrsa --san=DNS:server sign-req server server
```

2. 创建一个自定义文件夹，将新文件复制到该文件夹中，然后导航到该文件夹。

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. 将新文件导入到 ACM。确保将文件导入与 Client VPN 端点相同的区域中。

```
$ aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Client VPN 中的单点登录（基于 SAML 2.0 的联合身份验证）

AWS Client VPN 支持使用 Client VPN 端点的安全断言标记语言 2.0 (SAML 2.0) 进行身份联合。您可以使用支持 SAML 2.0 的身份提供商 (IdPs) 来创建集中式用户身份。然后，您可以将 Client VPN 端点配置为使用基于 SAML 的联合身份验证，并将其与 IdP 关联。用户随之使用其集中式凭证连接到 Client VPN 端点。

主题

- 启用 SAML AWS Client VPN
- 身份验证工作流
- 基于 SAML 的联合身份验证的要求和注意事项
- 基于 SAML 的 IdP 配置资源

启用 SAML AWS Client VPN

可以通过完成以下步骤为 Client VPN 启用单点登录 SAML。或者，如果您为 Client VPN 端点启用了自助服务门户，请指示用户转到自助服务门户来获取配置文件和 AWS 提供的客户端。有关更多信息，请参阅 AWS Client VPN 访问自助服务门户。

要使基于 SAML 的 IdP 能够用于 Client VPN 端点，您必须执行以下操作。

1. 在您选择的 IdP 中创建基于 SAML 的应用程序以与现有应用程序一起使用 AWS Client VPN，或使用现有应用程序。
2. 配置 IdP 以与 AWS建立信任关系 有关资源，请参阅基于 SAML 的 IdP 配置资源。
3. 在 IdP 中，生成和下载联合身份元数据文档，该文档将您的组织描述为 IdP。

   此签名 XML 文档用于在 AWS 和 IdP 之间建立信任关系。
4. 在与 Client VPN 终端节点相同的 AWS 账户中创建 IAM SAML 身份提供商。

   IAM SAML 身份提供商使用 IdP AWS 生成的元数据文档定义贵组织的 IdP 信任关系。有关更多信息，请参阅 IAM 用户指南 中的创建 IAM SAML 身份提供商。如果稍后更新 IdP 中的应用程序配置，请生成新的元数据文档并更新 IAM SAML 身份提供程序。

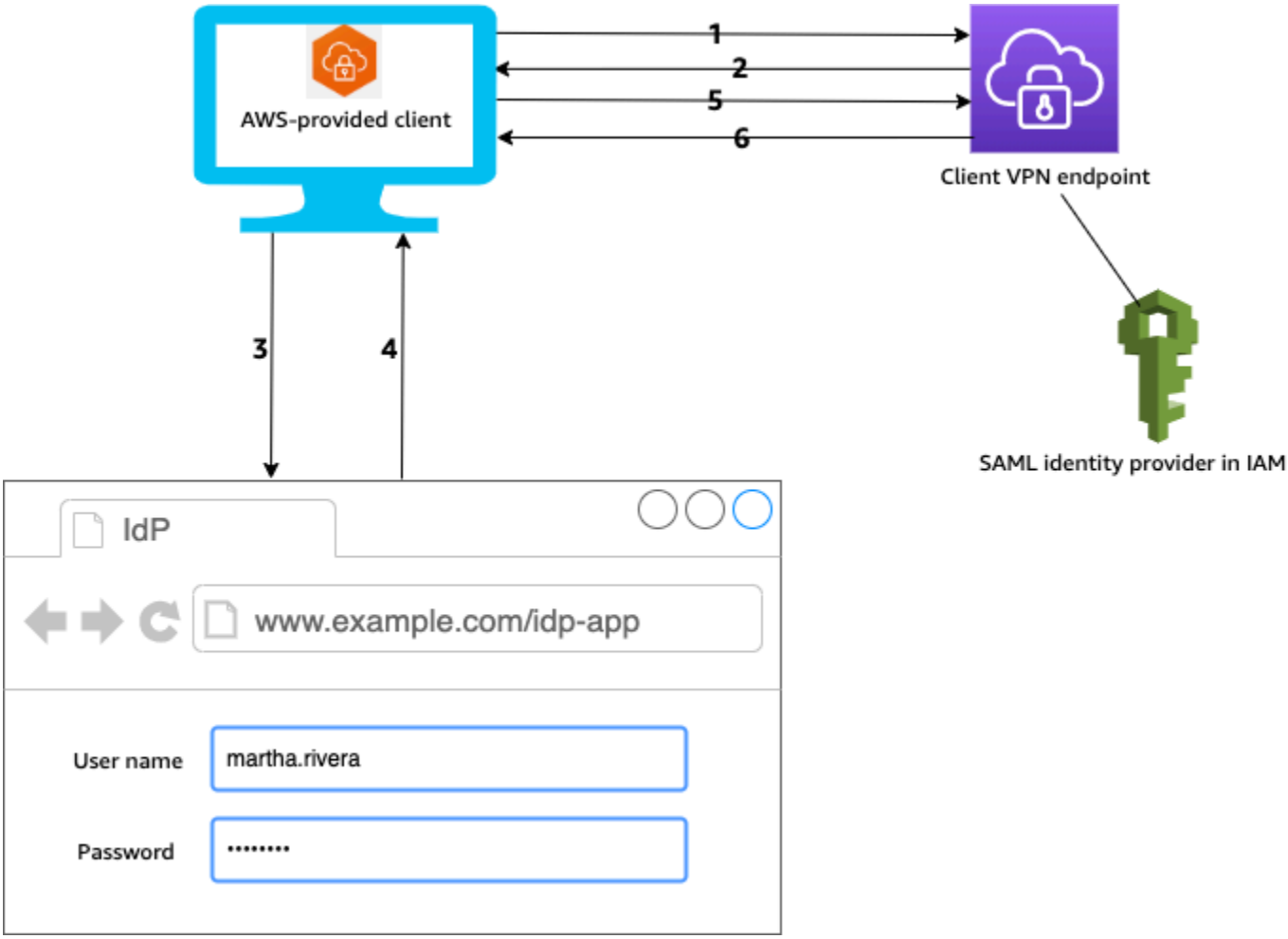
   > **Note**
   >
   > 您无需创建 IAM 角色即可使用 IAM SAML 身份提供程序。

5. 创建客户端 VPN 终端节点。

   将联合身份验证指定为身份验证类型，并指定您创建的 IAM SAML 身份提供程序。有关更多信息，请参阅创建 AWS Client VPN 终端节点。
6. 导出客户端配置文件并将其分发给用户。指示用户下载 AWS 提供的客户端的最新版本，然后使用它加载配置文件并连接到 Client VPN 端点。

身份验证工作流

下图针对使用基于 SAML 的联合身份验证的 Client VPN 端点，概述了其身份验证工作流。创建和配置 Client VPN 端点时，您需要指定 IAM SAML 身份提供商。



1. 用户在其设备上打开 AWS 提供的客户端，并启动与 Client VPN 端点的连接。
2. Client VPN 端点将根据 IAM SAML 身份提供商提供的信息，将 IdP URL 和身份验证请求发送回客户端。
3. AWS 提供的客户端会在用户设备上打开一个新的浏览器窗口。浏览器向 IdP 发出请求并显示登录页面。
4. 用户在登录页面上输入其凭证，IdP 将签名 SAML 断言发送回客户端。
5. AWS 提供的客户端将 SAML 声明发送到 Client VPN 端点。
6. Client VPN 端点验证断言，并允许或拒绝用户的访问。

基于 SAML 的联合身份验证的要求和注意事项

以下是基于 SAML 的联合身份验证的要求和注意事项。

- 有关在基于 SAML 的 IdP 中配置用户和组的配额和规则，请参阅用户和组配额。

- SAML 断言和 SAML 文档必须经过签名。
- AWS Client VPN 仅支持 SAML 断言中的 “ NotOnOrAfter” NotBefore 和 “” 和 “” 条件。AudienceRestriction
- 支持的最大 SAML 响应大小为 128 KB。
- AWS Client VPN 不提供签名的身份验证请求。
- 不支持 SAML 单点注销。用户可以通过与 AWS 提供的客户端断开连接来注销，也可以终止连接。
- Client VPN 端点仅支持单个 IdP。
- IdP 启用了 Multi-Factor Authentication (MFA) 时支持功能。
- 用户必须使用 AWS 提供的客户端连接到 Client VPN 端点。必须使用版本 1.2.0 或更高版本。有关更多信息，请参阅使用 AWS 提供的客户端进行 Connect。
- IdP 身份验证支持以下浏览器：Apple Safari、Google Chrome、Microsoft Edge 和 Mozilla Firefox。
- AWS 提供的客户端在用户设备上保留 TCP 端口 35001 用于 SAML 响应。
- 如果使用不正确或恶意 URL 更新了 IAM SAML 身份提供商的元数据文档，则可能会导致用户的身份验证问题，或导致网络钓鱼攻击。因此，建议您使用 AWS CloudTrail 监控对 IAM SAML 身份提供商所做的更新。有关更多信息，请参阅 IAM 用户指南中的使用 AWS CloudTrail记录 IAM 和 AWS STS 调用。
- AWS Client VPN 通过 HTTP 重定向绑定向 IdP 发送 AuthN 请求。因此，IdP 应该支持 HTTP 重定向绑定，并且它应该存在于 IdP 的元数据文档中。
- 对于 SAML 断言，您必须为 `NameID` 属性使用电子邮件地址格式。
- 当与 Client VPN 服务一起使用的证书更新时，无论是通过 ACM 自动轮换、手动导入新证书，还是通过 IAM Identity Center 的元数据更新，Client VPN 服务都将使用更新的证书自动更新客户端 VPN 终端节点。这是一个自动化流程，最多可能需要 5 个小时。

基于 SAML 的 IdP 配置资源

下表列出了我们测试过的基 IdPs 于 SAML 的产品 AWS Client VPN，以及可以帮助您配置 IdP 的资源。

IdP	资源
Okta	使用 SAM AWS Client VPN L 对用户进行身份验证

IdP	资源
微软 Entra ID（前身为 Azure 活动目录）	有关更多信息，请参阅微软文档网站上的教程：微软 Entra 单点登录 (SSO) 与 AWS ClientVPN 集成。
JumpCloud	与集成 AWS Client VPN
AWS IAM Identity Center	使用 IAM 身份中心和 AWS Client VPN 进行身份验证和授权

用于创建应用程序的服务提供商信息

要使用上表中未列出的 IdP 创建基于 SAML 的应用程序，请使用以下信息配置服务提供商信息。 AWS Client VPN

- 断言使用者服务 (ACS) URL：`http://127.0.0.1:35001`
- 受众 URI：`urn:amazon:webservices:clientvpn`

来自 IdP 的 SAML 响应中必须包含至少一个属性。以下是属性示例。

属性	描述
`FirstName`	用户的名字。
`LastName`	用户的姓氏。
`memberOf`	列出用户所属的一个或多个组。

> **Note**
>
> `memberOf` 属性是使用基于 Active Directory 或 SAML IdP 组的授权规则所必需的。此属性还区分大小写，且必须完全按照指定的方式进行配置。有关更多信息，请参阅 基于网络的授权 和 AWS Client VPN 授权规则。

支持自助服务门户

如果您为 Client VPN 端点启用了自助服务门户，用户将使用基于 SAML 的 IdP 凭证登录门户。

如果您的 IdP 支持多个断言消费者服务 (ACS) URLs，请将以下 ACS 网址添加到您的应用程序。

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

如果您在某个 GovCloud 区域中使用 Client VPN 终端节点，请改用以下 ACS URL。如果您使用同一 IDP 应用程序对标准版和 GovCloud 区域进行身份验证，则可以同时添加两者 URLs。

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

如果您的 IdP 不支持多个 ACS URLs，请执行以下操作：

1. 在您的 IdP 中创建其他基于 SAML 的应用程序，然后指定以下 ACS URL。

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. 生成并下载联合身份元数据文档。
3. 在与 Client VPN 终端节点相同的 AWS 账户中创建 IAM SAML 身份提供商。有关更多信息，请参阅 IAM 用户指南 中的创建 IAM SAML 身份提供商。

   > **Note**
   >
   > 除了为主应用程序创建的 IAM SAML 身份提供程序之外，还创建此 IAM SAML 身份提供程序。

4. 创建 Client VPN 端点，然后指定您创建的两个 IAM SAML 身份提供程序。

中的客户授权 AWS Client VPN

Client VPN 支持两种类型的客户端授权：安全组和基于网络的授权（使用授权规则）。

安全组

创建 Client VPN 端点时，您可以指定特定 VPC 中的安全组以应用到 Client VPN 端点。当您将子网与 Client VPN 端点关联时，我们会自动应用 VPC 的默认安全组。您可以在创建 Client VPN 端点之后更

改安全组。有关更多信息，请参阅在 AWS Client VPN中将安全组应用于目标网络。安全组与 Client VPN 网络接口关联。

您可以通过向应用程序的安全组添加规则，允许来自应用于关联的安全组的流量，从而允许 Client VPN 用户在 VPC 中访问您的应用程序。

反过来，您也可以通过不指定应用到关联的安全组或删除引用 Client VPN 端点安全组的规则来限制 Client VPN 用户的访问。您需要的安全组规则还可能取决于要配置的 VPN 访问类型。有关更多信息，请参阅Client VPN 场景和示例。

有关安全组的更多信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 的安全组。

基于网络的授权

使用授权规则实施基于网络的授权。对于每个要启用访问权限的网络，您必须配置授权规则来限制具有访问权限的用户。对于指定的网络，您可以配置允许访问的 Active Directory 组或基于 SAML 的 IdP 组。只有属于指定组的用户才能访问指定的网络。如果您未使用 Active Directory 或基于 SAML 的联合身份验证，或者您要对所有用户开放访问权限，则可以指定向所有客户端授予访问权限的规则。有关更多信息，请参阅 AWS Client VPN 授权规则。

任务

- 创建 AWS Client VPN 端点安全组规则

创建 AWS Client VPN 端点安全组规则

将子网与 Client VPN 相关联时应用的 VPC 的默认安全组可能会限制来自您想要允许的默认安全组流量，同时允许您不想要的流量。使用以下步骤可创建 Client VPN 端点安全组规则，以允许或限制与资源或应用程序关联的端点安全组的流量。有关安全组规则的更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

添加允许来自 Client VPN 端点安全组的流量的规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择安全组。
3. 选择与您的资源或应用程序关联的安全组，然后选择操作、编辑入站规则。
4. 选择 Add rule。
5. 对于 Type (类型)，请选择 All traffic (所有流量)。或者，您也可以限制访问特定类型的流量，例如 SSH。

对于源，请指定与 Client VPN 端点的目标网络（子网）关联的安全组的 ID。

6. 选择保存规则。

中的连接授权 AWS Client VPN

您可以为 Client VPN 端点配置客户端连接处理程序。使用处理程序，您可以根据设备、用户和连接属性运行授权新连接的自定义逻辑。客户端连接处理程序在 Client VPN 服务对设备和用户进行身份验证后运行。

要为 Client VPN 端点配置客户端连接处理程序，请创建一个 AWS Lambda 函数，该函数获取设备、用户和连接属性作为输入，然后向 Client VPN 服务返回允许或拒绝新连接的决定。您在 Client VPN 端点中指定该 Lambda 函数。当设备连接到 Client VPN 端点时，Client VPN 服务将代表您调用该 Lambda 函数。只允许该 Lambda 函数授权的连接来连接到 Client VPN 端点。

> **Note**
>
> 目前，唯一受支持的客户端连接处理程序类型是 Lambda 函数。

要求和注意事项

以下是客户端连接处理程序的要求和注意事项：

- Lambda 函数的名称必须以 `AWSClientVPN-` 前缀开头。
- 支持合格的 Lambda 函数。
- Lambda 函数必须与 Client VPN 终端节点位于同一个 AWS 区域和同一个 AWS 账户。
- Lambda 函数在 30 秒后超时。该值不能更改。
- Lambda 函数是同步调用的。在设备和用户身份验证之后、评估授权规则之前调用它。
- 如果为新连接调用了 Lambda 函数，但 Client VPN 服务没有从该函数获得预期响应，则 Client VPN 服务将拒绝连接请求。例如，如果 Lambda 函数受到限制、超时或遇到其他意外错误，或者函数的响应格式不是有效的，则可能会发生这种情况。
- 建议您为 Lambda 函数配置预置并发，以使其能够在不影响延迟的情况下进行扩展。
- 如果您更新 Lambda 函数，与 Client VPN 端点的现有连接不受影响。您可以终止现有连接，然后指示客户端建立新连接。有关更多信息，请参阅 终止 AWS Client VPN 客户端连接。

- 如果客户端使用 AWS 提供的客户端连接到 Client VPN 端点，则必须在 Windows 上使用 1.2.6 或更高版本，对于 macOS 必须使用 1.2.4 或更高版本。有关更多信息，请参阅使用 AWS 提供的客户端进行连接。

Lambda 接口

Lambda 函数从 Client VPN 服务获取设备属性、用户属性和连接属性作为输入。然后，它必须将是允许还是拒绝连接的决定返回给 Client VPN 服务。

请求 schema

Lambda 函数获取包含以下字段的 JSON blob 作为输入。

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id` – 到 Client VPN 端点的客户端连接的 ID。
- `endpoint-id` – Client VPN 端点的 ID。
- `common-name` – 设备标识符。在为设备创建的客户端证书中，公用名唯一标识设备。
- `username` – 用户标识符（如果适用）。对于 Active Directory 身份验证，这是用户名。对于基于 SAML 的联合身份验证，这是 `NameID`。对于双向身份验证，此字段为空。
- `platform` – 客户端操作系统平台。
- `platform-version` – 操作系统的版本。当 OpenVPN 客户端配置中存在 `--push-peer-info` 指令、客户端连接到 Client VPN 端点且客户端运行 Windows 平台时，Client VPN 服务会提供值。
- `public-ip` – 连接设备的公有 IP 地址。
- `client-openvpn-version` – 客户端使用的 OpenVPN 版本。

- `aws-client-version`— AWS 客户端版本。
- `groups` – 组标识符（如果适用）。对于 Active Directory 身份验证，这将是 Active Directory 组列表。对于基于 SAML 的联合身份验证，这将是身份提供商 (IdP) 组列表。对于双向身份验证，此字段为空。
- `schema-version` – schema 版本。默认为 `v3`。

响应 schema

Lambda 函数必须返回以下字段。

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `allow` – 必需。一个布尔值 (`true` | `false`)，指示是允许还是拒绝新连接。
- `error-msg-on-denied-connection` – 必需。最多包含 255 个字符的字符串，可用于在 Lambda 函数拒绝连接时向客户端提供步骤和指导。如果在 Lambda 函数运行期间出现故障（例如，由于限制），将向客户端返回以下默认消息。

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses` – 必需。如果您使用 Lambda 函数进行状况评估，则这是连接设备的状态列表。您可以根据设备的状况评估类别定义状态名称，例如 `compliant`、`quarantined`、`unknown` 等。每个名称最长可达 255 个字符。您最多可以指定 10 个状态。
- `schema-version` – 必需。schema 版本。默认为 `v3`。

您可以将同一个 Lambda 函数用于同一区域中的多个 Client VPN 端点。

有关创建 Lambda 函数的更多信息，请参阅 AWS Lambda 开发人员指南中的 AWS Lambda入门。

使用客户端连接处理程序进行状况评测

您可以使用客户端连接处理程序将 Client VPN 端点与现有设备管理解决方案集成，以评估连接设备的状况合规性。要使 Lambda 函数用作设备授权处理程序，请对 Client VPN 端点使用双向身份验证。为

将连接到 Client VPN 端点的每个客户端（设备）创建唯一的客户端证书和密钥。Lambda 函数可以使用客户端证书的唯一公用名（从 Client VPN 服务传递）来识别设备并从设备管理解决方案中获取其状况合规性状态。您可以将双向身份验证与基于用户的身份验证结合使用。

