為SaaS配置SD-WAN雲OnRamp

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 網路圖表
- 組態
  - 在傳輸介面上啟用NAT
  - 建立集中式AAR策略
  - 在vManage中啟用應用和直接網際網路訪問

驗證

相關資訊

簡介

本文檔介紹使用分支機構本地退出的Cloud OnRamp for Software as a Service (SaaS)配置。

必要條件

需求

思科建議您瞭解思科軟體定義廣域網(SD-WAN)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科vManage版本20.9.4
- Cisco WAN Edge路由器版本17.9.3a

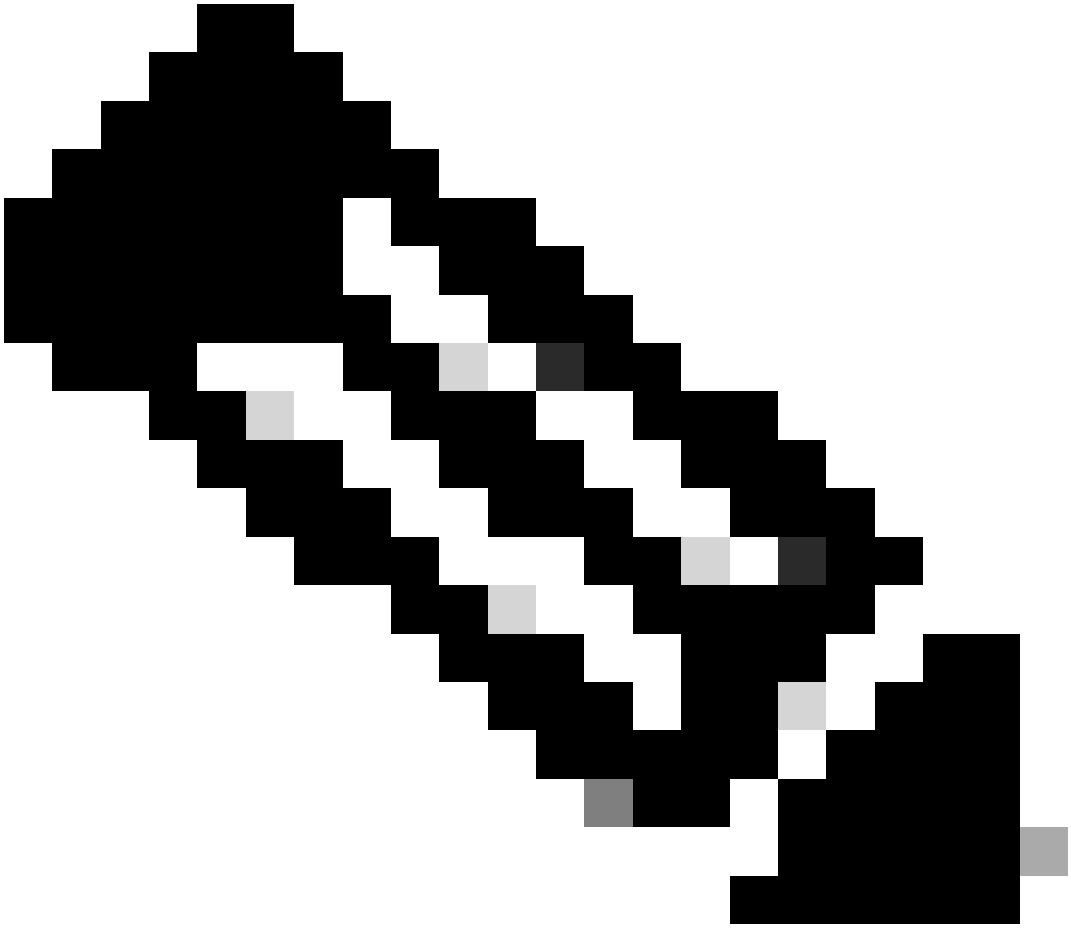
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

