快速入門手冊- Catalyst SD-WAN簡化配置和策略

目錄

簡介

本文檔介紹Catalyst SD-WAN的簡化配置和策略。

背景資訊

摘要

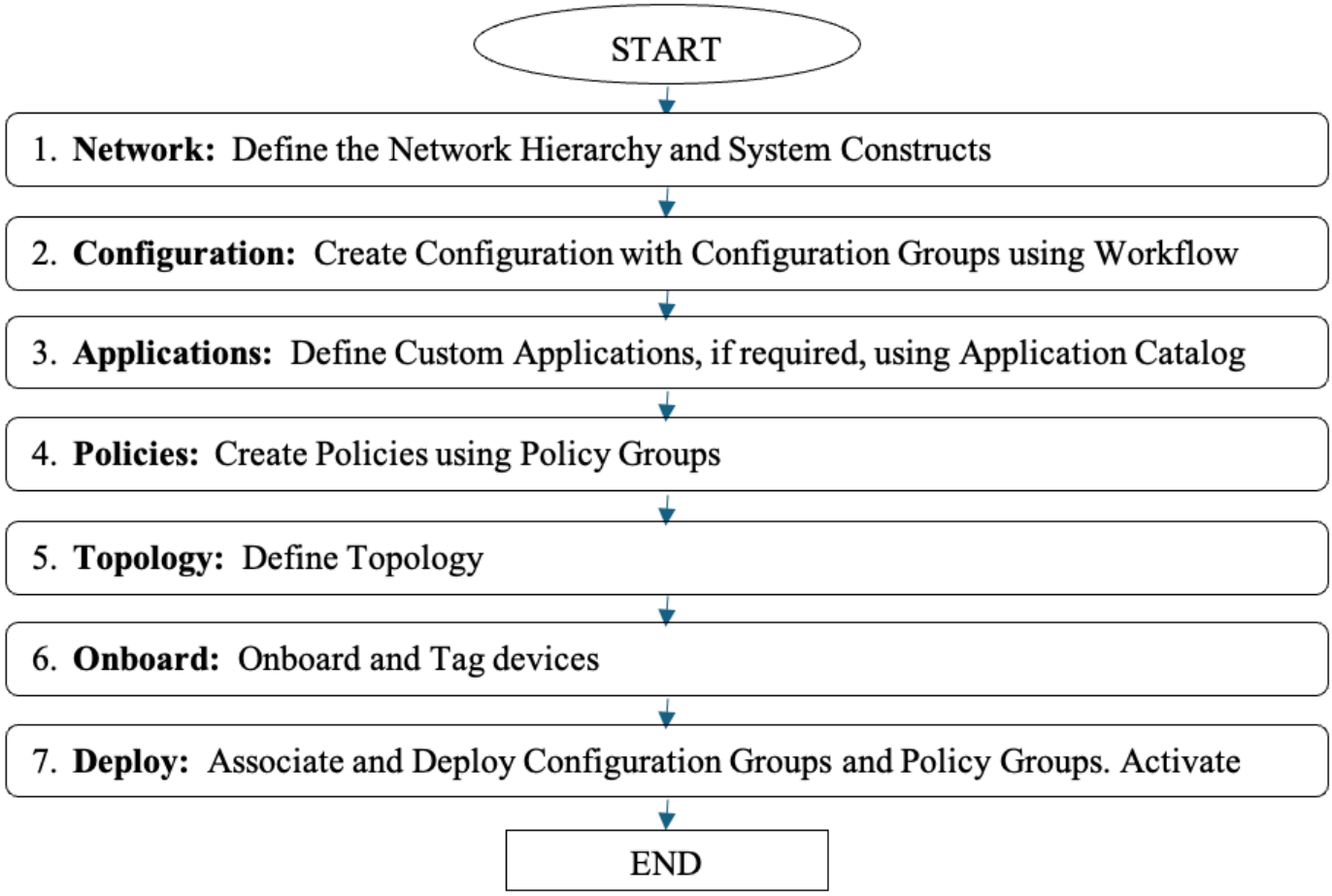
對於Cisco Catalyst SD-WAN軟體版本20.12/17.12，建議使用者開始從基於裝置和功能模板的傳統配置遷移到基於配置組和策略組的新配置方法。本文檔介紹了新配置方法的重要詳細資訊。

本文檔的主要目標是作為開始使用配置、策略和自行啟用的新結構的指南，以及20.12 Golden版本。 本檔案不涵蓋個別功能的說明。

新部署

要成功利用新的配置方法，您需要執行以下步驟：

1. 網路：定義網路層次結構和系統結構
2. 組態：使用工作流程建立具有組態群組的組態
3. 應用程式：視需要使用應用程式目錄定義自訂應用程式
4. 策略：使用策略組建立策略
5. 拓撲：定義拓撲
6. 板載：板載和標籤裝置
7. 部署：關聯和部署配置組和策略組。啟動拓撲。



新部署的流程圖

現有部署

1. 執行現有部署部分中提到的步驟
2. 使用Conversion tool將現有配置/策略轉換為新配置/策略

增強使用者體驗和簡化運營

Cisco Catalyst SD-WAN提供增強的使用者體驗並簡化操作。

- 通用UI：在Catalyst SD-WAN Manager和其他思科產品中引入了一個新的UX架構，旨在保證使用者體驗的一致性，並提供跨產品的通用外觀。
- 配置：透過基於直覺的意圖工作流程和使用思科推薦的智慧預設設定，簡化配置和策略建立與部署。
- 監控：藉助新小部件和可定製且增強的控制台，深入瞭解網路和應用效能及運行狀況。
- 故障排除：動態站點和網路拓撲檢視、基於情景的故障排除工具訪問、按計畫報告網路和應用效能。

優點

易於使用	直覺式與引導式工作流程

配置蔓延	減少無計畫擴張（與模型無關、可重複使用、結構化）
配置建立	使用智慧型預設值更快速、更輕鬆
配置修改	立即修改，稍後選擇性地部署
可視性	新儀表板、應用/站點效能監控
故障排除指南	站點拓撲、故障排除工具指南

定義網路層次結構和系統結構

網路層次結構

提供網路的「層次結構」概念，即站點、區域和區域。您可以根據網路建立此檔案。

範例：

Global (15 of 15 nodes)