或者，您可以在 Lambda 函数本身中进行基本状况评估。例如，您可以评估 Client VPN 服务传递给 Lambda 函数的 `platform` 和 `platform-version` 字段。

> **Note**
>
> 虽然连接处理程序可用于强制执行 AWS Client VPN 应用程序的最低版本，但连接处理程序`aws-client-version`中的字段仅适用于 AWS Client VPN 应用程序，并且是通过用户设备上的环境变量填充的。

启用客户端连接处理程序

要启用客户端连接处理程序，请创建或修改 Client VPN 端点，然后指定 Lambda 函数的 Amazon 资源名称（ARN）。有关更多信息，请参阅 创建 AWS Client VPN 终端节点 和 修改 AWS Client VPN 终端节点。

服务相关角色

AWS Client VPN 在您的账户中自动创建一个名AWSServiceRoleForClientVPNConnections为的服务相关角色。当与 Client VPN 端点建立连接时，该角色有权调用 Lambda 函数。有关更多信息，请参阅将服务相关角色用于 AWS Client VPN。

监控连接授权失败

您可以查看到 Client VPN 端点的连接的连接授权状态。有关更多信息，请参阅查看 AWS Client VPN 客户端连接。

当客户端连接处理程序用于状况评估时，您还可以在连接日志中查看连接到 Client VPN 端点的设备的状况合规性状态。有关更多信息，请参阅AWS Client VPN 端点的连接日志。

如果设备未通过连接授权，则连接日志中的 `connection-attempt-failure-reason` 字段将返回以下失败原因之一：

- `client-connect-failed` – Lambda 函数阻止建立连接。

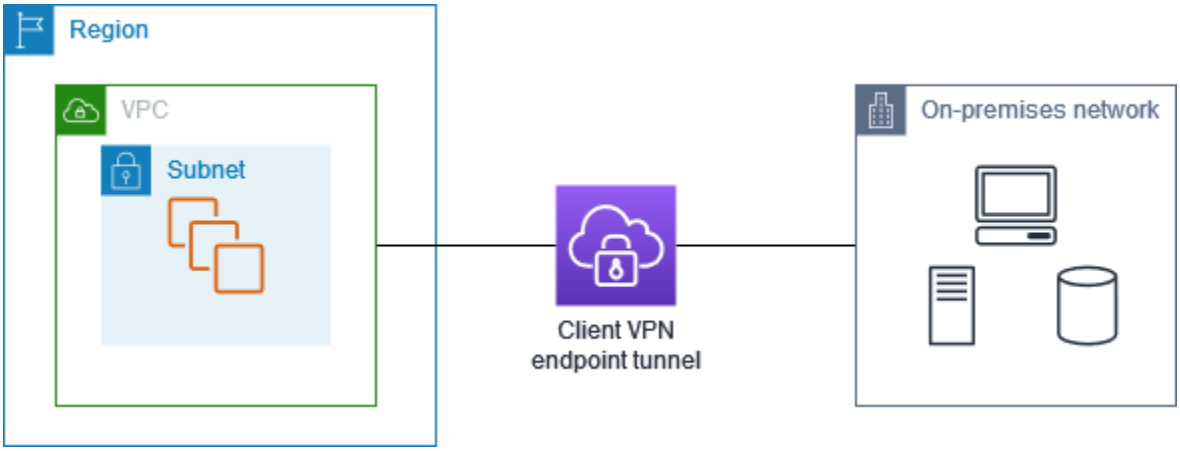
- `client-connect-handler-timed-out` – Lambda 函数超时。
- `client-connect-handler-other-execution-error` – Lambda 函数遇到意外错误。
- `client-connect-handler-throttled` – Lambda 函数受到限制。
- `client-connect-handler-invalid-response` – Lambda 函数返回的响应无效。
- `client-connect-handler-service-error` – 尝试连接期间出现服务端错误。

端点上的分割隧道 AWS Client VPN

默认情况下，当您拥有 Client VPN 端点时，所有来自客户端的流量都通过 Client VPN 隧道进行路由。当您在 Client VPN 端点上启用拆分隧道时，我们会将 Client VPN 端点路由表上的路由推送到连接到 Client VPN 端点的设备。这可确保仅目的地为与 Client VPN 端点路由表中的路由匹配的网络的流量能够通过 Client VPN 隧道进行路由。

当您不希望所有用户流量都通过 Client VPN 端点路由时，可以使用拆分隧道 Client VPN 端点。

在以下示例中，在 Client VPN 端点上启用了拆分隧道。只有发往 VPC（`172.31.0.0/16`）的流量才会通过 Client VPN 隧道进行路由。发往本地资源的流量不会通过 Client VPN 隧道进行路由。



拆分隧道的优势

Client VPN 端点上的拆分隧道提供了以下好处：

- 您可以通过只让 AWS 目标流量通过 VPN 隧道来优化来自客户端的流量的路由。
- 您可以减少来自的传出流量 AWS，从而降低数据传输成本。

路由注意事项

- 当您启用拆分隧道模式时，Client VPN 端点的路由表中的所有路由都将在建立 VPN 连接时添加到客户端的路由表中。此操作不同于默认行为，它将使用条目 `0.0.0.0/0` 覆盖客户端路由表，以便通过 VPN 路由所有流量。

> **Note**
>
> 使用分割隧道模式时向 Client VPN 终端节点的路由表中添加 0.0.0.0/0 路由可能会导致连接中断，因此不建议这样做

- 启用拆分隧道模式后，对 Client VPN 端点路由表的任何修改都将导致所有客户端连接重置。

启用拆分隧道

您可以在新的或现有的 Client VPN 端点上启用拆分隧道。有关更多信息，请参阅以下主题：

- 创建 AWS Client VPN 终端节点
- 修改 AWS Client VPN 终端节点

AWS Client VPN 端点的连接日志

连接日志是一项功能 AWS Client VPN ，可让您捕获 Client VPN 端点的连接日志。

连接日志包含连接日志条目，这些条目捕获有关连接事件的信息，例如客户端（最终用户）连接、尝试连接或断开连接 Client VPN 端点的时间。您可以使用此信息运行取证、分析 Client VPN 终端节点的使用方式或调试连接问题。

连接日志在所有可用的区域中都可 AWS Client VPN 用。连接日志会发布到您账户中的 CloudWatch 日志日志组。

> **Note**
>
> 不记录失败的双向身份验证尝试。

连接日志条目

连接日志条目是一个由键值对组成的采用 JSON 格式的 Blob。以下是一个示例连接日志条目。

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

连接日志条目包含以下键：

- `connection-log-type` – 连接日志条目的类型（`connection-attempt` 或 `connection-reset`）。
- `connection-attempt-status` – 连接请求的状态（`successful`、`failed`、`waiting-for-assertion` 或 NA）。
- `connection-reset-status` – 连接重置事件的状态（NA 或 `assertion-received`）。
- `connection-attempt-failure-reason` – 连接失败的原因（如果适用）。
- `connection-id` – 连接的 ID。
- `client-vpn-endpoint-id` – 与之建立连接的 Client VPN 端点的 ID。
- `transport-protocol` – 用于连接的传输协议。
- `connection-start-time` – 连接的开始时间。

- `connection-last-update-time` – 连接的上次更新时间。此值在日志中定期更新。
- `client-ip`— 客户端的 IP 地址，该地址是从客户端 VPN 端点的客户端 IPv4 CIDR 范围中分配的。
- `common-name` – 用于基于证书的身份验证的证书的公用名。
- `device-type` – 最终用户用于连接的设备类型。
- `device-ip` – 设备的公有 IP 地址。
- `port` – 连接的端口号。
- `ingress-bytes` – 连接的入口（入站）字节数。此值在日志中定期更新。
- `egress-bytes` – 连接的出口（出站）字节数。此值在日志中定期更新。
- `ingress-packets` – 连接的入口（入站）数据包的数量。此值在日志中定期更新。
- `egress-packets` – 连接的出口（出站）数据包的数量。此值在日志中定期更新。
- `connection-end-time` – 连接的结束时间。如果连接仍在进行中或连接尝试失败，则值为 `NA`。
- `posture-compliance-statuses` – 客户端连接处理程序返回的状况合规性状态（如果适用）。
- `username` — 当对端点使用基于用户的身份验证（AD 或 SAML）时，将记录用户名。
- `connection-duration-seconds` — 连接的持续时间（以秒为单位）。等于 “” 和 connection-start-time “connection-end-time” 之差。

有关启用连接日志记录的更多信息，请参阅 AWS Client VPN 连接日志。

Client VPN 扩展注意事项

创建 Client VPN 端点时，请考虑您计划支持的最大并发 VPN 连接数。您应考虑当前支持的客户端数量，并考虑您的 Client VPN 端点是否可以在需要时通过扩展来满足额外的需求。

以下因素会影响 Client VPN 端点上可支持的最大并发 VPN 连接数：

客户端 CIDR 范围大小

创建 Client VPN 端点时，必须指定客户端 CIDR 范围，即介于 /12 和 /22 网络 IPv4 掩码之间的 CIDR 块。将从客户端 CIDR 范围中为每个到 Client VPN 端点的 VPN 连接分配一个唯一的 IP 地址。客户端 CIDR 范围中的一部分地址还用于支持 Client VPN 端点的可用性模型，无法分配给客户端。创建 Client VPN 端点后，您无法更改客户端 CIDR 范围。

通常，建议您指定一个客户端 CIDR 范围，其中包含的 IP 地址数量是您计划在 Client VPN 端点上支持的 IP 地址数量（以及并发连接数量）的两倍。

关联子网的数量

当您将子网与 Client VPN 端点关联时，您允许用户建立与 Client VPN 端点的 VPN 会话。您可以将多个子网与一个 Client VPN 端点关联以实现高可用性，并实现附加连接容量。

以下是基于 Client VPN 端点的子网关联数的支持并发 VPN 连接的数量。

子网关联	支持的连接数
1	7,000
2	36,500
3	66,500
4	96,500
5	126,000

您无法将同一可用区内的多个子网与一个客户端 VPN 终端节点关联。因此，子网关联的数量还取决于一个区域中可用的可用 AWS 区域数量。

例如，如果您希望支持 8,000 个到 Client VPN 端点的 VPN 连接，请指定最小客户端 CIDR 范围大小 /18（16,384 个 IP 地址），并将至少 2 个子网与 Client VPN 端点关联。

如果您不确定 Client VPN 端点的预期 VPN 连接数量，建议您指定 /16 或更大的 CIDR 块大小。

有关使用客户端 CIDR 范围和目标网络的规则和限制的更多信息，请参阅使用 AWS Client VPN的规则和最佳实践。

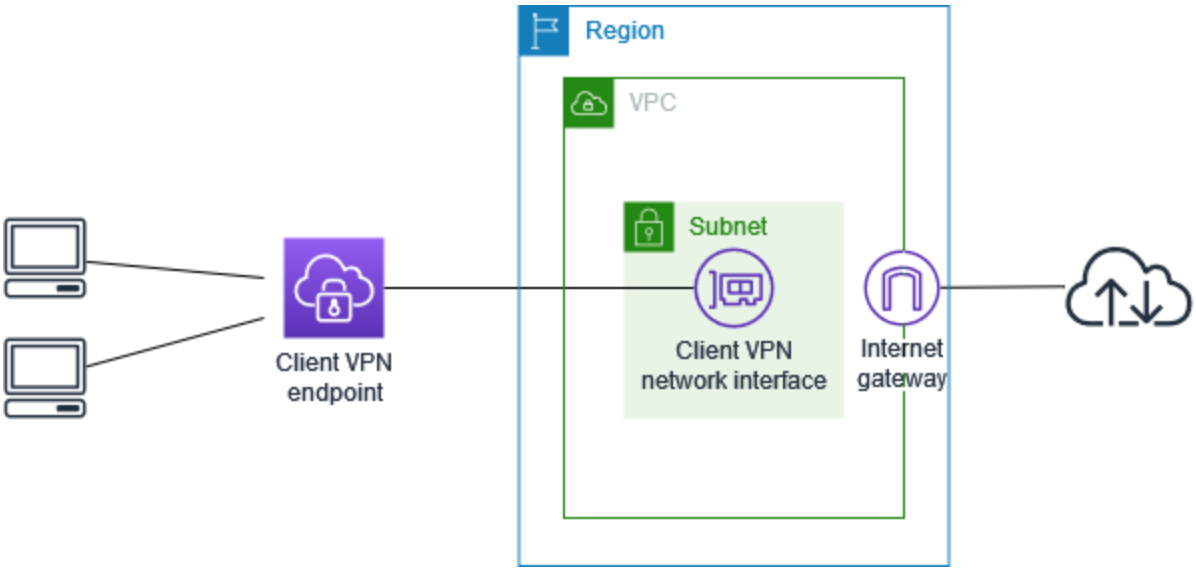
有关 Client VPN 端点配额的更多信息，请参阅AWS Client VPN 配额。

开始使用 AWS Client VPN

在本教程中，您将创建一个执行以下操作的 AWS Client VPN 端点：

- 为所有客户端提供对单个 VPC 的访问权限。
- 为所有客户端提供对 Internet 的访问权限。
- 使用双向身份验证。

下图表示完成本教程后 VPC 和 Client VPN 端点的配置。



步骤

- 先决条件
- 步骤 1：生成服务器和客户端证书以及密钥
- 步骤 2：创建 Client VPN 端点
- 步骤 3：关联目标网络
- 步骤 4：添加 VPC 的授权规则
- 步骤 5：提供对 Internet 的访问
- 步骤 6：验证安全组要求
- 步骤 7：下载 Client VPN 端点配置文件
- 步骤 8：连接到 Client VPN 端点

先决条件

在开始本入门教程之前，请确保您具有以下各项：

- 使用 Client VPN 端点所需的权限。
- 将证书导入到 AWS Certificate Manager中所需的权限。
- 至少有一个子网和一个 Internet 网关的 VPC。与您的子网关联的路由表必须具有通往 Internet 网关的路由。

步骤 1：生成服务器和客户端证书以及密钥

本教程使用双向身份验证。借助双向身份验证，Client VPN 使用证书在客户端和 Client VPN 端点之间执行身份验证。您将需要具有服务器证书和密钥，以及至少一个客户端证书和密钥。服务器证书至少需要导入 AWS Certificate Manager (ACM)，并在创建 Client VPN 端点时指定。将客户端证书导入 ACM 是可选的。

如果您还没有可用于此目的的证书，则可以使用 OpenVPN easy-rsa 实用程序创建它们。有关使用 OpenVPN easy-rsa 实用程序生成服务器和客户端证书和密钥并将其导入 ACM 的详细步骤，请参阅双向认证 AWS Client VPN。

> **Note**
>
> 服务器证书必须使用您要创建 Client VPN 终端节点的同一 AWS 区域配置或导入到 AWS Certificate Manager (ACM) 中。

步骤 2：创建 Client VPN 端点

Client VPN 终端节点是您创建并配置以用于启用和管理 Client VPN 会话的资源。这是所有 Client VPN 会话的终止点。

创建 Client VPN 端点

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 端点），然后选择 Create Client VPN endpoint（创建 Client VPN 端点）。
3. （可选）提供 Client VPN 终端节点的名称标签和描述。

4. 对于客户端 IPv4 CIDR，以 CIDR 表示法指定一个 IP 地址范围，从中分配客户端 IP 地址。

> **Note**
>
> 此地址范围不能与目标网络地址范围、VPC 地址范围或将与 Client VPN 端点关联的任何路由重叠。客户端地址范围必须至少为 /22 且不大于 /12 CIDR 块大小。创建 Client VPN 终端节点后，您无法更改客户端地址范围。

5. 对于 Server certificate ARN（服务器证书 ARN），选择您在步骤 1 中生成的服务器证书的 ARN。
6. 在 Authentication options（身份验证选项）下，选择 Use mutual authentication（使用双向身份验证），然后对于 Client certificate ARN（客户端证书 ARN），选择要用作客户端证书的证书的 ARN。

   如果服务器证书和客户端证书是由相同证书颁发机构（CA）颁发的，则您可以选择指定将服务器证书 ARN 同时 用于服务器和客户端证书。在这种情况下，可以使用与服务器证书对应的任何客户端证书进行身份验证。
7. （可选）指定用于 DNS 解析的 DNS 服务器。要使用自定义 DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）和 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定要使用的 DNS 服务器的 IP 地址。要使用 VPC DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）或 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定 IP 地址，并添加 VPC DNS 服务器 IP 地址。

> **Note**
>
> 验证客户端是否能访问 DNS 服务器。

8. 保留其余原定设置，然后选择 Create Client VPN endpoint（创建 Client VPN 端点）。

在您创建 Client VPN 端点后，其状态为 `pending-associate`。仅当您关联至少一个目标网络后，客户端才能建立 VPN 连接。

有关您可以为 Client VPN 端点指定的选项的更多信息，请参阅创建 AWS Client VPN 终端节点。

步骤 3：关联目标网络

要使客户端能够建立 VPN 会话，请将一个目标网络与 Client VPN 端点关联。目标网络是 VPC 中的一个子网。

将目标网络与 Client VPN 端点关联

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择您在上一过程中创建的 Client VPN 端点，然后依次选择 Target network associations（目标网络关联）和 Associate target network（关联目标网络）。
4. 对于 VPC，选择您要在其中放置子网的 VPC。
5. 对于 Choose a subnet to associate（选择要关联的子网），选择要与 Client VPN 终端节点关联的子网。
6. 选择 Associate target network（关联目标网络）。
7. 如果授权规则允许，则一个子网关联就足以供客户端访问 VPC 的整个网络。您可以关联其他子网，以便在可用区受损时提供高可用性。

当您将第一个子网与 Client VPN 端点关联时，会发生以下情况：

- Client VPN 端点的状态更改为 `available`。客户端现在可以建立 VPN 连接，但无法访问 VPC 中的任何资源，直到您添加授权规则。
- VPC 的本地路由会自动添加到 Client VPN 端点路由表中。
- VPC 的原定设置安全组将自动应用于 Client VPN 端点。

步骤 4：添加 VPC 的授权规则

要使客户端能够访问 VPC，Client VPN 端点的路由表中需要有到 VPC 的路由，并且需要有授权规则。在上一步中，已经自动添加路由。在本教程中，我们要向所有用户授予对 VPC 的访问权限。

添加 VPC 的授权规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要将授权规则添加到的 Client VPN 端点。选择授权规则，然后选择添加授权规则。
4. 对于 Destination network to enable access（要启用访问权限的目标网络），输入您要允许访问的网络的 CIDR。例如，要允许访问整个 VPC，请指定 VPC 的 IPv4 CIDR 块。
5. 对于授予访问权限，选择允许所有用户访问。
6. （可选）对于 Description（描述），输入授权规则的简要描述。

7. 选择添加授权规则。

步骤 5：提供对 Internet 的访问

您可以提供对连接到 VPC 的其他网络的访问权限，例如 AWS 服务、对等网络 VPCs、本地网络和互联网。对于每个额外的网络，您必须在 Client VPN 端点的路由表中添加到网络的路由，并配置授权规则以向客户端授予访问权限。

在本教程中，我们希望授予所有用户对 Internet 以及 VPC 的访问权限。您已经配置了对 VPC 的访问权限，因此这一步骤适用于对 Internet 的访问权限。

提供对 Internet 的访问权限

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择您为本教程创建的 Client VPN 端点。选择 Route Table（路由表），然后选择 Create Route（创建路由）。
4. 对于 Route destination (路由目标)，请输入 `0.0.0.0/0`。对于 Subnet ID for target network association（用于目标网络关联的子网 ID），指定用来路由流量的子网的 ID。
5. 选择 Create Route (创建路由)。
6. 选择 Authorization rules（授权规则），然后选择 Add authorization rule（添加授权规则）。
7. 对于 Destination network to enable access（要启用访问权限的目标网络），输入 `0.0.0.0/0`，并选择 Allow access to all users（允许所有用户访问）。
8. 选择添加授权规则。

