VMware SD-WAN 管理指南

VMware SD-WAN 3.4

您可以在 VMware 網站上找到最新的技術文件，網址如下：

https://docs.vmware.com/tw/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目錄

關於 VMware SD-WAN 管理指南

1

《VMware SD-WAN™ (以前稱為 VMware SD-WAN™ by VeloCloud®) 管理指南》提供 VMware SD-WAN Orchestrator 和核心 VMware 組態設定的相關資訊，包括如何設定和管理網路、網路服務、Edge、設定檔以及使用 SD-WAN Orchestrator 的客戶。

主要對象

本指南適用於網路管理員、網路分析員，以及負責部署、監控和管理企業分支網路的 IT 管理員。

從 4.4.0 版開始，VMware SD-WAN 隨附於 VMware SASE 中。若要存取適用於 Cloud Web Security 和 Secure Access 的 SASE 說明文件，以及 4.4.0 版和更新版本的版本說明，請參閱 VMware SASE。

新增功能

2

3.4.1 版的新增功能

功能	說明
支援私人區段	用於需要有限可見度才能解決使用者隱私權需求的流量。請參閱第 7 章 設定區段。
Syslog 防火牆記錄加強功能	啟用**所有區段 (All Segments)** 選項時，可允許 Syslog 收集器接收來自所有區段的防火牆記錄。此外，防火牆記錄訊息已透過新訊息欄位進行加強。請參閱在設定檔層級設定 Syslog 設定。
MPLS CoS 加強功能	設定 MPLS CoS 時，您可以強制執行嚴格 IP 優先順序，將服務類別合併到服務提供者網路中的較少類別數目。請參閱設定 MPLS CoS。

3.4 版的新增功能

功能	說明
條件式回傳	在啟用條件式回傳的情況下，每當沒有公用網際網路連結可供使用時，Edge 都能夠將網際網路繫結流量 (透過 IPsec 的直接網際網路流量和雲端安全性流量) 容錯移轉至 MPLS 連結。請參閱設定 Edge 叢集化和設定動作網路服務。
設定 DSL 設定	可支援 Metanoia xDSL SFP 模組 (MT 5311)，此為高度整合的 SFP 橋接數據機，能夠提供與插入式 SFP 相容的介面，以將現有的 DSL IAD 或主閘道裝置升級至更高的頻寬服務。請參閱設定 DSL 設定。
Edge 叢集化更新	如需 Edge 叢集化及其運作方式的相關更新資訊，請參閱以下幾節：關於 Edge 叢集化、Edge 叢集化的運作方式。
Edge 自訂資訊	可讓企業/MSP/操作員角色的標準管理員和超級使用者 (具有 UPDATE_EDGE 權限的使用者) 新增或更新 Edge 的自訂資訊。請參閱佈建新的 Edge。
Edge Wi-Fi 增強功能	在 Edge 層級上，根據為 Edge 設定的 Edge 型號和國家/地區，可讓您選取該 Edge 支援的無線電頻帶和通道。請參閱設定 Wi-Fi 無線電覆寫。
增強型 MPLS CoS	設定 MPLS CoS 時，有對應 DSCP 標籤的增強功能可供使用。您應將相同 IP 優先順序的 DSCP 標籤對應至相同的服務類別。請參閱設定 MPLS CoS。
企業報告	允許產生包含整體網路摘要的報告，且附帶 SD-WAN 流量和傳輸分配的相關資訊。報告可讓您對網路進行分析。請參閱監控報告。
中樞叢集化疑難排解	中樞叢集化有兩項疑難排解功能 (追蹤輪輻重新指派數目，以及在叢集內的中樞之間重新平衡輪輻)。這些功能可用於進行疑難排解或維護，以重新平衡中樞叢集中的所有輪輻。請參閱對 Edge 叢集化進行疑難排解。

功能	說明
Edge 上的 NAT 增強功能	使用者可以根據目的地 NAT 指定來源 NAT，或根據來源指定目的地 NAT，或者，使用者可同時對封包的來源和目的地 IP 進行 NAT 處理。請參閱 Edge 層級上的 LAN 端 NAT 規則。
Netflow 資料延伸	可讓使用者設定通道統計資料範本的匯出間隔。請參閱在設定檔層級設定 Netflow 設定。
510 LTE 和 610 的新式遠端診斷測試	「LTE 數據機資訊」診斷測試適用於已設定的 Edge 510 LTE 裝置。此測試會擷取診斷資訊，例如訊號強度與連線資訊等。請參閱設定裝置設定。
物件群組	物件群組由一個範圍的 IP 位址或連接埠號碼所組成。建立商務原則和防火牆規則時，您可以藉由在規則定義中包含物件群組，來定義 IP 位址範圍或 TCP/UDP 連接埠範圍的規則。請參閱第 16 章 物件群組。
可設定狀態的防火牆	可設定狀態的防火牆會監控並追蹤透過防火牆所傳入每個網路連線的作業狀態和特性，並使用這項資訊決定要允許哪些網路封包通過防火牆。請參閱設定防火牆規則。
支援 X710/XL710 NIC 搭配 DPDK 和 SR-IOV	對於新的 Intel X710/XL710 NIC，支援 SR-IOV 和 DPDK。請參閱 ■ VMware 虛擬 Edge 的部署必要條件 ■ 安裝 VMware 虛擬 Edge
Syslog 防火牆記錄	可用來將源自企業 SD-WAN Edges 的 SD-WAN Orchestrator 繫結事件和防火牆記錄，以原生 Syslog 格式收集到一或多個集中式遠端 Syslog 收集器 (伺服器)。請參閱在設定檔層級設定 Syslog 設定和在 Edge 層級設定 Syslog 設定。
Token 型驗證	使用者可使用 Token 來存取 SD-WAN Orchestrator API，而不使用工作階段型驗證。身為操作員超級使用者，您可以管理企業使用者的 API Token。請參閱 API Token。
Webhook 警示	Webhook 會將資料傳送至其他應用程式，由特定事件使用 HTTP POST 觸發。每當發生事件時，來源就會將 HTTP 要求傳送至針對 Webhook 設定的目標應用程式。請參閱 Webhook。

舊版 VMware SD-WAN

若要取得舊版 VMware SD-WAN 的產品說明文件，請連絡您的 VMware SD-WAN 代表。

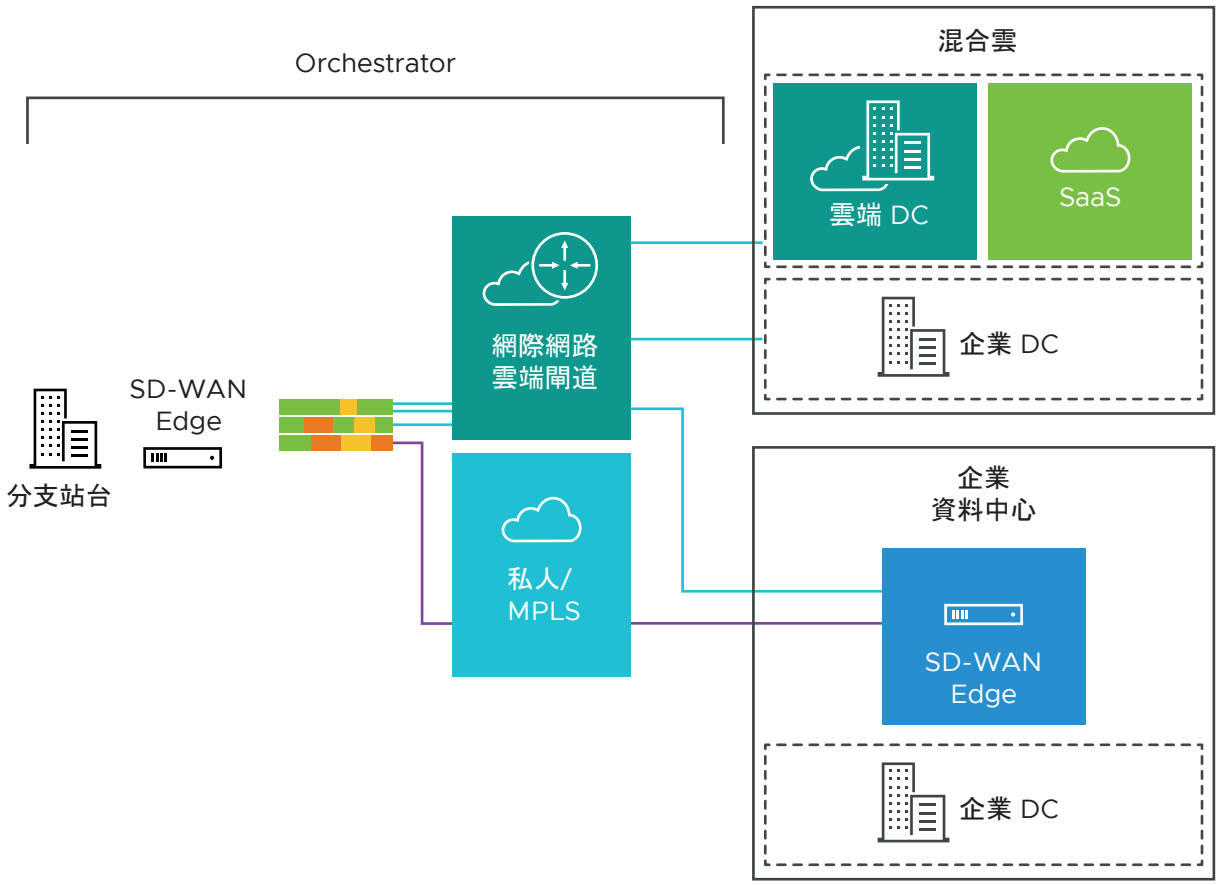
概觀

3

VMware SD-WAN 是一項雲端網路服務解決方案，可讓站台透過私人網路和網際網路寬頻快速部署對舊版和雲端應用程式的企業級存取。

雲端提供的軟體定義的 WAN 可確保企業能夠透過網際網路和混合 WAN 獲得雲端應用程式效能，同時簡化部署並降低成本。

下圖顯示 VMware SD-WAN 解決方案元件。以下幾節會詳細說明這些元件。



若要熟悉基本組態和 Edge 啟用，請參閱啟用 Edge。

本章節討論下列主題：

- 解決方案元件

解決方案元件

本節說明 VMware 解決方案元件。

VMware SD-WAN Edge

這是一種精簡的「Edge」，完全無需 IT 操作，而是從雲端佈建，可針對您的應用程式和虛擬化服務提供安全、最佳化的連線。SD-WAN Edges 是零接觸、企業級的裝置或虛擬軟體，可針對私人、公用和混合應用程式、計算和虛擬化服務提供安全且最佳化的連線。除了主控虛擬網路功能 (VNF) 服務以外，SD-WAN Edges 也會執行深度的應用程式辨識、應用程式和個別封包操控、隨選修復效能度量，以及端對端服務品質 (QoS)。您可以部署 Edge 配對，以提供高可用性 (HA)。Edge 可部署在分支、大型站台和資料中心。所有其他網路基礎結構都會在雲端中隨選提供。

VMware SD-WAN Orchestrator

VMware SD-WAN Orchestrator 可提供集中式企業範圍的組態和即時監控，並可透過 SD-WAN 覆疊網路協調資料流量。此外，它也透過集中式和區域企業服務中心和雲端，提供跨 Edge 的一鍵式虛擬服務佈建。

VMware SD-WAN Gateways

VMware SD-WAN 網路由部署在網路節點頂層的閘道和世界各地的雲端資料中心所組成，可讓 SD-WAN 服務順暢聯繫 SaaS、IaaS 和雲端網路服務，以及存取私人骨幹。多承租人的虛擬閘道會由 VMware SD-WAN 傳送和雲端服務提供者合作夥伴進行部署。閘道具有隨選、可擴充的備援雲端網路所帶來的優勢，可提供最佳化的雲端目的地路徑，以及零安裝應用程式。

SD-WAN Edge 效能和規模資料

本節介紹了 VMware SD-WAN Edge 的效能和規模架構。本文根據在設定有特定服務組合的各種 Edge 上執行的測試提供了相應的建議。此外，還說明了效能和規模資料點以及這些資料點的使用方式。

簡介

這些測試代表了常見的部署案例，可提供適用於大多數部署的建議。此處的測試資料並非全部包含的度量，也沒有涉及效能或規模限制。在一些實作中，觀察到的效能超出了測試結果，而在其他實作中，特定服務、極小的封包大小或其他因素可能會導致效能低於測試結果。

歡迎客戶執行獨立測試，結果可能會有所不同。但是，對於大多數部署，基於測試結果的建議已足夠。

VMware SD-WAN Edge

VMware SD-WAN Edge 是零接觸的企業級應用裝置，可針對私人、公用和混合應用程式，以及計算和虛擬化服務提供安全且最佳化的連線。除了支援其他虛擬化網路服務外，VMware SD-WAN Edge 還透過套用封包型的連結操控和隨選應用程式修復，執行對流量的深度應用程式辨識、衡量底層傳輸的效能度量測量，以及套用端對端服務品質。