對於使用SD-WAN的組織，預設情況下，分支站點通常會透過SD-WAN重疊鏈路將SaaS應用流量路由到資料中心。從資料中心，SaaS流量到達SaaS伺服器。

例如，在擁有中央資料中心和分支機構站點的大型組織中，員工可以在分支機構站點使用Office 365。預設情況下，分支站點的Office 365流量透過SD-WAN重疊鏈路路由到中央資料中心，然後從DIA出口路由到Office 365雲伺服器。

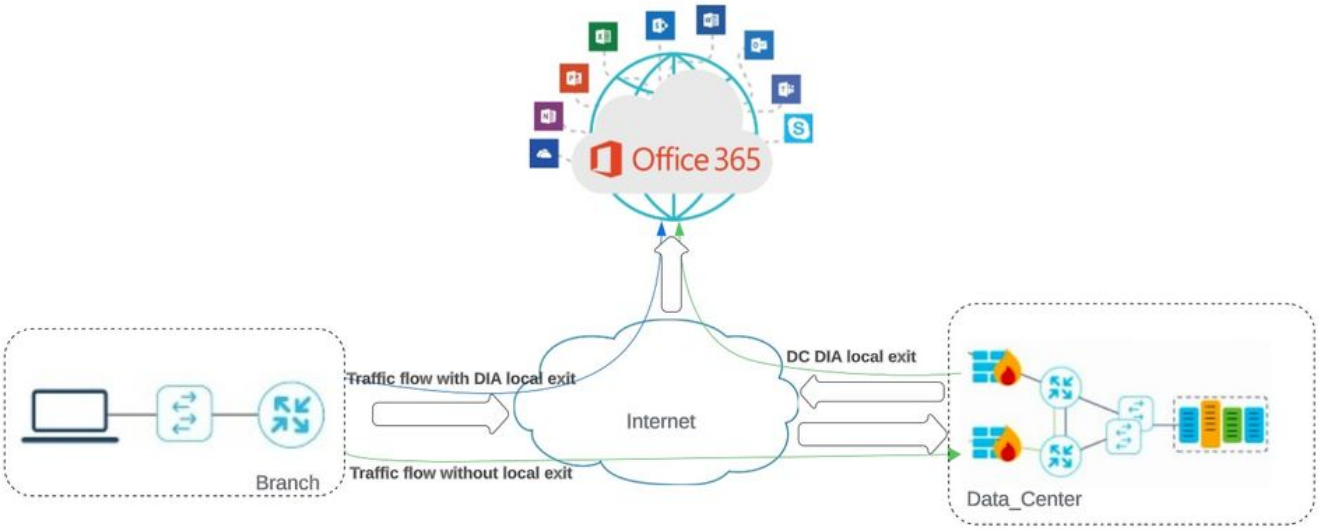
本文檔介紹此場景：如果分支機構站點具有直接網際網路接入(DIA)連線，您可以透過繞過資料中心將本地DIA路由SaaS流量來提高效能。