AMER

BR1_SanJose

BR2_NewYork

BR6_Dallas

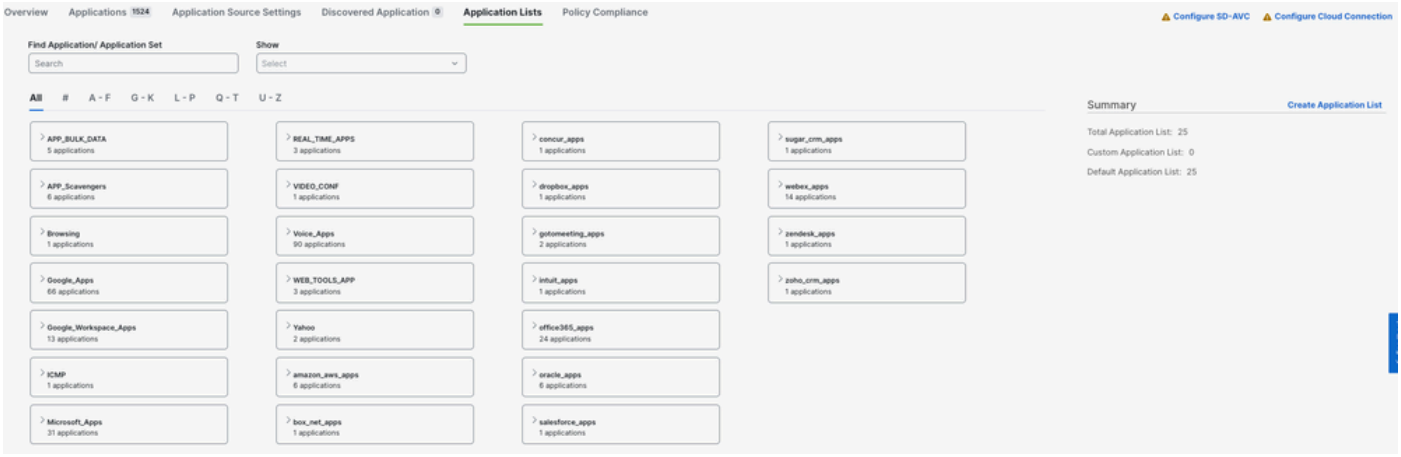
APJC

BR3_Mumbai

BR4_Singapore

包含連線到思科應用儲存庫的功能，應用簽名可以快速更新；這對於雲提供商更改託管位置或流量模式具有重大意義。

應用程式目錄允許根據伺服器名稱、ip地址、埠或協定的匹配情況建立自定義應用程式。 然後，該應用程式被定義為特定的應用程式系列、應用程式組、流量類別和業務相關性。



應用程式目錄

可將應用拖放到適當的業務相關性和/或流量分類中。 儲存變更後，即會在資料庫中更新定義。

注意：應用分類是全局性的，應用目錄中的更改會影響所有裝置分類。

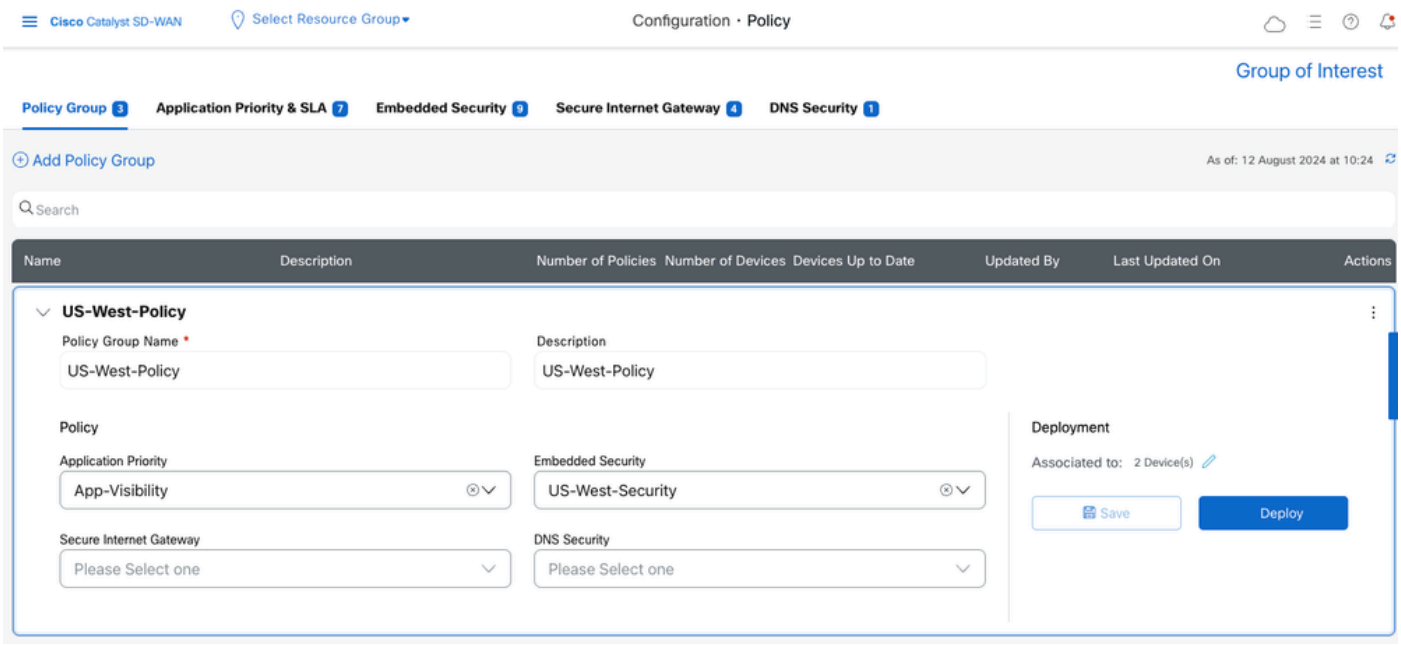
原則群組

與配置組類似，策略組是部署到與策略組關聯的裝置的一組策略。

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Policy-Groups/policy-groups/m-policy-groups.html