總流量效能測試拓撲

圖 3-1. 圖 1 : 1 Gbps (或更低) 的裝置總流量效能測試拓撲

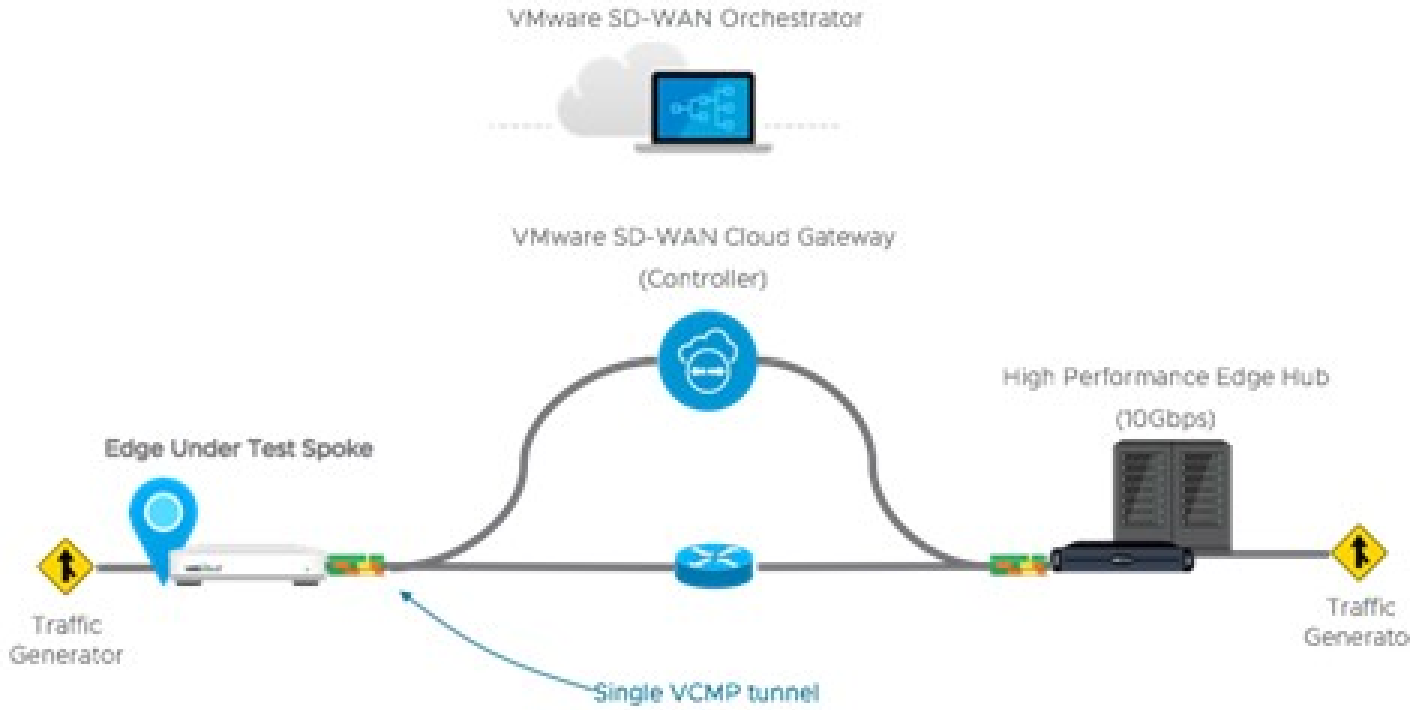
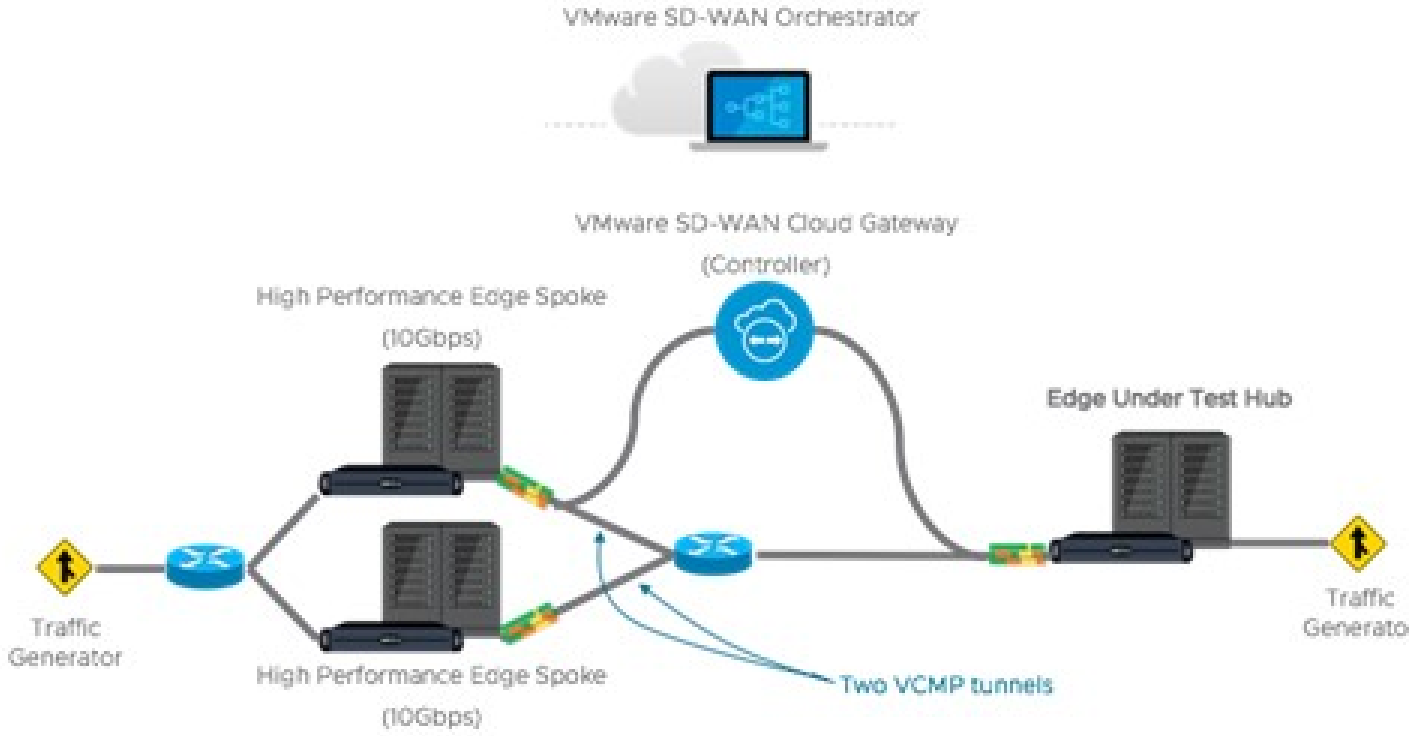


圖 3-2. 圖 2：高於 1 Gbps 的裝置總流量效能測試拓撲



測試方法

本小節詳述用來獲取結果的效能和規模測試方法。

效能測試方法

Edge 的測試方法使用業界效能評定標準 RFC 2544 作為架構，來執行總流量效能測試。測試期間使用的流量類型和設定的組態有具體的變更，如下所述：

1 可以使用具備完整功能的 SD-WAN 網路覆疊 (DMPO 通道) 測試拓撲，來測量效能，以便演練 SD-WAN 功能，並取得可用來適當調整 WAN 網路大小的結果。會使用可設定狀態的流量來執行測試，且這種流量會建立多流量 (連線)，且混合使用了已知的應用程式。流量數取決於正在測試的平台型號。平台是依 1 Gbps 以下和 1 Gbps 以上模型的預期總效能進行劃分。一般而言，需要數百個流量，才能充分演練及確定預期在低於 1 Gbps 執行之平台的最大總流量，且會使用數千個流量來演練超過 1 Gbps 的平台。

   流量設定檔會模擬兩項網路流量條件：

   - **大型封包**，1300 個位元組條件。
   - **IMIX**，封包大小的混合組合，平均為 417 個位元組條件。

   這些流量設定檔將分別用來測量每個設定檔的最大總流量。

2 會以封包捨棄率 (PDR) 0.01% 來記錄效能結果。PDR 標記可提供更真實的效能結果，該結果會將裝置中 SD-WAN 封包管線內可能發生的正常封包捨棄納入考量。PDR 0.01% 不會影響應用程式體驗，即使在單一連結部署案例中也是如此。

   - 正在測試的裝置設有以下 DMPO 功能：使用 AES-128 和 SHA1 進行雜湊的加密 IPSec、應用程式辨識、連結 SLA 測量、個別封包轉送。商務原則會設定為讓所有流量符合大量/低優先順序，以防止 DMPO NACK 或 FEC 執行以及不當變更流量產生器的封包計數追蹤。

測試結果

VMware SD-WAN Edge 效能和規模結果

效能度量是以上述的「測試方法」為基礎。

交換連接埠效能：依照設計，VMware SD-WAN Edge 可以部署成 LAN 與 WAN 之間的閘道路由器。但是，Edge 還提供靈活性，可滿足其他各種不同的部署拓撲。例如，SD-WAN Edge 可以將其介面設定成作為交換連接埠運作，從而允許在各種 LAN 介面之間切換 LAN 流量，而無需使用外部裝置。

將其介面設定成交換連接埠的 Edge，非常適合不需要高總流量的小型辦公室部署，因為處理流量交換需增加一層複雜性，而這會降低系統的整體效能。對於大多數部署，VMware 建議使用所有路由介面。

備註

- Edge 裝置的**最大總流量** 是正在測試之 Edge 的所有介面之間的總流量總和。
- **整體流量是指進出 Edge 裝置的所有流量的「彙總」。**

表 3-1. 實體 Edge 應用裝置

VMware SD-WAN Edge	510、510N	510-LTE	520	520V	540
最大大型封包 (1300 個位元組) 總流量					
路由模式 - 所有連接埠	350 Mbps	350 Mbps	350 Mbps	350 Mbps	1 Gbps
交換模式 - 所有連接埠	200 Mbps	200 Mbps	200 Mbps	200 Mbps	650 Mbps
最大網際網路流量的總流量 (IMIX)					
路由模式 - 所有連接埠	200 Mbps	200 Mbps	200 Mbps	200 Mbps	500 Mbps
交換模式 - 所有連接埠	80 Mbps	80 Mbps	80 Mbps	80 Mbps	200 Mbps
其他規模向量					
最大通道規模	50	50	50	50	100
每秒流量	2,400	2,400	2,400	2,400	4,800
最大並行流量	240K	240K	240K	240K	480K
最大路由數	100K	100K	100K	100K	100K

表 3-1. 實體 Edge 應用裝置 (續)

VMware SD-WAN Edge	510、510N	510-LTE	520	520V	540
最大區段數	128	128	128	128	128
最大 NAT 項目數	80K	80K	80K	80K	150K

表 3-2.