步骤 6：验证安全组要求

在本教程中，在步骤 2 中创建 Client VPN 端点期间没有指定安全组。这意味着，当关联目标网络时，VPC 的原定设置安全组会自动应用于 Client VPN 端点。因此，VPC 的原定设置安全组现在应与 Client VPN 端点关联。

验证以下安全组要求

- 与您正在用来路由流量的子网相关联的安全组（在本例中为原定设置的 VPC 安全组）允许向 Internet 发送出站流量。为此，添加一个允许所有流量到达目标 `0.0.0.0/0` 的出站规则。

- VPC 中资源的安全组具有一条规则，此规则支持从应用于 Client VPN 端点的安全组进行访问（此例中为原定设置的 VPC 安全组）。这将允许您的客户端访问 VPC 中的资源。

有关更多信息，请参阅 安全组。

步骤 7：下载 Client VPN 端点配置文件

下一步是下载并准备 Client VPN 端点配置文件。配置文件包含建立 VPN 连接所需的 Client VPN 端点详细信息和证书信息。您可以将此文件提供给需要连接到 Client VPN 端点的终端用户。终端用户使用此文件配置其 VPN 客户端应用程序。

下载并准备 Client VPN 端点配置文件

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择您为本教程创建的 Client VPN 端点，然后选择 Download client configuration（下载客户端配置）。
4. 找到步骤 1 中生成的客户端证书和密钥。可以在克隆的 OpenVPN easy-rsa 存储库中的以下位置找到客户端证书和密钥：
   - 客户端证书 – `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - 客户端密钥 – `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. 使用首选文本编辑器打开 Client VPN 终端节点配置文件。将 `<cert></cert>` 和 `<key></key>` 标签添加到文件中。将客户端证书的内容以及私有密钥的内容放在相应的标签之间，例如：

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. 保存并关闭 Client VPN 端点配置文件。
7. 将 Client VPN 端点配置文件分发给终端用户。

有关 Client VPN 端点配置文件的更多信息，请参阅AWS Client VPN 端点配置文件导出。

步骤 8：连接到 Client VPN 端点

您可以使用 AWS 提供的客户端或其他基于 OpenVPN 的客户端应用程序以及您刚刚创建的配置文件连接到 Client VPN 端点。有关更多信息，请参阅 AWS Client VPN 用户指南。

与... 一起工作 AWS Client VPN

以下主题说明使用 Client VPN 所需执行的主要管理任务：

- 访问自助服务门户：配置对 Client VPN 自助服务门户的访问权限，以便客户端可以自己下载 Client VPN 端点配置文件。有关访问自助服务门户的信息，请参阅 the section called “自助服务门户访问”。
- 授权规则：添加授权规则以控制客户端对指定网络的访问。有关添加授权规则的信息，请参阅 the section called “授权规则”。
- 客户端证书吊销列表：使用客户端证书吊销列表撤销对 Client VPN 端点的访问权限。有关客户端证书吊销列表的信息，请参阅 the section called “客户端证书吊销列表”。
- 客户端连接：查看或终止客户端与 Client VPN 端点的连接。有关查看或终止客户端连接的信息，请参阅 the section called “客户端连接”。
- 客户端登录横幅：建立 VPN 会话时在 Client VPN 桌面应用程序上添加文本横幅。您可以使用文本横幅满足监管和合规性需求。有关登录横幅的信息，请参阅 the section called “客户端登录横幅”。
- 客户端路由强制-在通过 VPN 连接的设备上强制执行管理员定义的路由。有关客户端路由强制的更多信息，请参阅the section called “使用客户端路由强制执行”。
- Client VPN 端点：配置 Client VPN 端点以管理和控制所有 VPN 会话。有关配置端点的信息，请参阅 the section called “了解如何查看、监控和管理 SageMaker 端点。”。
- 连接日志：为新的或现有的 Client VPN 端点启用连接日志记录，以开始捕获连接日志。有关连接日志记录的信息，请参阅 the section called “连接日志”。
- 客户端配置文件导出：配置 Client VPN 客户端建立 VPN 连接所需的客户端配置文件。配置该文件后，将其下载（导出）以分发给客户端。有关导出客户端配置文件的更多信息，请参阅 the section called “客户端配置文件导出”。
- 路由：为每个 Client VPN 路由配置授权规则，以指定哪些客户端可以访问目标网络。有关配置授权规则的信息，请参阅 the section called “授权规则”。
- 目标网络：将目标网络与 Client VPN 端点相关联，使客户端能够连接到此网络并建立 VPN 连接。有关目标网络的信息，请参阅 the section called “目标网络”。
- 最长 VPN 会话持续时间：设置最长 VPN 会话持续时间选项，以满足您的安全性和合规性要求。有关最长 VPN 会话持续时间的信息，请参阅 the section called “最长 VPN 会话持续时间”。

AWS Client VPN 访问自助服务门户

如果您为 Client VPN 端点启用了自助服务门户，则可以为客户端提供自助服务门户 URL。客户端可以在 Web 浏览器中访问门户，并使用基于用户的凭证登录。在门户中，客户端可以下载 Client VPN 端点配置文件，也可以下载所 AWS 提供客户端的最新版本。

以下规则适用：

- 自助服务门户不适用于使用双向身份验证进行身份验证的客户端。
- 自助服务门户中提供的配置文件与您使用 Amazon VPC 控制台或导出的配置文件相同 AWS CLI。如果在将配置文件分发给客户端之前需要对其进行自定义，则必须自行将自定义文件分发给客户端。
- 您必须为 Client VPN 端点启用自助服务门户选项，否则客户端无法访问门户。如果未启用此选项，您可以修改 Client VPN 端点以启用它。

启用自助服务门户选项后，为客户提供以下内容之一 URLs：

- `https://self-service.clientvpn.amazonaws.com/`

  如果客户端使用此 URL 访问门户，则必须输入 Client VPN 端点的 ID，然后才能登录。
- `https://self-service.clientvpn.amazonaws.com/endpoints/`*`<endpoint-id>`*

  例如*`<endpoint-id>`*，将前面的 URL 替换为您的 Client VPN 终端节点的 ID `cvpn-endpoint-0123456abcd123456`。

您还可以在describe-client-vpn-endpoints AWS CLI 命令输出中查看自助服务门户的 URL。或者，该 URL 可在 Amazon VPC 控制台的 Client VPN Endpoints（Client VPN 端点）页面上的 Details（详细信息）选项卡中找到。

有关配置自助服务门户以用于联合身份验证的更多信息，请参阅支持自助服务门户。

AWS Client VPN 授权规则

授权规则充当授予网络访问权限的防火墙规则。通过添加授权规则，您可以向特定客户端授予对指定网络的访问权限。对于要授予访问权限的每个网络，您都应该设置一个授权规则。可以使用控制台和 AWS CLI向 Client VPN 端点添加授权规则。

> **Note**
>
> 在评估授权规则时，Client VPN 会使用最长前缀匹配。有关更多详细信息，请参阅 Amazon VPC 用户指南中的故障排查主题 故障排除 AWS Client VPN：Active Directory 群组的授权规则未按预期运行 和路由优先级。

可供了解授权规则的关键点

以下几点解释了授权规则的一些行为：

- 要允许访问目标网络，必须显式添加授权规则。原定设置行为是拒绝访问。
- 您无法添加授权规则以限制 对目标网络的访问。
- `0.0.0.0/0` CIDR 作为特殊情况进行处理。无论创建授权规则的顺序如何，它都是最后处理的。
- `0.0.0.0/0` CIDR 可被视为“任何目标”或“其他授权规则未定义的任何目标”。
- 最长前缀匹配是优先的规则。

主题

- Client VPN 授权规则场景示例
- 向 AWS Client VPN 端点添加授权规则
- 从 AWS Client VPN 端点删除授权规则
- 查看 AWS Client VPN 授权规则

Client VPN 授权规则场景示例

本节介绍授权规则的工作原理 AWS Client VPN。它包括可供了解授权规则的关键点、示例架构以及对映射到示例架构的示例场景的讨论。

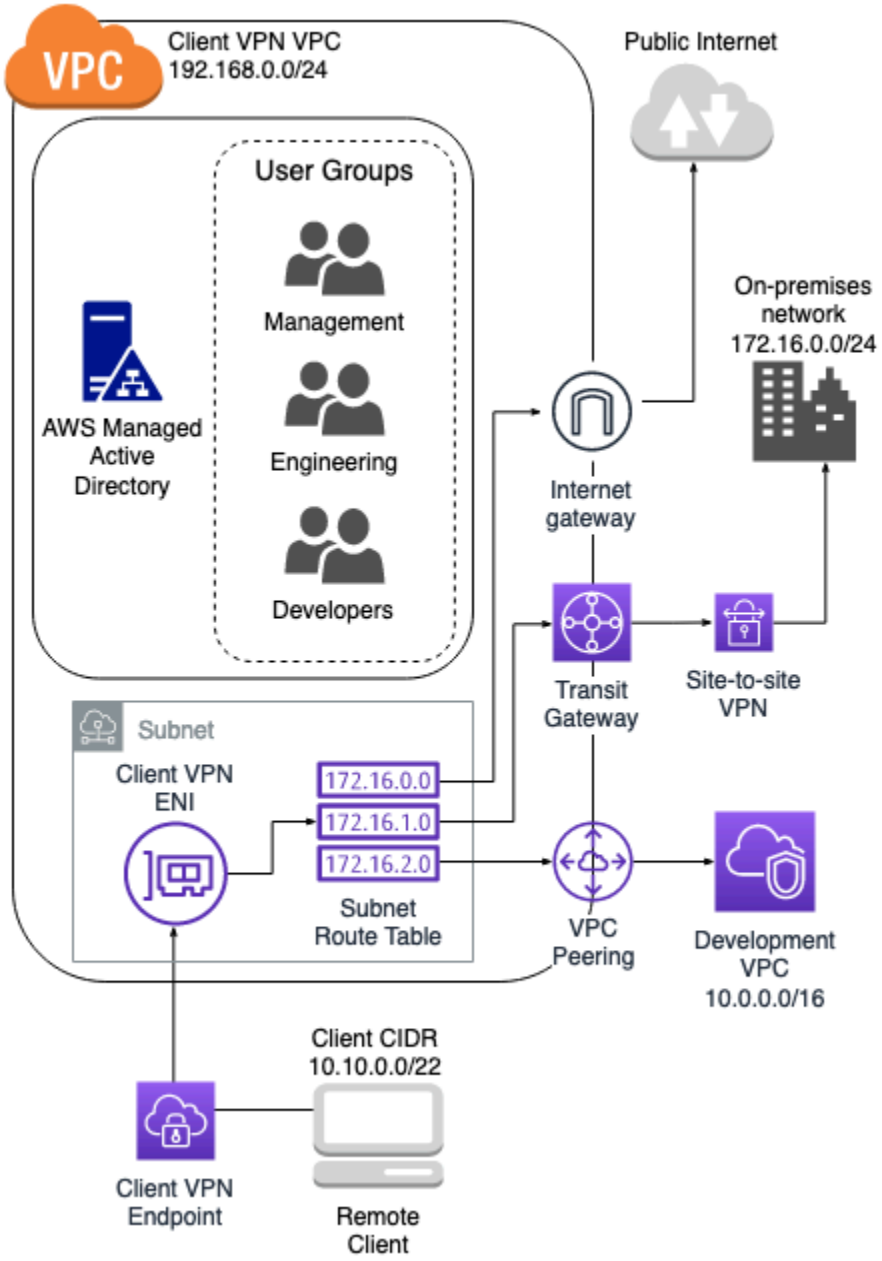
场景

- the section called “示例架构”
- the section called “访问单个目标”
- the section called “使用任何目标（0.0.0.0/0）CIDR”
- the section called “更长的 IP 前缀匹配”

- the section called “重叠 CIDR（同一个组）”
- the section called “其他 0.0.0.0/0 规则”
- the section called “为 192.168.0.0/24 添加规则”
- the section called “访问所有用户组”

授权规则场景的示例架构

下图显示了用于本节中的示例场景的示例架构。



访问单个目标

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
向经理组提供对 Client VPN VPC 的访问权限	S-xxxxx16	False	192.168.0.0/24

产生的行为

- 工程组只能访问 `172.16.0.0/24`。
- 开发组只能访问 `10.0.0.0/16`。
- 经理组只能访问 `192.168.0.0/24`。
- 所有其他流量都由 Client VPN 端点丢弃。

> **Note**
>
> 在这种情况下，任何用户组都无法访问公共互联网。

使用任何目标（0.0.0.0/0）CIDR

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
	S-xxxxx15	False	10.0.0.0/16

规则描述	组 ID	允许所有用户访问	目标 CIDR
向开发组提供对开发 VPC 的访问权限			
向经理组提供对任何目标的访问权限	S-xxxxx16	False	0.0.0.0/0

产生的行为

- 工程组只能访问 `172.16.0.0/24`。
- 开发组只能访问 `10.0.0.0/16`。
- 经理组可以访问公共互联网和 `192.168.0.0/24`，但无法访问 `172.16.0.0/24` 或 `10.0.0/16`。

> **Note**
>
> 在这种情况下，因为没有规则引用 `192.168.0.0/24`，所以访问该网络的权限也由 `0.0.0.0/0` 规则提供。
> 包含 `0.0.0.0/0` 的规则始终最后求值，而无论创建规则的顺序如何。因此，请记住，在 `0.0.0.0/0` 之前求值的规则在确定 `0.0.0.0/0` 授予对哪些网络的访问权限方面起着重要作用。

更长的 IP 前缀匹配

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
	S-xxxxx16	False	0.0.0.0/0

规则描述	组 ID	允许所有用户访问	目标 CIDR
向经理组提供对任何目标的访问权限			
向经理组提供对开发 VPC 中单个主机的访问权限	S-xxxxx16	False	10.0.2.119/32

产生的行为

- 工程组只能访问 `172.16.0.0/24`。
- 开发组可以访问 `10.0.0.0/16`，但单个主机 `10.0.2.119/32` 除外。
- 经理组可以访问公共互联网、`192.168.0.0/24` 以及开发 VPC 中的单个主机（`10.0.2.119/32`），但无权访问 `172.16.0.0/24` 或开发 VPC 中的任何剩余主机。

> **Note**
>
> 在这里，您可以看到具有较长 IP 前缀的规则如何优先于具有较短 IP 前缀的规则。如果您想让开发组有权访问 `10.0.2.119/32`，则需要添加一条附加规则向开发团队授予对 `10.0.2.119/32` 的访问权限。

重叠 CIDR（同一个组）

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
	S-xxxxx16	False	0.0.0.0/0

规则描述	组 ID	允许所有用户访问	目标 CIDR
向经理组提供对任何目标的访问权限			
向经理组提供对开发 VPC 中单个主机的访问权限	S-xxxxx16	False	10.0.2.119/32
向工程组提供对本地网络中较小子网的访问权限	S-xxxxx14	False	172.16.0.128/25

产生的行为

- 开发组可以访问 `10.0.0.0/16`，但单个主机 `10.0.2.119/32` 除外。
- 经理组可以访问公共互联网、`192.168.0.0/24` 以及 `10.0.2.119/32` 网络中的单个主机（`10.0.0.0/16`），但无权访问 `172.16.0.0/24` 或 `10.0.0.0/16` 网络中的任何剩余主机。
- 工程组有权访问 `172.16.0.0/24`，包括更具体的子网 `172.16.0.128/25`。

其他 0.0.0.0/0 规则

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
向经理组提供对任何目标的访问权限	S-xxxxx16	False	0.0.0.0/0

规则描述	组 ID	允许所有用户访问	目标 CIDR
向经理组提供对开发 VPC 中单个主机的访问权限	S-xxxxx16	False	10.0.2.119/32
向工程组提供对本地网络中较小子网的访问权限	S-xxxxx14	False	172.16.0.128/25
向工程组提供对任何目标的访问权限	S-xxxxx14	False	0.0.0.0/0

产生的行为

- 开发组可以访问 `10.0.0.0/16`，但单个主机 `10.0.2.119/32` 除外。
- 经理组可以访问公共互联网、`192.168.0.0/24` 以及 `10.0.2.119/32` 网络中的单个主机（`10.0.0.0/16`），但无权访问 `172.16.0.0/24` 或 `10.0.0.0/16` 网络中的任何剩余主机。
- 工程组可以访问公共互联网、`192.168.0.0/24` 以及 `172.16.0.0/24`，包括更具体的子网 `172.16.0.128/25`。

> **Note**
>
> 请注意，工程组和经理组现在都可以访问 `192.168.0.0/24`。这是因为这两个组都有权访问 `0.0.0.0/0`（任何目标）且 没有其他规则在引用 `192.168.0.0/24`。

为 192.168.0.0/24 添加规则

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24

规则描述	组 ID	允许所有用户访问	目标 CIDR
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
向经理组提供对任何目标的访问权限	S-xxxxx16	False	0.0.0.0/0
向经理组提供对开发 VPC 中单个主机的访问权限	S-xxxxx16	False	10.0.2.119/32
向工程组提供对本地网络中子网的访问权限	S-xxxxx14	False	172.16.0.128/25
向工程组提供对任何目标的访问权限	S-xxxxx14	False	0.0.0.0/0
向经理组提供对 Client VPN VPC 的访问权限	S-xxxxx16	False	192.168.0.0/24

产生的行为

- 开发组可以访问 10.0.0.0/16，但单个主机 10.0.2.119/32 除外。
- 经理组可以访问公共互联网、192.168.0.0/24 以及 10.0.2.119/32 网络中的单个主机（10.0.0.0/16），但无权访问 172.16.0.0/24 或 10.0.0.0/16 网络中的任何剩余主机。
- 工程组可以访问公共互联网、172.16.0.0/24 以及 172.16.0.128/25。

> **Note**
>
> 请注意，添加供经理组访问 `192.168.0.0/24` 的规则会导致开发组不再具有访问该目标网络的权限。

访问所有用户组

规则描述	组 ID	允许所有用户访问	目标 CIDR
向工程组提供对本地网络的访问权限	S-xxxxx14	False	172.16.0.0/24
向开发组提供对开发 VPC 的访问权限	S-xxxxx15	False	10.0.0.0/16
向经理组提供对任何目标的访问权限	S-xxxxx16	False	0.0.0.0/0
向经理组提供对开发 VPC 中单个主机的访问权限	S-xxxxx16	False	10.0.2.119/32
向工程组提供对本地网络中子网的访问权限	S-xxxxx14	False	172.16.0.128/25
向工程组提供对所有网络的访问权限	S-xxxxx14	False	0.0.0.0/0
向经理组提供对 Client VPN VPC 的访问权限	S-xxxxx16	False	192.168.0.0/24
	不适用	True	0.0.0.0/0

规则描述	组 ID	允许所有用户访问	目标 CIDR
向所有组提供访问权限			

产生的行为

- 开发组可以访问 10.0.0.0/16，但单个主机 10.0.2.119/32 除外。
- 经理组可以访问公共互联网、192.168.0.0/24 以及 10.0.2.119/32 网络中的单个主机（10.0.0.0/16），但无权访问 172.16.0.0/24 或 10.0.0.0/16 网络中的任何剩余主机。
- 工程组可以访问公共互联网、172.16.0.0/24 以及 172.16.0.128/25。
- 任何其他用户组（例如“管理员组”）可以访问公共互联网，但不能访问在其他规则中定义的任何其他目标网络。

向 AWS Client VPN 端点添加授权规则

可以使用 AWS Management Console添加授权规则，以授予或限制对 Client VPN 端点的访问。可以使用 Amazon VPC 控制台或者使用命令行或 API 向 Client VPN 端点添加授权规则。

