为SaaS配置SD-WAN Cloud OnRamp

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 配置
  - 在传输接口上启用NAT
  - 创建集中式AAR策略
  - 在vManage中启用应用和直接互联网访问

确认

相关信息

简介

本文档介绍使用分支机构本地出口对软件即服务(SaaS)的Cloud OnRamp进行配置。

先决条件

要求

思科建议您了解思科软件定义广域网(SD-WAN)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科vManage版本20.9.4
- 思科广域网边缘路由器版本17.9.3a

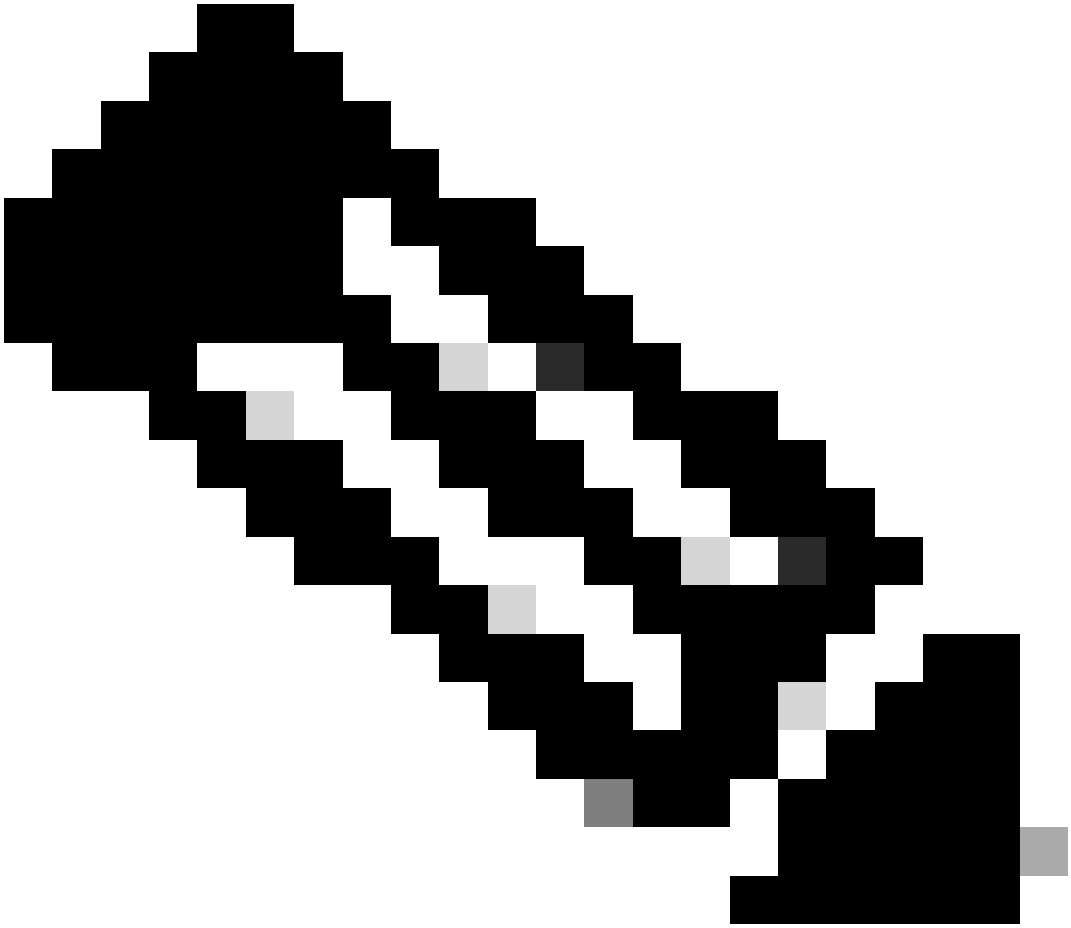
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

对于使用SD-WAN的组织，默认情况下，分支站点通常会通过SD-WAN重叠链路将SaaS应用流量路由到数据中心。SaaS流量从数据中心到达SaaS服务器。

例如，在具有中央数据中心和分支站点的大型组织中，员工可以在分支机构站点使用Office 365。默认情况下，分支机构站点的Office 365流量通过SD-WAN重叠链路路由至一个集中式数据中心，然后从DIA出口路由至Office 365云服务器。