VMware SD-WAN Edge	640、640C、640N	680、680C、680N	840	2000	3400、3400C
最大大型封包 (1300 個位元組) 總流量					
路由模式 - 所有連接埠	3 Gbps	6 Gbps	4 Gbps	10 Gbps	7 Gbps
交換模式 - 所有連接埠	1 Gbps	1 Gbps	1 Gbps	1.2 Gbps	1.2 Gbps
最大網際網路流量的總流量 (IMIX)					
路由模式 - 所有連接埠	1 Gbps	2 Gbps	1.5 Gbps	5 Gbps	2.5 Gbps
交換模式 - 所有連接埠	350 Mbps	350 Mbps	350 Mbps	350 Mbps	900 Mbps
其他規模向量					
最大通道規模	400	800	400	6,000	4,000
每秒流量	19,200	19,200	19,200	38,400	38,400
最大並行流量	1.9M	1.9M	1.9M	1.9M	1.9M
最大路由數	100K	100K	100K	100K	100K
最大區段數	128	128	128	128	128
最大 NAT 項目數	650K	650K	650K	960K	960K

- **大型封包**效能是以開啟了 AES-128 加密和 DPI 的大型封包 (1300 個位元組) 裝載為基礎。
- **網際網路流量 (IMIX)** 效能是以開啟了 AES-128 加密和 DPI 的平均封包大小 (417 個位元組) 裝載為基礎。

備註 可以在叢集中部署多個 SD-WAN Edge，以達到數千兆位元的效能。

表 3-3. 防火牆 VNF 為主動服務鏈結時的 Edge 最大總流量：

Edge 型號	520V	620、620C、620N	640、640C、640N	680、680C、680N	840	3400、3
最大總流量，帶有 FW VNF (1300 個位元組)	100 Mbps	300 Mbps	600 Mbps	1 Gbps	1 Gbps	2 Gb

表 3-4. 增強型高可用性 (HA) 連結效能

Edge 型號	510、510N	510-LTE	520、520v	610、610C、610N	610-L
跨增強型 HA 連結的最大總流量 (IMIX)	90 Mbps	90 Mbps	100 Mbps	200 Mbps	200 M

Edge 型號	640、640C、640N	680、680C、680N	840	2000	3400、3400C
跨增強型 HA 連結的最大總流量 (IMIX)	800 Mbps	800 Mbps	800 Mbps	800 Mbps	800 Mbps

備註 **啟用了 Edge Network Intelligence 的效能：**

- 啟用分析後，效能影響高達 20%。
- 由於分析所需的額外記憶體和處理，當啟用分析時，流量容量會減少一半。

虛擬 Edge

表 3-5. 私有雲 (Hypervisor)

Edge 裝置	最大總流量	通道數目上限	每秒流量	最大並行流量	路由數目上
ESXi 虛擬 Edge (2 核心，VMXNET3)	2 Gbps (1300 個位元組) 800 Mbps (IMIX)	50	2400	240K	35
KVM 虛擬 Edge (2 核心，Linux 橋接器)	500 Mbps (1300 個位元組) 200 Mbps (IMIX)	50	2400	240K	35
KVM 虛擬 Edge (2 核心，SR-IOV)	1.25 Gbps (1300 個位元組) 600 Mbps (IMIX)	50	2400	240K	35
ESXi 虛擬 Edge (4 核心，VMXNET3)	2 Gbps (1300 個位元組) 1.5 Gbps (IMIX)	400	19200	1.9M	35
ESXi 虛擬 Edge (4 核心，SR-IOV)	2 Gbps (1300 個位元組) 1.5 Gbps (IMIX)	400	19200	1.9M	35
KVM 虛擬 Edge (4 核心，Linux 橋接器)	1 Gbps (1300 個位元組) 350 Mbps (IMIX)	400	4800	480K	35
KVM 虛擬 Edge (4 核心，SR-IOV)	2 Gbps (1300 個位元組) 1 Gbps (IMIX)	400	19200	1.9M	35
ESXi 虛擬 Edge (8 核心，VMXNET3)	5 Gbps (1300 個位元組) 2.5 Gbps (IMIX)	800	38400	1.9M	35

表 3-5. 私有雲 (Hypervisor) (續)

Edge 裝置	最大總流量		通道數目上限	每秒流量	最大並行流量	路由數目上
ESXi 虛擬 Edge (8 核心，SR-IOV)	3.4 版或更舊版本： 5 Gbps (1300 個位元組) 2.5 Gbps (IMIX)	4.0 版或更新版本： 9 Gbps (1300 個位元組) 4 Gbps (IMIX)	800	38400	1.9M	35
KVM 虛擬 Edge (8 核心，SR-IOV)	3.4 版或更舊版本： 3.5 Gbps (1300 個位元組) 1 Gbps (IMIX)	4.0 版或更新版本： 9 Gbps (1300 個位元組) 3 Gbps (IMIX)	800	38400	1.9M	35

	2 個 vCPU	4 個 vCPU	8 個 vCPU	10 個 vCPU
最小記憶體 (DRAM)	4 GB	8 GB	8 GB	8 GB
儲存區下限	8 GB	8 GB	8 GB	8 GB
支援的 Hypervisor	軟體版本 3.4 或更舊版本： ■ ESXi 6.0、6.5U1、6.7U1 ■ KVM Ubuntu 14.04 LTS 或 16.04 軟體版本 4.0 及更新版本： ■ ESXi 6.5U1、6.7U1、7.0 ■ KVM Ubuntu 16.04 和 18.04			
支援的公有雲	AWS、Azure、GCP 和 Alibaba			
支援網路 I/O	SR-IOV、VirtIO、VMXNET3			
建議的主機設定	2.0 GHz 或更高的 CPU CPU 指令集： ■ AES-NI ■ AVX2 或 AVX512 ■ SSE3、SSE4 和 RDTSC 指令集 已停用超執行緒			

備註 效能度量是以使用 Intel® Xeon® CPU E5-2683 v4 (2.10 GHz) 的系統為基礎。

公有雲

表 3-6. Amazon Web Services (AWS)

AWS 執行個體類型	c5.large	c5.xlarge	c5.2xlarge
最大總流量	100 Mbps (1300 個位元組) 50 Mbps (IMIX)	200 Mbps (1300 個位元組) 100 Mbps (IMIX)	7 Gbps (1300 個位元組) 2.4 Gbps (IMIX)
通道數目上限	50	400	800
每秒流量	1,200	2,400	4,800
最大並行流量	125,000	250,000	550,000

表 3-6. Amazon Web Services (AWS) (續)

AWS 執行個體類型	c5.large	c5.xlarge	c5.2xlarge
路由數目上限	35,000	35,000	35,000
區段數目上限	128	128	128

備註 c5.2xlarge 效能和規模數是以正在啟用的 AWS 增強型網路 (ENA SR-IOV 驅動程式) 為基礎。

表 3-7. Microsoft Azure

Azure 虛擬機器系列	D2d v4	D4d v4	D8d v4
最大總流量	100 Mbps (1300 個位元組) 50 Mbps (IMIX)	200 Mbps (1300 個位元組) 100 Mbps (IMIX)	1 Gbps (1300 個位元組) 450 Mbps (IMIX)
通道數目上限	50	400	800
每秒流量	1,200	2,400	4,800
最大並行流量	125,000	250,000	550,000
路由數目上限	35,000	35,000	35,000
區段數目上限	128	128	128

備註 支援 Azure 加速網路，但可用性受限。如需有關詳細資料，請連絡您的銷售代表。

功能

本節說明 VMware SD-WAN 功能。

動態多重路徑最佳化

VMware 動態多重路徑最佳化由自動連結監控、動態連結操控和隨選修復所組成。

連結操控和修復

系統會根據應用程式的商務優先順序、應用程式的網路需求內嵌知識，以及每個連結的即時容量和效能，以自動執行動態且應用程式感知的個別封包連結操控。依需求透過前饋式錯誤修正、抖動緩衝處理和負值通知 Proxy 緩解個別連結降級，也可讓注重優先順序和網路的應用程式保有其效能。在動態個別封包連結操控與隨選緩解的相互結合下，可有效防範低於一秒的封鎖和限制狀況，以改善應用程式可用性、效能和使用者體驗。

雲端 VPN

雲端 VPN 是與 VPNC 相容的站台間 IPSec VPN，只要按一下即可連線 VMware 與 Non VMware SD-WAN Sites，同時提供站台的即時狀態和健全狀況。雲端 VPN 可根據服務層級目標和應用程式效能，為所有分支建立動態的 Edge 對 Edge 通訊。雲端 VPN 也可透過 PKI 可擴充金鑰管理，提供所有分支間的安全連線。新的分支在加入 VPN 網路後，即自動可存取其他分支、企業資料中心和第三方資料中心 (如 Amazon AWS) 中的所有資源。

多重來源輸入 QoS

VMware 可對超過 3000 個啟用智慧控制的應用程式進行分類。開箱即用的預設值會為不同的應用程式類型設定多重來源輸入服務品質 (QoS) 參數，IT 人員只需建立應用程式優先順序即可。瞭解不同應用程式類型的網路需求、自動連結容量測量和動態流量監控，可以自動設定 QoS 和配置頻寬。

防火牆

VMware 提供可設定狀態且可感知內容 (應用程式、使用者、裝置) 的整合式應用程式感知防火牆，可精細控制子應用程式，且支援跳通訊協定的應用程式 – 例如 Skype 和其他點對點應用程式 (例如，停用 Skype 視訊和聊天，但允許 Skype 語音)。安全防火牆服務具備使用者和裝置作業系統感知功能，並且可區隔語音、視訊、資料和合規性流量。對於公司網路上的 BYOD 裝置 (如 Apple iOS、Android、Windows 和 Mac OS)，可以輕易控制其原則。

網路服務插入

VMware 解決方案支援以一個平台主控多個虛擬化網路功能，可免除單一功能應用裝置的使用需求，並降低分支 IT 複雜性。VMware 可針對從分支到雲端式和企業區域中樞服務的流量建立服務鏈結，同時確保效能、安全性和可管理性。分支可使用整合的安全性和網路服務，包括 Zscaler 和 Websense 等合作夥伴所提供的服務。使用按一下即可啟用的簡易介面，您可以透過應用程式特定原則，在雲端和內部部署中插入服務。

啟用

在零接觸部署中，SD-WAN Edge 應用裝置在連線至網際網路後，即會自動驗證、連線和接收組態指示。它們提供具有 SD-WAN Edge 備援通訊協定的高可用性部署，並且可與現有的網路整合，而能夠支援 OSPF 路由通訊協定，並受益於動態學習和自動化。

覆疊流量控制

SD-WAN Edge 會透過 OSPF 和 BGP 學習來自相鄰路由器的路由。它會將學習的路由傳送至閘道/控制器。閘道/控制器的運作方式類似於路由反射程式，會將學習的路由傳送至其他 SD-WAN Edges。覆疊流量控制 (OFC) 可實現企業範圍的路由可見度和控制，以便進行程式設計以及完整和部分覆疊。

OSPF

VMware 支援對 OSPF 芳鄰、OE1/OE2 路由類型、MD5 驗證的輸入/輸出篩選器。透過 OSPF 學習的路由將自動重新分配至雲端或內部部署中主控的控制器。

BGP

VMware 支援輸入/輸出篩選器，且篩選器可設定為「拒絕」，或選擇性地新增/變更 BGP 屬性以影響路徑選取，即 RFC 1998 社群、MED、AS 路徑附加和本機喜好設定。

分割

網路分割對企業和服務提供者而言都是重要功能。在最基本的形式中，分割可基於管理和安全考量提供網路隔離。最常見的分割形式是 L2 的 VLAN 和 L3 的 VRF。

分割的一般使用案例：

- 業務線區隔：工程、人力資源等。(基於安全/稽核考量)
- 使用者資料區隔：客體、PCI、公司流量區隔
- 企業在不同的 VRF 中使用重疊的 IP 位址

但是，傳統方法僅限於單一設備或兩個實體連線的裝置。若要延伸功能，必須跨網路傳輸分割資訊。

VMware 可啟用端對端的分割。當封包周遊經過 Edge 時，系統會將區段識別碼新增至封包，並轉送至中樞和雲端閘道，以允許從 Edge 到雲端和資料中心的網路服務隔離。這可讓您將首碼分組到唯一的路由表中，使商務原則能夠感知區段。

路由

在動態路由中，SD-WAN Edge 會透過 OSPF 或 BGP 學習來自相鄰路由器的路由。SD-WAN Orchestrator 會在名為「覆疊流量控制」的全域路由表中維護所有動態學習的路由。覆疊流量控制可讓您在「覆疊流量控制同步」和「輸入/輸出篩選組態有所變更」的情況下管理動態路由。輸入篩選中的首碼從 IGNORE 變更為 LEARN 後，將會從覆疊流量控制中擷取首碼，並安裝到整合路由表中。

如需詳細資訊，請參閱第 18 章 使用 OSPF 或 BGP 設定動態路由。

商務原則架構

系統會根據商務原則和應用程式優先順序自動套用服務品質 (QoS)、資源組態、連結/路徑操控和錯誤修正。請根據私人和公用連結、原則定義和連結特性所定義的傳輸群組來協調流量。

通道額外負荷和 MTU

如同任何覆疊，VMware 也會對周遊網路的流量產生額外負荷。本節將先說明在傳統 IPsec 網路中增加的額外負荷，及其與 VMware 的比較，然後說明這些增加的額外負荷與網路中的 MTU 和封包分段行為有何關聯。

IPsec 通道額外負荷

在傳統 IPsec 網路中，通常會在端點之間以 IPsec 通道傳送流量。標準 IPsec 通道案例 (使用 ESP [封裝安全性裝載] 的 AES 128 位元加密) 在加密流量時會產生多種類型的額外負荷，如下所述：

- **填補**
  - AES 會以 16 位元組的區塊 (我們稱之為「區塊」大小) 加密資料。
  - 如果封包的主體小於區塊大小，或無法以此大小整除，則會進行填補以符合區塊大小。
  - 範例：
    - 1 位元組的封包會填補 15 個位元組而變為 16 位元組的封包。
    - 1400 位元組的封包會填補 8 個位元組而變為 1408 位元組的封包。
    - 64 位元組的封包不需要任何填補。
- **IPsec 標頭和尾端：(IPsec headers and trailers:)**
  - NAT 周遊 (NAT-T) 的 UDP 標頭。
  - IPsec 通道模式的 IP 標頭。
  - ESP 標頭和尾端。