要向 Client VPN 端点添加授权规则，请使用以下命令 AWS Management Console

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要向其中添加授权规则的 Client VPN 端点，然后依次选择授权规则和添加授权规则。
4. 对于 Destination network to enable access（要启用访问的目标网络），输入您希望用户访问的 IP 地址，以 CIDR 表示法表示（例如，VPC 的 CIDR 块）。
5. 指定允许哪些客户端访问指定的网络。对于 For grant access to (将访问权限授予)，执行以下操作之一：
   - 要向所有客户端授予访问权限，请选择 Allow access to all users (允许所有用户访问)。
   - 要将访问限制到特定客户端，请选择 Allow access to users in a specific access group (允许特定访问组中的用户进行访问)，然后对于 Access group ID (访问组 ID)，输入要授予访问权限的组的 ID。例如，Active Directory 组的安全标识符 (SID)，或在基于 SAML 的身份提供商 (IdP) 中定义的组的 ID/名称。

- （Active Directory）要获取 SID，你可以使用 Microsoft Powershell Get-ADGroup cmdlet，例如：

```
Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
```

  或者，打开“Active Directory 用户和计算机”工具，查看组的属性，转到“属性编辑器”选项卡，获取 `objectSID` 的值。如有必要，请先选择查看、高级功能以启用“属性编辑器”选项卡。
- （基于 SAML 的联合身份验证）组 ID/名称应与 SAML 断言中返回的组属性信息匹配。

6. 对于 Description (描述)，输入授权规则的简要描述。
7. 选择添加授权规则。

将授权规则添加到 Client VPN 端点（AWS CLI）

使用 authorize-client-vpn-ingress 命令。

从 AWS Client VPN 端点删除授权规则

可以使用控制台和 AWS CLI删除特定 Client VPN 端点的授权规则。

删除授权规则（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要向其中添加授权规则的 Client VPN 端点，然后选择授权规则。
4. 选择要删除的授权规则，选择删除授权规则，然后再次选择删除授权规则以确认删除。

删除授权规则（AWS CLI）

使用 revoke-client-vpn-ingress 命令。

查看 AWS Client VPN 授权规则

可以使用控制台和 AWS CLI查看特定 Client VPN 端点的授权规则。

查看授权规则（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。

3. 选择要查看其授权规则的 Client VPN 端点，然后选择 Authorization rules（授权规则）。

查看授权规则 (AWS CLI)

使用 describe-client-vpn-authorization-rules 命令。

AWS Client VPN 客户证书吊销列表

针对特定客户端证书，使用 Client VPN 客户端证书吊销列表撤销对 Client VPN 端点的访问权限。您可以生成吊销列表或导入现有列表。您也可以将当前列表导出为吊销列表文件。在 Linux/macOS 或 Windows 上使用 OpenVPN 软件生成列表。可以使用 Amazon VPC 控制台或 AWS CLI 完成导入和导出。

有关生成服务器和客户端证书和密钥的更多信息，请参阅双向认证 AWS Client VPN

> **Note**
>
> 如果客户端证书吊销列表已过期，则无法连接到 Client VPN 端点。你需要创建一个新的，然后将其导入 Client VPN 终端节点。

只能向客户端证书吊销列表中添加有限数量的条目。有关可以添加到吊销列表中的条目数的更多信息，请参阅 客户端 VPN 配额。

任务

- 生成 AWS Client VPN 客户证书吊销列表
- 导入 AWS Client VPN 客户证书吊销列表
- 导出 AWS Client VPN 客户证书吊销列表

生成 AWS Client VPN 客户证书吊销列表

您可以在 Linux/macOS 或 Windows 操作系统上生成 Client VPN 证书吊销列表。针对特定证书，使用吊销列表撤销对 Client VPN 端点的访问权限。有关客户端证书吊销列表的更多信息，请参阅客户端证书吊销列表。

Linux/macOS

在以下过程中，您使用 OpenVPN easy-rsa 命令行实用程序生成客户端证书吊销列表。

使用 OpenVPN easy-rsa 生成客户端证书吊销列表

1. 登录到托管 easyrsa 安装（用于生成证书）的服务器。
2. 导航到本地存储库中的 `easy-rsa/easyrsa3` 文件夹。

```
$ cd easy-rsa/easyrsa3
```

3. 撤销客户端证书并生成客户端吊销列表。

```
$ ./easyrsa revoke client1.domain.tld
$ ./easyrsa gen-crl
```

出现提示时输入 `yes`。

Windows

以下过程使用 OpenVPN 软件生成客户端吊销列表。它假定您遵循了使用 OpenVPN 软件生成客户端和服务器证书和密钥的步骤。

使用 EasyRSA 版本 3.x.x 生成客户端证书吊销列表

1. 打开命令提示符并导航至 EasyRSA-3.x.x 目录，该目录的具体位置取决于它在系统上的安装位置。

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. 运行 `EasyRSA-Start.bat` 文件以启动 EasyRSA Shell。

```
C:\> .\EasyRSA-Start.bat
```

3. 在 EasyRSA shell 中，吊销该客户端证书。

```
# ./easyrsa revoke client_certificate_name
```

4. 出现提示时输入 `yes`。
5. 生成客户端吊销列表。

```
# ./easyrsa gen-crl
```

6. 系统将在以下位置创建客户端吊销列表：

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

使用 EasyRSA 的早期版本生成客户端证书吊销列表

1. 打开命令提示符，然后导航到 OpenVPN 目录。

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. 运行 `vars.bat` 文件。

```
C:\> vars
```

3. 撤销客户端证书并生成客户端吊销列表。

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

导入 AWS Client VPN 客户证书吊销列表

您必须拥有要导入的 Client VPN 客户端证书吊销列表文件。有关生成客户端证书吊销列表的更多信息，请参阅生成 AWS Client VPN 客户证书吊销列表。

可以使用控制台和 AWS CLI导入客户端证书吊销列表。

导入客户端证书吊销列表（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要为其导入客户端证书吊销列表的 Client VPN 端点。
4. 选择 Actions (操作)，然后选择 Import Client Certificate CRL (导入客户端证书 CRL)。
5. 对于 Certificate Revocation List (证书吊销列表)，输入客户端证书吊销列表文件的内容，然后选择 Import client certificate CRL（导入客户端证书 CRL）。

导入客户端证书吊销列表 (AWS CLI)

使用 import-client-vpn-client-certificate-revocation-list 命令。

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

导出 AWS Client VPN 客户证书吊销列表

可以使用控制台和 AWS CLI导出 Client VPN 客户端证书吊销列表。

导出客户端证书吊销列表（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要导出其客户端证书吊销列表的 Client VPN 端点。
4. 选择 Actions（操作），选择 Export Client Certificate CRL（导出客户端证书 CRL），然后选择 Export Client Certificate CRL（导出客户端证书 CRL）。

导出客户端证书吊销列表 (AWS CLI)

使用 export-client-vpn-client-certificate-revocation-list 命令。

AWS Client VPN 客户端连接

AWS Client VPN 连接是指客户端与特定 Client VPN 端点建立的主动 VPN 会话，以及该端点在过去 60 分钟内终止的连接。当客户端成功连接到 Client VPN 端点时，即表明建立了连接。终止会话将结束客户端与 Client VPN 端点的连接。

您可以查看和终止 Client VPN 连接。查看连接信息会返回诸如从客户端 CIDR 块范围分配的 IP 地址以及端点 ID 和时间戳等信息。终止会话将结束与端点的指定 VPN 连接。可以使用 Amazon VPC 控制台或 AWS CLI 来查看和终止会话。如果无法连接到端点，请参阅故障排除，根据错误情况，了解解决问题所需采取的步骤。

任务

- 查看 AWS Client VPN 客户端连接
- 终止 AWS Client VPN 客户端连接

查看 AWS Client VPN 客户端连接

可以使用 Amazon VPC 控制台或 AWS CLI 查看活动 Client VPN 连接。

查看 Client VPN 客户端连接（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要查看其客户端连接的 Client VPN 端点。
4. 选择连接选项卡。连接 选项卡列出所有处于活动状态和已终止的客户端连接。

查看 Client VPN 客户端连接（AWS CLI）

使用 describe-client-vpn-connections 命令。

终止 AWS Client VPN 客户端连接

您可以使用亚马逊 VPC 控制台或 AWS CLI 终止 Client VPN 客户端连接。

终止 Client VPN 客户端连接（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择客户端连接到的 Client VPN 端点，然后选择连接。
4. 选择要终止的连接，选择终止连接，然后再次选择终止连接确认终止。

终止 Client VPN 客户端连接（AWS CLI）

使用 terminate-client-vpn-connections 命令。

AWS Client VPN 客户登录横幅

AWS Client VPN 提供了建立 VPN 会话时在 AWS 提供的 Client VPN 桌面应用程序上显示文本横幅的选项。您可以定义文本横幅的内容以满足监管和合规性需求。最多可以使用 1400 个 UTF-8 编码的字符。

> **Note**
>
> 客户端登录横幅启用后，它将仅在新创建的 VPN 会话上显示。现有的 VPN 会话不会中断，但现有的会话重新建立时也会显示横幅。

横幅创建

登录横幅最初在创建 Client VPN 端点期间创建和启用。有关在 Client VPN 端点创建期间启用客户端登录横幅的步骤，请参阅创建 AWS Client VPN 终端节点。

任务

- 为现有 AWS Client VPN 终端节点配置客户端登录横幅
- 停用现有 AWS Client VPN 端点的客户端登录横幅
- 在 AWS Client VPN 端点上修改现有横幅文本
- 查看当前配置的 AWS Client VPN 登录横幅

为现有 AWS Client VPN 终端节点配置客户端登录横幅

请按照以下步骤为现有 Client VPN 端点配置客户端登录横幅。

在 Client VPN 端点上启用客户端登录横幅（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要修改的 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN Endpoint（修改 Client VPN 终端节点）。
4. 在页面上向下滚动至 Other parameters（其他参数）部分。
5. 开启 Enable client login banner（启用客户端登录横幅）。
6. 对于客户端登录横幅文本，输入建立 VPN 会话时将在 AWS 提供的客户端上的横幅中显示的文本。只能使用 UTF-8 编码字符，并且最多允许使用 1400 个字符。
7. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

在 Client VPN 端点上启用客户端登录横幅（AWS CLI）

使用 modify-client-vpn-endpoint 命令。

停用现有 AWS Client VPN 端点的客户端登录横幅

请按照以下步骤为现有的 Client VPN 端点停用客户端登录横幅。

在 Client VPN 端点上停用客户端登录横幅（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要修改的 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。
4. 在页面上向下滚动至 Other parameters（其他参数）部分。
5. 关闭 Enable client login banner?（启用客户端登录横幅?）。
6. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

在 Client VPN 端点上停用客户端登录横幅（AWS CLI）

使用 modify-client-vpn-endpoint 命令。

在 AWS Client VPN 端点上修改现有横幅文本

按照以下步骤修改 Client VPN 客户端登录横幅的现有文本。

在 Client VPN 端点上修改现有横幅文本（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要修改的 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。
4. 对于 Enable client login banner?（启用客户端登录横幅?），验证它是否已开启。
5. 对于客户端登录横幅文本，请将现有文本替换为在建立 VPN 会话时要在 AWS 所提供客户端的横幅中显示的新文本。只能使用 UTF-8 编码字符，并且最多可以使用 1400 个字符。
6. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

在 Client VPN 端点上修改客户端登录横幅（AWS CLI）

使用 modify-client-vpn-endpoint 命令。

查看当前配置的 AWS Client VPN 登录横幅

按照以下步骤查看当前配置的 Client VPN 客户端登录横幅。

查看 Client VPN 端点的当前登录横幅（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要查看的 Client VPN 终端节点。
4. 验证已经选择了 Details（详细信息）选项卡。
5. 在 Client login banner text（客户端登录横幅文本）旁查看当前配置的登录横幅文本。

查看 Client VPN 端点当前配置的登录横幅（AWS CLI）

使用 describe-client-vpn-endpoints 命令。

AWS Client VPN 客户端路由强制执行

客户端路由强制有助于在通过 VPN 连接的设备上强制执行管理员定义的路由。此功能可确保来自已连接客户端的网络流量不会无意中发送到 VPN 隧道之外，从而帮助改善您的安全状况。

客户端路由强制监控所连接设备的主路由表，并根据客户端 VPN 端点中配置的网络路由，确保出站网络流量流向 VPN 隧道。这包括在检测到与 VPN 隧道冲突的路由时修改设备上的路由表。

要求

客户端路由强制仅适用于以下 AWS 提供的 Client VPN 版本：

- Windows 版本 5.2.0 或更高版本
- macOS 版本 5.2.0 或更高版本
- Ubuntu 版本 5.2.0 或更高版本

路由冲突

当客户端连接到 VPN 时，会对客户端的本地路由表和终端的网络路由进行比较。如果两个路由表条目之间存在网络重叠，则会发生路由冲突。重叠网络的一个例子是：

- `172.31.0.0/16`

- `172.31.1.0/24`

在本示例中，这些 CIDR 块构成路由冲突。例如，`172.31.0.0/16`可能是 VPN 隧道 CIDR。由于`172.31.1.0/24`前缀更长，因此更具体，因此它通常优先，并有可能将 `172.31.1.0/24` IP 范围内的 VPN 流量重定向到另一个目的地。这可能会导致意想不到的路由行为。但是，启用客户端路由强制后，后一个 CIDR 将被删除。使用此功能时，应考虑潜在的路由冲突。

全通道 VPN 连接通过 VPN 连接引导所有网络流量。因此，如果启用了客户端路由强制功能，则连接到 VPN 的设备将无法访问本地网络 (LAN) 资源。如果需要访问本地 LAN，请考虑使用分割隧道模式而不是全隧道模式。有关分割隧道的更多信息，请参阅。拆分隧道 Client VPN

注意事项

在激活 “客户端路由强制” 之前，应考虑以下信息。

- 在连接时，如果检测到路由冲突，该功能将更新客户端的路由表，将流量引导到 VPN 隧道。在建立连接之前存在并被此功能删除的路由将被恢复。
- 该功能仅在主路由表上强制执行，不适用于其他路由机制。例如，执法不适用于以下情况：
  - 基于策略的路由
  - 接口范围路由
- 客户端路由强制在 VPN 隧道打开时对其进行保护。隧道断开后或客户端重新连接时没有任何保护。

OpenVPN 指令对云路由强制执行的影响

OpenVPN 配置文件中的一些自定义指令与客户端路由强制有特定的交互：

- `route` 指令
  - 向 VPN 网关添加路由时。例如，将路由添加`192.168.100.0 255.255.255.0`到 VPN 网关。

    与任何其他 VPN 路由一样，添加到 VPN 网关的路由由客户端路由强制监控。将检测并删除其中的任何冲突路由。
  - 向非 VPN 网关添加路由时。例如，添加路线`192.168.200.0 255.255.255.0 net_gateway`。

    添加到非 VPN 网关的路由会被排除在客户端路由强制之外，因为它们会绕过 VPN 隧道。其中允许有冲突的路由。在上面的示例中，客户端路由强制将不对上述路由进行监控。
- 该`route-ipv6`指令。

由于客户端路由强制仅支持 IPv4地址，因此不处理此指令。

忽略的路由

客户端路由强制将忽略到以下网络的路由：

- `127.0.0.0/8`— 为本地主机保留
- `169.254.0.0/16`— 保留给本地链路地址
- `224.0.0.0/4`— 保留用于组播
- `255.255.255.255/32`— 保留用于广播

主题

- 为 AWS Client VPN 终端节点激活客户端路由强制
- 从终端停用客户端路由强制 AWS Client VPN

为 AWS Client VPN 终端节点激活客户端路由强制

您可以使用控制台或在现有 Client VPN 终端上激活 “客户端路由强制” AWS CLI。

使用控制台激活客户端路由强制

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN endpoints（Client VPN 端点）。
3. 选择要修改的 Client VPN 端点，选择操作，然后选择修改客户端 VPN 端点。
4. 在页面上向下滚动至 Other parameters（其他参数）部分。
5. 打开 “客户端路由强制”。
6. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

要激活客户端路由强制，请使用 AWS CLI)

- 使用 modify-client-vpn-endpoint 命令。

从终端停用客户端路由强制 AWS Client VPN

您可以使用控制台或 Client VPN 终端上禁用 Client VPN 端点上的客户端路由强制功能。 AWS CLI

使用控制台停用客户端路由强制

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN endpoints（Client VPN 端点）。
3. 选择要修改的 Client VPN 端点，选择操作，然后选择修改客户端 VPN 端点。
4. 在页面上向下滚动至 Other parameters（其他参数）部分。
5. 关闭 “客户端路由强制”。
6. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

要使用 “禁用客户端路由强制” AWS CLI

- 使用 modify-client-vpn-endpoint 命令。

AWS Client VPN 端点

所有 AWS Client VPN 会话都与 Client VPN 端点建立通信。可以通过管理 Client VPN 端点创建、修改、查看和删除与该端点进行的 Client VPN 会话。可以使用 Amazon VPC 控制台或 AWS CLI 创建和修改端点。

创建 Client VPN 端点的要求

> **Important**
>
> 必须在配置预期目标网络的同一 AWS 账户中创建 Client VPN 端点。您还需要生成服务器证书，并根据需要生成客户端证书。有关更多信息，请参阅 中的客户端身份验证 AWS Client VPN。

在您开始之前，请确保您已执行以下操作：

- 查看 使用 AWS Client VPN的规则和最佳实践中的规则和限制。
- 生成服务器证书，并（如果需要）获取客户端证书。有关更多信息，请参阅 中的客户端身份验证 AWS Client VPN。

端点修改

创建完 Client VPN 后，您可以修改以下任意设置：

- 描述
- 服务器证书
- 客户端连接日志记录选项
- 客户端连接处理程序选项
- DNS 服务器
- 拆分隧道选项
- 路由（在使用拆分隧道选项时）
- 证书撤销列表（CRL）
- 授权规则
- VPC 和安全组关联
- VPN 端口号
- 自助服务门户选项
- 最长 VPN 会话持续时间
- 启用或禁用会话超时自动重新连接
- 启用或禁用客户端登录横幅文本
- 客户端登录横幅文本

> **Note**
>
> 对客户端 VPN 端点的修改（包括证书吊销列表 (CRL, Certificate Revocation List) 更改）将在客户端 VPN 服务接受请求后最多 4 小时生效。
>
> 创建 IPv4 Client VPN 端点后，您无法修改客户端 CIDR 范围、身份验证选项、客户端证书或传输协议。

当您修改 Client VPN 端点上的以下任何参数时，连接将重置：

- 服务器证书
- DNS 服务器
- 拆分隧道选项（打开或关闭支持）

- 路由（当您使用拆分隧道选项时）
- 证书撤销列表（CRL）
- 授权规则
- VPN 端口号

任务

- 创建 AWS Client VPN 终端节点
- 查看 AWS Client VPN 终端节点
- 修改 AWS Client VPN 终端节点
- 删除 AWS Client VPN 终端节点

创建 AWS Client VPN 终端节点

创建客户端 VPN 终端节点，使您的客户端能够使用 Amazon VPC 控制台或建立 VPN 会话 AWS CLI。

在创建端点之前，请先熟悉各项要求。有关更多信息，请参阅 the section called “创建 Client VPN 端点的要求”。

使用控制台创建 Client VPN 端点

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 端点），然后选择 Create Client VPN Endpoint（创建 Client VPN 端点）。
3. （可选）提供 Client VPN 终端节点的名称标签和描述。
4. 对于客户端 IPv4 CIDR，以 CIDR 表示法指定一个 IP 地址范围，从中分配客户端 IP 地址。例如 `10.0.0.0/22`。

   > **Note**
   >
   > 此地址范围不能与目标网络地址范围、VPC 地址范围或将与 Client VPN 端点关联的任何路由重叠。客户端地址范围必须至少为 /22 且不大于 /12 CIDR 块大小。创建 Client VPN 终端节点后，您无法更改客户端地址范围。