策略組基於意圖處理策略的建立和部署。簡化的UI和工作流程使建立策略、將策略分組和部署到裝置成為一項輕鬆的任務。

先決條件： 配置組關聯和部署到裝置是策略組部署到該裝置的先決條件。



原則群組

應用優先順序和SLA

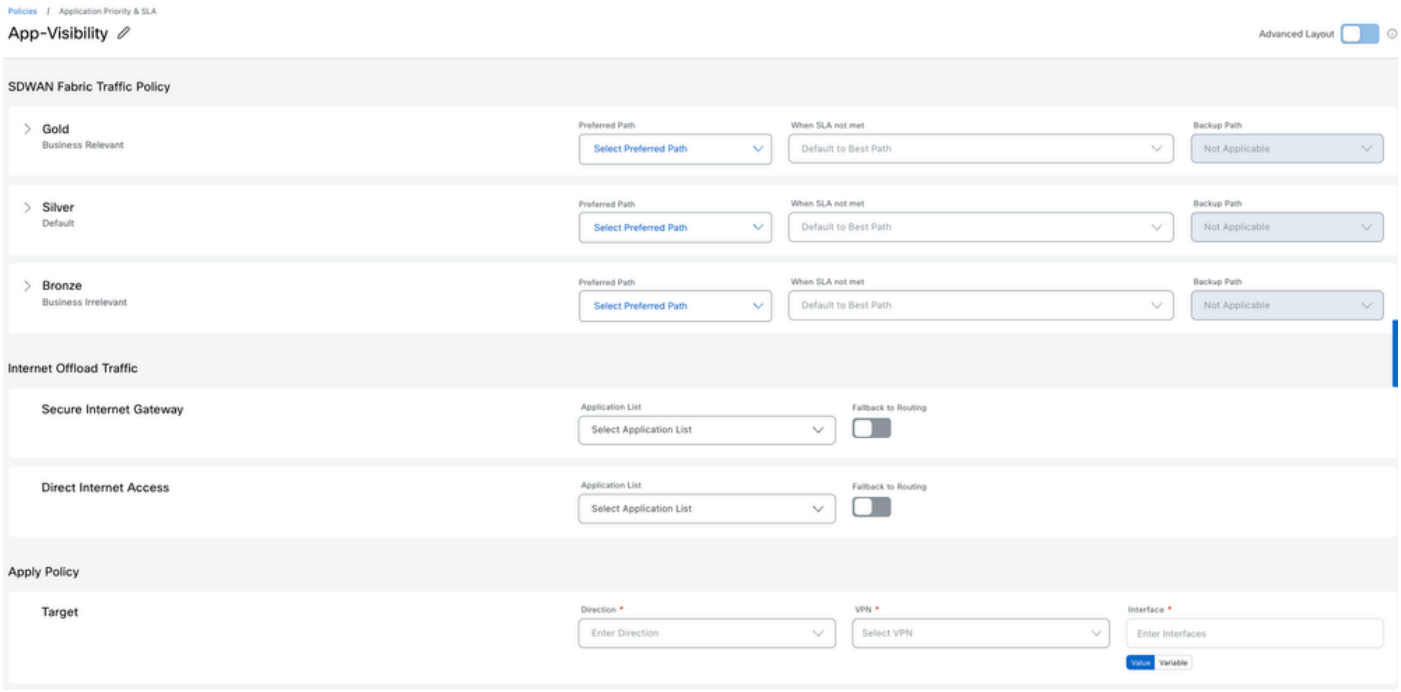
使用此策略意圖，可以指定：

- 應用感知路由和SLA策略
- QoS策略
- 流量資料策略
- DIA策略
- SIG策略

提供了兩種模式。

簡單模式

這是預設模式。



簡單模式

這樣可以快速輕鬆地定義網路的應用優先順序和SLA。

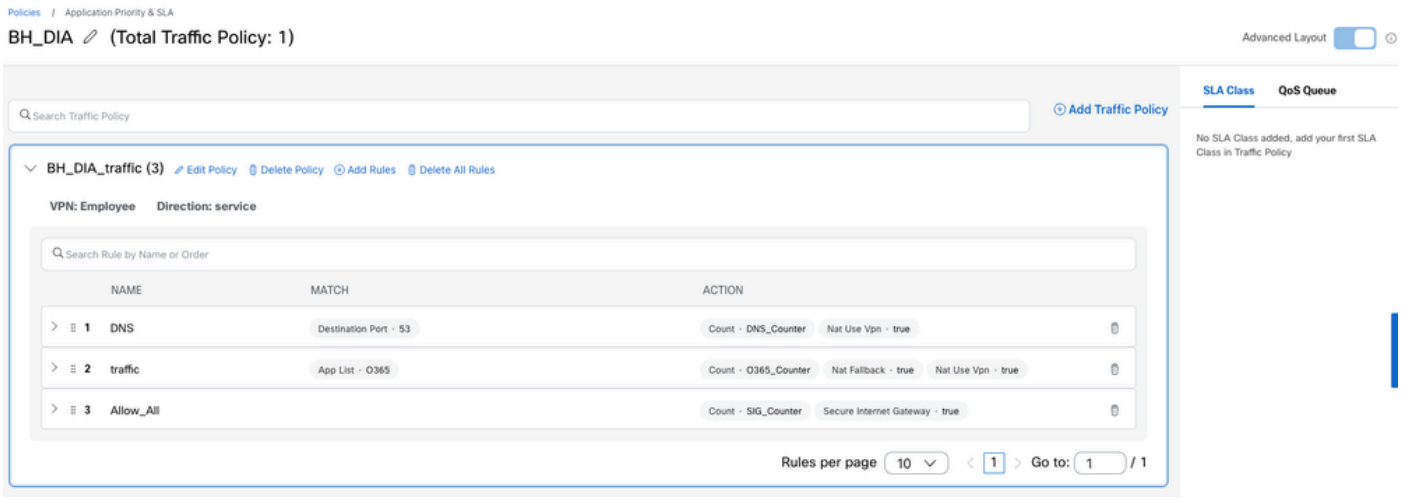