元素	大小 (以位元組為單位)
IP 標頭	20
UDP 標頭	8
IPsec 序號	4
IPsec SPI	4
初始化向量	16
填補	0 – 15
填補長度	1
下一個標頭	1
驗證資料	12
總計	66-81

備註 提供的範例假設至少有一個裝置位於 NAT 裝置後方。若未使用 NAT，IPsec 額外負荷將會減少 20 個位元組，因為不需要 NAT-T。無論 NAT 是否存在，都不會變更 VMware 的行為 (一律啟用 NAT-T)。

VMware 通道額外負荷

為了支援 Dynamic Multipath Optimization™ (DMPO)，VMware 會將封包封裝在名為 VeloCloud 多重路徑通訊協定 (VCMP) 的通訊協定中。VCMP 會為使用者封包增加 31 個位元組的額外負荷，以在單一通道內支援重新排序、錯誤修正、網路分析和網路分割。VCMP 會在 IANA 登錄的連接埠 UDP 2426 上運作。為了確保在所有可能的情況下 (未加密、已加密並位於 NAT 後方、已加密但不在 NAT 後方) 都會有一致的行為，VCMP 會使用傳輸模式 IPsec 進行加密，並使用特殊的 NAT-T 連接埠 2426 強制將 NAT-T 設為 true。

依預設不會對透過 SD-WAN Gateway 傳送至網際網路的封包加密，因為這些封包會在退出閘道時輸出至開放的網際網路。因此，網際網路多重路徑流量的額外負荷會少於 VPN 流量。

備註 服務提供者可選擇透過閘道來加密網際網路流量，且他們若選擇使用此選項，「VPN」額外負荷也會套用至網際網路流量。

VPN 流量 (VPN Traffic)

元素	大小 (以位元組為單位)
IP 標頭	20
UDP 標頭	8
IPsec 序號	4
IPsec SPI	4
VCMP 標頭	23
VCMP 資料標頭	8
初始化向量	16
填補	0 – 15
填補長度	1
下一個標頭	1
驗證資料	12
總計	97 – 112

網際網路多重路徑流量 (Internet Multipath Traffic)

元素	大小 (以位元組為單位)
IP 標頭	20
UDP 標頭	8
VCMP 標頭	23

元素	大小 (以位元組為單位)
VCMP 資料標頭	8
總計	59

路徑 MTU 探索

在判斷將套用多少額外負荷後，SD-WAN Edge 必須探索允許的 MTU 上限，以計算客戶封包的有效 MTU。為了尋找允許的 MTU 上限，Edge 會執行路徑 MTU 探索：

- 針對公用網際網路 WAN 連結：
  - 對所有鬧道執行路徑 MTU 探索。
  - 所有通道的 MTU 都將設定為探索到的最小 MTU。
- 針對私人 WAN 連結：
  - 對客戶網路中的所有其他 Edge 執行路徑 MTU 探索。
  - 系統會根據路徑 MTU 探索的結果來設定每個通道的 MTU。

Edge 會先嘗試進行 RFC 1191 路徑 MTU 探索，其中目前已知連結 MTU (預設值：1500 個位元組) 的封包會使用 IP 標頭中設定的「不分段」(DF) 位元以傳送至對等。如果在遠端 Edge 或鬧道上接收到此封包，則會將相同大小的確認封包傳回至 Edge。如果封包因 MTU 限制而無法送至遠端 Edge 或鬧道，則預期中繼裝置應會傳送 ICMP 目的地無法連線 (需要分段) 的訊息。Edge 在接收到 ICMP 無法連線的訊息時，將會驗證訊息 (以確保報告的 MTU 為正常值)，且一經驗證後就會調整 MTU。然後，此程序會重複執行，直到探索到 MTU 為止。

在某些案例中 (例如 USB LTE Dongle)，即使封包太大，中繼裝置也不會傳送 ICMP 無法連線的訊息。如果 RFC 1191 失敗 (Edge 未接收到確認或 ICMP 無法連線的訊息)，則會回復至 RFC 4821 封包化層路徑 MTU 探索。Edge 會嘗試執行二進位搜尋以探索 MTU。

探索到對等的 MTU 時，此對等的所有通道將會設定為相同的 MTU。這表示，如果 Edge 的一個連結具有 1400 位元組的 MTU，而另一個連結的 MTU 為 1500 位元組，則所有通道都將具有 1400 位元組的 MTU。這可確保隨時都能使用相同的 MTU 在任何通道上傳送封包。我們稱之為**有效 Edge MTU (Effective Edge MTU)**。根據目的地 (VPN 或網際網路多重路徑)，系統會減去前述的額外負荷，以計算**有效封包 MTU (Effective Packet MTU)**。直接網際網路或其他底層流量的額外負荷為 0 個位元組，且由於不需要進行連結容錯移轉，有效封包 MTU 與探索到的 WAN 連結 MTU 相同。

備註 VMware RFC 4821 封包化層路徑 MTU 探索可測量到 1300 位元組以上的 MTU。如果您的 MTU 少於 1300 位元組，則必須手動設定 MTU。

VPN 流量和 MTU

SD-WAN Edge 現已探索到 MTU 並計算出額外負荷，接下來即可為用戶端流量計算有效 MTU。Edge 會嘗試盡可能有效地對接收到的各種可能流量類型強制執行此 MTU。

TCP 流量 (TCP Traffic)

Edge 會自動對接收到的 TCP 封包執行 TCP MSS (最大區段大小) 調整。當 SYN 和 SYN|ACK 封包通過 Edge 時，系統會根據有效封包 MTU 重新寫入 MSS。

未設定 DF 位元的非 TCP 流量 (Non-TCP Traffic without DF bit set)

如果封包大於有效封包 MTU，則 Edge 會依據 RFC 791 自動執行 IP 分段。

設定了 DF 位元的非 TCP 流量 (Non-TCP Traffic with DF bit set)

如果封包大於有效封包 MTU：

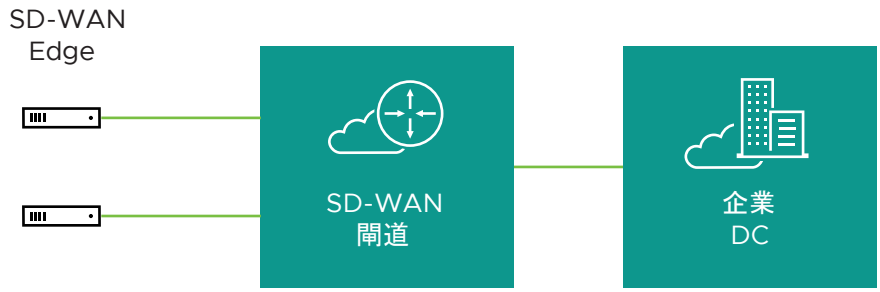
- 第一次收到此流量 (IP 5 元組) 的封包時，Edge 會捨棄封包，並根據 RFC 791 傳送 ICMP 目的地無法連線 (需要分段) 的訊息。
- 如果後續接收到相同流程的封包，但仍然過大，這些封包將會分段為多個 VCMP 封包，並且先明確地進行重組再遞交至遠端。

網路拓撲

本節說明適用於分支和資料中心的網路拓撲。

分支到私人第三方 (VPN)

具有私人資料中心或雲端資料中心的客戶很可能會想要能直接將其包含在網路中，而無須定義從個別分公司站台到資料中心的通道。將站台定義為 Non VMware SD-WAN Site，即可從最接近的 SD-WAN Gateway 到客戶現有的路由器或防火牆建立單一通道。所有需要與站台通訊的 SD-WAN Edges 都將連線至相同的 SD-WAN Gateway，以透過通道轉送封包，從而簡化整體網路組態和新站台的顯示。



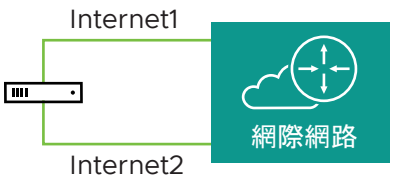
VMware 可簡化分支部署，並且為企業提供絕佳的應用程式效能，或適用於雲端和/或內部部署應用程式的公用/私人連結。

分支站台拓撲

VMware 服務會定義兩個或更多指定為銅級、銀級和金級的不同分支拓撲。此外，可以在分支位置的高可用性 (HA) 組態中設定 SD-WAN Edges 的配對。

銅級站台拓撲

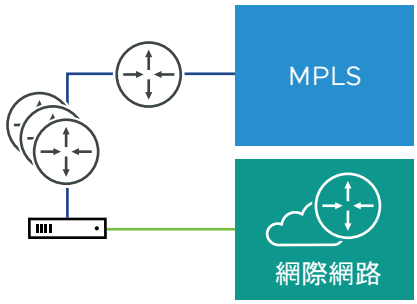
銅級拓撲代表有一或兩個 WAN 連結連線至公用網際網路的一般小型站台部署。銅級拓撲中沒有 MPLS 連線，且 SD-WAN Edge 的 LAN 端也沒有 L3 交換器。下圖顯示銅級拓撲的概觀。



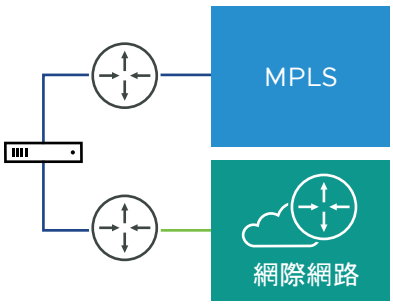
銀級站台拓撲

銀級拓撲代表除了一或多個公用網際網路連結以外還具有 MPLS 連線的站台。此拓撲有兩種變體。

第一個變體是具有一或多個公用網際網路連結和一個 MPLS 連結的單一 L3 交換器 (MPLS 連結可在 CE 上終止，並且可透過 L3 交換器來存取)。在此情況下，SD-WAN Edge 會在 L3 交換器與網際網路之間運作 (取代現有的防火牆/路由器)。

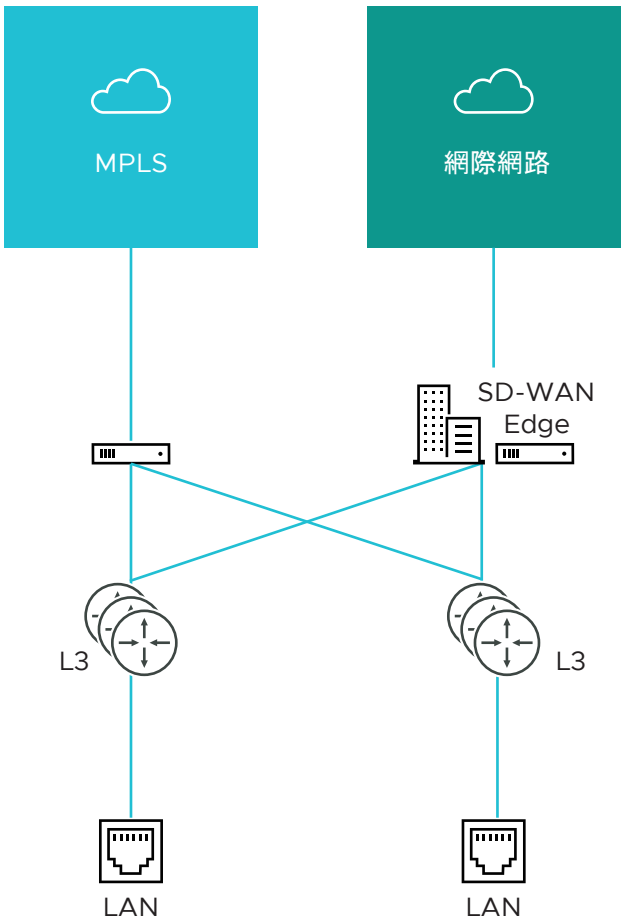


第二個變體包含使用 HSRP 部署的 MPLS 和網際網路路由器，且 LAN 端會有 L2 交換器。在此情況下，SD-WAN Edge 會取代 L2 交換器。

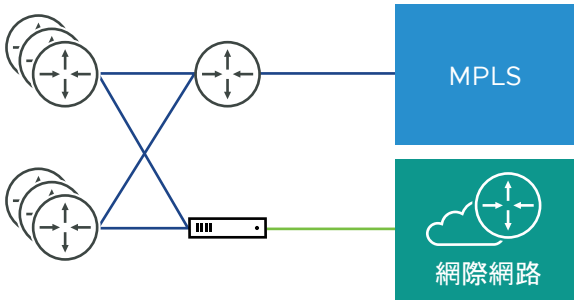


金級站台拓撲

金級拓撲是典型的大型分支站台拓撲。此拓撲包含使用 OSPF 或 BGP 來傳輸路由的雙 L3 交換器、一或多個公用網際網路連結，和一個 MPLS 連結；MPLS 連結可在同樣與 OSPF 或 BGP 聯繫的 CE 路由器上終止，並且可透過 L3 交換器進行存取。