注意：不支援在站點使用環回作為傳輸定位器(TLOC)介面時為SaaS配置雲OnRamp。

設定

網路圖表

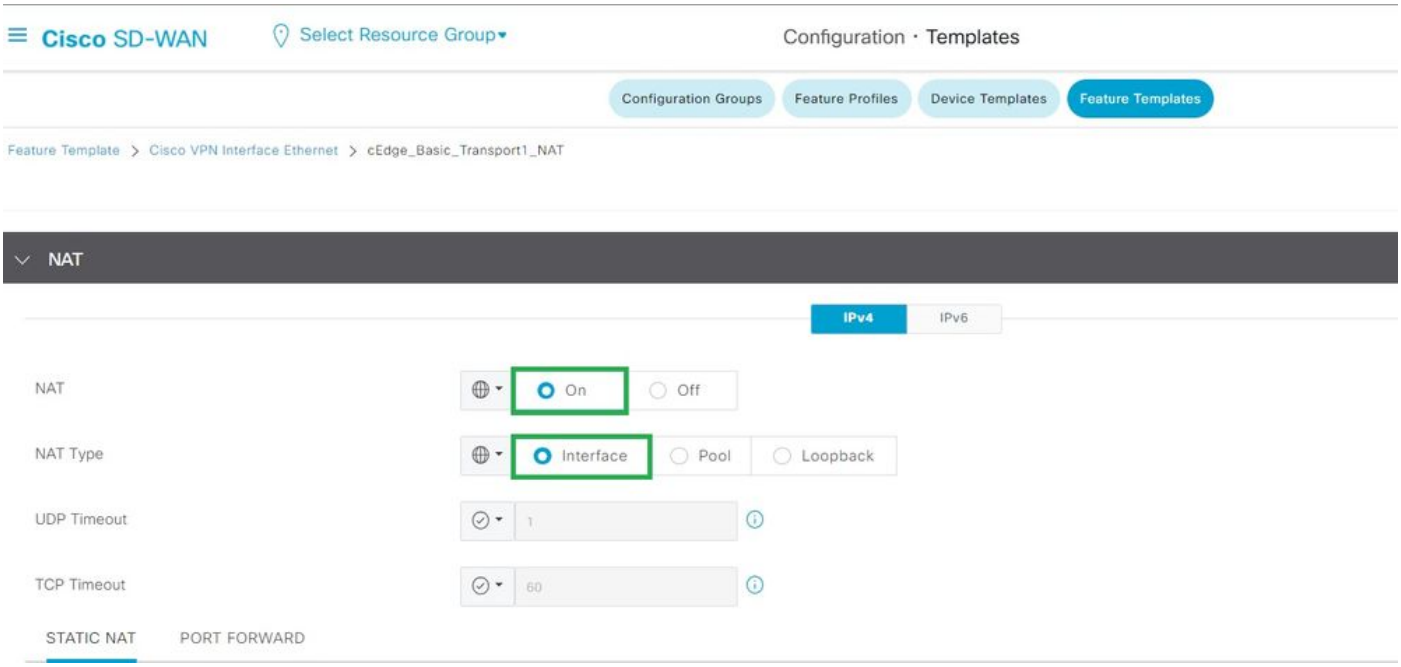


網路拓撲

組態

在傳輸介面上啟用NAT

導航到Feature Template 。 **選擇模Transport VPN interface 板並啟用NAT。**



啟用介面*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