附註：

1. 預設策略操作為DROP

2. 符合條件只能是應用模組。如果您需要「前置字元」，請使用「進階」模式

進階模式

這是一種完整且靈活的模式。



進階模式

附註：

1. 預設策略操作為DROP

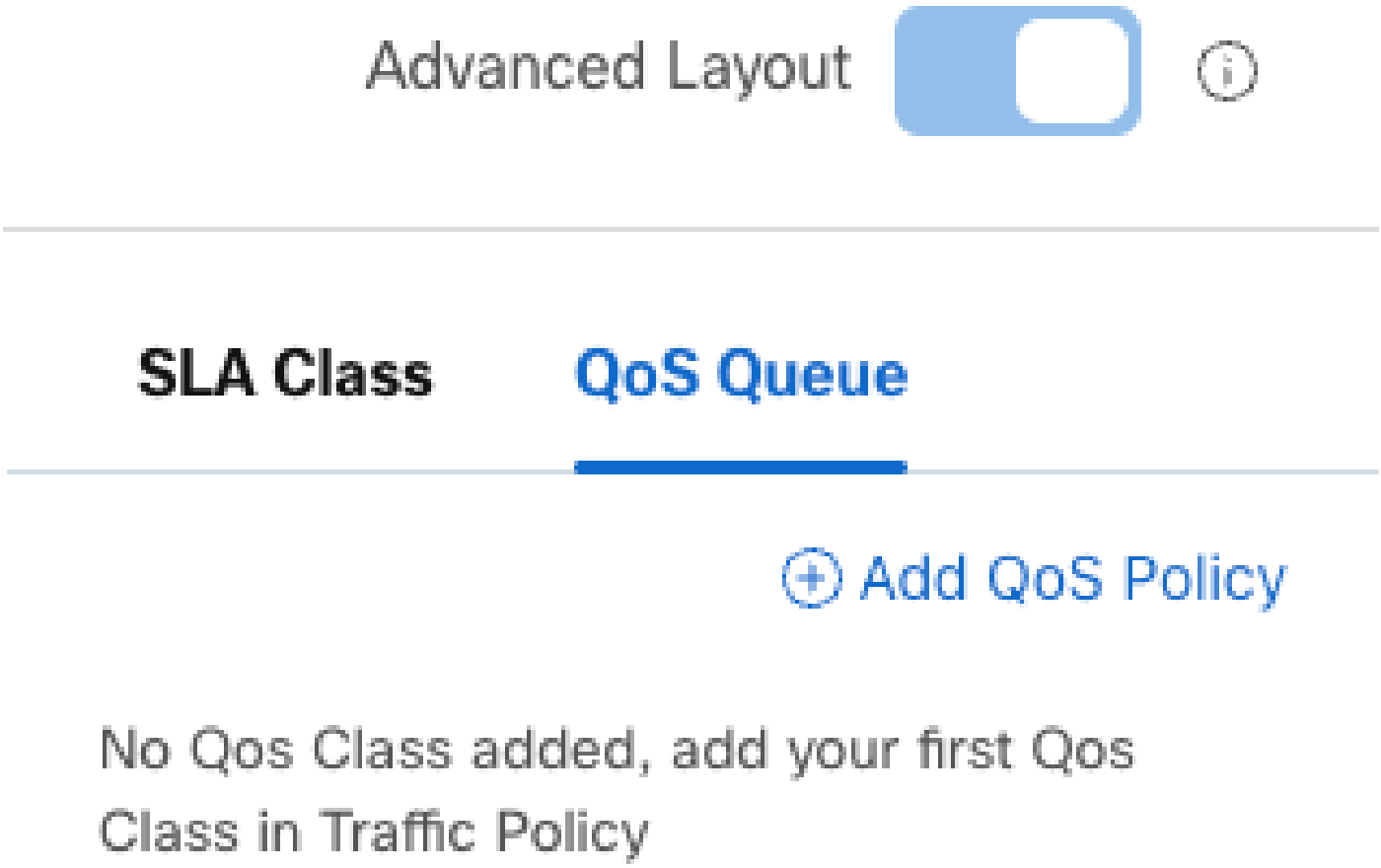
2. 「應用清單」和「流量類」實際上是「應用」清單。

其中任何一個都可用於匹配應用程式清單。可以在應用目錄中完成應用到流量類的對映。

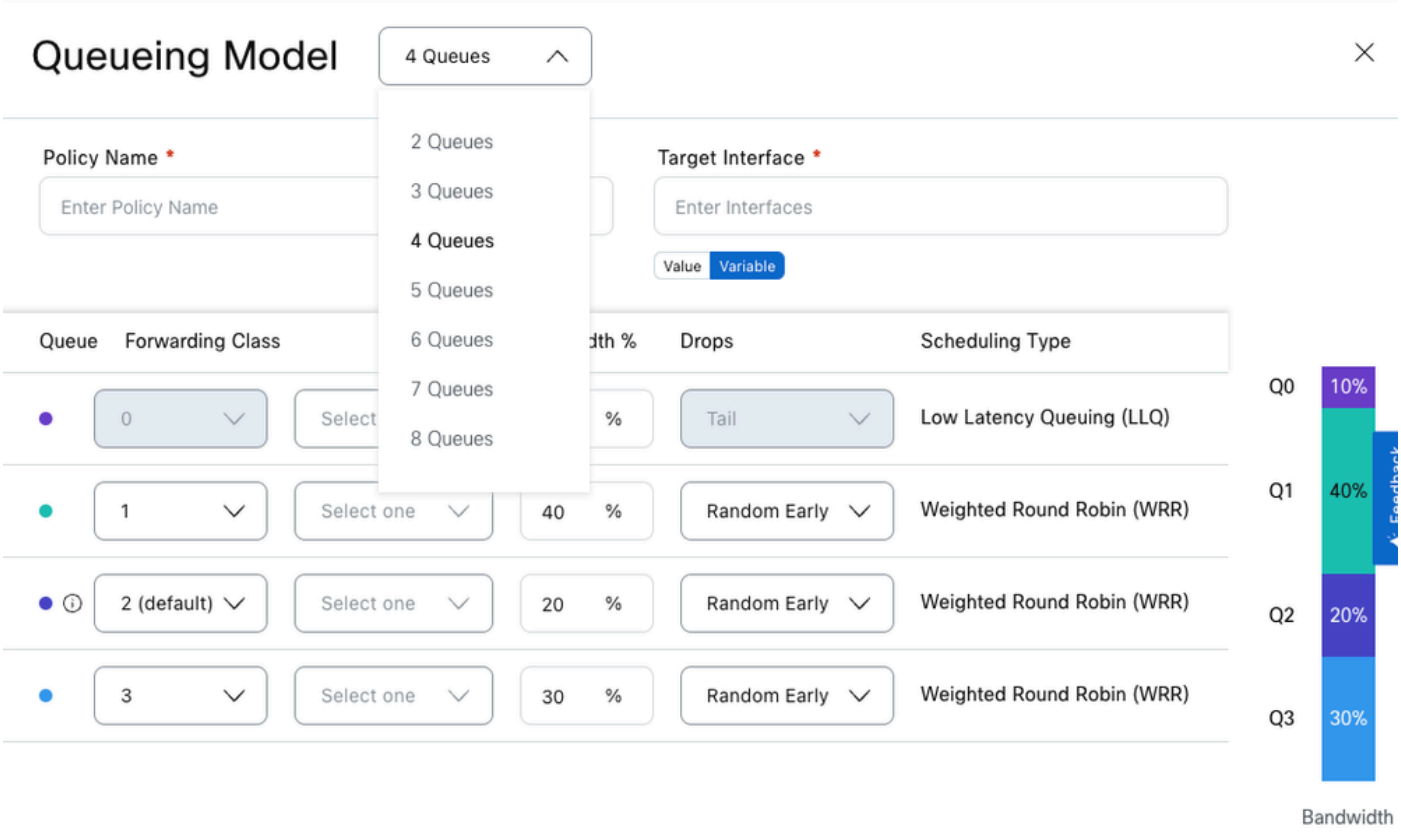
「簡單」模式使用其中任何一項或兩項來產生規則，而「進階」模式僅提供「應用程式清單」。