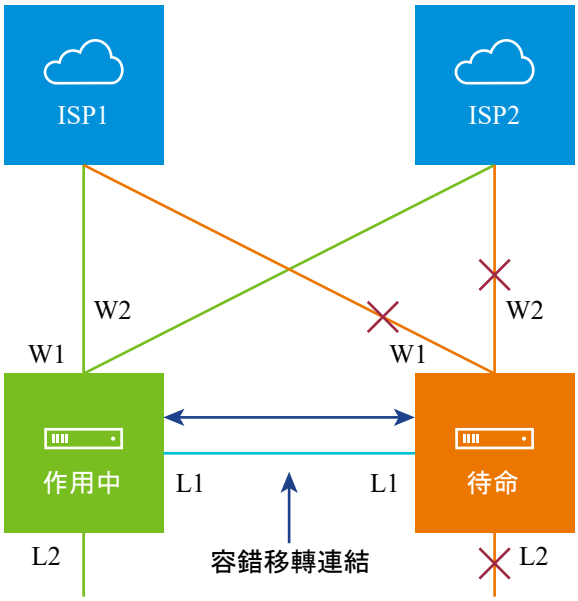


此處主要的差異點在於，單一 WAN 連結可透過兩個路由介面來存取。為了對此提供支援，虛擬 IP 位址會佈建在 Edge 內部，並且可以透過 OSPF、BGP 或靜態路由至介面進行通告。



高可用性 (HA) 組態

下圖概略說明使用兩個 SD-WAN Edges (一個主動、一個備用) 的 VMware 高可用性組態概念。



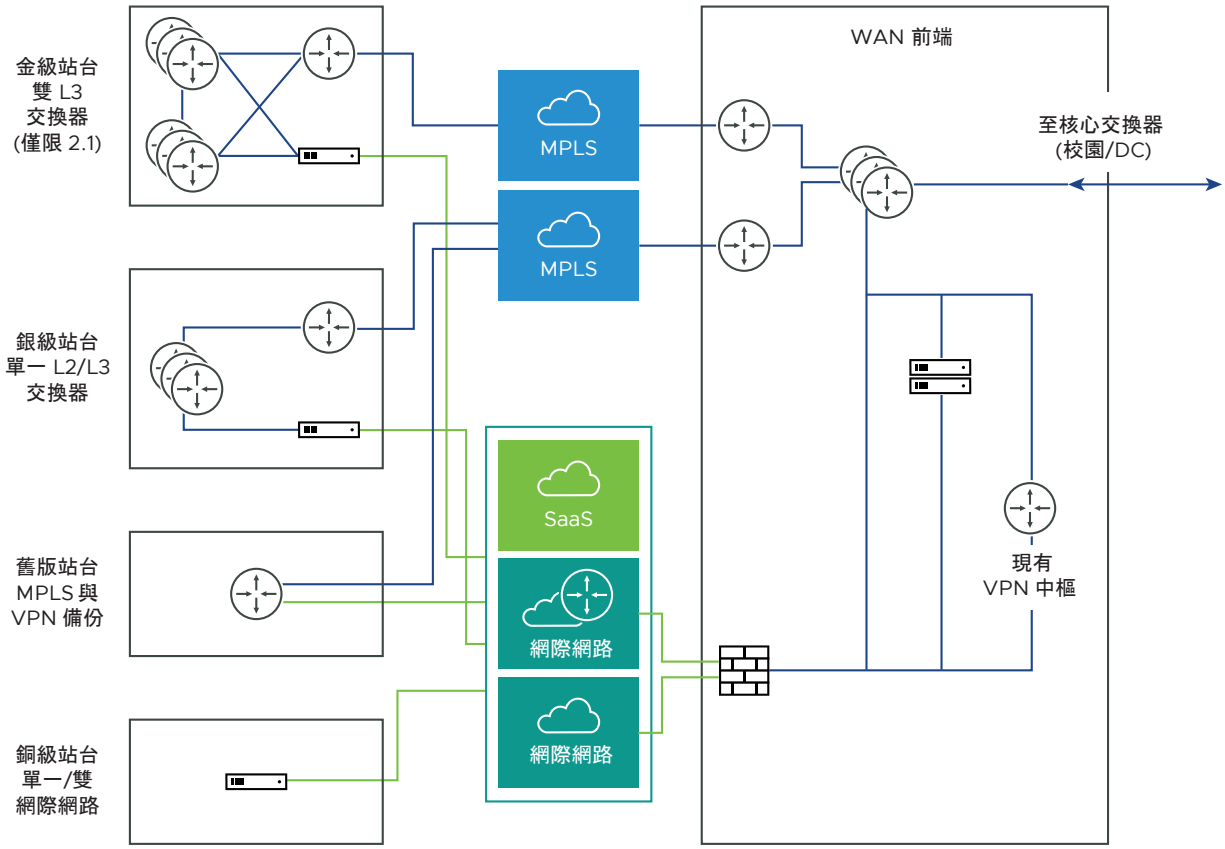
連接每個 Edge 上的 L1 連接埠，可建立容錯移轉連結。備用 SD-WAN Edge 會封鎖 L1 連接埠以外的所有連接埠，使其無法用於容錯移轉連結。

內部部署拓撲

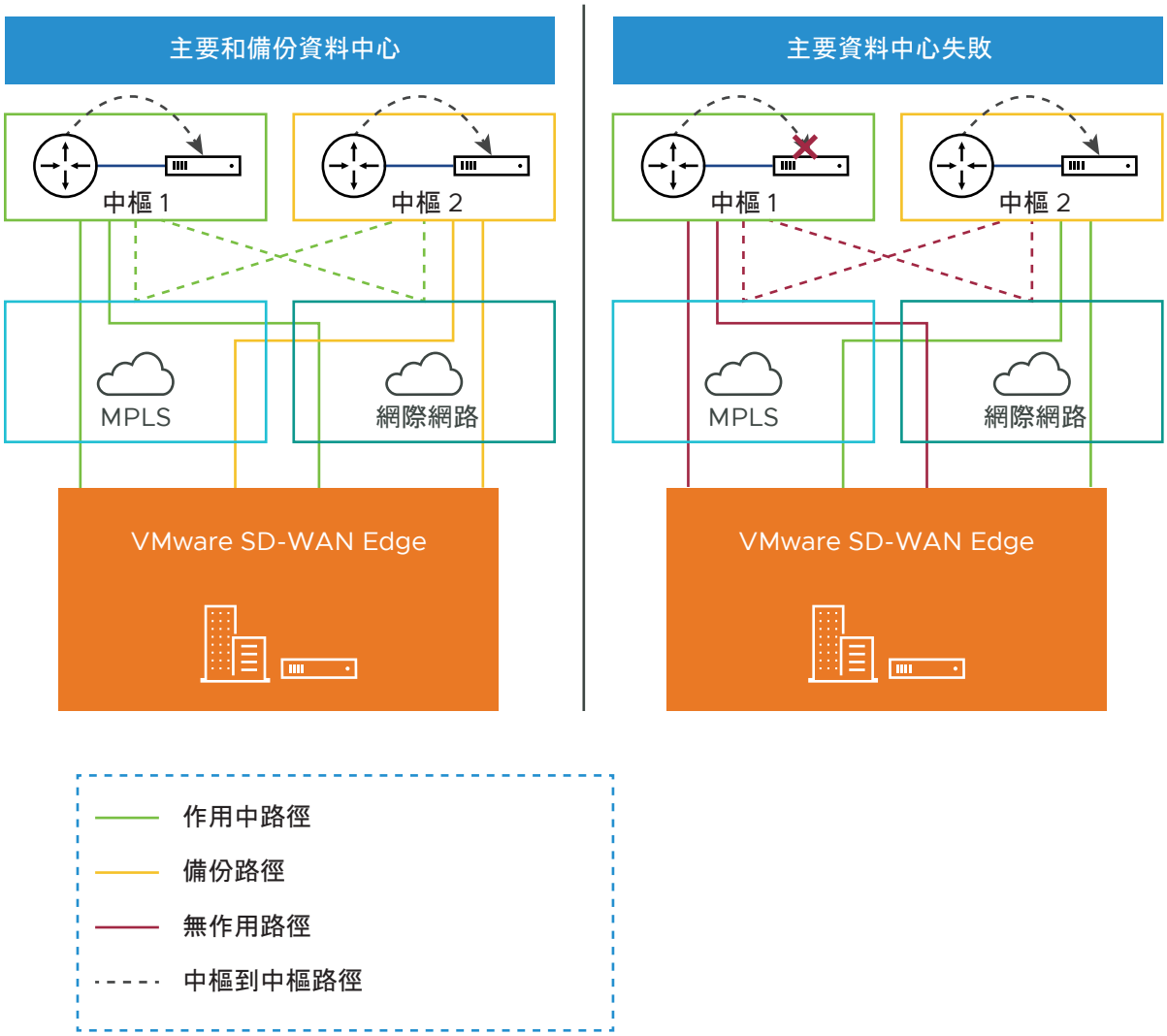
內部部署拓撲由兩個中樞和多個分支組成 (有些具有 SD-WAN Edge，有些則否)。每個中樞都有混合的 WAN 連線。分支有數種類型。

備註 金級站台目前不在此版本的範圍內，將於後續新增。

MPLS 網路會執行 BGP，並且與所有 CE 路由器對等。在中樞 1、中樞 2 和銀級 1 站台上，L3 交換器會透過 CE 路由器和防火牆執行 OSPF 或 BGP (如果是中樞站台)。



在某些案例中，可能會有備援的資料中心，以不同的成本通告相同的子網路。在這種情況下，可以將兩個資料中心都設定為 Edge 對 Edge 的 VPN 中樞。所有 Edge 會會直接連線至每個中樞，而中樞實際上也會直接相互連線。根據路由成本，流量會導向至慣用的作用中資料中心。



在先前的版本中，使用者可以使用 Zscaler 或 Palo Alto Network 建立企業物件作為一般 Non VMware SD-WAN Site。在 3.4 中，該物件現已成為第一類物件 Non VMware SD-WAN Site。

雲端提供的 VMware 解決方案結合了混合 WAN 的經濟效益和彈性，以及雲端式服務部署快速和維護成本低廉的優勢。它提供從雲端到分公司的虛擬化服務，從而大幅簡化了 WAN。VMware 客戶部署裝置、SD-WAN Edge、在分支辦公室匯總多個寬頻連結 (例如，纜線、DSL、4G-LTE)，並將流量傳送至 SD-WAN Gateways。服務可以使用以雲端為基礎的協調，將分支辦公室連線到任何類型的資料中心：企業、雲端或軟體即服務。

SD-WAN Edge 是一種從雲端佈建的精簡 Edge 裝置，可提供安全、最佳化的應用程式和資料連線。閘道叢集可全域部署於頂層雲端資料中心，以提供可擴充的隨選雲端網路服務。透過 Edge 的運用，叢集可提供動態、多重路徑的最佳化，使多個一般的寬頻連結如同單一的高頻寬連結。Orchestrator 管理提供虛擬服務的集中式設定、即時監控和單鍵式佈建等功能。

角色和權限層級

VMware 有具備不同權限集的預先定義角色。

- IT 管理員 (或管理員)
- 已部署 SD-WAN Edge 裝置的每個站台的站台連絡人
- IT 操作員 (或操作員)
- IT 合作夥伴 (或合作夥伴)

管理員

管理員可設定、監控和管理 VMware 服務作業。管理員角色有三種：

管理員角色	說明
企業標準管理員	可執行所有組態和監控工作。
企業超級使用者	可執行與企業標準管理員相同的工作，也可以建立具有企業標準管理員、企業 MSP 和客戶支援角色的其他使用者。
企業支援	可執行組態檢查和監控工作，但無法檢視使用者識別應用程式統計資料，而只能檢視組態資訊。

備註 管理員應徹底熟悉企業的網路概念、Web 應用程式以及需求和程序。

站台連絡人

站台連絡人負責 SD-WAN Edge 的實體安裝與 VMware 服務的啟用。站台連絡人屬於非 IT 人員，必須能夠接收電子郵件，並執行電子郵件中有關於 Edge 啟用的指示。

操作員

操作員可執行管理員能夠執行的所有工作，以及其他操作員特定工作，例如建立和管理客戶、雲端 Edge 和閘道。操作員角色有四種：

操作員角色	說明
標準操作員	可執行所有組態和監控工作。
超級使用者操作員	可檢視和建立其他具有操作員角色的使用者。
商務專員操作員	可建立和管理客戶帳戶。
客戶支援操作員	可監控 Edge 和活動。

操作員應徹底熟悉企業的網路概念、Web 應用程式以及需求和程序。

合作夥伴

合作夥伴可執行管理員能夠執行的所有工作，以及其他合作夥伴特定工作，例如建立和管理客戶。合作夥伴角色有四種：

合作夥伴角色	說明
標準管理員	可執行所有組態和監控工作。
超級使用者	可檢視和建立其他具有合作夥伴角色的使用者。
商務專員	可執行組態和監控工作，但無法檢視使用者識別應用程式統計資料。
客戶支援	可執行組態檢查和監控工作，但無法檢視使用者識別應用程式統計資料，而只能檢視組態資訊。