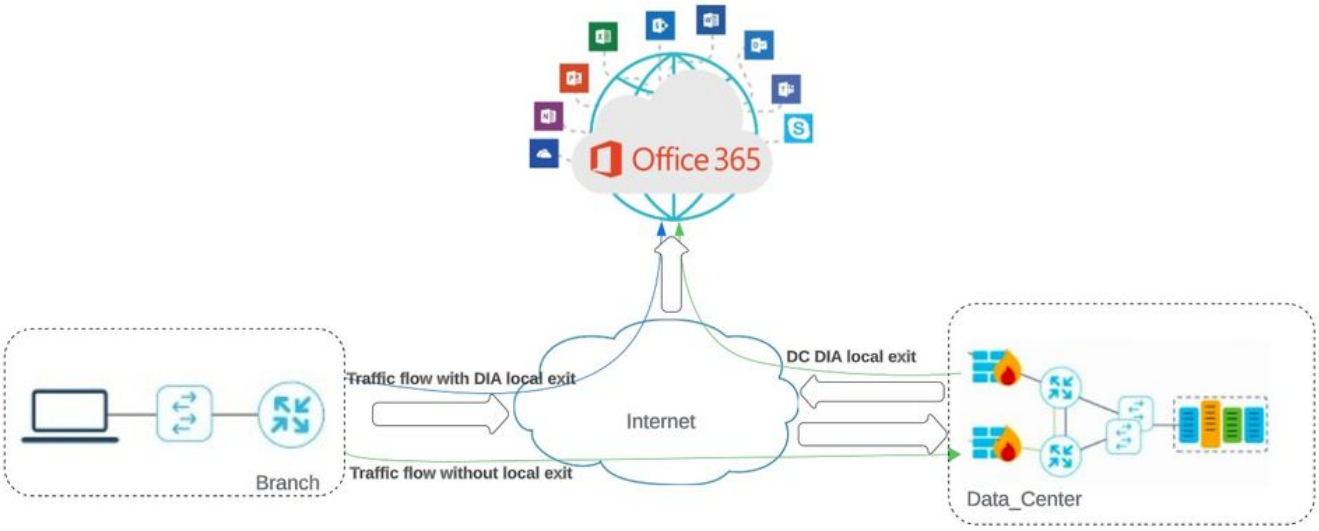
本文档介绍了以下场景：如果分支机构站点具有直接互联网接入(DIA)连接，则可以通过绕过数据中心将软件即服务流量路由到本地DIA来提高性能。