服務品質

在QoS Queue選項中，可以增加QoS策略：



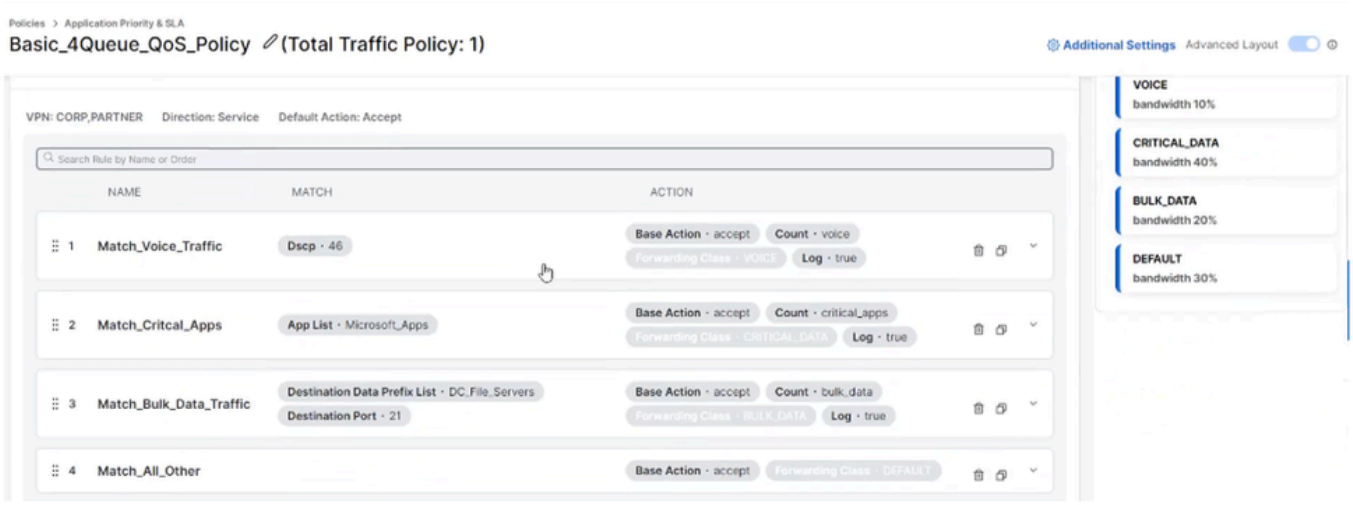
增加QoS策略



排隊模型

接下來，您可以定義流量資料策略(增加流量策略)。

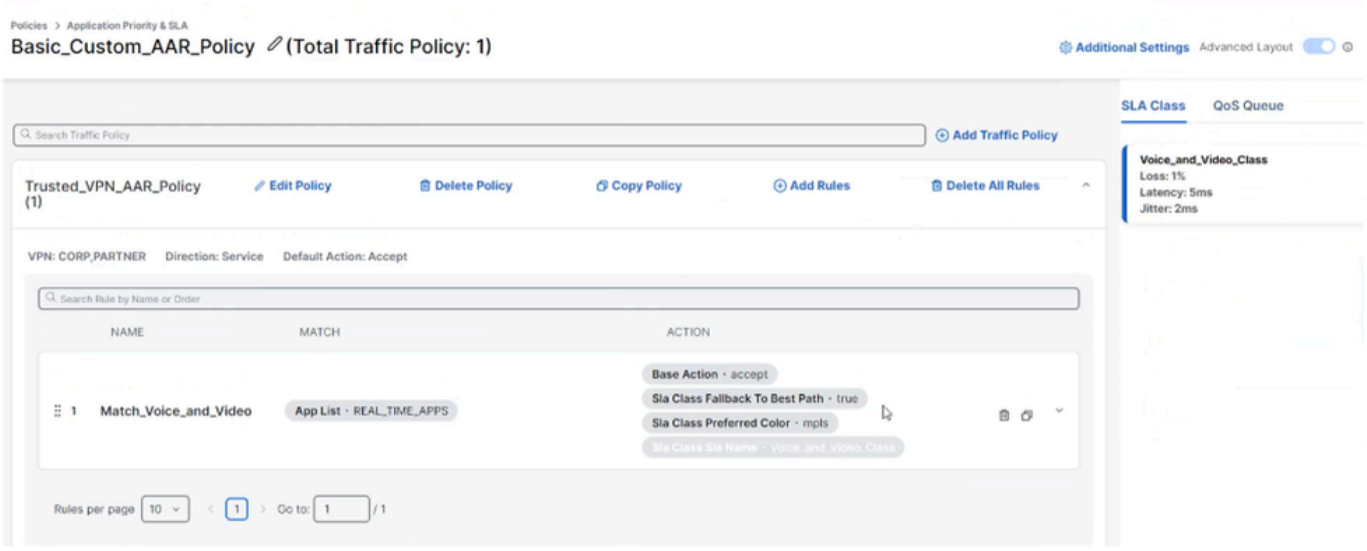
增加規則以匹配所需流量並重定向到相應的轉發類。



QoS策略2

應用感知路由

您可以定義SLA類並在流量策略中使用它們以實現AAR策略的意圖。



AAR策略

應用/流可視性

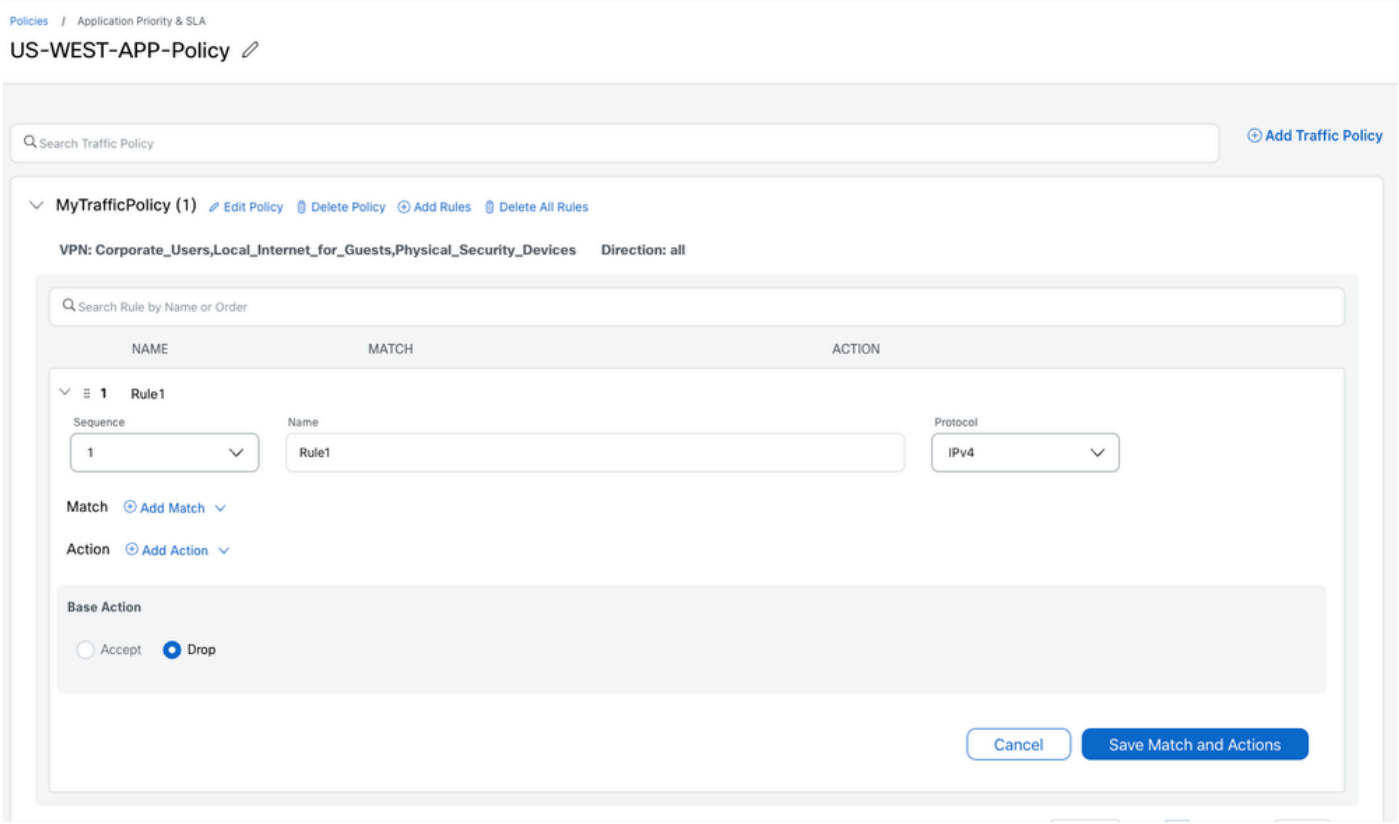
要啟用應用可視性和流可視性，請在配置組中使用CLI配置檔案/包。

(在20.13及更高版本中，該選項位於「策略組」中的高級設定下)

但是，在20.12中，如果配置了AAR策略，則會啟用應用/流可視性。並且不需要使用CLI配置檔案/包裹進行配置。

流量策略

流量策略還可用於建立DIA策略、SIG重定向等。視需要新增規則。



流量策略

> 附註：
>
> 如果在簡單模式下建立應用優先順序和SLA策略，然後切換到「高級」模式，則無法使用某些「匹配」選項進行選擇。示例：「目標資料字首」呈灰色。
> 要使這些選項可用，請根據需要將Protocol從BOTH更改為IPv4或IPv6。