合作夥伴應徹底熟悉企業的網路概念、Web 應用程式以及需求和程序。

使用者角色對照表

本節說明根據 VMware 使用者角色的功能存取權。

操作員層級 SD-WAN Orchestrator 功能的使用者角色對照表

下表列出可存取 SD-WAN Orchestrator 功能的操作員層級使用者角色。

- R：讀取
- W：寫入 (修改/編輯)
- D：刪除
- NA：無存取權

SD-WAN Orchestrator 功能	操作員：超級使用者操作員	操作員：標準操作員	合作夥伴：商務專員	合作夥伴：客戶支援操作員	超級使用者	標準管理員	商務專員	客戶支援
監控客戶	R	R	R	R	R	R	R	R
管理客戶	RWD	RWD	RWD	R	RWD	RWD	RWD	R
管理合作夥伴	RWD	RWD	RWD	R	NA	NA	NA	NA
(管理 Edge) 軟體映像	RWD	RWD	R	R	*請參閱附註	*請參閱附註	*請參閱附註	*請參閱附註
系統內容	RWD	R	NA	R	NA	NA	NA	NA
操作員事件	R	R	NA	R	NA	NA	NA	NA
操作員設定檔	RWD	RWD	R	R	NA	NA	NA	NA
操作員使用者	RWD	R	R	R	NA	NA	NA	NA
閘道集區	RWD	RW	R	R	RWD	RWD	NA	R
閘道 (Gateways)	RWD	RWD	R	R	RW	RW	NA	R
閘道診斷服務包	RWD	RWD	R	R	NA	NA	NA	NA

SD-WAN Orchestrator 功能	操作員：超級使用者操作員	操作員：標準操作員	合作夥伴：商務專員	合作夥伴：客戶支援操作員	超級使用者	標準管理員	商務專員	客戶支援
應用程式對應	RWD	RWD	R	R	NA	NA	NA	NA
CA 摘要	RW	R	R	R	NA	NA	NA	NA
Orchestrator 驗證	RWD	R	NA	R	NA	NA	NA	NA
複寫	RW	R	NA	R	NA	NA	NA	NA

備註 操作員超級使用者具有憑證相關組態的「RWD」存取權，而標準操作員具有憑證相關組態的唯讀存取權。這些使用者可以從導覽面板中的**設定 (Configure) > Edge** 存取憑證相關組態。*

備註 所有層級的企業使用者都無法存取操作員層級的功能。

合作夥伴層級 SD-WAN Orchestrator 功能的使用者角色對照表

下表列出可存取 SD-WAN Orchestrator 功能的合作夥伴層級使用者角色。

- R：讀取
- W：寫入 (修改/編輯)
- D：刪除
- NA：無存取權

SD-WAN Orchestrator 功能	合作夥伴：超級使用者	合作夥伴：標準管理員	商務專員	CustomerSupport
監控客戶	R	R	R	R
管理客戶	RWD	RWD	RWD	R
事件	R	R	NA	R
管理員	RWD	R	NA	R
概觀	R	R	R	R
設定	RW	R	R	R
閘道集區	RW	RWD	NA	R
閘道 (Gateways)	RW	RW	NA	R

企業層級 SD-WAN Orchestrator 功能的使用者角色對照表

下表列出可存取 SD-WAN Orchestrator 功能的企業層級使用者角色。

- R：讀取
- W：寫入 (修改/編輯)

- D：刪除
- NA：無存取權

SD-WAN Orchestrator 功能	企業：超級使用者	企業：標準管理員	客戶支援	唯讀
監控 (Monitor) > Edge	R	R	R	R
監控 (Monitor) > 網路服務 (Network Services)	R	R	R	R
監控 (Monitor) > 路由 (Routing)	R	R	R	NA
監控 (Monitor) > 警示 (Alerts)	R	R	R	NA
監控 (Monitor) > 事件 (Events)	R	R	R	NA
設定 (Configure) > Edge	RWD	RWD	R	NA
設定 (Configure) > 設定檔 (Profiles)	RWD	RWD	R	NA
設定 (Configure) > 網路 (Networks)	RWD	RWD	R	NA
設定 (Configure) > 區段 (Segments)	RWD	RWD	R	NA
設定 (Configure) > 覆疊流量控制 (Overlay Flow Control)	RWD	RWD	R	NA
設定 (Configure) > 網路服務 (Network Services)	RWD	RWD	R	NA
設定 (Configure) > 警示和通知 (Alerts & Notifications)	RW	RW	R	NA
測試和疑難排解 (Test & Troubleshoot) > 遠端診斷 (Remote Diagnostics)	RW	RW	RW	NA
測試和疑難排解 (Test & Troubleshoot) > 遠端動作 (Remote Actions)	RW	RW	RW	NA
測試和疑難排解 (Test & Troubleshoot) > 封包擷取 (Packet Capture)	RW	RW	RW	NA
測試和疑難排解 (Test & Troubleshoot) > 診斷服務包 (Diagnostic Bundles)	RWD	RWD	RWD	NA
管理 (Administration) > 系統設定 (System Settings)	RW	RW	RW	NA
管理 (Administration) > 管理員 (Administrators)	RW	R	R	NA

備註 操作員使用者可完整存取 SD-WAN Orchestrator 功能。

重要概念

本節說明 SD-WAN Orchestrator 的主要概念及核心組態。

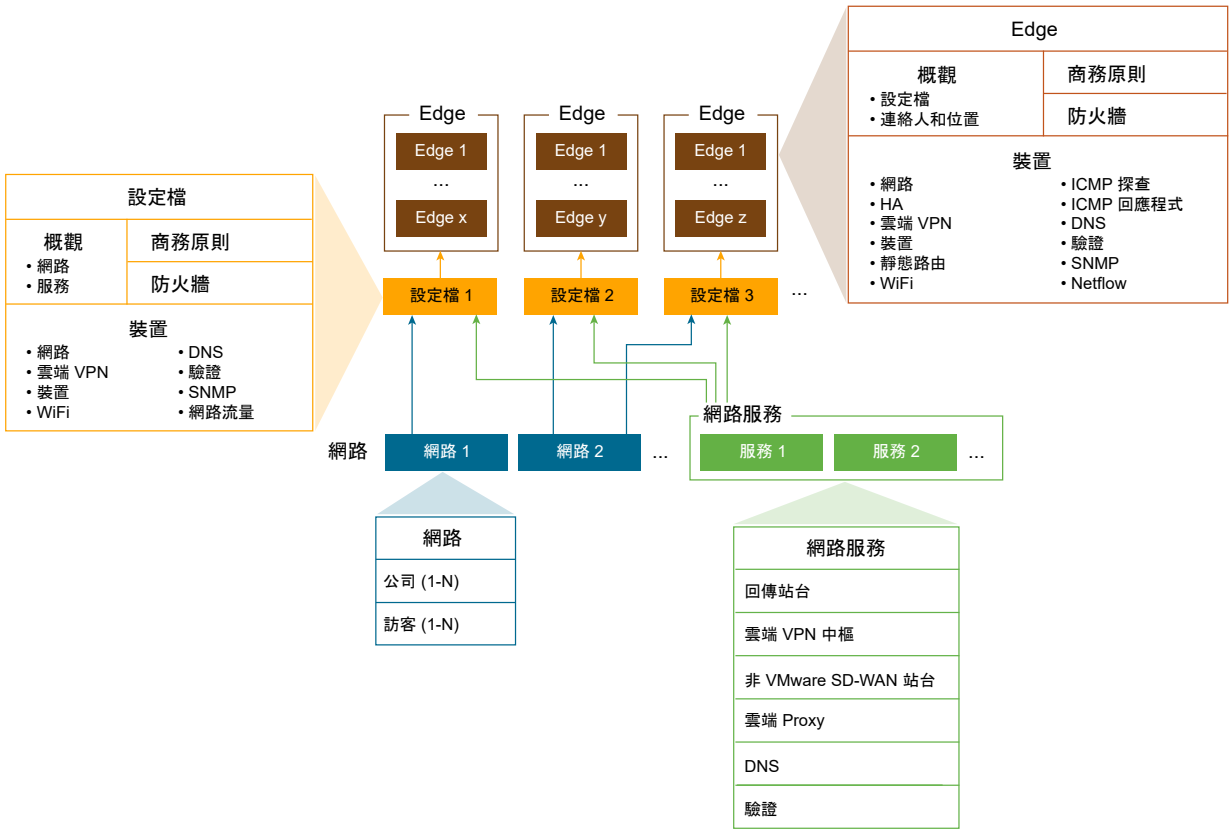
組態

VMware 服務有四個具有階層關聯性的核心組態。在 SD-WAN Orchestrator 中建立這些組態。

下表提供組態的概觀。

組態	說明
網路 (Network)	定義基本網路設定，例如 IP 定址和 VLAN。網路可指定為公司或客體，且每個網路可能有多個定義。
網路服務 (Network Services)	定義 VMware 服務所使用的數個常用服務，例如回傳站台、雲端 VPN 中樞、Non VMware SD-WAN Sites、雲端 Proxy 服務、DNS 服務和驗證服務。
設定檔 (Profile)	定義可套用至多個 Edge 的範本組態。藉由選取網路和網路服務而設定的設定檔。一個設定檔可套用至一或多個 Edge 型號，以及定義 LAN、網際網路、無線 LAN 和 WAN Edge 介面的設定。設定檔也可提供 Wi-Fi 無線電、SNMP、Netflow、商務原則和防火牆組態的設定。
Edge	組態會提供可下載至 Edge 裝置的完整設定群組。Edge 組態是由選取的設定檔、選取的網路和網路服務的設定所組成的。Edge 組態也可覆寫設定，或將已排序的原則新增至設定檔、網路和網路服務中定義的原則。

下圖顯示多個 Edge、設定檔、網路和網路服務的關聯性和組態設定詳細概觀。



單一設定檔可指派給多個 Edge。個別網路組態可在多個設定檔中使用。網路服務組態會用於所有設定檔中。

網路

網路是定義 Edge 的網路位址空間和 VLAN 指派的標準組態。您可以設定下列網路類型：

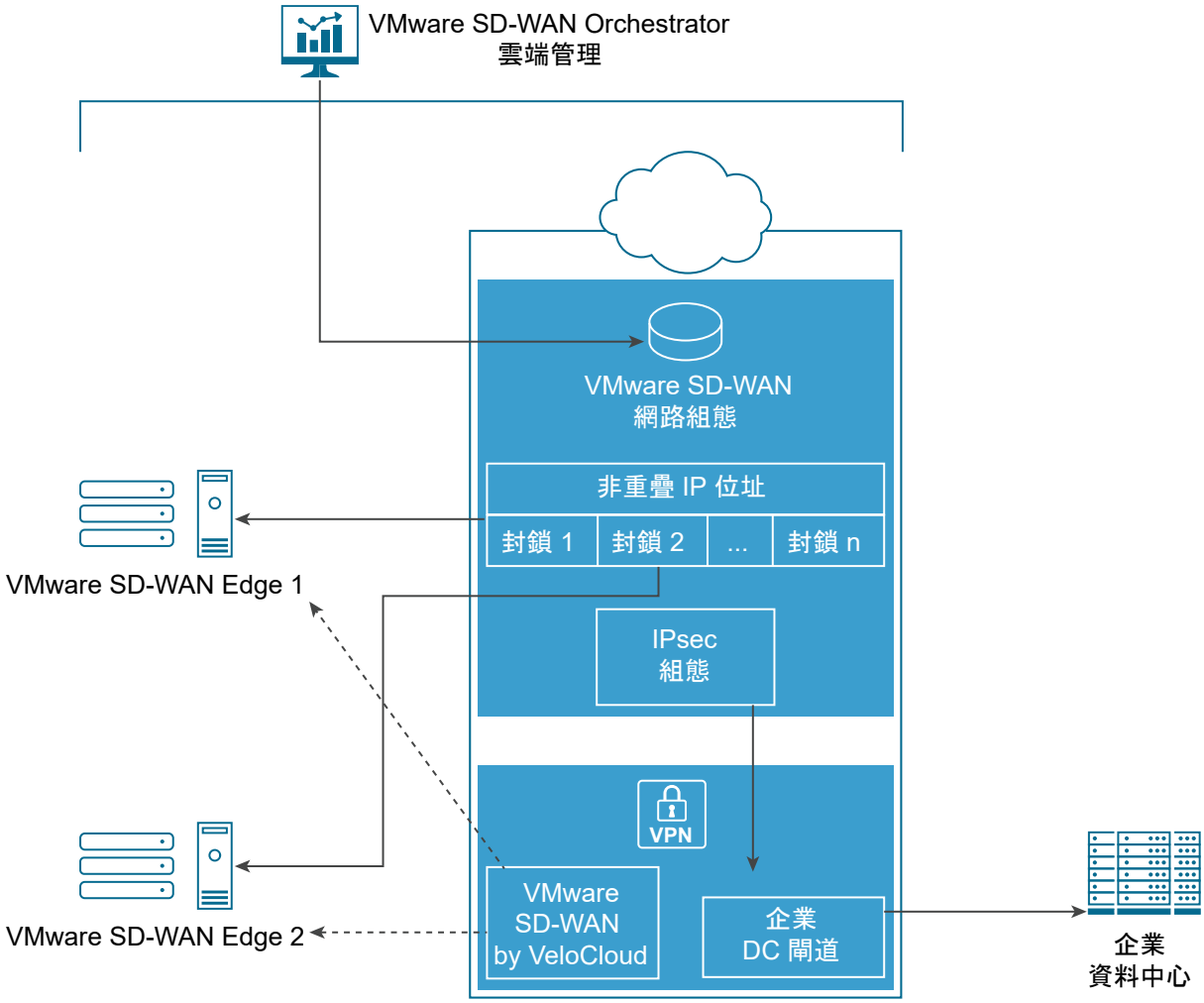
- 公司或受信任網路，其可透過重疊位址或非重疊位址進行設定。
- 客體或不受信任的網路，其一律會使用重疊位址。