建立集中式AAR策略

要建立集中策略，必須遵循以下步驟：

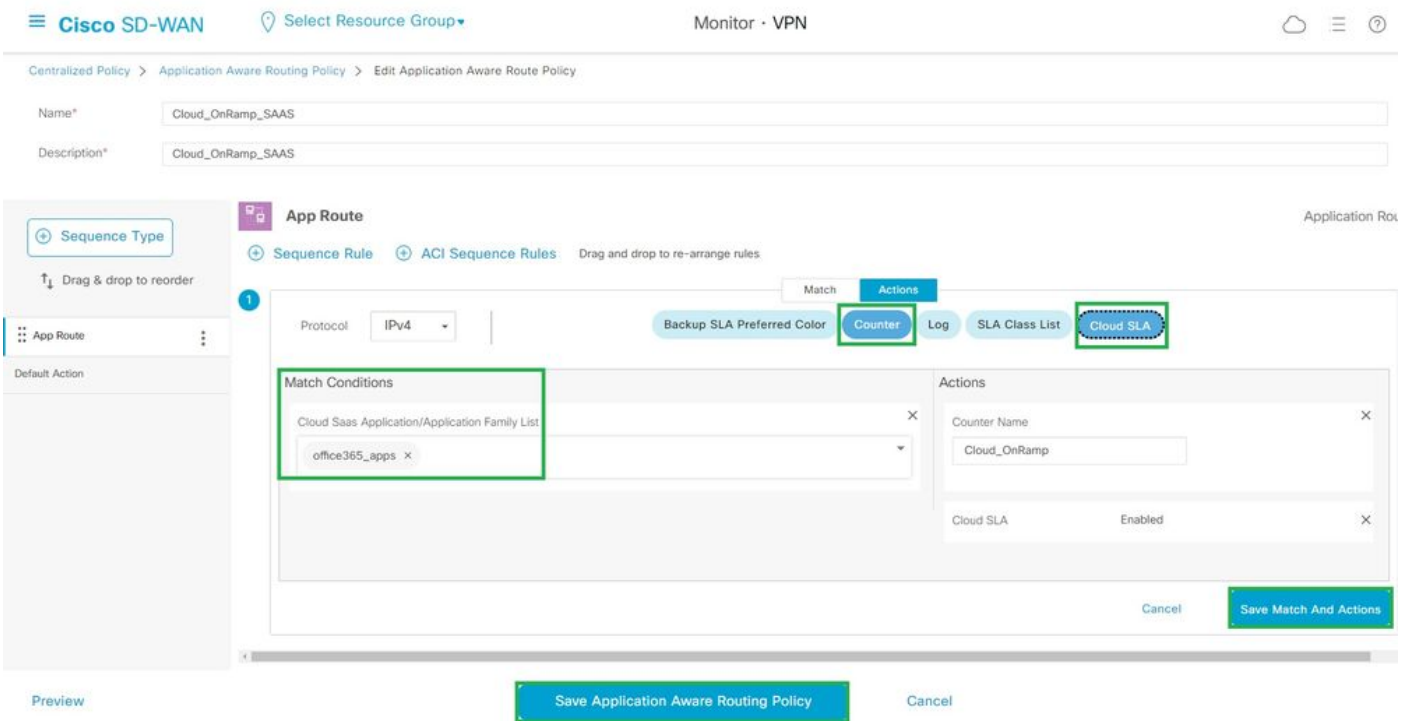
步驟 1.建立網站清單：

VPN介面NAT模板

步驟 2.建立VPN清單：

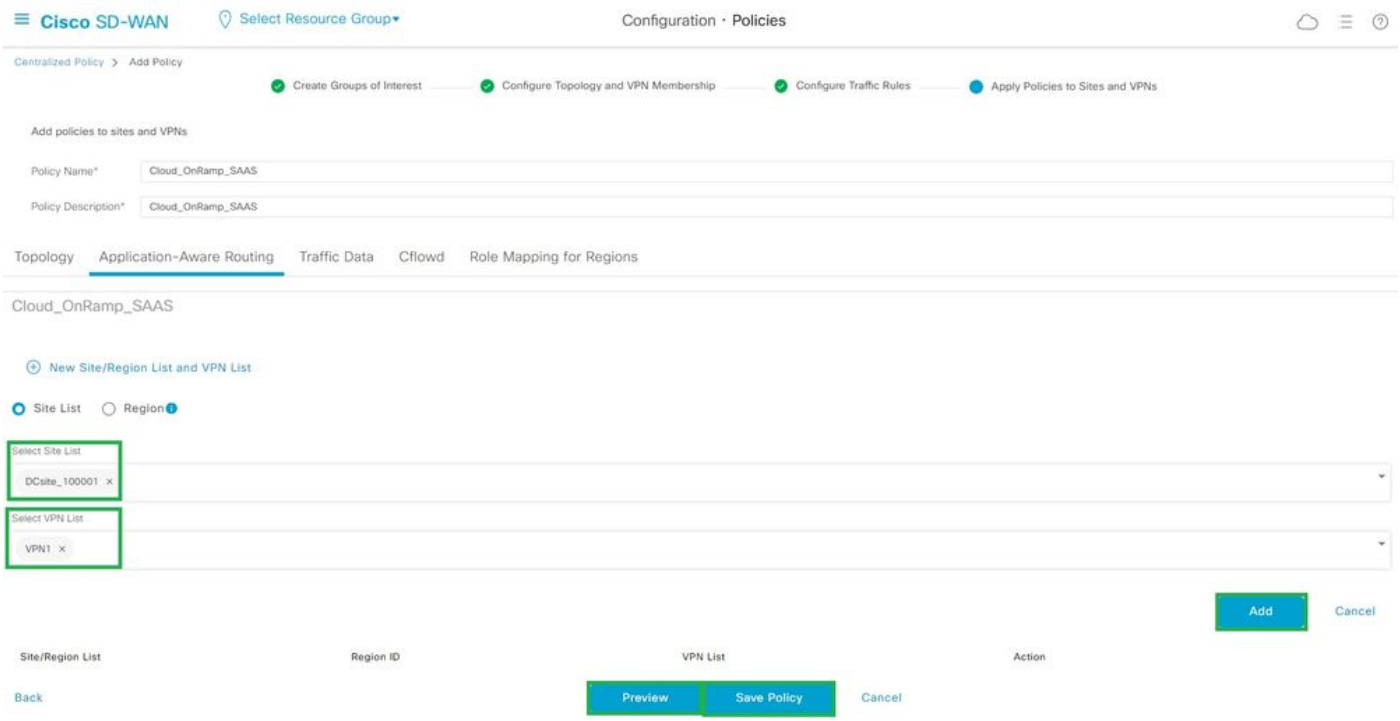
集中策略自定義站點清單

步驟 3.配置Traffic Rules 並建立Application Aware Routing Policy。