5. 对于 Server certificate ARN（服务器证书 ARN），请指定服务器要使用的 TLS 证书的 ARN。客户端使用服务器证书对它们正在连接的 Client VPN 终端节点进行身份验证。

> **Note**
>
> 服务器证书必须存在于您正在创建 Client VPN 端点的区域的 AWS Certificate Manager (ACM) 中。可以使用 ACM 预置证书，也可以导入到 ACM 中。
> 有关在 ACM 中配置或导入证书的步骤，请参阅《AWS Certificate Manager 用户指南》中的AWS Certificate Manager 证书。

6. 指定当客户端建立 VPN 连接时要用来对客户端进行身份验证的身份验证方法。您必须选择身份验证方法。

   - 要使用基于用户的身份验证，请选择 Use user-based authentication（使用基于用户的身份验证），然后选择以下选项之一：
     - Active Directory authentication（Active Directory 身份验证）：为 Active Directory 身份验证选择此选项。对于 Directory ID（目录 ID），指定要使用的 Active Directory 的 ID。
     - Federated authentication（联合身份验证）：为基于 SAML 的联合身份验证选择此选项。

       对于 SAML provider ARN（SAML 提供商 ARN），指定 IAM SAML 身份提供商的 ARN。

       （可选）对于 Self-service SAML provider ARN（自助服务 SAML 提供商 ARN），指定您为支持自助服务门户而创建的 IAM SAML 身份提供商的 ARN（如果适用）。
   - 要使用相互证书身份验证，请选择 “使用相互身份验证”，然后在 “客户端证书 ARN” 中，指定在 (ACM) 中配置的客户证书的 ARN。 AWS Certificate Manager

   > **Note**
   >
   > 如果服务器证书和客户端证书是由相同证书颁发机构 (CA) 颁发，则您可以将服务器证书 ARN 用于服务器和客户端。如果客户端证书是由其他 CA 颁发，则应指定客户端证书 ARN。

7. （可选）对于连接日志，请指定是否使用 Amazon Log CloudWatch s 记录有关客户端连接的数据。开启 Enable log details on client connections（在客户端连接上启用日志详细信息）。在CloudWatch 日志日志组名称中，输入要使用的日志组的名称。在CloudWatch 日志日志流名称中，输入要使用的日志流的名称，或者将此选项留空以让我们为您创建日志流。
8. （可选）对于 Client Connect Handler（客户端连接处理程序），开启 Enable client connect handler（启用客户端连接处理程序），以运行允许或拒绝与 Client VPN 端点的新连接的自定义代码。对于 Client Connect Handler ARN（客户端连接处理程序 ARN），指定包含允许或拒绝连接的逻辑的 Lambda 函数的 Amazon 资源名称（ARN）。

9. （可选）指定用于 DNS 解析的 DNS 服务器。要使用自定义 DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）和 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定要使用的 DNS 服务器的 IP 地址。要使用 VPC DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）或 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定 IP 地址，并添加 VPC DNS 服务器 IP 地址。

> **Note**
>
> 验证客户端是否能访问 DNS 服务器。

10. （可选）原定设置情况下，Client VPN 端点使用 UDP 传输协议。若要改用 TCP 传输协议，对于 Transport Protocol（传输协议），选择 TCP。

> **Note**
>
> UDP 通常能比 TCP 提供更好的性能。创建 Client VPN 端点后，无法更改传输协议。

11. （可选）要使端点成为拆分隧道 Client VPN 端点，请开启 Enable split-tunnel（启用拆分隧道）。默认情况下，Client VPN 端点会禁用拆分隧道功能。
12. （可选）对于 VPC ID，请选择要与 Client VPN 端点关联的 VPC。对于安全组 IDs，选择一个或多个 VPC 的安全组以应用于 Client VPN 终端节点。
13. （可选）对于 VPN port（VPN 端口），选择 VPN 端口号。默认值为 443。
14. （可选）要为客户端生成 self-service portal URL（自助服务门户 URL），请开启 Enable self-service portal（启用自助服务门户）。
15. （可选）对于 Session timeout hours（会话超时时间），请从可用的选项中选择所需的最长 VPN 会话持续时间（以小时为单位），也可保留 24 小时的原定设置。
16. （可选）对于会话超时时断开连接，请选择是否要在达到最大会话时间时终止会话。选择此选项要求用户在会话超时时时手动重新连接到终端；否则，Client VPN 将自动尝试重新连接。
17. （可选）指定是否启用客户端登录横幅文本。开启 Enable client login banner（启用客户端登录横幅）。对于 Client login banner text（客户端登录横幅文本），输入 VPN 会话建立时将在 AWS 提供的客户端上显示的横幅文本。仅支持 UTF-8 编码字符。最多可使用 1400 个字符。
18. 选择 Create Client VPN Endpoint（创建 Client VPN 终端节点）。

创建 Client VPN 端点后，请执行以下操作以完成配置并使客户端能够连接：

- Client VPN 端点的初始状态为 `pending-associate`。仅当您关联第一个目标网络后，客户端才能连接到 Client VPN 端点。
- 创建授权规则，以指定哪些客户端具有网络访问权限。
- 下载并准备要分发给客户端的 Client VPN 端点配置文件。
- 指示您的客户使用 AWS 提供的客户端或其他基于 OpenVPN 的客户端应用程序连接到 Client VPN 端点。有关更多信息，请参阅 AWS Client VPN 《用户指南》。

使用创建 Client VPN 终端节点 AWS CLI

使用 create-client-vpn-endpoint 命令。

查看 AWS Client VPN 终端节点

可以使用 Amazon VPC 控制台或 AWS CLI查看有关 Client VPN 端点的信息。

查看 Client VPN 端点（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要查看的 Client VPN 端点。
4. 使用 Details（详细信息）、Target network associations（目标网络关联）、Security groups（安全组）、Authorization rules（授权规则）、Route table（路由表）、Connections（连接）和 Tags（标签）选项卡以查看有关现有 Client VPN 端点的信息。

   还可以使用筛选条件来帮助优化搜索。

查看 Client VPN 端点（AWS CLI）

使用 describe-client-vpn-endpoints 命令。

修改 AWS Client VPN 终端节点

可以使用 Amazon VPC 控制台或 AWS CLI修改 Client VPN 端点。有关可以修改的 Client VPN 字段的更多信息，请参阅the section called “端点修改”。

> **Note**
>
> 对客户端 VPN 端点的修改（包括证书吊销列表 (CRL, Certificate Revocation List) 更改）将在客户端 VPN 服务接受请求后最多 4 小时生效。
> 创建 IPv4 Client VPN 端点后，您无法修改客户端 CIDR 范围、身份验证选项、客户端证书或传输协议。

修改 Client VPN 端点（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要修改的 Client VPN 端点，选择 Actions（操作），然后选择 Modify Client VPN endpoint（修改 Client VPN 端点）。
4. 对于 Description（描述），输入 Client VPN 端点的简短描述。
5. 对于 Server certificate ARN（服务器证书 ARN），请指定服务器要使用的 TLS 证书的 ARN。客户端使用服务器证书对它们正在连接的 Client VPN 终端节点进行身份验证。

   > **Note**
   >
   > 服务器证书必须存在于您正在创建 Client VPN 端点的区域的 AWS Certificate Manager (ACM) 中。可以使用 ACM 预置证书，也可以导入到 ACM 中。

6. 指定是否使用 Amazon CloudWatch 日志记录有关客户端连接的数据。对于 Enable log details on client connections（在客户端连接上启用日志详细信息），执行以下操作之一：
   - 要激活客户端连接日志记录，请开启 Enable log details on client connections（在客户端连接上启用日志详细信息）。在CloudWatch日志日志组名称中，选择要使用的日志组的名称。在CloudWatch 日志日志流名称中，选择要使用的日志流名称，或者将此选项留空以让我们为您创建日志流。
   - 要停用客户端连接日志记录，请关闭 Enable log details on client connections（在客户端连接上启用日志详细信息）。
7. 对于 Client connect handler（客户端连接处理程序），要激活 client connect handler（客户端连接处理程序），请开启 Enable client connect handler（启用客户端连接处理程序）。对于 Client Connect Handler ARN（客户端连接处理程序 ARN），指定包含允许或拒绝连接的逻辑的 Lambda 函数的 Amazon 资源名称 (ARN)。

8. 打开或关闭 Enable DNS servers（启用 DNS 服务器）。要使用自定义 DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）和 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定要使用的 DNS 服务器的 IP 地址。要使用 VPC DNS 服务器，对于 DNS Server 1 IP address（DNS 服务器 1 IP 地址）或 DNS Server 2 IP address（DNS 服务器 2 IP 地址），指定 IP 地址，并添加 VPC DNS 服务器 IP 地址。

> **Note**
>
> 验证客户端是否能访问 DNS 服务器。

9. 打开或关闭 Enable split-tunnel（启用拆分隧道）。原定设置情况下，拆分隧道在 VPN 端点上处于关闭状态。
10. 对于 VPC ID，请选择要与 Client VPN 端点关联的 VPC。对于安全组 IDs，选择一个或多个 VPC 的安全组以应用于 Client VPN 终端节点。
11. 对于 VPN port（VPN 端口），选择 VPN 端口号。默认值为 443。
12. 要为客户端生成 self-service portal URL（自助服务门户 URL），请开启 Enable self-service portal（启用自助服务门户）。
13. 对于 Session timeout hours（会话超时时间），请从可用的选项中选择所需的最长 VPN 会话持续时间（以小时为单位），也可保留 24 小时的原定设置。
14. 对于会话超时时断开连接，请选择是否要在达到最大会话时间时终止会话。选择此选项要求用户在会话超时时时手动重新连接到终端；否则，Client VPN 将自动尝试重新连接。
15. 开启或关闭 Enable client login banner（启用客户端登录横幅）。如果要使用客户端登录横幅，请输入 VPN 会话建立时将在 AWS 提供的客户端上显示的横幅文本。仅支持 UTF-8 编码字符。最多可使用 1400 个字符。
16. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

修改 Client VPN 端点（AWS CLI）

使用 modify-client-vpn-endpoint 命令。

删除 AWS Client VPN 终端节点

您需要取消关联所有目标网络，然后才能删除 Client VPN 端点。在删除 Client VPN 端点时，其状态将更改为 `deleting`，客户端不再能够连接到它。

可以使用控制台或 AWS CLI删除 Client VPN 端点。

删除 Client VPN 端点（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要删除的 Client VPN 端点。依次选择 Actions（操作）和 Delete Client VPN endpoint（删除 Client VPN 端点）。
4. 在确认窗口中输入 delete（删除），然后选择 Delete（删除）。

删除 Client VPN 端点（AWS CLI）

使用 delete-client-vpn-endpoint 命令。

AWS Client VPN 连接日志

您可以为新的或现有的 Client VPN 端点启用连接日志记录，并开始捕获连接日志。连接日志显示 Client VPN 端点的日志事件顺序。启用连接日志记录时，可以在日志组中指定日志流的名称。如果未指定日志流，Client VPN 服务会为您创建一个日志流。然后，连接日志记录会记录以下信息：客户端连接请求、客户端连接结果（成功或不成功）、连接不成功的原因以及客户端与端点终止连接的时间。

开始之前，您的账户中必须有一个 Log CloudWatch s 日志组。有关更多信息，请参阅 Amazon 日志用户指南中的使用日志组和 CloudWatch 日志流。使用 CloudWatch 日志需要付费。有关更多信息，请参阅 Amazon CloudWatch 定价。

可以使用 Amazon VPC 控制台或 AWS CLI 创建 Client VPN 连接日志。

任务

- 为新的 AWS Client VPN 端点启用连接日志记录
- 为现有 AWS Client VPN 端点启用连接日志记录
- 查看 AWS Client VPN 连接日志
- 关闭 AWS Client VPN 连接日志

为新的 AWS Client VPN 端点启用连接日志记录

您可以在使用控制台或命令行创建新的 Client VPN 端点时启用连接日志记录。

使用控制台为新的 Client VPN 端点启用连接日志记录

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN 端点，然后选择创建 Client VPN 端点。
3. 填写这些选项，直至到达 Connection Logging (连接日志记录) 部分。有关选项的更多信息，请参阅创建 AWS Client VPN 终端节点。
4. 在 Connection logging（连接日志记录）中，开启 Enable log details on client connections（在客户端连接上启用日志详细信息）。
5. 在CloudWatch 日志日志组名称中，选择 CloudWatch 日志日志组的名称。
6. （可选）在CloudWatch 日志日志流名称中，选择 CloudWatch 日志日志流的名称。
7. 选择 Create Client VPN Endpoint（创建 Client VPN 终端节点）。

要为新 Client VPN 端点启用连接记录，请使用 AWS CLI

使用create-client-vpn-endpoint命令并指定`--connection-log-options`参数。您可以按 JSON 格式指定连接日志信息，如以下示例所示。

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

为现有 AWS Client VPN 端点启用连接日志记录

可以使用控制台或命令行为现有的 Client VPN 端点启用连接日志记录。

使用控制台为现有的 Client VPN 端点启用连接日志记录

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。
4. 在 Connection logging（连接日志记录）下，开启 Enable log details on client connections（在客户端连接上启用日志详细信息）。
5. 在CloudWatch 日志日志组名称中，选择 CloudWatch 日志日志组的名称。

6. （可选）在CloudWatch 日志日志流名称中，选择 CloudWatch 日志日志流的名称。
7. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

使用 AWS CLI为现有的 Client VPN 端点启用连接日志记录

使用 modify-client-vpn-endpoint 命令指定 `--connection-log-options` 参数。您可以按 JSON 格式指定连接日志信息，如以下示例所示。

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

查看 AWS Client VPN 连接日志

您可以使用日志控制台查看 Client VPN 连接 CloudWatch 日志。

使用控制台查看连接日志

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 Log groups (日志组)，然后选择包含连接日志的日志组。
3. 为您的 Client VPN 端点选择日志流。

> **Note**
> 时间戳列显示连接日志发布到 CloudWatch 日志的时间，而不是连接的时间。

有关搜索日志数据的更多信息，请参阅 Amazon Logs 用户指南中的使用筛选模式搜索 CloudWatch 日志数据。

关闭 AWS Client VPN 连接日志

可以使用控制台或命令行为 Client VPN 端点关闭连接日志记录。关闭连接日志记录时，不会删除 “日志” 中的现有连接 CloudWatch 日志。

使用控制台关闭连接日志记录

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。
4. 在 Connection logging（连接日志记录）下，关闭 Enable log details on client connections（在客户端连接上启用日志详细信息）。
5. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

要关闭连接日志记录，请使用 AWS CLI

使用modify-client-vpn-endpoint命令并指定`--connection-log-options`参数。确保 `Enabled` 设置为 `false`。

AWS Client VPN 端点配置文件导出

AWS Client VPN 端点配置文件是客户端（用户）用来与客户端 VPN 端点建立 VPN 连接的文件。您必须下载（导出）此文件并将其分发给所有需要访问 VPN 的客户端。或者，如果您已为 Client VPN 端点启用自助服务门户，客户端可以登录该门户并自行下载配置文件。有关更多信息，请参阅 AWS Client VPN 访问自助服务门户。

如果您的 Client VPN 端点使用双向身份验证，则您必须将客户端证书和客户端私有密钥添加到您下载的 .ovpn 配置文件中。在您添加信息后，客户端可以将 .ovpn 文件导入到 OpenVPN 客户端软件中。

> **Important**
>
> 如果未将客户端证书和客户端私有密钥信息添加到该文件中，则使用双向身份验证进行身份验证的客户端将无法连接到 Client VPN 端点。

默认情况下，OpenVPN 客户端配置中的 “remote-random-hostname” 选项启用通配符 DNS。由于已启用通配符 DNS，因此客户端不会缓存端点的 IP 地址，并且您将无法对端点的 DNS 名称执行 ping 操作。

如果 Client VPN 端点使用 Active Directory 身份验证，并且您在分发客户端配置文件后在目录上启用了 Multi-Factor Authentication（MFA），则必须下载新文件并将其重新分发给客户端。客户端无法使用以前的配置文件连接到 Client VPN 端点。

任务

- 导出 AWS Client VPN 客户机配置文件
- 添加用于相互身份验证的 AWS Client VPN 客户端证书和密钥信息

导出 AWS Client VPN 客户机配置文件

可以使用控制台或 AWS CLI导出 Client VPN 客户端配置。

导出客户端配置（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要为其下载客户端配置的 Client VPN 端点，然后选择下载客户端配置。

导出客户端配置 (AWS CLI)

使用 export-client-vpn-client-config uration 命令并指定输出文件名。

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

添加用于相互身份验证的 AWS Client VPN 客户端证书和密钥信息

如果您的 Client VPN 端点使用双向身份验证，则您必须将客户端证书和客户端私有密钥添加到您下载的 .ovpn 配置文件中。

使用双向身份验证时，您无法修改客户端证书。

添加客户端证书和密钥信息（双向身份验证）

您可以使用以下任一选项。

（选项 1）将客户端证书和密钥与 Client VPN 端点配置文件一起分发给客户端。在此情况下，请在该配置文件中指定证书和密钥的路径。使用您的首选文本编辑器打开该配置文件，并在文件末尾添加以下内容。*/path/*替换为客户端证书和密钥的位置（该位置相对于连接到端点的客户端）。

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

（选项 2）将 <cert></cert> 标记之间的客户端证书内容以及 <key></key> 标记之间的私有密钥内容添加到配置文件中。如果选择此选项，则只将配置文件分发给客户端。

如果您为将连接到 Client VPN 端点的每个用户生成了单独的客户端证书和密钥，请针对每个用户重复执行此步骤。

以下是包含客户端证书和密钥的 Client VPN 配置文件格式的示例。

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

AWS Client VPN 路线

每个 AWS Client VPN 终端节点都有一个路由表，描述了可用的目的网络路由。路由表中的每个路由决定了将网络流量指引到何处。您必须为每个 Client VPN 端点路由配置授权规则，以指定哪些客户端可以访问目标网络。

当您将 VPC 中的子网与 Client VPN 端点关联时，VPC 的路由会自动添加到 Client VPN 端点的路由表中。要允许访问其他网络，例如对等网络、本地网络 VPCs、本地网络（使客户端能够相互通信）或 Internet，您必须手动将路由添加到 Client VPN 终端节点的路由表中。

> **Note**
>
> 如果您需要将多个子网关联到 Client VPN 端点，则应确保为每个子网创建路由，如此处所述：故障排除 AWS Client VPN：对等互连 VPC、Amazon S3 或互联网的访问是间歇性的。每个关联的子网应该具有一组相同的路由。

在 Client VPN 端点上使用拆分隧道的注意事项

当您在 Client VPN 端点上使用拆分隧道时，Client VPN 路由表中的所有路由都将在建立 VPN 时添加到客户端路由表中。如果在 VPN 建立后添加路由，则您必须重置连接以将新路由发送到客户端。

建议您在修改 Client VPN 端点路由表之前，考虑客户端设备可以处理的路由数。

任务

- 创建 AWS Client VPN 终端节点路由
- 查看 AWS Client VPN 终端节点路由
- 删除 AWS Client VPN 终端节点路由

创建 AWS Client VPN 终端节点路由

在创建 Client VPN 端点路由时，您应指定如何指引目标网络的流量。

要允许客户端访问 Internet，请添加目标 `0.0.0.0/0` 路由。

可以使用控制台和 AWS CLI向 Client VPN 端点添加路由。

创建 Client VPN 端点路由（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要添加路由的 Client VPN 端点，选择 Route table（路由表），然后选择 Create route（创建路由）。
4. 在 “路由目标” 中，指定目的网络的 IPv4 CIDR 范围。例如：
   - 要为 Client VPN 终端节点的 VPC 添加路由，请输入 VPC 的 IPv4 CIDR 范围。
   - 要添加 Internet 访问的路由，请输入 `0.0.0.0/0`。
   - 要为对等互连 VPC 添加路由，请输入对等互连 VPC 的 IPv4 CIDR 范围。