您可以定義多個公司和客體網路，並將 VLAN 指派給這兩個網路。

在位址重疊的情況下，所有使用網路的 Edge 都有相同的位址空間。重疊位址會與非 VPN 組態相關聯。

在非重疊位址中，位址空間會分成位址數目相同的區塊。非重疊位址會與 VPN 組態相關聯。位址區塊會指派給使用網路的 Edge，而使每個 Edge 都具有一組唯一的位址。**Edge 對 Edge (Edge-to-Edge)** 和 **Edge 對** Non VMware SD-WAN Site 的 VPN 通訊都需要非重疊位址。VMware 組態會建立存取企業資料中心閘道以進行 VPN 存取時所需的資訊。企業資料中心閘道的管理員會使用在 Non VMware SD-WAN Site VPN 設定期間產生的 IPSec 組態資訊，以將 VPN 通道設定為 Non VMware SD-WAN Site。

下列映像顯示如何將網路組態中的唯一 IP 位址區塊指派給 SD-WAN Edges。



備註 使用非重疊位址時，SD-WAN Orchestrator 會自動將位址區塊分配給 Edge。組態會根據可能使用網路組態的 Edge 數目上限進行。

網路服務

您可以定義企業網路服務，並在所有設定檔之間使用這些服務。這包括驗證、雲端 Proxy、Non VMware SD-WAN Sites 和 DNS 的服務。定義的網路服務僅在指派給設定檔時才會予以使用。

設定檔

設定檔是一種具名組態，可定義 VLAN、雲端 VPN 設定、有線和無線介面設定，以及網路服務，例如 DNS 設定、驗證設定、雲端 Proxy 設定，以及 Non VMware SD-WAN Sites 的 VPN 連線的清單。您可以使用設定檔為一或多個 SD-WAN Edges 定義標準組態。

設定檔可為針對 VPN 設定的 Edge 提供雲端 VPN 設定。雲端 VPN 設定可啟用或停用 Edge 對 Edge 和 Edge 對 Non VMware SD-WAN Site 的 VPN 連線。

設定檔也可定義商務原則和防火牆設定的規則和組態。

Edge

您可以將設定檔指派給 Edge，而 Edge 會從設定檔衍生大部分的組態。

您可以使用設定檔、網路或網路服務中定義的大多數設定，而無需在 Edge 組態中進行修改。但是，您可以覆寫 Edge 組態元素的設定，以針對特定案例量身定制 Edge。 其中包括介面、Wi-Fi 無線電設定、DNS、驗證、商務原則和防火牆的設定。

此外，您可以設定 Edge 以擴充設定檔或網路組態中不存在的設定。這包括子網路定址、靜態路由設定，以及用於連接埠轉送和 1:1 NAT 的輸入防火牆規則。

Orchestrator 組態工作流程

VMware 支援多個組態案例。下表列出一些常見案例：

案例	說明
SaaS	用於在 Edge 之間、對於 Non VMware SD-WAN Site 或 VMware SD-WAN Site 不需要 VPN 連線的 Edge。此工作流程假設公司網路的定址是使用重疊定址。
透過 VPN 的 Non VMware SD-WAN Site	用於需透過 VPN 連線至 Non VMware SD-WAN Site 的 Edge，例如 Amazon Web Services、Zscaler、Cisco ISR 或 ASR 1000 Series。此工作流程假設公司網路的定址是使用非重疊定址，且 Non VMware SD-WAN Sites 會定義於設定檔中。
VMware SD-WAN Site VPN	用於需透過 VPN 連線至 VMware SD-WAN Site 的 Edge，例如 Edge 中樞或雲端 VPN 中樞。此工作流程假設公司網路的定址是使用非重疊定址，且 VMware SD-WAN Sites 會定義於設定檔中。

對於每個案例，請依照下列順序在 SD-WAN Orchestrator 中執行組態：

步驟 1：網路

步驟 2：網路服務

步驟 3：設定檔

步驟 4：Edge

下表提供每個工作流程的快速入門組態的高層級概觀。您可以使用預先設定的網路、網路服務和設定檔組態進行快速入門組態。對於 VPN 組態，修改現有的 VPN 設定檔，並設定 VMware SD-WAN Site 或 Non VMware SD-WAN Site。最後一步是建立新的 Edge 並加以啟動。

快速入門設定步驟	SaaS	Non VMware SD-WAN Site VPN	VMware SD-WAN Site VPN
步驟 1：網路	選取快速入門網際網路	選取快速入門 VPN 網路	選取快速入門 VPN 網路
步驟 2：網路服務	使用預先設定的網路服務	使用預先設定的網路服務	使用預先設定的網路服務
步驟 3：設定檔	選取快速入門網際網路設定檔	選取快速入門 VPN 設定檔 啟用雲端 VPN 並設定 Non VMware SD-WAN Sites	選取快速入門 VPN 設定檔 啟用雲端 VPN 並設定 VMware SD-WAN Sites
步驟 4：Edge	新增 Edge 並啟動 Edge	新增 Edge 並啟動 Edge	新增 Edge 並啟動 Edge

如需詳細資訊，請參閱啟用 Edge。

支援的瀏覽器

若要獲得最佳體驗，VMware 建議使用 Google Chrome 或 Mozilla Firefox。

SD-WAN Orchestrator 支援下列瀏覽器。

合格的瀏覽器	瀏覽器版本
Google Chrome	77 – 79.0.3945.130
Firefox	69.0.2 - 72.0.2
Internet Explorer	11.765.17134.0 - 11.592.18362.0
Microsoft Edge	42.17134.1.0 - 44.18362.449.0
Safari	12.1.2 - 13.0.3

支援的數據機

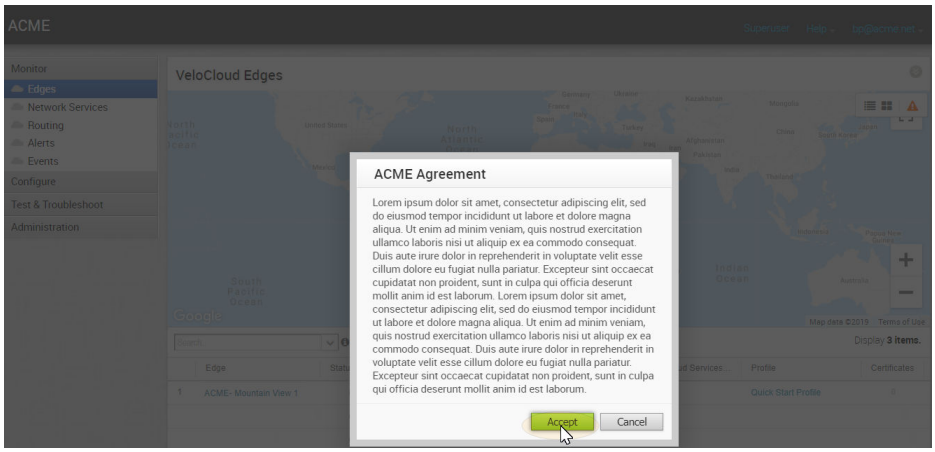
本節說明如何取得支援的數據機清單。

如需受支援數據機的詳細清單，請參閱 https://sdwan.vmware.com/get-started/supported-modems。

使用者合約

4

企業超級使用者或合作夥伴超級使用者在登入 SD-WAN Orchestrator 時可能會看到使用者合約。使用者必須接受合約，才能取得 SD-WAN Orchestrator 的存取權。如果使用者不接受合約，則會自動登出。



企業使用者使用 SSO 登入 VMware SD-WAN Orchestrator

5

說明如何以企業使用者的身分使用單一登入 (SSO) 登入 VMware SD-WAN Orchestrator。

若要以企業使用者的身分使用 SSO 登入 SD-WAN Orchestrator：

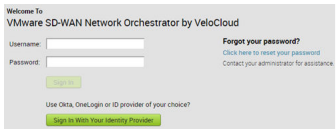
必要條件

- 請確定您已在 SD-WAN Orchestrator 中設定 SSO 驗證。如需詳細資訊，請參閱設定企業使用者的單一登入。
- 請確定您已在慣用 IDP 中為 SSO 設定角色、使用者和 OIDC 應用程式。如需詳細資訊，請參閱設定單一登入的 IDP。

程序

1 在網頁瀏覽器中，以企業使用者的身分啟動 SD-WAN Orchestrator 應用程式。

此時會顯示 VMware SD-WAN Orchestrator 畫面。



2 按一下**使用您的身分識別提供者登入 (Sign In With Your Identity Provider)**。

3 在**輸入您的組織網域 (Enter your Organization Domain)** 文字方塊中，輸入用於 SSO 組態的網域名稱，然後按一下**登入 (Sign In)**。

針對 SSO 設定的 IDP 將會驗證使用者，並將使用者重新導向至已設定的 SD-WAN Orchestrator URL。

備註 使用者一旦使用 SSO 登入 SD-WAN Orchestrator，即不允許他們再次使用原生使用者的身分重新登入。

監控企業

6

SD-WAN Orchestrator 提供監控功能，可讓您觀察 VMware SD-WAN Edges 的各種效能及營運特性。在導覽面板的**監控 (Monitor)** 區域可存取監控功能。