應用感知路由策略

步驟 4.將策略增加到目標Sites中，VPN：



將策略增加到站點和*VPN*

CLI等效策略：

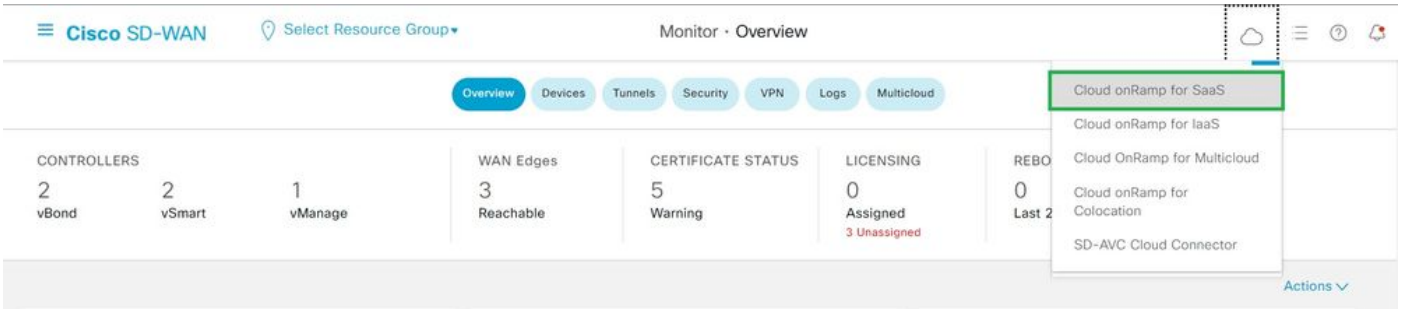
viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1

```
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
!
!
```