注意：不支持在站点使用环回作为传输定位器(TLOC)接口时为SaaS配置Cloud OnRamp。

配置

网络图

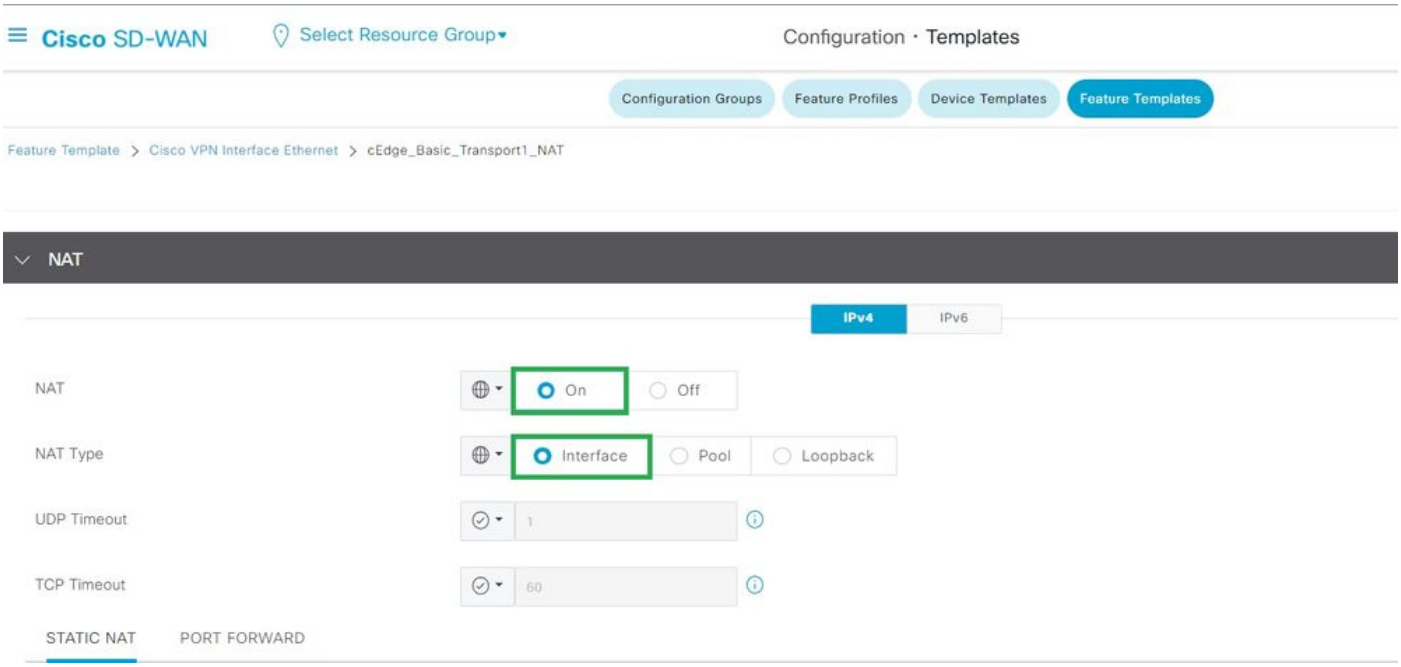


网络拓扑

配置

在传输接口上启用NAT

导航到Feature Template 。 选择模**Transport VPN interface** 板并启用**NAT**。



启用接口*NAT*

等效的CLI配置：

```
interface GigabitEthernet2
ip nat outside
```

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

创建集中式AAR策略

要建立集中策略，必须遵循以下步骤：

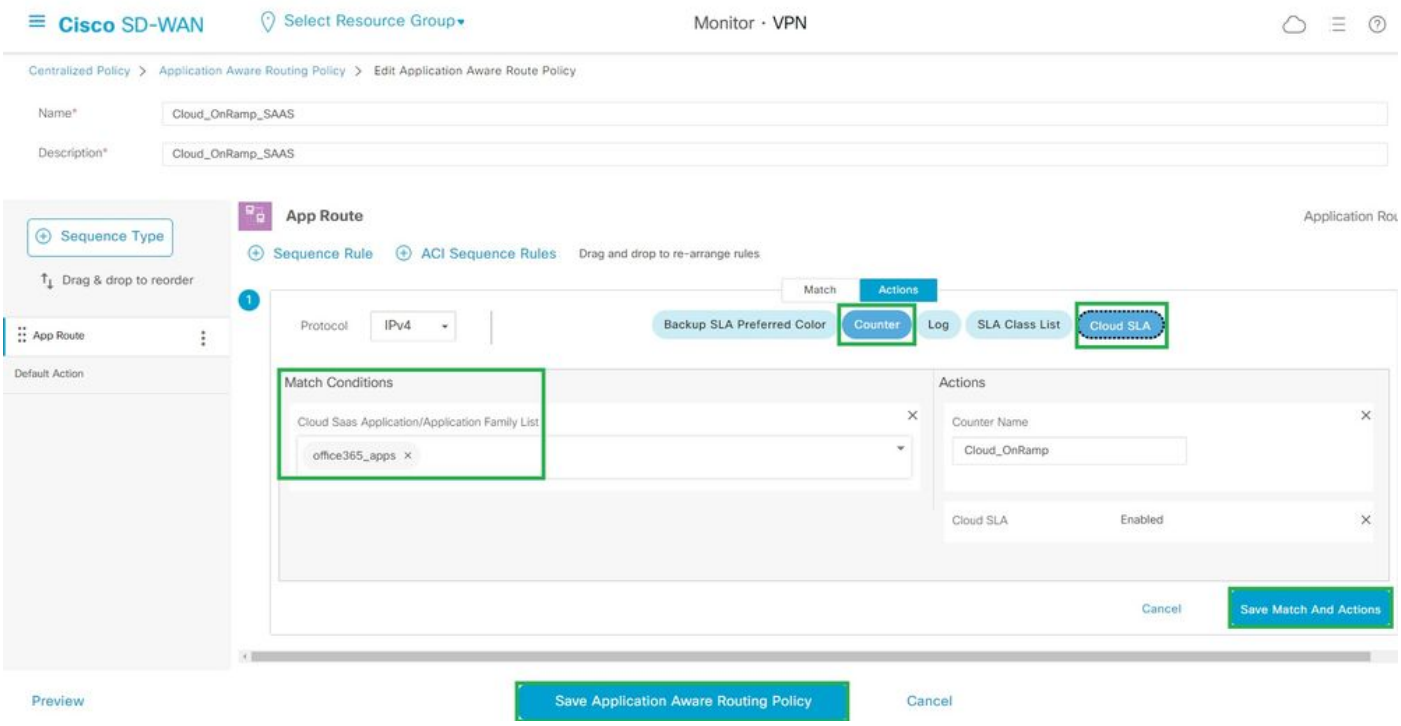
步骤1:创建站点列表：

VPN接口NAT模板

第二步：创建VPN列表：

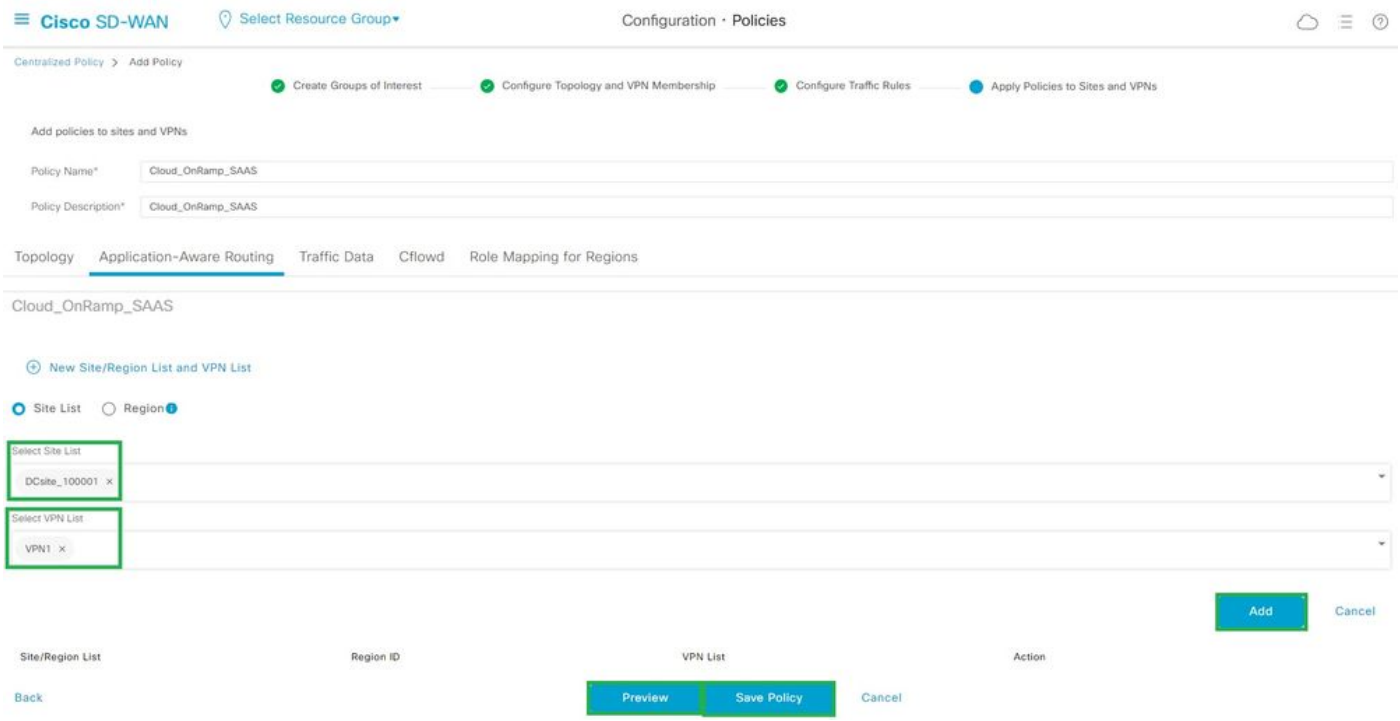
集中策略自定义站点列表

第三步：配置Traffic Rules 并创建Application Aware Routing Policy。



应用感知路由策略

第四步：将策略添加到目标Sites中，然后VPN：



将策略添加到站点和*VPN*

等效的CLI策略：