- 要为本地网络添加路由，请输入 AWS Site-to-Site VPN 连接的 IPv4 CIDR 范围。

5. 对于 Subnet ID for target network association（用于目标网络关联的子网 ID），选择与 Client VPN 端点关联的子网。

   或者，如果要为本地 Client VPN 端点网络添加路由，请选择 `local`。

6. （可选）对于 Description（描述），输入路由的简短描述。
7. 选择创建路由。

创建 Client VPN 端点路由（AWS CLI）

使用 create-client-vpn-route 命令。

查看 AWS Client VPN 终端节点路由

可以使用控制台或 AWS CLI查看特定 Client VPN 端点的路由。

查看 Client VPN 端点路由（控制台）

1. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
2. 选择要查看其路由的 Client VPN 端点，然后选择 Route table（路由表）。

查看 Client VPN 端点路由（AWS CLI）

使用 describe-client-vpn-routes 命令。

删除 AWS Client VPN 终端节点路由

只能删除您手动添加的 Client VPN 路由。您无法删除在将子网与 Client VPN 端点关联时自动添加的路由。要删除自动添加的路由，必须解除最初创建的子网与 Client VPN 端点的关联。

可以使用控制台或 AWS CLI从 Client VPN 端点删除路由。

删除 Client VPN 端点路由（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要删除其路由的 Client VPN 端点，然后选择 Route table（路由表）。
4. 选择要删除的路由，然后依次选择 Delete route（删除路由）和 Delete route（删除路由）。

删除 Client VPN 端点路由（AWS CLI）

使用 delete-client-vpn-route 命令。

AWS Client VPN 目标网络

目标网络是 VPC 中的一个子网。 AWS Client VPN 端点必须至少有一个目标网络，客户端才能连接到该网络并建立 VPN 连接。

有关可以配置的访问类型（例如，允许客户端访问 Internet）的更多信息，请参阅 Client VPN 场景和示例。

Client VPN 目标网络要求

在创建目标网络时，应遵循以下规则：

- 子网必须具有至少一个 /27 位掩码的 CIDR 块，例如 10.0.0.0/27。子网还必须始终具有至少 20 个可用 IP 地址。
- 子网的 CIDR 块不能与 Client VPN 端点的客户端 CIDR 范围重叠。
- 如果您将多个子网与 Client VPN 端点关联，则每个子网必须位于不同的可用区中。我们建议您至少关联两个子网，以提供可用区冗余。
- 如果您在创建 Client VPN 端点时指定了 VPC，则子网必须位于相同 VPC 中。如果您尚未将 VPC 与 Client VPN 端点关联，则可以在任何 VPC 中选择任何子网。

  所有其他子网关联都必须来自相同 VPC。要关联不同 VPC 的子网，您必须先修改 Client VPN 端点并更改与其关联的 VPC。有关更多信息，请参阅 修改 AWS Client VPN 终端节点。

当您将子网与 Client VPN 端点关联时，我们会自动将在其中预置关联子网的 VPC 的本地路由添加到 Client VPN 端点的路由表中。

> **Note**
>
> 关联目标网络后，当您在连接的 VPC 中添加或移除其他 CIDRs 网络时，必须执行以下操作之一来更新 Client VPN 终端节点路由表的本地路由：
>
> - 从目标网络中取消关联您的 Client VPN 端点，然后将 Client VPN 端点关联到目标网络。
> - 手动将路由添加到 Client VPN 端点路由表或从表中删除路由。

将第一个子网与 Client VPN 端点关联后，Client VPN 端点的状态将从 `pending-associate` 更改为 `available`，并且客户端能够建立 VPN 连接。

任务

- 将目标网络与 AWS Client VPN 端点相关联
- 在 AWS Client VPN中将安全组应用于目标网络
- 查看 AWS Client VPN 目标网络
- 取消目标网络与 AWS Client VPN 端点的关联

将目标网络与 AWS Client VPN 端点相关联

您可以使用 Amazon VPC 控制台或 AWS CLI 将一个或多个目标网络（子网）与客户端 VPN 终端节点关联起来。将目标网络与 Client VPN 端点相关联之前，请先熟悉相关要求。请参阅 创建目标网络的要求。

将目标网络与 Client VPN 端点相关联（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要与目标网络关联的 Client VPN 端点，然后依次选择 Target network associations（目标网络关联）和 Associate target network（关联目标网络）。
4. 对于 VPC，选择您要在其中放置子网的 VPC。如果您在创建 Client VPN 端点时指定了 VPC，或者如果您有以前的子网关联，则这必须是相同的 VPC。
5. 对于 Choose a subnet to associate（选择要关联的子网），选择要与 Client VPN 终端节点关联的子网。
6. 选择 Associate target network（关联目标网络）。

将目标网络与 Client VPN 端点相关联（AWS CLI）

使用 associate-client-vpn-target-network 命令。

在 AWS Client VPN中将安全组应用于目标网络

创建 Client VPN 端点时，您可以指定要应用于目标网络的安全组。当您将第一个目标网络与 Client VPN 端点关联时，我们会自动应用关联子网所在 VPC 的默认安全组。有关更多信息，请参阅 安全组。

您可以更改 Client VPN 端点的安全组。您需要的安全组规则取决于要配置的 VPN 访问类型。有关更多信息，请参阅 Client VPN 场景和示例。

将安全组应用于目标网络（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要应用安全组的 Client VPN 端点。
4. 选择 Security Groups（安全组），然后选择 Apply Security Groups（应用安全组）。
5. 从安全组中选择适当的安全组 IDs。
6. 选择 Apply Security Groups（应用安全组）。

将安全组应用于目标网络 (AWS CLI)

使用 apply-security-groups-to-client-vpn-target-network 命令。

查看 AWS Client VPN 目标网络

可以使用控制台或 AWS CLI查看与 Client VPN 端点关联的目标。

查看目标网络（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择相应的 Client VPN 端点，然后选择 Target network associations（目标网络关联）。

要查看目标网络，请使用 AWS CLI

使用 describe-client-vpn-target-networks 命令。

取消目标网络与 AWS Client VPN 端点的关联

当您取消关联目标网络时，手动添加到 Client VPN 端点的路由表的所有路由，以及在建立目标网络关联时自动创建的路由（VPC 的本地路由）都将被删除。如果您取消所有目标网络与 Client VPN 端点的关联，则客户端不再能够建立 VPN 连接。

取消目标网络与 Client VPN 端点的关联（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择与目标网络关联的 Client VPN 端点，然后选择 Target network associations（目标网络关联）。
4. 选择要取消关联的目标网络，选择 Disassociate（取消关联），然后选择 Disassociate target network（取消目标网络关联）。

取消目标网络与 Client VPN 端点之间的关联（AWS CLI）

使用 disassociate-client-vpn-target-network 命令。

AWS Client VPN 最长 VPN 会话持续时间超时

AWS Client VPN 为最长 VPN 会话持续时间提供了多个选项，即允许客户端连接到 Client VPN 端点的最长时间。您可以配置一个更短的最长 VPN 会话持续时间，以帮助满足安全性和合规性要求。默认情况下，最长 VPN 会话持续时间为 24 小时。设置了最长会话持续时间后，您可以控制达到该超时时后该会话会发生什么。会话超时时断开连接选项允许您终止会话或自动尝试重新连接终端节点。通过强制执行最长 VPN 会话持续时间，终止会话可以更好地控制端点安全。如果会话设置为在达到最大时间时终止，则用户需要重新连接并提供身份验证凭据才能重新建立 VPN 连接。

当会话时断开连接超时设置为自动重新连接并且达到最大会话时间时，

- 如果使用缓存的用户凭据（Active Directory）或基于证书的身份验证（相互身份验证），则会自动建立新的会话。要完全断开连接而不自动重新连接，这些用户应手动断开连接。
- 对于联合身份验证 (SAML)，不会自动建立新会话。这些用户必须在会话超时到期后再次进行身份验证才能重新建立 VPN 连接。

> **Note**
>
> - 从当前值降低最长 VPN 会话持续时间值时，与端点连接的时间长于新设持续时间的任何活动 VPN 会话都会断开连接。
> - 更改 “会话超时时断开连接” 选项会将新设置应用于所有当前打开的会话。

在创建 AWS Client VPN 端点期间配置最大 VPN 会话数

可以在创建 Client VPN 端点期间配置 VPN 会话持续时间。有关创建 Client VPN 端点和设置最长会话持续时间的步骤，请参阅创建 AWS Client VPN 终端节点。

任务

- 查看 AWS Client VPN 当前最长 VPN 会话持续时间
- 修改最长 AWS Client VPN 会话持续时间和超时行为

查看 AWS Client VPN 当前最长 VPN 会话持续时间

按照以下步骤查看当前的 Client VPN 最长 VPN 会话持续时间。

查看 Client VPN 端点当前的最长 VPN 会话持续时间（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN Endpoints（Client VPN 终端节点）。
3. 选择要查看的 Client VPN 终端节点。
4. 验证已经选择了 Details（详细信息）选项卡。
5. 在 “会话超时时间” 旁边查看当前最长 VPN 会话持续时间，以及是否启用或禁用了超时断开连接。

查看 Client VPN 端点当前的最长 VPN 会话持续时间（AWS CLI）

使用 describe-client-vpn-endpoints 命令。

修改最长 AWS Client VPN 会话持续时间和超时行为

使用以下步骤修改现有 Client VPN 最长 VPN 会话持续时间并更改会话时断开连接超时行为。

修改 Client VPN 端点现有的最长 VPN 会话持续时间（控制台）

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Client VPN endpoints（Client VPN 端点）。
3. 选择要修改的 Client VPN 终端节点，选择 Actions（操作），然后选择 Modify Client VPN Endpoint（修改 Client VPN 终端节点）。
4. 对于 Session timeout hours（会话超时时间），选择所需的最长 VPN 会话持续时间（以小时为单位）。

5. 对于会话超时时断开连接，请选择是否要在达到最大会话超时时时断开会话连接。默认情况下，当您第一次修改端点时，此功能处于关闭状态。
6. 选择 Modify Client VPN endpoint（修改 Client VPN 终端节点）。

修改 Client VPN 端点现有的最长 VPN 会话持续时间（AWS CLI）

使用 modify-client-vpn-endpoint 命令。

安全性 AWS Client VPN

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS Client VPN，请参阅按合规计划划分的范围内的AWSAWS服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

AWS Client VPN 是亚马逊 VPC 服务的一部分。有关 Amazon VPC 中的安全性的更多信息，请参阅《Amazon VPC 用户指南》中的安全性。

此文档将帮助您了解如何在使用 Client VPN 时应用责任共担模式。以下主题说明如何配置 Client VPN 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Client VPN 资源。

主题

- 中的数据保护 AWS Client VPN
- 的身份和访问管理 AWS Client VPN
- 韧性在 AWS Client VPN
- 中的基础设施安全 AWS Client VPN
- 以下方面的安全最佳实践 AWS Client VPN
- IPv6 的注意事项 AWS Client VPN

中的数据保护 AWS Client VPN

责任 AWS 共担模式分适用于 AWS Client VPN 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧

洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，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) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你使用控制台、API 或 AWS 服务 使用其他方式使用 Client VPN AWS CLI 时 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

传输中加密

AWS Client VPN 使用传输层安全 (TLS) 1.2 或更高版本提供来自任何位置的安全连接。

互联网络流量隐私

启用互联网络访问

您可以让客户端通过 Client VPN 端点连接到您的 VPC 和其他网络。有关更多信息以及示例，请参阅 Client VPN 场景和示例。

限制对网络的访问

您可以配置 Client VPN 端点以限制对 VPC 中特定资源的访问。对于基于用户的身份验证，您还可以根据访问客户端 VPN 终端节点的用户组限制对网络各部分的访问。有关更多信息，请参阅使用 Client VPN 限制对网络的访问。

对客户端进行身份验证

身份验证在进入 AWS 云的第一个入口点实施。它用于确定是否允许客户端连接到客户端 VPN 终端节点。如果身份验证获得成功，客户端连接到客户端 VPN 终端节点并建立 VPN 会话。如果身份验证失败，连接被拒绝，客户端无法建立 VPN 会话。

客户端 VPN 提供以下类型的客户端身份验证：

- Active Directory 身份验证（基于用户）
- 双向身份验证额（基于证书）
- 单点登录（基于 SAML 的联合身份验证）（基于用户）

的身份和访问管理 AWS Client VPN

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）并获得授权（具有权限）来使用 Client VPN 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 AWS Client VPN 与 IAM 配合使用
- 适用于 AWS Client VPN的基于身份的策略示例
- 对 AWS Client VPN 身份和访问进行故障排除
- 将服务相关角色用于 AWS Client VPN

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Client VPN 中所做的工作。

服务用户 – 如果使用 Client VPN 服务来完成任务，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 Client VPN 功能来完成工作时，您可能需要额外权限。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 Client VPN 中的功能，请参阅 对 AWS Client VPN 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Client VPN 资源，则您可能具有 Client VPN 的完全访问权限。您有责任确定您的服务用户应访问哪些 Client VPN 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 Client VPN 结合使用的更多信息，请参阅 如何 AWS Client VPN 与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解有关如何编写策略以管理对 Client VPN 的访问权限的详细信息。要查看您可在 IAM 中使用的 Client VPN 基于身份的策略示例，请参阅 适用于 AWS Client VPN的基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

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

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。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》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都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 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。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

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，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您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。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

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，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用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。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，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

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代入。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 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

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。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用

IAM Identity Center，则需要配置权限集。为控制您的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 用户可代入 IAM 用户或角色，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。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 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代理）。要了解用于跨账户访问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 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 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 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当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项操作的权限。有关发出 FAS 请求时的策略详情，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分派的 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-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 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证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。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 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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，假设您有一个允许 `iam:GetRole` 操作的策略。拥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、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。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。委托人可以包括账户、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 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

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

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 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 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Client VPN 与 IAM 配合使用

在使用 IAM 管理对 Client VPN 的访问之前，了解哪些 IAM 功能可与 Client VPN 结合使用。

您可以在 C AWS lient VPN 中使用的 IAM 功能

IAM 功能	Client VPN 支持
基于身份的策略	是
基于资源的策略	否

IAM 功能	Client VPN 支持
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	是

Client VPN 的基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。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。

Client VPN 的基于身份的策略示例

要查看 Client VPN 基于身份的策略示例，请参阅 适用于 AWS Client VPN的基于身份的策略示例。

Client VPN 内基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。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。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。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 中的跨账户资源访问。

Client VPN 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 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 Client VPN 操作列表，请参阅《服务授权参考》中的 AWS Client VPN 定义的操作。