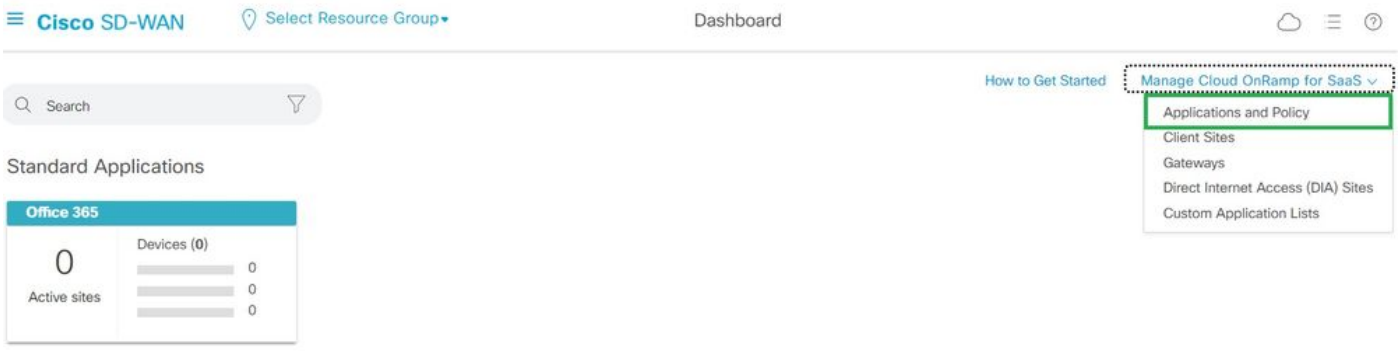
在vManage中啟用應用和直接網際網路訪問

步驟 1.導航到Cloud OnRamp for SaaS。



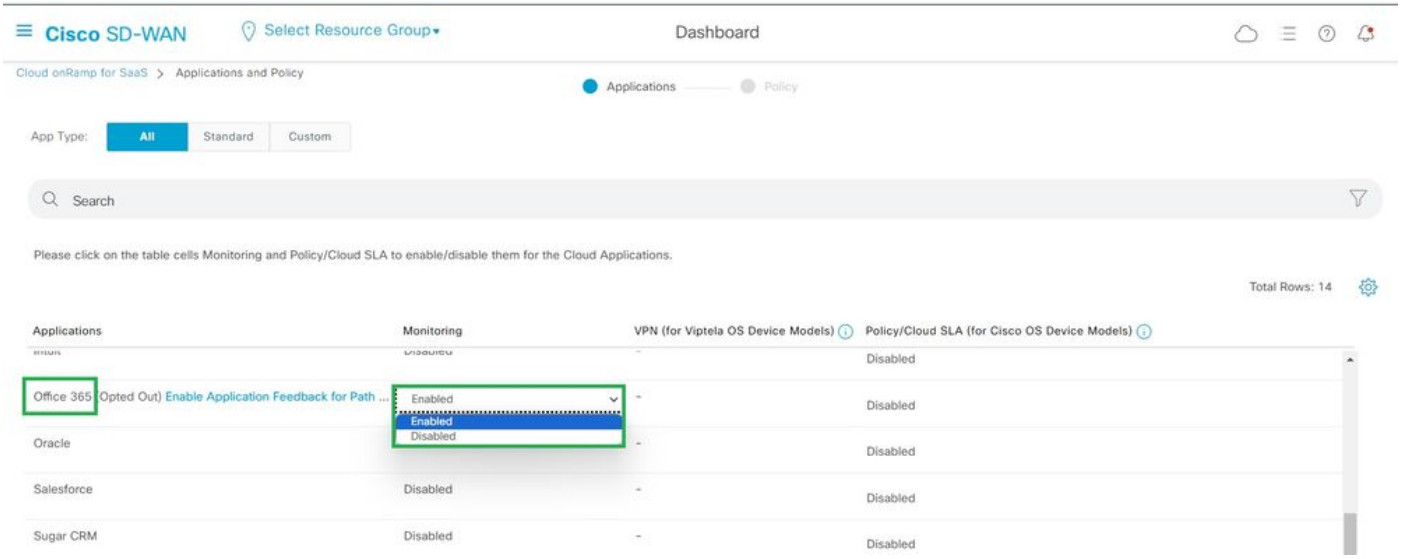
選擇*SaaS*的雲*onRamp*

步驟 2.導航到Applications and Policy。



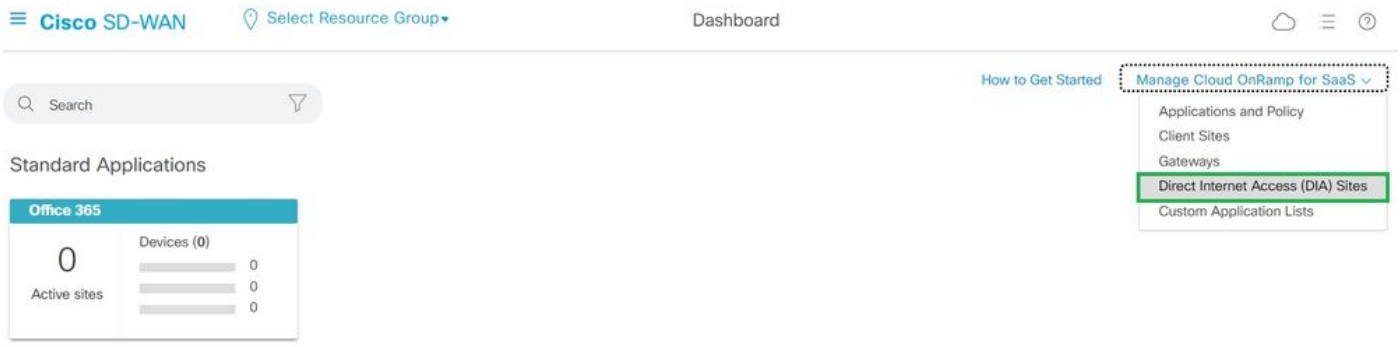
選擇應用程式和策略

步驟 3.導航到Application > Enable和 Save。然後按一下Next。



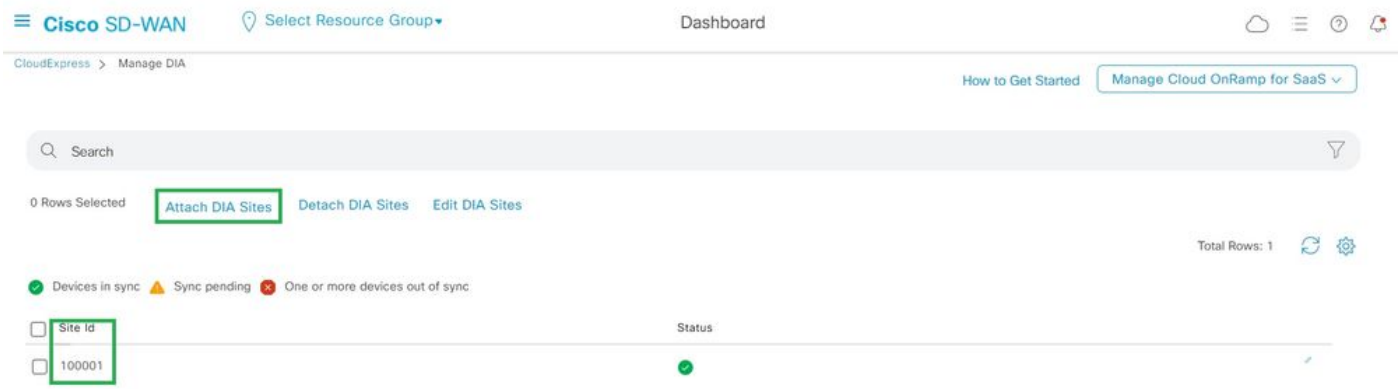
選取應用程式並啟用監督

步驟 4.導航到 Direct Internet Access (DIA) Sites。



選擇直接網際網路接入站點

步驟 5.切換作業選項至 Attach DIA Sites **並選擇「地點」。**



附加*DIA*站點

驗證

本節介紹驗證SaaS雲OnRamp的結果。

- 此輸出顯示Cloudexpress local-exit：

```
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
```

- 此輸出顯示Cloudexpress應用程式：

```
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
```