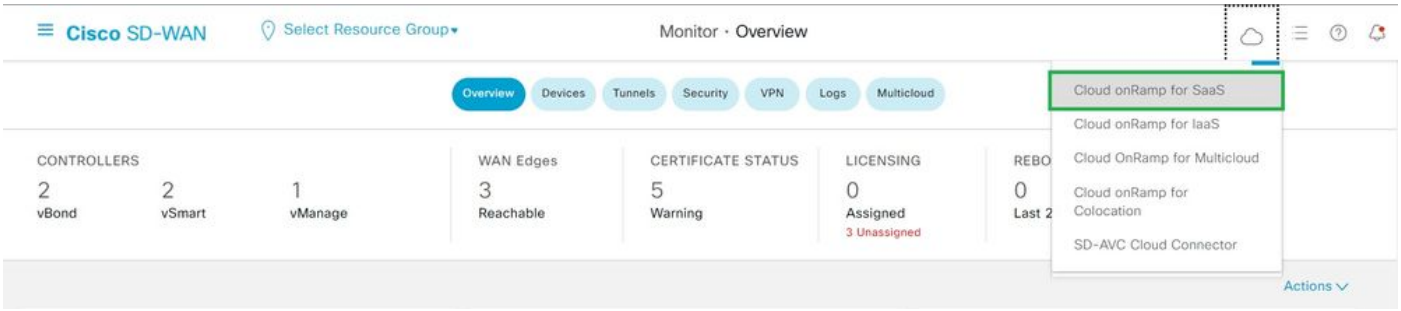
```
viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1
```

```
sequence 1
match
cloud-saas-app-list office365_apps
source-ip 0.0.0.0/0
!
action
count Cloud_OnRamp_-92622761
!
!
!
lists
app-list office365_apps
app skype
app ms_communicator
app windows_marketplace
app livemail_mobile
app word_online
app excel_online
app onedrive
app yammer
app sharepoint
app ms-office-365
app hockeyapp
app live_hotmail
app live_storage
app outlook-web-service
app skydrive
app ms_teams
app skydrive_login
app sharepoint_admin
app ms-office-web-apps
app ms-teams-audio
app share-point
app powerpoint_online
app ms-lync-video
app live_mesh
app ms-lync-control
app groove
app ms-live-accounts
app office_docs
app owa
app ms_sway
app ms-lync-audio
app live_groups
app office365
app windowslive
app ms-lync
app ms-services
app ms_translator
app microsoft
app sharepoint_blog
app ms_onenote
app ms-teams-video
app ms-update
app ms-teams-media
app ms_planner
app lync
app outlook
app sharepoint_online
```

```
app lync_online
app sharepoint_calendar
app ms-teams
app sharepoint_document
!
site-list DCsite_100001
site-id 100001
!
vpn-list VPN1
vpn 1
!
!
!
apply-policy
site-list DCsite_100001
app-route-policy _VPN1_Cloud_OnRamp_SAAS
!
!
```