Client VPN 中的策略操作在操作前使用以下前缀：

```
ec2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

要查看 Client VPN 基于身份的策略示例，请参阅 适用于 AWS Client VPN的基于身份的策略示例。

Client VPN 的策略资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。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 Client VPN 资源类型及其列表 ARNs，请参阅《服务授权参考》中的 AWS Client VPN 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 AWS Client VPN 定义的操作。

要查看 Client VPN 基于身份的策略示例，请参阅 适用于 AWS Client VPN的基于身份的策略示例。

Client VPN 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，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。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。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 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Client VPN 条件密钥列表，请参阅《服务授权参考》中的 AWS Client VPN 条件密钥。要了解可以使用条件键的操作和资源，请参阅 AWS Client VPN 定义的操作。

要查看 Client VPN 基于身份的策略示例，请参阅 适用于 AWS Client VPN的基于身份的策略示例。

ACLs 在 Client VPN 中

支持 ACLs：否

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

ABAC 以及 Client VPN

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。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，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证用于 Client VPN

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您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》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Client VPN 的跨服务主体权限

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当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项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Client VPN 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

Client VPN 的服务相关角色

支持服务相关角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

适用于 AWS Client VPN的基于身份的策略示例

原定设置情况下，用户和角色没有创建或修改 Client VPN 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 策略。管理员随后可以向角色添加 IAM 策略，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 策略（控制台）。

有关 Client VPN 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 AWS Client VPN 的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践

- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Client VPN 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管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 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

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

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam: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 Client VPN 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Client VPN 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Client VPN 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我 AWS 账户 的 Client VPN 资源

我无权在 Client VPN 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `ec2:`*`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:
 ec2: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 `ec2:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Client VPN。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Client VPN 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我 AWS 账户 的 Client VPN 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Client VPN 是否支持这些功能，请参阅 如何 AWS Client VPN 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。

- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

将服务相关角色用于 AWS Client VPN

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Client VPN 直接关联的独特类型的 IAM 角色。服务相关角色由 Client VPN 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

主题

- 将角色用于 AWS Client VPN
- 在 Client VPN 中使用角色进行连接授权；

将角色用于 AWS Client VPN

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Client VPN 直接关联的独特类型的 IAM 角色。服务相关角色由 Client VPN 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Client VPN，因为您不必手动添加必要的权限。Client VPN 定义其服务相关角色的权限，除非另外定义，否则只有 Client VPN 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

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

客户端 VPN 的服务相关角色权限

Client VPN 使用名为 AWSServiceRoleForClientVPN 的服务相关角色——允许 Client VPN 创建和管理与您的 VPN 连接相关的资源。

AWSServiceRoleForClientVPN 服务相关角色信任以下服务来代入该角色：

- `clientvpn.amazonaws.com`

此服务相关角色使用托管策略客户端VPNServiceRolePolicy。要查看此策略的权限，请参阅《AWS 托管策略参考》VPNServiceRolePolicy中的 “客户端”。

为 Client VPN 创建服务相关角色

您无需手动创建服务相关角色。当您使用 AWS Management Console、或 AWS API 在账户中创建第一个客户端 VPN 终端节点时 AWS CLI，Client VPN 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您在账户中创建第一个 Client VPN 端点时，Client VPN 将再次为您创建服务相关角色。

编辑 Client VPN 的服务相关角色

Client VPN 不允许您编辑 AWSService RoleForClient VPN 服务相关角色。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。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色描述。

删除 Client VPN 的服务相关角色

如果您不再需要使用 Client VPN，我们建议您删除 AWSServiceRoleForClientVPN 服务相关角色。

您必须首先删除相关的客户端 VPN 资源。这可确保您不会无意中删除访问这些资源的权限。

使用 IAM 控制台、IAM CLI 或 IAM API 删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

在 Client VPN 中使用角色进行连接授权；

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Client VPN 直接关联的独特类型的 IAM 角色。服务相关角色由 Client VPN 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Client VPN，因为您不必手动添加必要的权限。Client VPN 定义其服务相关角色的权限，除非另外定义，否则只有 Client VPN 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

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

客户端 VPN 的服务相关角色权限

Client VPN 使用名为 AWSServiceRoleForClientVPNConnections“服务关联角色” 的服务相关角色进行客户端 VPN 连接。

AWSServiceRoleForClientVPNConnections 服务相关角色信任以下服务来代入该角色：

- `clientvpn-connections.amazonaws.com`

名为 Client 的角色权限策略VPNServiceConnectionsRolePolicy 允许 Client VPN 对指定资源完成以下操作：

- 操作：`arn:aws:lambda:*:*:function:AWSClientVPN-*` 上的 `lambda:InvokeFunction`

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。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 Client VPN 创建服务相关角色

您无需手动创建服务相关角色。当您使用 AWS Management Console、或 AWS API 在账户中创建第一个客户端 VPN 终端节点时 AWS CLI，Client VPN 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您在账户中创建第一个 Client VPN 端点时，Client VPN 将再次为您创建服务相关角色。

编辑 Client VPN 的服务相关角色

Client VPN 不允许您编辑 AWSServiceRoleForClientVPNConnections 服务相关角色。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。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色描述。

删除 Client VPN 的服务相关角色

如果您不再需要使用 Client VPN，我们建议您删除AWSServiceRoleForClientVPNConnections服务相关角色。

您必须首先删除相关的客户端 VPN 资源。这可确保您不会无意中删除访问这些资源的权限。

使用 IAM 控制台、IAM CLI 或 IAM API 删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

韧性在 AWS Client VPN

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效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结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

除 AWS 全球基础设施外，还 AWS Client VPN 提供有助于支持您的数据弹性和备份需求的功能。

多个目标网络以实现高可用性

可以将目标网络与 Client VPN 端点相关联以使客户端能够建立 VPN 会话。目标网络是 VPC 中的子网。与 Client VPN 端点关联的每个子网必须属于不同的可用区。您可以将多个子网与一个 Client VPN 终端节点关联以实现高可用性。

中的基础设施安全 AWS Client VPN

作为一项托管服务， AWS Client VPN 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Client VPN。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

以下方面的安全最佳实践 AWS Client VPN

AWS Client VPN 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

授权规则

使用授权规则限制哪些用户可以访问您的网络。有关更多信息，请参阅 授权规则。

安全组

使用安全组来控制用户可以在您的 VPC 中访问哪些资源。有关更多信息，请参阅 安全组。

客户端证书吊销列表

针对特定客户端证书，使用客户端证书吊销列表撤销对 Client VPN 端点的访问权限。例如，当用户离开组织时。有关更多信息，请参阅 客户端证书吊销列表。

会话超时时断开连接

在达到最长 Client VPN 会话时间时断开会话，强制规定最长 VPN 会话持续时间。有关更多信息，请参阅 最长 VPN 会话持续时间。

监控工具

使用监控工具跟踪 Client VPN 端点的可用性和性能。有关更多信息，请参阅 监控 Client VPN。

身份和访问管理

管理对 Client VPN 资源的访问权限，并 APIs 使用适用于您的 IAM 用户和 IAM 角色的 IAM 策略。有关更多信息，请参阅 的身份和访问管理 AWS Client VPN。

IPv6 的注意事项 AWS Client VPN

当前，Client VPN 服务不支持通过 VPN 隧道路由 IPv6 流量。但是，在某些情况下，应将 IPv6 流量路由到 VPN 隧道以防止 IPv6 泄漏。 IPv6 当 IPv4 和 IPv6 都启用并连接到 VPN 时，可能会发生泄漏，但是 VPN 不会将 IPv6 流量路由到其隧道中。在这种情况下，当连接到 IPv6 已启用的目的地时，您实际上仍在使用互联网服务提供商提供 IPv6 的地址进行连接。这会泄露你的真实 IPv6 地址。以下说明说明如何将 IPv6 流量路由到 VPN 隧道。

应将以下 IPv6相关指令添加到您的 Client VPN 配置文件中，以防止 IPv6 泄漏：

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

举个例子：

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

在本示例中，`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1`将本地隧道设备 IPv6 地址设置为，将`fd15:53b6:dead::2`远程 VPN 端点 IPv6 地址设置为`fd15:53b6:dead::1`。

下一个命令`route-ipv6 2000::/4`将 IPv6 地址从到路由`2000:0000:0000:0000:0000:0000:0000:0000`到`2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` VPN 连接。

> **Note**
>
> 例如，对于 Windows 中的 TAP 设备路由，`ifconfig-ipv6` 的第二个参数将被用作 `--route-ipv6` 的路由目标。

企业应配置 `ifconfig-ipv6` 本身的两个参数，并且可以使用 `100::/64`（从`0100:0000:0000:0000:0000:0000:0000:0000` 到`0100:0000:0000:0000:ffff:ffff:ffff:ffff`）或 `fc00::/7`（从`fc00:0000:0000:0000:0000:0000:0000:0000` 到`fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`)中的地址。`100::/64` 是仅丢弃的地址块，`fc00::/7` 为唯一本地。

另一个示例是：

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

在本示例中，配置会将当前分配的所有 IPv6 流量路由到 VPN 连接。

验证

您的组织可能会有自己的测试。基本验证是设置全隧道 VPN 连接，然后使用该 IPv6地址对 IPv6 服务器运行 ping6。服务器的地 IPv6 址应在`route-ipv6`命令指定的范围内。此 ping 测试将失败。但是，如果将来向 Client VPN 服务添加 IPv6 支持，这种情况可能会改变。如果 ping 成功，并且您能够在以全通道模式连接时访问公共站点，则可能需要执行进一步的故障排除。还有一些公开提供的工具可用。

监控 AWS Client VPN

监控是维护和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS Client VPN 您可以使用以下特征监控您的 Client VPN 端点，分析流量模式，以及解决与您的 Client VPN 端点相关的问题。

Amazon CloudWatch

实时监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

AWS CloudTrail

捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。所有 Client VPN 操作均由亚马逊 EC2 API 参考记录 CloudTrail 并记录在案。

Amazon CloudWatch 日志

使您能够监控尝试连接到 AWS Client VPN 端点的操作。可以查看 Client VPN 连接的连接尝试和连接重置。对于连接尝试，您可以查看成功的和失败的连接尝试。您可以指定 Log CloudWatch s 日志流来记录连接详细信息。有关更多信息，请参阅AWS Client VPN 端点的连接日志和 Amazon CloudWatch 日志用户指南。

主题

- 以下各项的亚马逊 CloudWatch 指标 AWS Client VPN

以下各项的亚马逊 CloudWatch 指标 AWS Client VPN

AWS Client VPN 向亚马逊发布您的客户端 VPN 终端节点 CloudWatch 的以下指标。指标 CloudWatch 每五分钟向 Amazon 发布一次。

指标	描述
ActiveConnectionsCount	与 Client VPN 端点的活动连接数。

指标	描述
	单位：计数
AuthenticationFailures	Client VPN 端点的身份验证失败次数。 单位：计数
CrlDaysToExpiry	在 Client VPN 端点上配置的证书吊销列表（CRL）到期之前的天数。 单位：天
EgressBytes	从 Client VPN 端点发送的字节数。 单位：字节
EgressPackets	从 Client VPN 端点发送的数据包数。 单位：计数
IngressBytes	Client VPN 端点接收的字节数。 单位：字节
IngressPackets	Client VPN 端点接收的数据包数。 单位：计数
SelfServicePortalClientConfigurationDownloads	从自助服务门户下载 Client VPN 端点配置文件的次数。 单位：计数

AWS Client VPN 为您的 Client VPN 终端发布以下状态评估指标。

指标	描述
ClientConnectHandlerTimeouts	为 Client VPN 端点连接调用客户端连接处理程序的超时次数。

指标	描述
	单位：计数
ClientConnectHandlerInvalidResponses	客户端连接处理程序为与 Client VPN 端点连接返回的无效响应数。 单位：计数
ClientConnectHandlerOtherExecutionErrors	为 Client VPN 端点连接运行客户端连接处理程序时出现的意外错误数。 单位：计数
ClientConnectHandlerThrottlingErrors	为 Client VPN 端点连接调用客户端连接处理程序时出现的节流次数。 单位：计数
ClientConnectHandlerDeniedConnections	Client VPN 端点连接的客户端连接处理程序拒绝连接的次数。 单位：计数
ClientConnectHandlerFailedServiceErrors	为 Client VPN 端点连接运行客户端连接处理程序时出现的服务端错误数。 单位：计数

可以按端点筛选 Client VPN 端点的指标。

CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。每个数据点都有关联的时间戳和可选的测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控指定的指标，并在该指标超出您认为可接受的范围时启动操作（例如向电子邮件地址发送通知）。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

任务

- 在亚马逊上查看 Client VPN 终端节点指标 CloudWatch

在亚马逊上查看 Client VPN 终端节点指标 CloudWatch

您可以按照以下方法查看 Client VPN 端点的指标。

使用 CloudWatch 控制台查看指标

指标的分组首先依据服务命名空间，然后依据每个命名空间内的各种维度组合。

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 在 All metrics（所有指标）下，选择 ClientVPN 指标命名空间。
4. 要查看指标，请选择指标维度 by endpoint（按端点）。

要查看指标，请使用 AWS CLI

在命令提示窗口中，使用以下命令可列出可用于Client VPN 的指标

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

AWS Client VPN 配额

您的 AWS 账户具有以下与 Client VPN 终端节点相关的配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要请求增加可调配额，请选择 Adjustable（可调）列中的 Yes（是）。有关更多信息，请参阅《Service Quotas 用户指南》中的请求增加配额。

客户端 VPN 配额

名称	默认值	可调整
每个 Client VPN 端点的授权规则数	200	是
每个区域的 Client VPN 端点数	5	是
每个 Client VPN 端点的并发客户端连接数	此值取决于每个终端节点的子网关联数。 • 1 – 7,000 • 2 – 36,500 • 3 – 66,500 • 4 – 96,500 • 5 – 126,000	是
每个 Client VPN 端点的并发操作数	10	否
Client VPN 端点的客户端证书吊销列表中的条目数	20000	否
每个 Client 的路由 VPN 目标网络关联	100	是

操作包括：

- 关联和取消关联子网
- 创建或删除安全组

用户和组配额

为 Active Directory 或基于 SAML 的 IdP 配置用户和组时，应用以下配额：

- 用户最多可以属于 200 个组。系统将忽略第 200 个组之后的所有组。
- 组 ID 的最大长度为 255 个字符。
- 名称 ID 的最大长度为 255 个字符。系统在 255 个字符后截断字符。

一般注意事项

在使用 Client VPN 端点时，请注意以下事项：

- 如果您使用 Active Directory 对用户进行身份验证，则 Client VPN 端点必须与用于 Active Directory 身份验证的 AWS Directory Service 资源属于同一个帐户。
- 如果您使用基于 SAML 的联合身份验证对用户进行身份验证，则 Client VPN 终端节点必须与您为定义 IdP 信任关系而创建的 IAM SAML 身份提供商属于同一个账户。 AWS IAM SAML 身份提供商可以在同一个 AWS 账户中的多个 Client VPN 终端节点之间共享。

故障排除 AWS Client VPN

以下各节可帮助您排查可能遇到的 Client VPN 端点问题。

有关排查客户端用于连接到 Client VPN 的基于 OpenVPN 的软件问题的更多信息，请参阅《AWS Client VPN 用户指南》中的 排查 Client VPN 连接问题。

常见问题

- 疑难解答 AWS Client VPN：无法解析 Client VPN 端点 DNS 名称
- 故障排除 AWS Client VPN：流量未在子网之间进行分配
- 故障排除 AWS Client VPN：Active Directory 群组的授权规则未按预期运行
- 故障排除 AWS Client VPN：客户端无法访问对等 VPC、Amazon S3 或互联网
- 故障排除 AWS Client VPN：对等互连 VPC、Amazon S3 或互联网的访问是间歇性的
- 疑难解答 AWS Client VPN：客户端软件在尝试连接到 Client VPN 时返回 TLS 错误
- 故障排除 AWS Client VPN：客户端软件返回用户名和密码错误 — Active Directory 身份验证
- 故障排除 AWS Client VPN：客户端软件返回用户名和密码错误-联合身份验证
- 故障排除 AWS Client VPN：客户端无法连接 — 双向认证
- 疑难解答 AWS Client VPN：客户端在 Client VPN — 联合身份验证中返回凭据超过最大大小错误
- 故障排除 AWS Client VPN：客户端无法打开端点浏览器 — 联合身份验证
- 故障排除 AWS Client VPN：客户端返回无可用端口错误-联合身份验证
- 故障排除 AWS Client VPN：由于 IP 不匹配导致连接终止
- 故障排除 AWS Client VPN：将流量路由到 LAN 未按预期工作
- 故障排除 AWS Client VPN：验证 Client VPN 端点的带宽限制
- 故障排除 AWS Client VPN：与 VPC 的隧道连接问题

疑难解答 AWS Client VPN：无法解析 Client VPN 端点 DNS 名称

问题

我无法解析 Client VPN 端点的 DNS 名称。

原因

Client VPN 端点配置文件包含一个名为 `remote-random-hostname` 的参数。此参数强制客户端在 DNS 名称前添加随机字符串以防止 DNS 缓存。某些客户端无法识别此参数，因此它们不会在 DNS 名称的前面添加所需的随机字符串。

解决方案

使用首选文本编辑器打开 Client VPN 终端节点配置文件。找到指定 Client VPN 端点 DNS 名称的那一行，并在其前面添加一个随机字符串，格式为。*`random_string.displayed_DNS_name`*例如：

- 原始 DNS 名称：`cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- 修改的 DNS 名称：`asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

故障排除 AWS Client VPN：流量未在子网之间进行分配

问题

我正在尝试在两个子网之间分割网络流量。私有流量将通过私有子网路由，而 Internet 流量将通过公有子网路由。但仅使用了一个路由，即便我已将两个路由添加到 Client VPN 端点路由表中也是如此。

原因

虽然可以将多个子网与 Client VPN 端点关联，但每个可用区只能关联一个子网。多子网关联旨在为客户端提供高可用性和可用区冗余。但您无法通过 Client VPN 选择性地分割与 Client VPN 端点关联的各个子网之间的流量。

客户端根据 DNS 轮询算法连接到客户端 VPN 终端节点。这意味着当客户端建立连接时，其流量可以通过任何关联的子网路由。因此，如果客户端登录没有所需路由条目的关联子网，它们可能会遇到连接问题。

例如，假设您配置了以下子网关联和路由：

- 子网关联
  - 关联 1：子网 A (us-east-1a)
  - 关联 2：子网 B (us-east-1b)
- 路线
  - 路由 1：10.0.0.0/16 路由到子网 A
  - 路由 2：172.31.0.0/16 路由到子网 B

在此示例中，连接时登录子网 A 的客户端无法访问路由 2，而连接时登录子网 B 的客户端无法访问路由 1。

解决方案

验证客户端 VPN 终端节点是否具有针对每个关联网络的目标的相同路由条目。这将确保客户端有权访问所有路由，而不管其流量通过哪个子网路由。

故障排除 AWS Client VPN：Active Directory 群组的授权规则未按预期运行

问题

我已为我的 Active Directory 组配置授权规则，但这些规则未按预期工作。我为添加了授权规则`0.0.0.0/0`来授权所有网络的流量，但是特定目的地的流量仍然会失败 CIDRs。

原因

授权规则已在网络 CIDRs上建立索引。授权规则必须授予 Active Directory 组访问特定网络的权限 CIDRs。针对 `0.0.0.0/0` 的授权规则将作为特殊情况处理，并在最后进行评估，无论授权规则的创建顺序如何。

例如，假设您按以下顺序创建五个授权规则：

- 规则 1：组 1 有权访问 `10.1.0.0/16`
- 规则 2：组 1 有权访问 `0.0.0.0/0`
- 规则 3：组 2 有权访问 `0.0.0.0/0`
- 规则 4：组 3 有权访问 `0.0.0.0/0`
- 规则 5：组 2 有权访问 `172.131.0.0/16`

在此示例中，最后评估规则 2、规则 3 和规则 4。组 1 仅有权访问 `10.1.0.0/16`，组 2仅有权访问 `172.131.0.0/16`。组 3 无权访问 `10.1.0.0/16` 或 `172.131.0.0/16`，但它有权访问所有其他网络。如果删除规则 1 和规则 5，则所有三个组都有权访问所有网络。

在评估授权规则时，客户端 VPN 会使用最长前缀匹配。有关更多详细信息，请参阅 Amazon VPC 用户指南中的路由优先级。

解决方案

确认您创建的授权规则明确授予 Active Directory 组访问特定网络的权限 CIDRs。如果添加针对 `0.0.0.0/0` 的授权规则，请记住此规则将最后进行评估，并且以前的授权规则可能会限制其授予访问权限的网络。

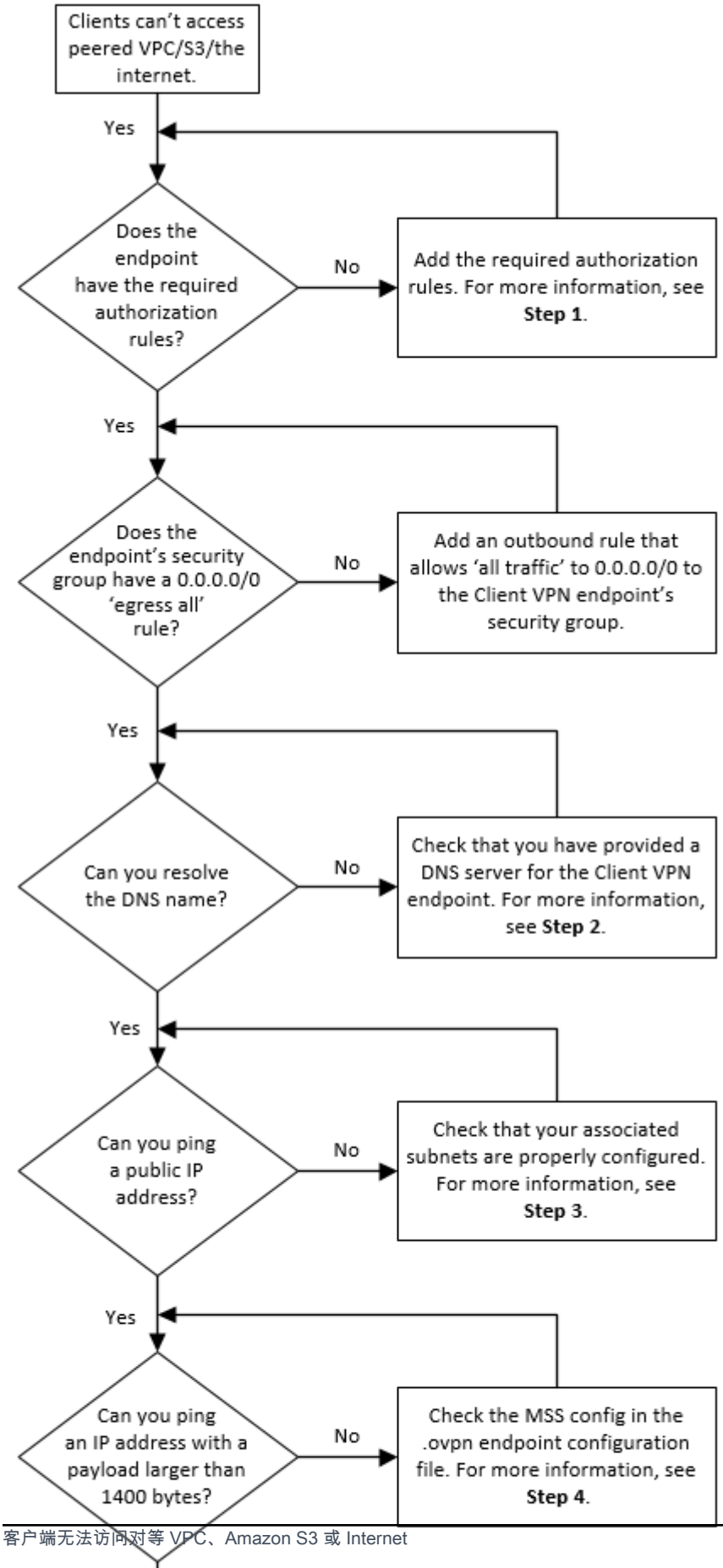
故障排除 AWS Client VPN：客户端无法访问对等 VPC、Amazon S3 或互联网

问题

我已正确配置 Client VPN 端点路由，但我的客户端无法访问对等 VPC、Amazon S3 或 Internet。

解决方案

以下流程图包含诊断 Internet、对等 VPC 和 Amazon S3 连接问题的步骤。


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. 要访问 Internet，请添加针对 `0.0.0.0/0` 的授权规则。

   要访问对等互连 VPC，请为 VPC 的 IPv4 CIDR 范围添加授权规则。

   要访问 S3，请指定 Amazon S3 端点的 IP 地址。
2. 检查您是否能够解析 DNS 名称。

   如果您无法解析 DNS 名称，请验证您是否已为 Client VPN 端点指定 DNS 服务器。如果您管理自己的 DNS 服务器，请指定其 IP 地址。验证是否能够从 VPC 访问 DNS 服务器。

   如果您不确定要为 DNS 服务器指定哪个 IP 地址，请在 VPC 中的 .2 IP 地址处指定 VPC DNS 解析程序。
3. 对于 Internet 访问，请检查您是否能够 ping 公有 IP 地址或公共网站，例如 `amazon.com`。如果您未收到响应，请确保关联子网的路由表具有针对互联网网关或 NAT 网关的默认路由。如果路由已就绪，请确认关联子网没有阻止入站和出站流量的网络访问控制列表规则。

   如果您无法访问对等 VPC，请验证关联子网的路由表是否具有对等 VPC 的路由条目。

   如果您无法访问 Amazon S3，请验证关联子网的路由表是否具有网关 VPC 端点的路由条目。
4. 检查您是否能够对负载大于 1400 字节的公有 IP 地址执行 ping 操作。使用以下命令之一：

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

   如果您无法对负载大于 1400 字节的 IP 地址执行 ping 操作，请使用首选文本编辑器打开 Client VPN 端点 `.ovpn` 配置文件，并添加以下内容。

   ```
   mssfix 1328
   ```

故障排除 AWS Client VPN：对等互连 VPC、Amazon S3 或互联网的访问是间歇性的

问题

我在连接到对等 VPC、Amazon S3 或 Internet 时遇到间歇性连接问题，但对关联子网的访问未受到影响。我需要先断开连接，然后重新连接才能解决连接问题。

原因

客户端根据 DNS 轮询算法连接到客户端 VPN 终端节点。这意味着当客户端建立连接时，其流量可以通过任何关联的子网路由。因此，如果客户端登录没有所需路由条目的关联子网，它们可能会遇到连接问题。

解决方案

验证客户端 VPN 终端节点是否具有针对每个关联网络的目标的相同路由条目。这将确保客户端有权访问所有路由，而不管其流量通过哪个关联子网路由。

例如，假设您的 Client VPN 端点有三个关联的子网（子网 A、子网 B 和子网 C），并且您希望为您的客户端启用 Internet 访问。为此，您必须添加三个 `0.0.0.0/0` 路由 - 每个关联子网各一个路由：

- 路由 1：`0.0.0.0/0`（针对子网 A）
- 路由 2：`0.0.0.0/0`（针对子网 B）
- 路由 3：`0.0.0.0/0`（针对子网 C）

疑难解答 AWS Client VPN：客户端软件在尝试连接到 Client VPN 时返回 TLS 错误

问题

我曾经能够成功地将我的客户端连接到 Client VPN，但现在基于 OpenVPN 的客户端在尝试连接时返回以下错误之一：

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

可能的原因 1

如果您使用的是双向身份验证，并且已导入一个客户端证书吊销列表，则该客户端证书吊销列表可能已过期。在身份验证阶段，Client VPN 端点会根据您导入的客户端证书吊销列表检查客户端证书。如果客户端证书吊销列表已过期，则无法连接到 Client VPN 端点。

解决方案 1

使用 OpenSSL 工具检查客户端证书吊销列表的到期日期。

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

输出将显示到期日期和时间。如果客户端证书吊销列表已过期，则必须创建一个新的客户端证书吊销列表并将其导入 Client VPN 端点。有关更多信息，请参阅 AWS Client VPN 客户证书吊销列表。

可能的原因 2

用于 Client VPN 端点的服务器证书已过期。

解决方案 2

在 AWS Certificate Manager 控制台中或使用 AWS CLI 检查服务器证书的状态。如果服务器证书已过期，请创建新证书并将其上传到 ACM。有关使用 OpenVPN easy-rsa 实用程序生成服务器和客户端证书和密钥并将其导入 ACM 的详细步骤，请参阅双向认证 AWS Client VPN。

或者，客户端用于连接到 Client VPN 的基于 OpenVPN 的软件可能出现了问题。有关排查基于 OpenVPN 的软件问题的更多信息，请参阅《AWS Client VPN 用户指南》中的排查 Client VPN 连接问题。

故障排除 AWS Client VPN：客户端软件返回用户名和密码错误 — Active Directory 身份验证

问题

我对我的 Client VPN 端点使用的是 Active Directory 身份验证，并且我曾经能够将我的客户端成功连接到 Client VPN。但是现在，客户端收到了无效用户名和密码错误。

可能的原因

如果您使用的是 Active Directory 身份验证，并且在分发客户端配置文件后启用了 Multi-Factor Authentication (MFA)，则该文件不包含用于提示用户输入 MFA 代码的必要信息。系统提示用户仅输入其用户名和密码，但身份验证失败。

解决方案

下载新的客户端配置文件并将它分发给您的客户端。确认此新文件包含以下行。