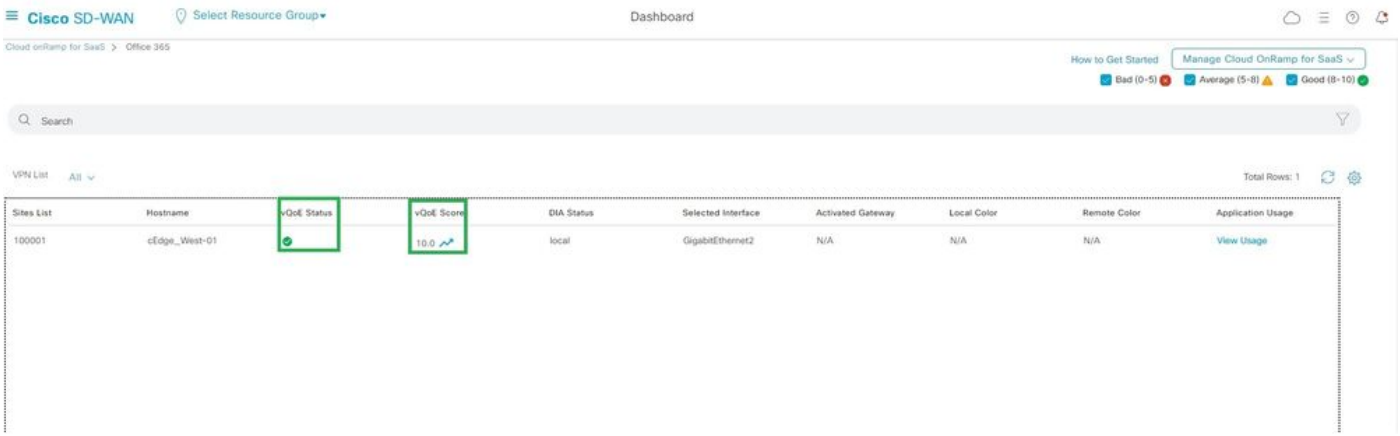
- 此輸出顯示相關流量的遞增計數器：

<#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
```

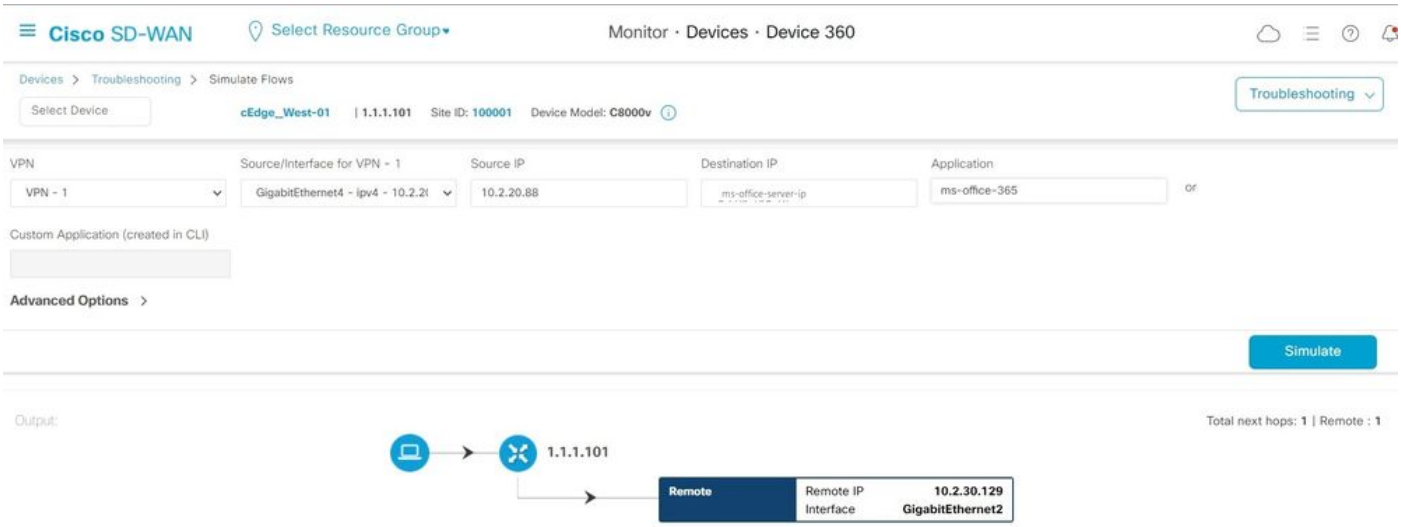
```
Cloud_OnRamp_-403085179             600      432292
```

- 此輸出顯示vQoE狀態和分數：



*vQoE*狀態和分數

- 此輸出顯示來自vManage GUI的服務路徑：



服務路徑

- 此輸出顯示來自裝置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
```

相關資訊

- Cisco Catalyst SD-WAN雲OnRamp配置指南
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。