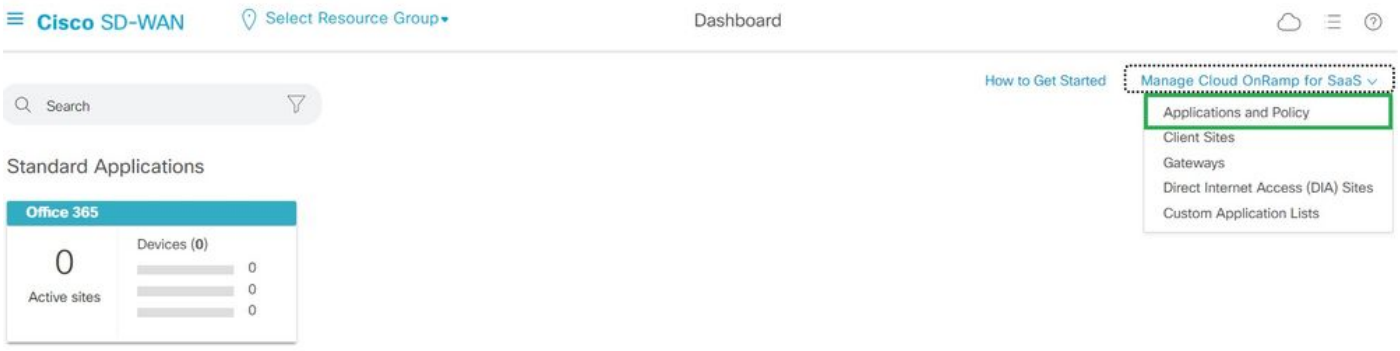
在vManage中启用应用和直接互联网访问

步骤1:导航到Cloud OnRamp for SaaS。



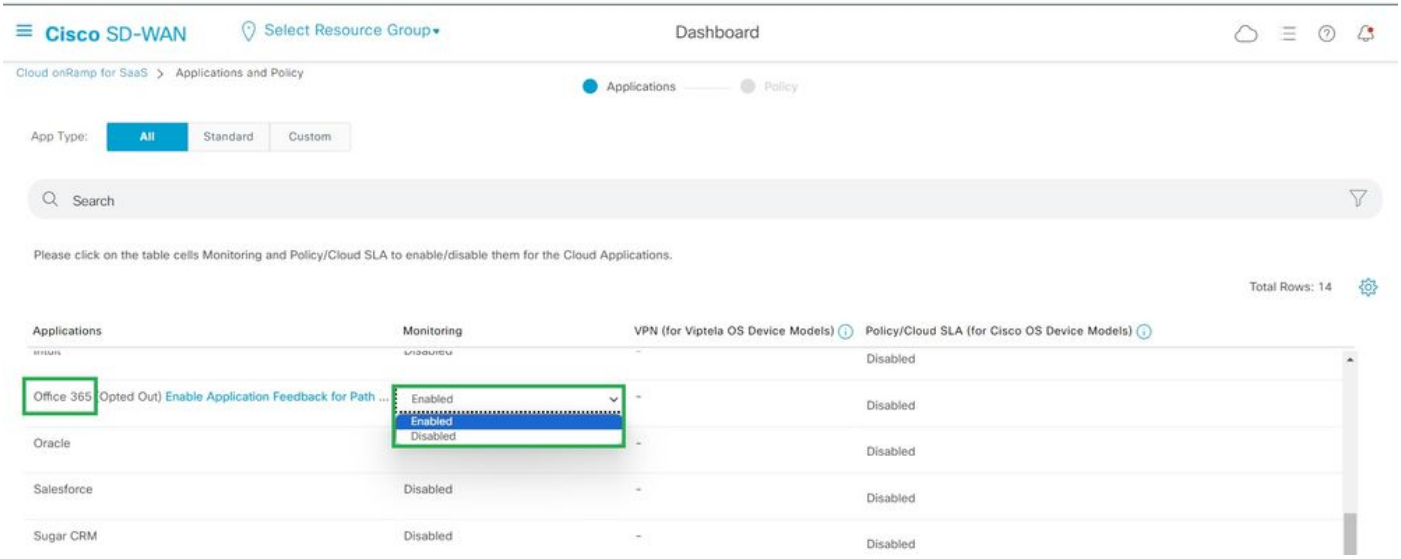
为*SaaS*选择*Cloud onRamp*

第二步：导航到Applications and Policy。



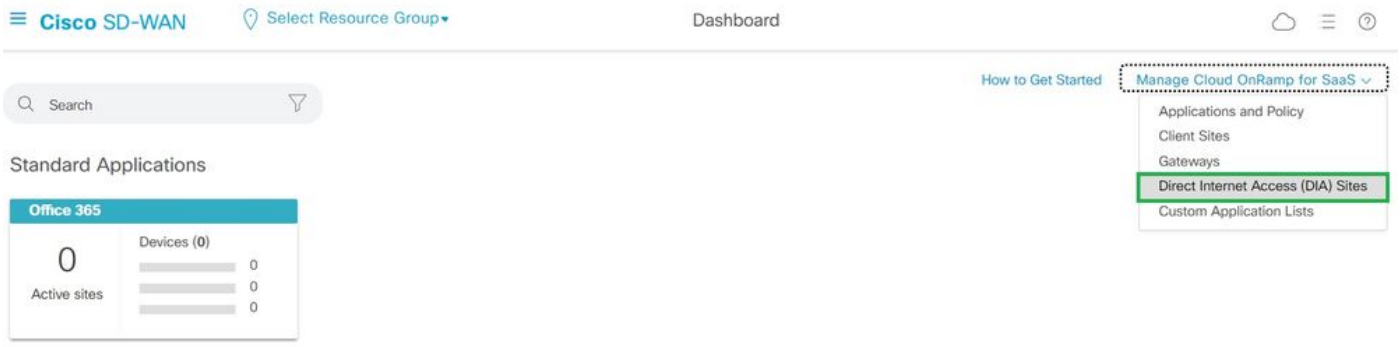
选择应用和策略

第三步：导航到Application > Enable和 Save。？？然后单击.Next



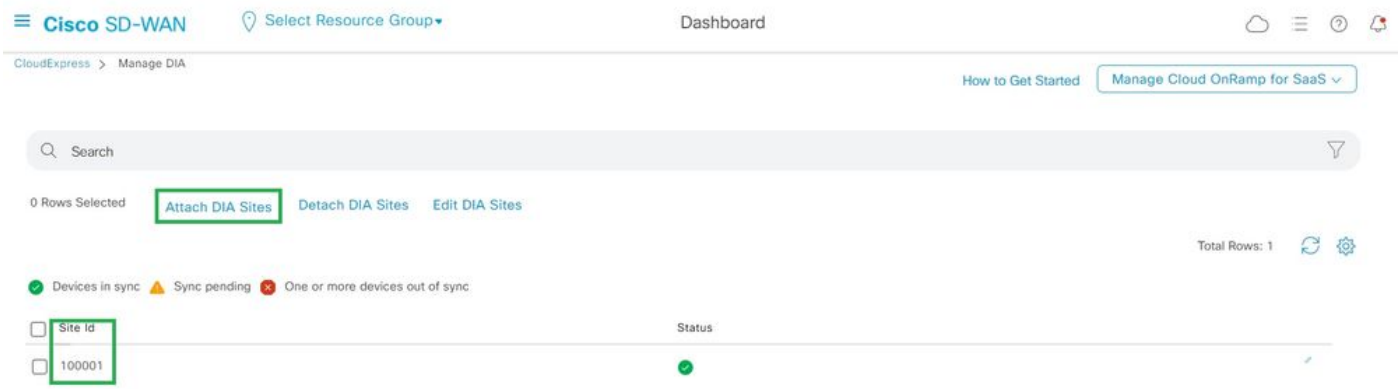
选择应用并启用监控

第四步：**导航到**Direct Internet Access (DIA) Sites。



选择直接互联网接入站点

第五步：**导航到**Attach DIA Sites **并选择站点。**



附加*DIA*站点

确认

本节介绍用于验证SaaS云OnRamp的结果。

- 此输出显示Cloudexpress local-exts：

```
cEdge_West-01#sh sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 2 type app-group subapp 0 GigabitEthernet2
application office365
latency 6
loss 0
```

- 此输出显示Cloudexpress应用程序：

```
cEdge_West-01#sh sdwan cloudexpress applications
cloudexpress applications vpn 1 app 2 type app-group subapp 0
application office365
exit-type local
interface GigabitEthernet2
latency 6
loss 0
```