內嵌安全性

定義機載NGFW、IPS、惡意軟體和內容過濾的安全策略

安全網際網路閘道/安全服務邊緣

定義為基於雲的內容和安全實體（如思科安全訪問）建立隧道所需的設定。

> 附註：
>
> 在傳統配置方法中，此功能可用作功能模板。

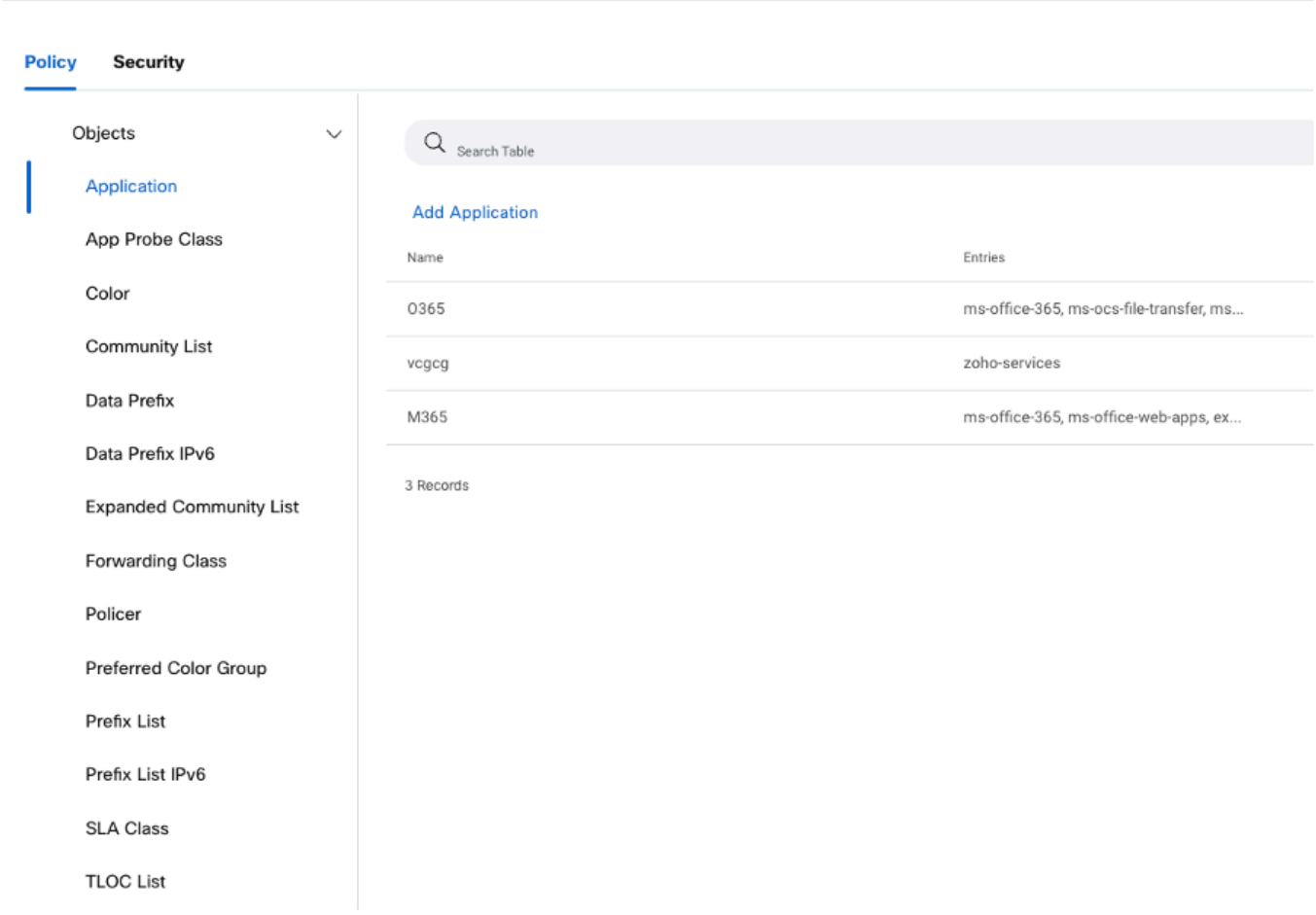
DNS安全性

定義允許使用基於雲的DNS安全服務進行內容過濾的設定。

興趣組

定義要在策略中使用的對象清單。示例：應用清單、VPN清單、站點清單、字首清單等。

此外，對於安全策略，請定義高級檢查配置檔案、SSL解密策略等配置檔案。



策略組-興趣組

關聯和部署

與配置組類似，將裝置關聯到策略組並進行部署。

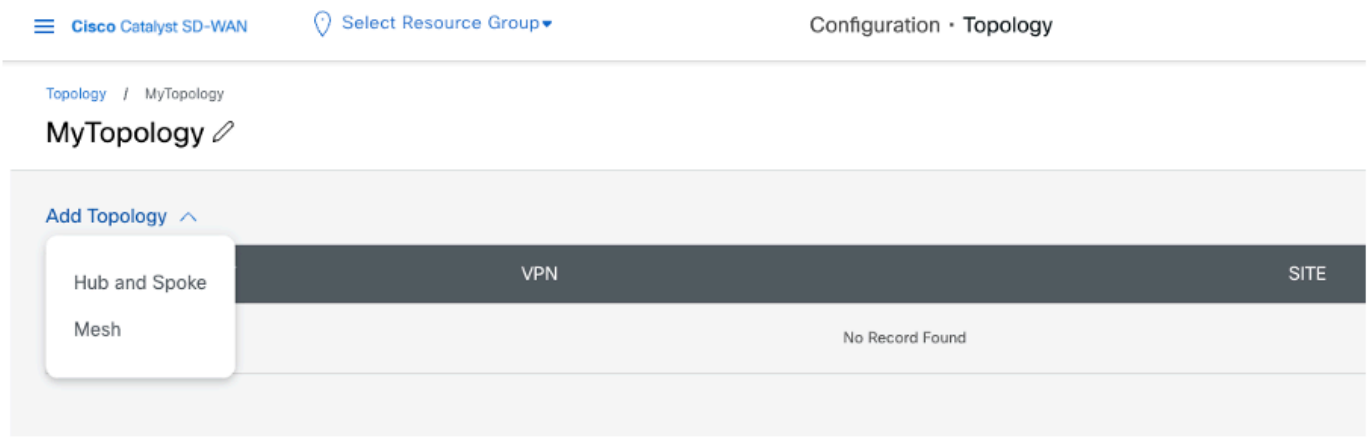
在地化的策略

ACL、路由策略、裝置訪問策略等在地化策略在配置組中定義。

拓撲

定義網路拓撲。

從全網狀網或星型網開始，並在需要時進行自定義。



拓撲功能表

拓撲和VPN

建立拓撲和指定VPN時，請記住這些設計更改。

新設計允許VPN名稱到VPN ID的動態對映，而不是1:1對映。

對映到多個VPN ID的VPN名稱

圖例：
假設在兩個不同的配置組中有一個名稱為Corporate的VPN。

一個具有VPN ID 10，另一個具有VPN ID 20。

拓撲工作流VPN清單只顯示了企業 VPN的一個例項。

選擇Corporate VPN後，SD-WAN Manager將根據拓撲確定VPN ID。
假設在2個站點中有2個裝置：
1. 站點100中的Device1帶有Corporate作為VPN 10
2. 站點200中的Device2與Corporate一起作為VPN 20

如果站點100和站點200都是拓撲的一部分，則SD-WAN Manager會建立一個VPN清單，其中將同時具有兩個VPN ID （ 10和20 ）。
如果只有站點100是拓撲的一部分，則SD-WAN Manager會建立只具有VPN ID 10的VPN清單。
如果只有站點200是拓撲的一部分，則SD-WAN Manager會建立一個VPN清單，該清單將僅包含VPN ID 20。