```
static-challenge "Enter MFA code " 1
```

有关更多信息，请参阅 AWS Client VPN 端点配置文件导出。测试 Active Directory 的 MFA 配置，而无需使用 Client VPN 端点来验证 MFA 是否按预期工作。

故障排除 AWS Client VPN：客户端软件返回用户名和密码错误-联合身份验证

问题

在通过联合身份验证尝试使用用户名和密码登录时，出现错误“收到的凭证不正确。请联系您的 IT 管理员”。

原因

出现此错误可能是由于来自 IdP 的 SAML 响应中没有包含至少一个属性。

解决方案

确保来自 IdP 的 SAML 响应中至少包含一个属性。参阅 基于 SAML 的 IdP 配置资源 了解更多信息。

故障排除 AWS Client VPN：客户端无法连接 — 双向认证

问题

我对我的 Client VPN 端点使用了双向身份验证。客户端收到 TLS 密钥协商失败错误和超时错误。

可能的原因

向客户端提供的配置文件不包含客户端证书和客户端私有密钥，或者证书和密钥不正确。

解决方案

确保该配置文件包含正确的客户端证书和密钥。如有必要，修复配置文件并将它重新分发给您的客户端。有关更多信息，请参阅 AWS Client VPN 端点配置文件导出。

疑难解答 AWS Client VPN：客户端在 Client VPN — 联合身份验证中返回凭据超过最大大小错误

问题

我对我的客户端 VPN 终端节点使用了联合身份验证。当客户端在基于 SAML 的身份提供商 (IdP) 浏览器窗口中输入其用户名和密码时，收到的凭证超过支持的最大大小错误。

原因

IdP 返回的 SAML 响应超出了支持的最大大小。有关更多信息，请参阅 基于 SAML 的联合身份验证的要求和注意事项。

解决方案

尝试在 IdP 中减少用户所属的组数，然后再次尝试连接。

故障排除 AWS Client VPN：客户端无法打开端点浏览器 — 联合身份验证

问题

我对我的客户端 VPN 终端节点使用了联合身份验证。当客户端尝试连接到端点时，客户端软件没有打开浏览器窗口，而是改为显示用户名和密码弹出窗口。

原因

提供给客户端的配置文件不包含 `auth-federate` 标记。

解决方案

导出最新的配置文件，将其导入 AWS 提供的客户端，然后重试连接。

故障排除 AWS Client VPN：客户端返回无可用端口错误-联合身份验证

问题

我对我的客户端 VPN 终端节点使用了联合身份验证。当客户端尝试连接到端点时，客户端软件返回以下错误：

```
The authentication flow could not be initiated. There are no available ports.
```

原因

AWS 提供的客户端需要使用 TCP 端口 35001 来完成身份验证。有关更多信息，请参阅 基于 SAML 的联合身份验证的要求和注意事项。

解决方案

验证客户端的设备未阻止 TCP 端口 35001，或者正在将其用于其他进程。

故障排除 AWS Client VPN：由于 IP 不匹配导致连接终止

问题

VPN 连接终止并且客户端软件返回以下错误："The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."

原因

AWS 提供的客户端要求其连接的 IP 地址与支持 Client VPN 端点的 VPN 服务器的 IP 相匹配。有关更多信息，请参阅 使用 AWS Client VPN的规则和最佳实践。

解决方案

确认 AWS 提供的客户端和 Client VPN 端点之间没有 DNS 代理。

故障排除 AWS Client VPN：将流量路由到 LAN 未按预期工作

问题

当 LAN IP 地址范围不在以下标准私有 IP 地址范围之内时，无法将流量路由到局域网（LAN）：`10.0.0.0/8`、`172.16.0.0/12`、`192.168.0.0/16` 或 `169.254.0.0/16`。

原因

如果检测到客户端 LAN 地址范围超出上述标准范围，Client VPN 端点会将 OpenVPN 指令“redirect-gateway block-local”自动推送到客户端，从而强制所有 LAN 流量进入 VPN。有关更多信息，请参阅使用 AWS Client VPN的规则和最佳实践。

解决方案

如果您需要在 VPN 连接期间访问 LAN，建议您为 LAN 使用上面列出的常规地址范围。

故障排除 AWS Client VPN：验证 Client VPN 端点的带宽限制

问题

我需要验证 Client VPN 端点的带宽限制。

原因

吞吐量取决于多个因素，例如，来自您的位置的连接容量，以及计算机上的 Client VPN 桌面应用程序与 VPC 端点之间的网络延迟。对于每个用户连接，支持的最小带宽为 10 Mbps。

解决方案

运行以下命令以验证带宽。

```
sudo iperf3 -s -V
```

在客户端上：

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

故障排除 AWS Client VPN：与 VPC 的隧道连接问题

当您的 AWS Client VPN 连接遇到连接问题时，请按照这种系统的故障排除方法来识别并解决问题。本节提供了诊断远程客户端与 Amazon VPC 资源之间常见的 Client VPN 连接问题的 step-by-step程序。

主题

- 网络连接先决条件
- 检查 Client VPN 端点状态
- 验证客户端连接
- 验证客户端身份验证
- 查看授权规则
- 验证 Client VPN 路由
- 验证安全组和网络 ACLs
- 测试客户端连接
- 诊断客户端设备
- 解决 DNS 解析问题
- 排除性能故障
- 监控 Client VPN 指标
- 查看 Client VPN 日志
- 常见问题和解决方案

网络连接先决条件

在对 Client VPN 连接进行故障排除之前，请验证以下网络先决条件：

- 确保 Client VPN 端点子网具有互联网连接（通过 Internet Gateway 或 NAT 网关）。
- 验证 Client VPN 终端节点是否与不同可用区域中的子网相关联，以实现高可用性。
- 检查 VPC 是否有足够的 IP 地址空间并且与客户端 CIDR 块没有冲突。
- 确认目标子网具有正确的路由表关联。

检查 Client VPN 端点状态

首先，验证您的 Client VPN 端点是否处于正确的状态：

1. 使用 AWS CLI 来检查 Client VPN 终端节点状态：

```
aws ec2 describe-client-vpn-endpoints --region your-region
```

2. 在输出中查找端点状态。状态应该是available。
3. 验证终端节点是否关联了目标网络（子网）。
4. 如果状态不是available，请检查是否存在任何可能表明配置问题的错误消息或待处理状态。

验证客户端连接

检查与您的客户端 VPN 终端节点的客户端连接状态：

1. 检查活跃的客户端连接：

```
aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id
 --region your-region
```

2. 查看连接状态和输出中的所有错误消息。
3. 检查客户端身份验证日志中是否有失败的身份验证尝试。
4. 确认客户端正在从配置的客户端 CIDR 块接收 IP 地址。

> **Note**
>
> 如果客户端无法连接，则可能是身份验证配置、授权规则或网络连接出现问题。

验证客户端身份验证

身份验证问题是 Client VPN 连接问题的常见原因：

- 对于相互身份验证，请确保客户端证书有效且未过期。
- 要进行活动目录身份验证，请验证用户凭据和域连接。
- 对于基于 SAML 的联合身份验证，请检查 IdP 配置和用户权限。
- 查看身份验证登录 CloudWatch 以获取详细的错误信息。
- 验证在端点上配置的身份验证方法是否与客户端配置相匹配。

查看授权规则

授权规则控制客户端可以访问哪些网络资源：

1. 列出当前的授权规则：

```
aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. 验证是否存在适用于客户端需要访问的目标网络的规则。
3. 检查规则是否指定了正确的 Active Directory 组（如果使用 AD 身份验证）。
4. 确保授权规则处于`active`状态。

验证 Client VPN 路由

正确的路由配置对于 Client VPN 连接至关重要：

1. 检查 Client VPN 终端节点路由：

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. 验证是否存在客户端需要访问的目标网络的路由。
3. 检查 Amazon VPC 路由表，确保返回流量可以到达客户端 VPN 终端节点：

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-region
```

4. 验证目标网络关联的配置是否正确。

验证安全组和网络 ACLs

安全组和网络 ACLs 可以阻止 Client VPN 流量：

1. 检查安全组中是否有目标 EC2 实例：

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxxx --region your-region
```

2. 验证入站规则允许来自 Client VPN CIDR 区块的流量：
   - 来自 Client VPN 的 SSH（端口 22）CIDR：`10.0.0.0/16`
   - 来自 Client VPN 的 HTTP（端口 80）CIDR：`10.0.0.0/16`

- 来自 Client VPN 的 HTTPS（端口 443）CIDR：`10.0.0.0/16`
- 根据需要自定义应用程序端口

3. 对于 Client VPN 端点安全组（如果适用），请确保它允许：
   - 来自 0.0.0.0/0 的 UDP 端口 443 (OpenVPN)
   - 所有出站到 VPC CIDR 块的流量
4. 检查网络 ACLs 是否没有阻塞流量。网络 ACLs 是无状态的，因此必须配置入站和出站规则。
5. 验证您要发送的特定流量的入站和出站规则。

测试客户端连接

测试从 Client VPN 客户端到 Amazon VPC 资源的连接：

1. 通过连接的 Client VPN 客户端，测试与 Amazon VPC 资源的连接：

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. 测试特定的应用程序连接：

```
telnet vpc-resource-ip port
```

3. 如果使用私有 DNS 名称，请验证 DNS 解析：

```
nslookup private-dns-name
```

4. 如果启用了分割隧道，则测试与 Internet 资源的连接。

诊断客户端设备

在客户端设备上执行以下检查：

1. 验证客户端配置文件 (.ovpn) 包含正确的设置：
   - 正确的服务器端点 URL
   - 有效的客户证书和私钥
   - 正确的身份验证方法配置

2. 检查客户端日志中是否存在连接错误：
   - Windows：事件查看器 → 应用程序和服务日志 → OpenVPN
   - macOS：主机应用程序，搜索 “Tunnelblick” 或 “OpenVPN”
   - Linux：`/var/log/openvpn/`或 systemd 日记
3. 测试来自客户端的基本网络连接：

```
ping 8.8.8.8
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

解决 DNS 解析问题

DNS 问题可能会阻止使用私有 DNS 名称访问资源：

1. 检查 Client VPN 终端节点中是否配置了 DNS 服务器：

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --
query 'ClientVpnEndpoints[0].DnsServers'
```

2. 测试来自客户端的 DNS 解析：

```
nslookup private-resource.internal
dig private-resource.internal
```

3. 如果使用自定义 DNS 解析，请验证 Route 53 解析器规则。
4. 检查安全组是否允许从 Client VPN CIDR 到 DNS 服务器的 DNS 流量（UDP/TCP 端口 53）。

排除性能故障

解决 Client VPN 连接的性能问题：

- 使用 ingress/egress 字节 CloudWatch 指标监控带宽利用率。
- 使用来自客户端的持续 ping 测试来检查数据包丢失。
- 确认 Client VPN 端点未达到连接限制。
- 考虑使用多个 Client VPN 端点进行负载分配。
- 在不同的客户地点进行测试，以确定区域绩效问题。

监控 Client VPN 指标

使用 CloudWatch以下方法监控 Client VPN 端点指标：

1. 检查活动连接指标：

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name ActiveConnectionsCount \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Average
```

2. 查看身份验证失败指标：

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name AuthenticationFailures \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Sum
```

3. 查看其他可用指标，例如入口和出口字节和数据包。

查看 Client VPN 日志

Client VPN 连接日志提供有关连接尝试和错误的详细信息：

- 如果尚未配置，请启用 Client VPN 连接日志。
- 查看 CloudWatch 日志以了解连接尝试、身份验证失败和授权错误。
- 查找指明连接问题根本原因的特定错误代码和消息。
- 检查失败的连接中是否存在可能表明存在配置问题的模式。

常见问题和解决方案

可能影响 Client VPN 连接的常见问题：

身份验证失败次数

客户端证书已过期或无效，或者活动目录凭据不正确。验证身份验证配置和凭证有效性。

缺少授权规则

由于授权规则缺失或不正确，客户端无法访问目标网络。为所需网络添加适当的授权规则。

分割隧道问题

由于分割隧道配置，流量路由不正确。根据需要查看和调整分割隧道设置。

客户端 IP 池耗尽

客户端 CIDR 块中没有可用的 IP 地址。扩大客户端 CIDR 范围或断开未使用的客户端。

MTU 问题

由于 MTU 大小限制，大型数据包被丢弃。尝试将 MTU 设置为 1436 字节或在客户端设备上启用 Path MTU 发现。

DNS 解析问题

客户端无法解析私有 DNS 名称。验证 DNS 服务器配置并确保允许 DNS 流量通过安全组。

重叠的 IP 范围

客户端 CIDR 块与本地网络范围冲突。检查并解决客户端 CIDR 和本地网络之间是否存在任何重叠的 IP 地址范围。

TLS 握手失败

TLS 协商期间连接失败。检查证书有效性，确保密码套件正确，并验证客户端和服务器证书的配置是否正确。

路径传播延迟

客户端无法立即使用新路由。更改 Client VPN 路由后，留出 1-2 分钟的时间进行路由传播。

连接中断/不稳定

频繁断开连接或连接不稳定。检查客户端设备上的网络拥塞、防火墙干扰或电源管理设置。

《Client VPN 用户指南》的文档历史记录

下表介绍了《 AWS Client VPN 管理员指南》的更新。

变更	说明	日期
客户端路由强制功能	增加了客户端路由强制功能。	2025年4月20日
增加了 Client VPN 配额	将每个 Client VPN 端点配额的授权规则从 50 增加到 200。	2025 年 3 月 13 日
Support 支持在会话超时时断开连接	会话超时现在支持在达到最大会话持续时间时断开连接。	2025 年 1 月 13 日
增加配额	每个客户端 VPN 端点的授权规则和每个客户端 VPN 端点的路由配额分别从 50 和 10 增加到 100。	2024 年 12 月 19 日
授权规则示例	添加了授权规则的示例场景。	2022 年 9 月 15 日
最长 VPN 会话持续时间	您可以配置一个更短的最长 VPN 会话持续时间，以满足安全性和合规性要求。	2022 年 1 月 20 日
客户端登录横幅	建立 VPN 会话后，您可以在 AWS 提供的 Client VPN 桌面应用程序上启用文本横幅，以满足监管和合规需求。	2022 年 1 月 20 日
客户端连接处理程序	您可以为客户端 VPN 终端节点启用客户端连接处理程序来运行授权新连接的自定义逻辑。	2020 年 11 月 4 日
自助服务门户	您可以在客户端 VPN 终端节点上为客户端启用自助服务门户。	2020 年 10 月 29 日

Client-to-client access	您可以允许连接到客户端 VPN 终端节点的多个客户端相互连接。	2020 年 9 月 29 日
基于 SAML 2.0 的联合身份验证	您可以使用基于 SAML 2.0 的联合身份验证对客户端 VPN 用户进行身份验证。	2020 年 5 月 19 日
在创建过程中指定安全组	您可以在创建 AWS Client VPN 终端节点时指定 VPC 和安全组。	2020 年 3 月 5 日
可配置 VPN 端口	您可以为 AWS Client VPN 终端节点指定支持的 VPN 端口号。	2020 年 1 月 16 日
Multi-Factor Authentication (MFA) 支持	如果您的活动目录启用了 MFA，则您的 AWS Client VPN 终端节点支持 MFA。	2019 年 9 月 30 日
拆分隧道支持	您可以在终端上启用分割隧道。 AWS Client VPN	2019 年 7 月 24 日
初始版本	此版本引入了 AWS Client VPN。	2018 年 12 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。