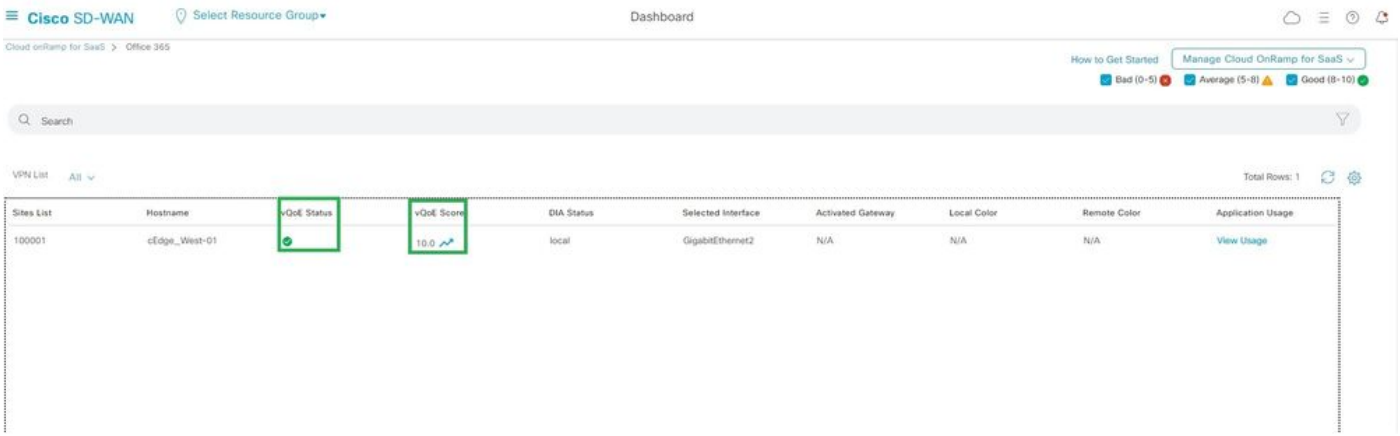
- 此输出显示感兴趣流量的递增计数器：

<#root>

```
cEdge_West-01#sh sdwan policy app-route-policy-filter
NAME                        NAME        COUNTER NAME                        PACKETS     BYTES
-------------------------------------------------------------------------------------------------
_VPN1_Cloud_OnRamp_SAAS     VPN1        default_action_count                640         66303
```

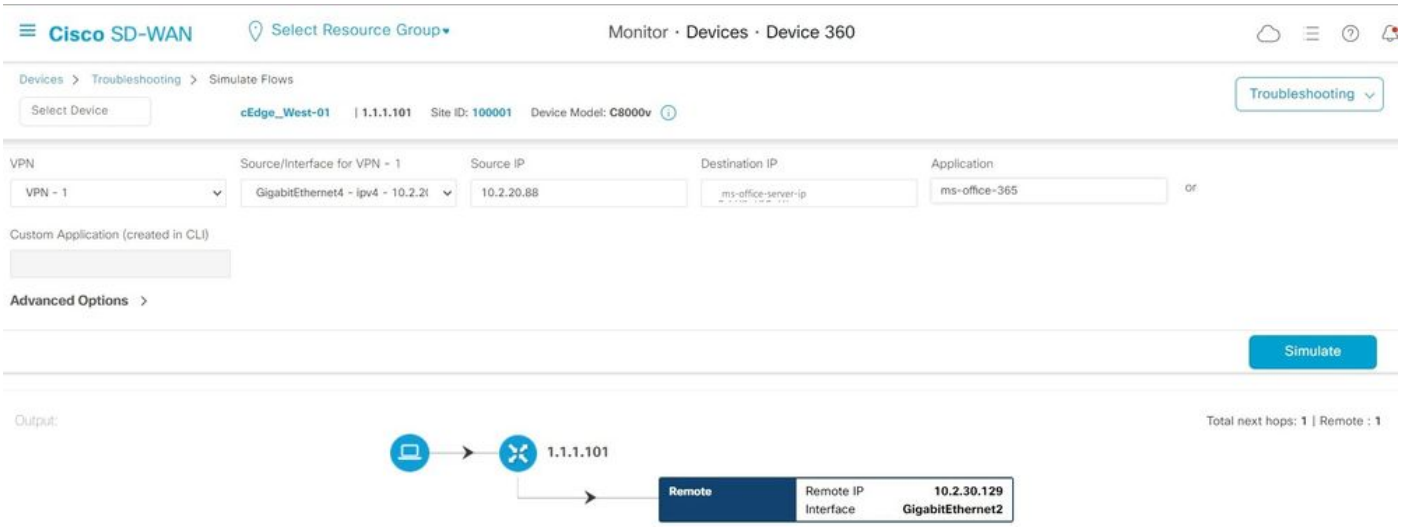
```
Cloud_OnRamp_-403085179             600      432292
```

- 此输出显示vQoE状态和得分：



*vQoE*状态和分数

- 此输出显示来自vManage GUI的服务路径：



服务路径

- 此输出显示来自设备CLI的service-path：

```
cEdge_West-01#sh sdwan policy service-path vpn 1 interface GigabitEthernet4 source-ip 10.2.20.70 dest-i
Next Hop: Remote
Remote IP: 10.2.30.129, Interface GigabitEthernet2 Index: 8
```

相关信息

- Cisco Catalyst SD-WAN Cloud OnRamp配置指南
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。