對映到同一VPN ID的多個VPN名稱

您可以使用相同的VPN名稱配置對映到不同站點中不同VPN ID的多個拓撲策略。

SD-WAN Manager根據與哪些站點關聯的拓撲確定實際對映。

圖例：

兩個使用者可建立兩個不同的配置組。

一個將VPN ID 100指定為Finance VPN，另一個將其指定為Engineering VPN。

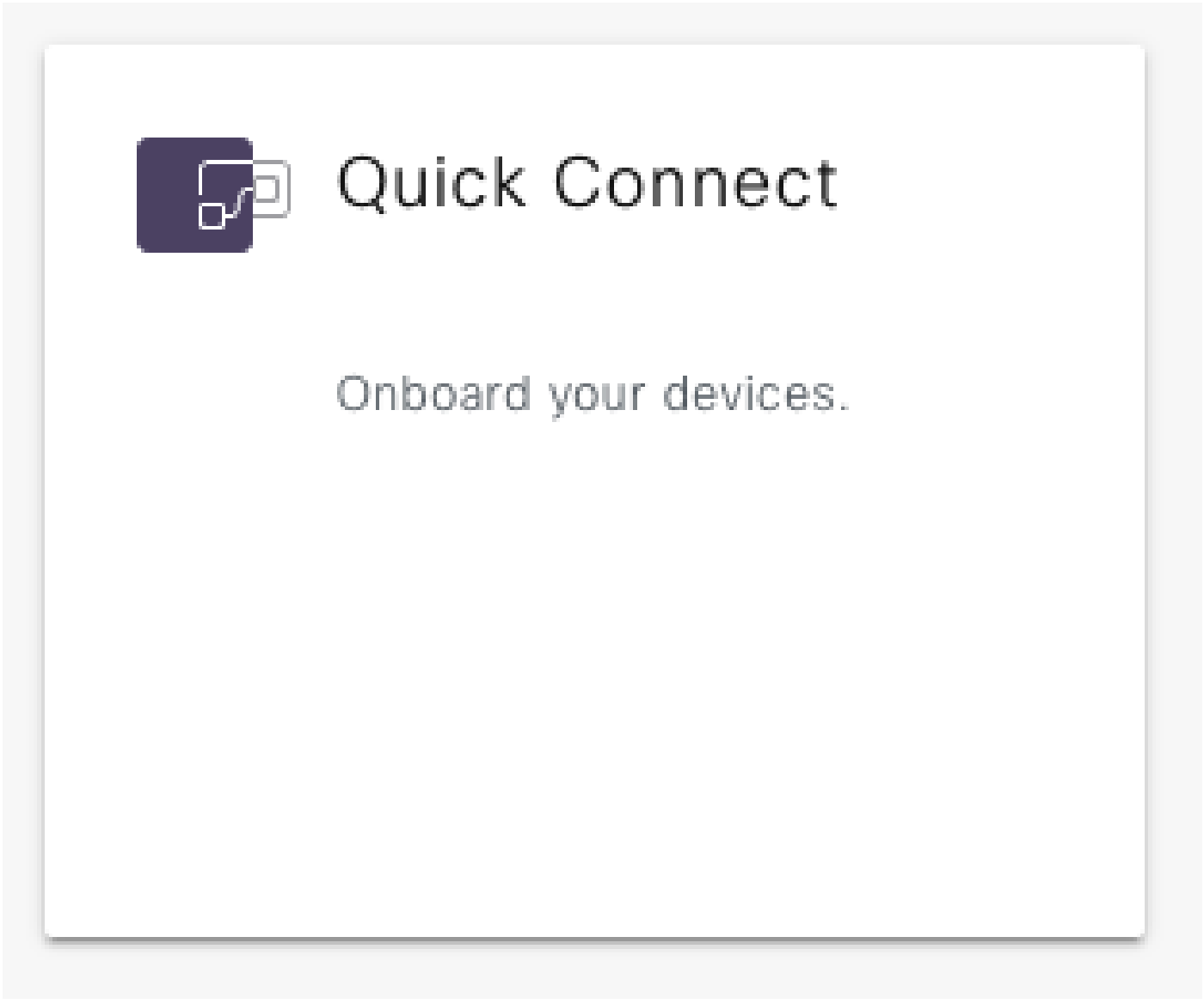
然後可以使用各自的VPN名稱建立拓撲。

自註冊

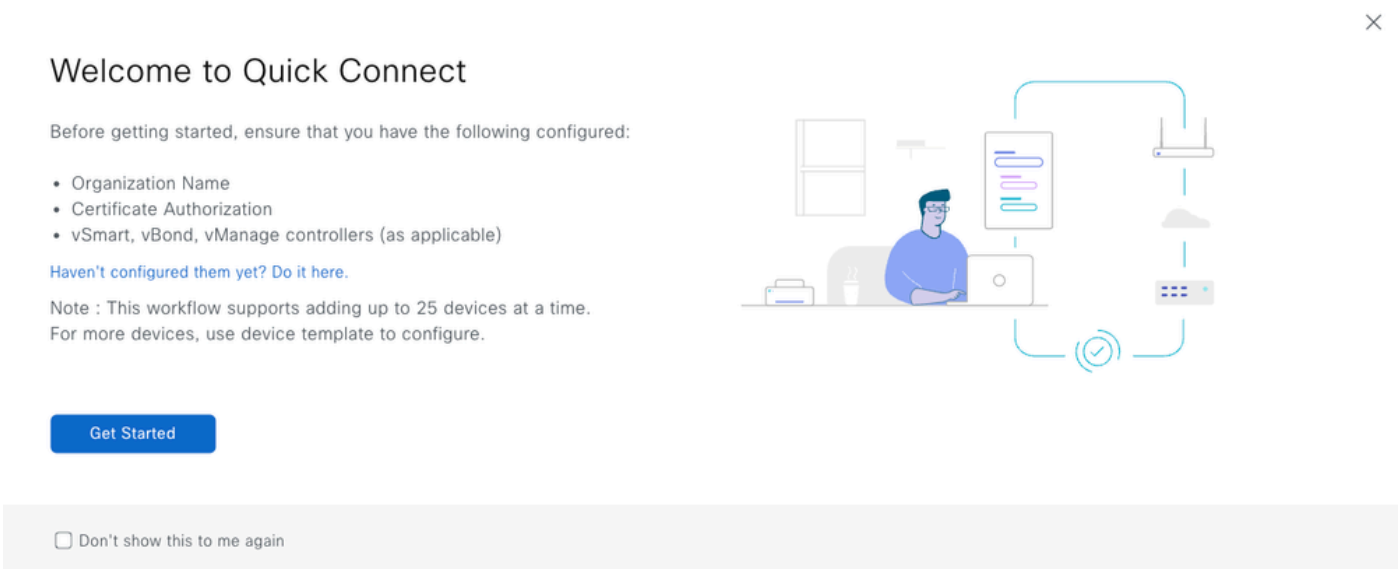
對於自註冊物理路由器，請使用快速連線工作流。

使用此工作流程，為要登入的裝置預先定義主機名、系統IP和站點名稱/ID。Manager會自動產生這些物件，但如果您要修改，可以修改它們。您還可以標籤裝置，然後使用這些裝置將裝置自動關聯到配置組。

在PnP ZTP自註冊過程中，裝置會建立到SD-WAN Manager的控制平面隧道連線。SD-WAN Manager現在將預定義的交換矩陣配置推送到裝置上，並且裝置加入SD-WAN交換矩陣。



快速連線工作流程



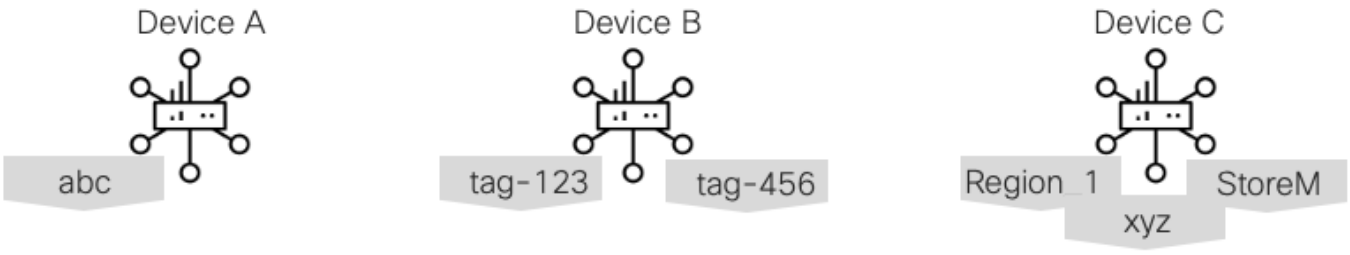
快速連線工作流程描述

標籤

裝置可以與使用者定義的標籤關聯。

標籤可用於分組、描述、查詢或管理裝置。

標籤可啟用裝置分組，然後可在其他功能中使用。



標籤範例

示例：配置組與裝置的關聯。

配置組規則可以設定為使具有特定標籤的裝置自動與該配置組關聯。

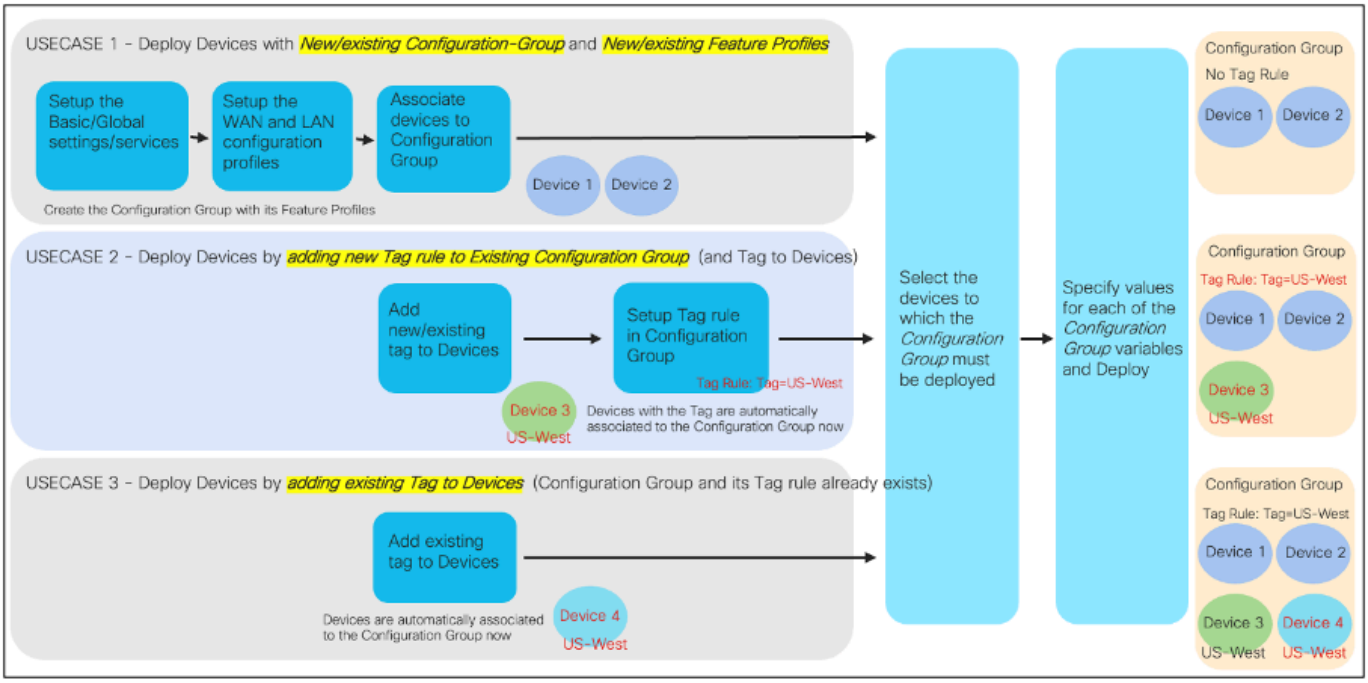
增加標籤

在Configuration -> Devices中，可以建立/增加/刪除裝置中的標籤。

標籤配置組中的規則

在「配置組」(Configuration Group) ->「關聯裝置」(Associated Devices)頁面中，可以增加/編輯標籤規則。

插圖



標籤插圖

現有部署

在SD-WAN網路中，使用傳統配置和策略的裝置可以使用簡化配置和策略與裝置共存。

本部分為希望利用簡化配置和策略的客戶提供一些建議，本部分提供一些建議。

第一步是需要將裝置從裝置模板遷移到配置組。 完成此操作後，即可部署策略組和/或拓撲。

配置組

裝置模板和配置組提供邊緣裝置配置。 所以很容易出現共存。 從裝置模板遷移到配置組的步驟如下：

步驟 1	從裝置模板中提取裝置值的副本。 這是從「配置模板」中完成，按一下裝置組右側的省略號(...)並選擇「導出CSV」。
步驟 2	建立組態群組（手動或使用轉換工具）。
步驟 3	將裝置範本與裝置分離。 此時，裝置會在連線點維護配置；但不會收到將來對裝置模板（或任何元件功能模板）所做的任何更改。
步驟 4	將裝置關聯到新配置組。

步驟 5	部署與配置組關聯的裝置。 若要簡化此程式，請開啟[匯出的CSV檔案]，並變更CSV欄標頭以符合組態群組的新變數。
步驟 6	在裝置變數輸入螢幕之後，您可以預覽裝置配置。 這可以讓您預覽配置組的哪些部分與上一個例項不匹配，或者哪些變數已從裝置模板更改。

為變數維護一致的命名方案可簡化特定於裝置的設定。 如果所有裝置值都位於單個CSV中，則只需重新命名列標題一次。

注意：存在一個Python指令碼，該指令碼與裝置模板或配置組的CSV檔案配合使用，用於合併列標題並按字母順序排列。 您可以在以下位置取得指令碼： https://github.com/BradEdgeworth/CSVMerger

原則群組

透過配置組配置的裝置可以使用集中策略或向策略組遷移；但不能同時為同一應用程式遷移兩者。實質上，目標是為邊緣裝置保留相同的底層策略。 策略組將原始AAR和資料策略組合成單個應用優先順序和SLA PG元件。 實質上，我們只是在更改策略配置的構建方式（而不是傳送到SD-WAN管理器）。

請注意，資料策略或AAR策略不能引用具有應用程式優先順序和SLA元件的站點的站點清單，因為它們都配置相同的設定。

在集中策略配置不同元件時，可以僅使用具有應用程式優先順序和SLA的策略組的站點引用控制策略的集中策略。

將裝置從集中策略遷移到策略組的步驟包括以下步驟：

步驟 1	建立必要的策略組元件（應用優先順序和SLA、嵌入式安全、安全網際網路網關/安全服務邊緣、DNS安全）。
步驟 2	建立原則群組並關聯必要的元件。
步驟 3	取消站點ID與AAR或資料策略中引用的任何SiteList的關聯。 此時，SD-WAN Manager將更新的配置傳送到控制器，然後控制器將從邊緣裝置刪除任何活動資料策略指令。 請注意，這可能會導致此時出現意外的流量。

步驟 4	將裝置關聯到策略組並儲存策略組。
步驟 5	將策略組部署到所選裝置。 此時，SD-WAN Manager將更新的配置傳送到邊緣裝置（用於QoS/SIG）和控制器；以便控制器可以向邊緣裝置傳送更新的資料策略。

注意：雖然策略組可以與集中策略共存，但建議在將邊緣裝置轉換為配置組時保持集中策略（適用於AAR和資料策略）。 然後，開始從「集中策略」遷移到「策略組」，以實現「應用優先順序和SLA」元件中的功能。

這樣做純粹是為了簡化操作，減少操作人員的困惑。

附註：
策略組引擎以不同的格式儲存內容。因此，必須在策略組中重新建立集中策略中使用的字首清單。對於網站清單等其他專案，可能會發生這種情況。

拓撲

透過配置組配置的裝置可以使用集中策略，也可以向拓撲遷移。實質上，目標是為SD-WAN控制器保留相同的底層控制策略。拓撲是最新版的控制策略。

必須注意的是，不能讓某個站點清單的控制策略引用與某個站點關聯的拓撲，因為這兩個站點配置的設定相同。

在配置不同元件時，可以使用僅具有資料策略和/或AAR策略的集中策略和拓撲策略。

將裝置從集中策略遷移到策略組的步驟：

步驟 1	建立必要的拓撲元件
步驟 2	從集中策略中的舊拓撲清單中取消關聯端。
步驟 3	取消站點ID與AAR或資料策略中引用的任何站點清單的關聯。 此時，SD-WAN Manager會將更新的配置傳送到控制器，然後控制器會刪除要遷移的站點的所有活動拓撲配置。 請注意，此時這可能會造成意外的流量。
步驟 4	啟動拓撲。此時，SD-WAN Manager會將更新的配置傳送到控制器，並修改

	傳送到邊緣裝置的任何路由。

注意：雖然拓撲可以與集中策略共存，但建議在將邊緣裝置轉換為配置組時保持集中策略（用於拓撲和路由操作）。 然後，開始從集中策略遷移到拓撲，以便執行修改拓撲和路由控制的功能。

這樣做純粹是為了簡化操作，減少操作人員的困惑。

轉換工具

範圍

Conversion Tool （轉換工具）會將1對1的範本轉換為組態群組。該工具從SD-WAN Manager例項收集模板，將其轉換為配置組（包括功能配置檔案和功能包），並將新轉換的構造上載到SD-WAN Manager。

* 暫預計2024年10月在轉換工具中將提供將政策轉化為政策小組的服務。

訪問詳細資訊

該工具的Beta版可用。有關詳細資訊，請訪問sdwan-ux-conversion-tool@cisco.com。

使用方法

必備條件

使用工具之前，請確保SD-WAN Manager正在運行20.12.x。如果不是，請先升級到20.12，再繼續進行。

轉換工具工作流程

步驟 1	使用思科提供的憑證登入工具。(注意：這些不是CCO證明資料。有關詳細資訊，請訪問sdwan-ux-conversion-tool@cisco.com)。
步驟 2	從首頁中選擇「轉換工具」工作流。 · 如果您以前曾執行過此工作流程，並且擁有包含轉換後配置的JSON檔案，則必須選擇「從檔案上傳」工作流程。
步驟 3	登入: 提供您的SD-WAN Manager IP或URL以及使用者憑證。

	· 使用者必須具有讀取/寫入存取權。 · 埠和子域欄位是可選的。
步驟 4.	匯入： 按一下「收集」按鈕，從SD-WAN Manager中檢索所有舊結構（裝置模板、功能模板、策略及其相關結構）。 · 收集完成後，您必須下載包含所有配置的JSON檔案。此檔案必須稍後在此步驟中使用，而不是再次從SD-WAN Manager收集。
步驟 5.	選取： 選擇要轉換為新等效項的模板和策略。按一下[移轉]轉換選取的建構。
步驟 6.	轉型: 此頁面顯示所有新轉換的建構。準備就緒後，按一下「上傳」將這些配置推送到SD-WAN Manager。 · 如果您尚未準備好推送到SD-WAN Manager，則可以將這些轉換的配置下載為JSON檔案，並在以後使用「從檔案上傳」工作流程。
步驟 7.	摘要: 此時，在SD-WAN Manager中推送和建立配置。在推送配置時，您可以看到進度欄。上傳完成後，您可以看到上傳配置的摘要。 · 您可以使用「配置組」、「功能配置檔案」和「策略組」快速連結來檢視SD-WAN Manager中的新結構。 · 若發生錯誤或錯誤，此步驟也可使用倒回。執行回滾將刪除在此工作流/會話期間推送到SD-WAN Manager的所有結構。

轉換後

您的新建構現已可供使用。執行「現有部署」部分中的步驟，將裝置遷移到新轉換的配置組。

考量

- 該工具所提供的轉換旨在作為指導。在生產環境中部署之前，請先進行分析和測試。
- 此工具不考慮配置組的裝置無關功能。使用者可以在選擇轉換或分析轉換的配置組之前分析其模板，並相應地關聯裝置，以從與裝置無關的功能中獲益。
- 舊有建構的變數名稱和全域值會複製到新轉換的建構中。

- 該工具不會將配置推送到裝置。執行轉換後，使用者負責將裝置從模板分離並將它們關聯到新的配置組。

20.12考慮因素

編號	料號摘要
1	在運行版本低於17.12的邊緣上部署配置組時，需要透過CLI附加配置檔案推送DNS配置。
2	建立拓撲需要選擇站點，而不是選擇在NHM中定義的區域。
3	建立配置組工作流程不會在廣域網配置檔案中建立VPN512和此VPN中的介面。如果需要，可透過編輯Configuration組手動建立此配置。
4	能夠複製/複製功能配置檔案，策略不受支援。　一組Python指令碼可以完成此任務，它們位於： https://github.com/dbrown92700/configGroups/
5	在建立任何與策略配置（在地化的策略）相關的功能包之前，策略對象配置檔案必須與配置組關聯。範例：ACL
6	為介面變數匯入CSV會在字串中插入分號，但失敗
7	AppQoE最佳化（TCP Opt和DRE）和丟失糾正（FEC和Pkt Dup）配置繼續使用傳統模板/策略。還可以透過配置/策略組中的CLI配置檔案進行配置。（20.14使用者介面包裹）
8	適用於SaaS的雲OnRamp繼續使用傳統模板/策略。
9	僅CLI配置檔案支援TrustSec/SGT
10	僅CLI配置檔案支援UC語音/DSP場/SRST（UI Parcel中從20.13開始）

相關資訊

- Cisco SD-WAN和雲網路YouTube頻道：https://www.youtube.com/@CiscoSDWANandCloudNetworking
- UX2.0 -操作簡化：1.配置單個路由器站點：https://www.youtube.com/watch?v=98z-d3knd
- 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）。