本章節討論下列主題：

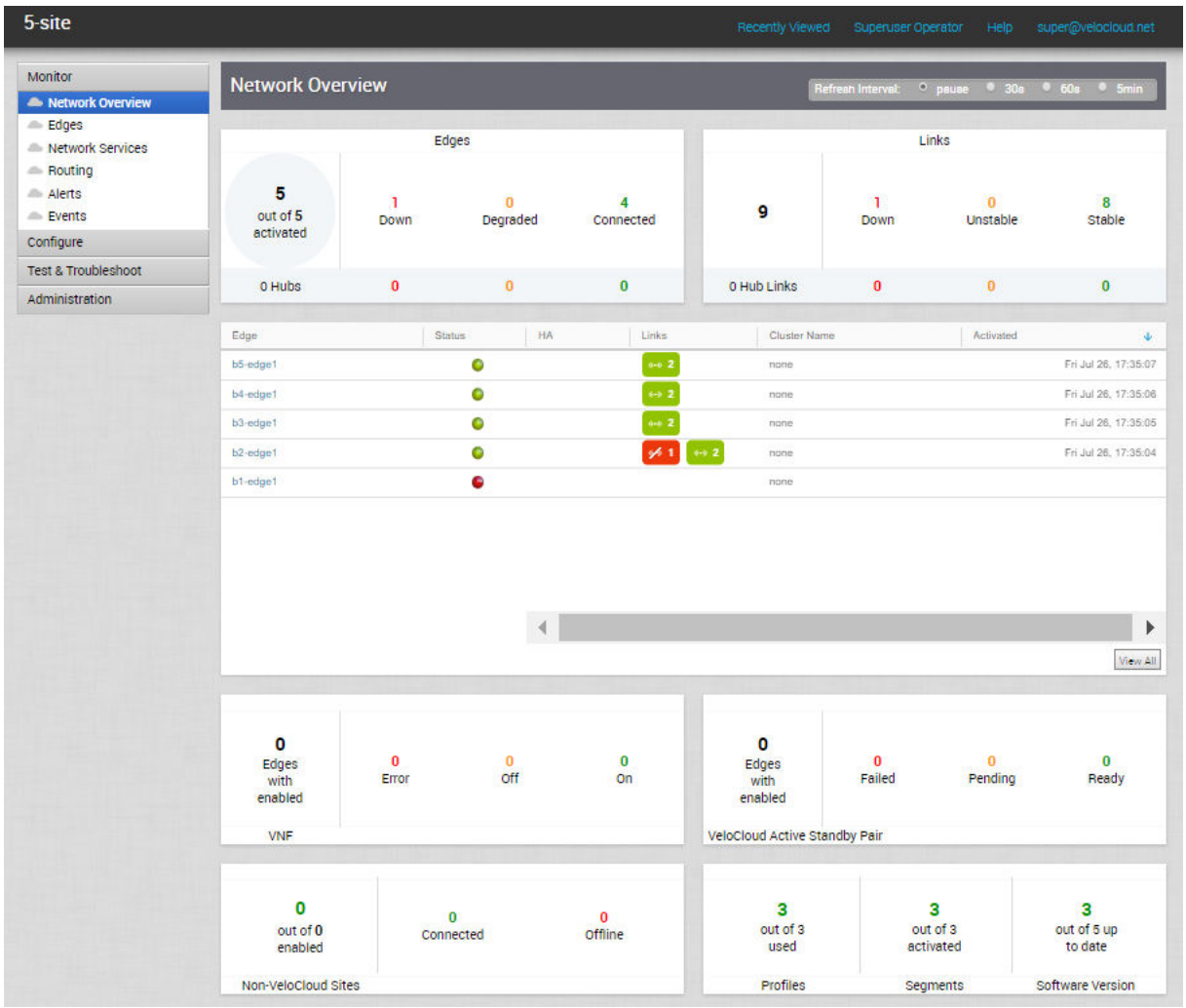
監控導覽面板

導覽面板中的**監控 (Monitor)** 下會顯示下列監控功能。

- 網路概觀
- 監控 Edge
- 監控網路服務
- 監控路由
- 監控警示
- 監控事件

網路概觀

網路概觀 (Network Overview) 功能可協助您藉由檢查 Edge 和連結 (已啟動 Edge) 狀態摘要來監控網路。在導覽面板中按一下**監控 (Monitor)** > **網路概觀 (Network Overview)**，會開啟**網路概觀 (Network Overview)** 畫面，其中提供下列資訊的視覺摘要：執行 SD-WAN Edge 裝置的企業、Non VMware SD-WAN Sites、設定檔、區段、軟體版本，及其系統組態時間和執行階段狀態。



下表說明 Edge、Edge 中樞、連結和中樞連結的連線狀態類型與定義：

顏色	意義
綠色	已連線
琥珀色	已降級
紅色	關閉

網路概觀 (Network Overview) 畫面會在三個儀表板區段中顯示關於網路的整體摘要資訊：

- SD-WAN Edge 統計資料 - 包含下列關於 Edge 和連結的資訊：
  - Edge 總數
  - Edge 中樞總數
  - 連結總數
  - 中樞連結總數

  - Edge/Edge 中樞計數 (已連線、已降級和關閉)
  - 連結/中樞連結計數 (穩定、不穩定和關閉)
- 摘要儀表板資料表 - 包含一個資料表，系統會根據在 SD-WAN Edge 統計資料區段中選取的篩選準則，顯示依上次連絡時間排序的前十個 Edge、Edge 中樞、連結或中樞連結。
- 非 Edge 統計資料 - 包含下列非 Edge 相關資訊：
  - 已啟用虛擬網路功能 (VNF) 的 Edge 總數
  - 已啟用 VNF 的 Edge 計數 (錯誤、開啟和關閉)
  - 已啟用 VMware 主動備用配對的 Edge 總數
  - 已啟用 VMware 主動備用配對的 Edge 計數 (失敗、擱置中和就緒)
  - 已啟用 Non VMware SD-WAN Sites 的總數
  - Non VMware SD-WAN Sites 計數 (已連線和離線)
  - 為企業設定的設定檔總數之中，已使用的設定檔計數。
  - 為企業設定的區段總數之中，已啟動的區段計數。
  - 為企業設定的 Edge 總數之中，具有最新軟體版本的 Edge 計數。

    備註 Edge 的最低支援版本為 2.4.0。您可以使用系統內容 `product.edge.version.minimumSupported`，變更要與 Edge 進行比較的目標 Edge 版本。

您也可以按一下**網路概觀 (Network Overview)** 畫面中特定項目或度量的連結，以取得該項目的詳細資訊。例如，按一下摘要儀表板資料表中的 **Edge** 連結，系統便會將您導向至所選 Edge 的 Edge 詳細資料儀表板。

您可以將 [網路概觀 (Network Overview)] 儀表板畫面中顯示之資訊的重新整理時間間隔設定為下列其中一個選項：

- **暫停 (pause)**
- **30 秒 (30s)**
- **60 秒 (60s)**
- **5 分鐘 (5min)**

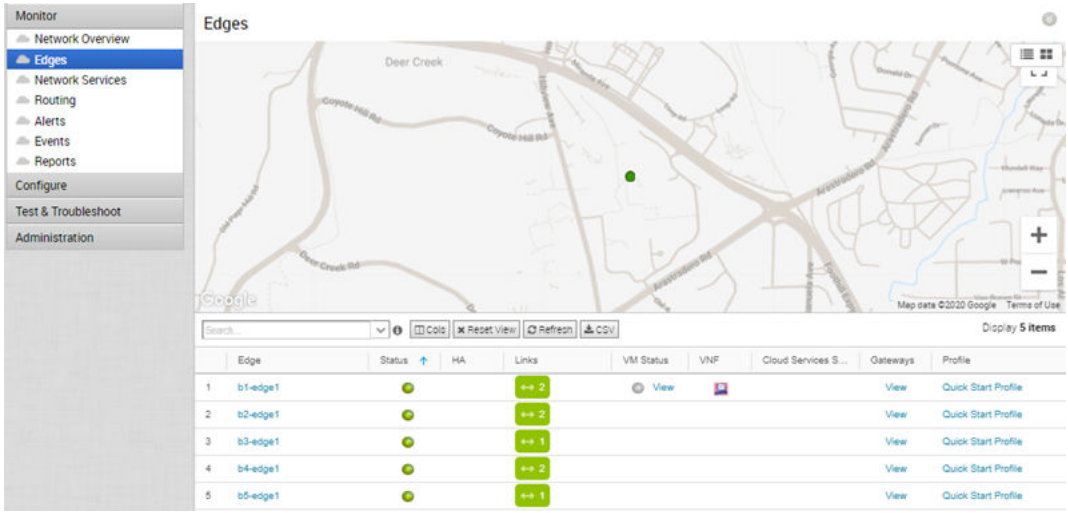
監控 Edge

您可以監控 Edge 的狀態，並檢視每個 Edge 的詳細資料，例如 WAN 連結、Edge 最常使用的前幾個應用程式、透過網路來源和流量目的地的使用量資料、網路流量的商務優先順序、系統資訊、連線至 Edge 之閘道的詳細資料等。

若要監控 Edge 詳細資料：

1 在企業入口網站中，按一下**監控 (Monitor) > Edge**。

2 **Edge** 頁面會顯示與企業相關聯的 Edge。



此頁面會顯示 Edge 的下列詳細資料：

- Edge 資料表 – 列出網路中佈建的所有 Edge。
- 搜尋 – 輸入用來搜尋特定詳細資料的詞彙。按一下下拉式箭頭，依特定準則篩選視圖。
- 資料行 – 按一下以顯示或隱藏資料行。依預設會顯示 Edge 和狀態資訊。
- 重設 – 按一下以將視圖重設為預設設定。
- 重新整理 – 按一下以使用最新資料重新整理顯示的詳細資料。
- 匯出 – 按一下將所有資料以 CSV 格式匯出至檔案。

按一下 Edge 的連結，可檢視與所選 Edge 有關的詳細資料。按一下相關的索引標籤，可檢視對應的資訊。每個索引標籤都會在頂端顯示一個下拉式清單，可讓您選取特定的時段。索引標籤會顯示所選期間的詳細資料。

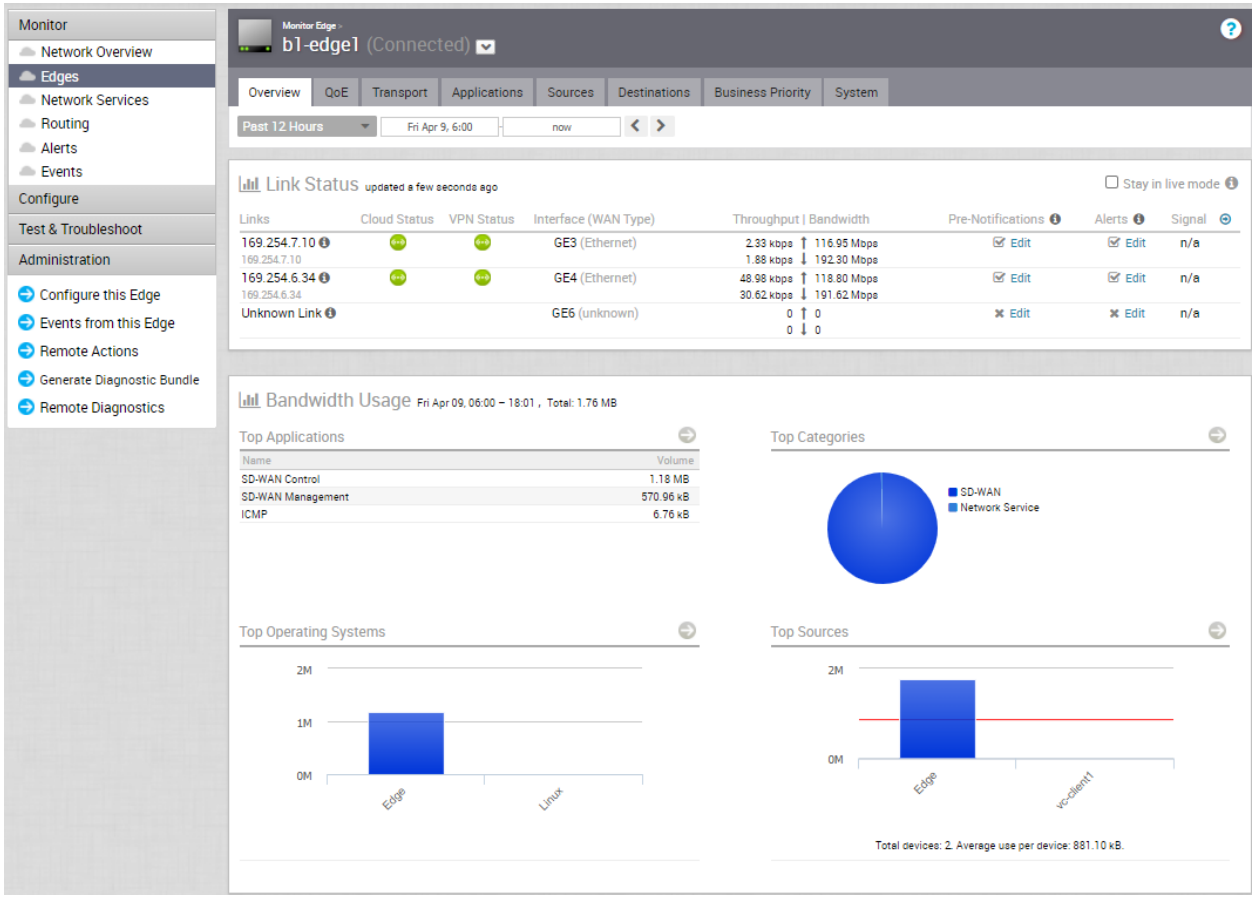
對於每個 Edge，您可以檢視下列詳細資料：

- 概觀索引標籤
- QoE 索引標籤
- 傳輸索引標籤
- 應用程式索引標籤
- 來源索引標籤
- 目的地索引標籤
- 商務優先順序索引標籤
- 系統索引標籤

概觀索引標籤

在監控儀表板中，Edge 的 [概觀 (Overview)] 索引標籤會顯示 WAN 連結以及頻寬耗用量和網路使用量的詳細資料。

概觀 (Overview) 索引標籤會顯示具有狀態和頻寬耗用量之連結的詳細資料。



您可以選擇**保持即時模式 (Stay in live mode)** 核取方塊，以選擇即時檢視 Edge 資訊。此模式啟用時，系統會執行 Edge 的即時監控，並且在每次發生變更時更新頁面中的資料。在一段時間後，即時模式會自動進入離線模式，以降低網路負載。

[連結狀態 (Links Status)] 區段會顯示下列詳細資料：

選項	**說明**
連結 (Links)	所選 Edge 的介面和 WAN 連結
雲端狀態 (Cloud Status)	對閘道連結的連線狀態。
VPN 狀態 (VPN Status)	IPSec 通道至閘道連結的連線狀態。
介面 (WAN 類型)	連線至連結的介面。
總流量 (Throughput)	指定方向的位元組總計除以時間總計。時間總計是從 Edge 上傳統計資料的週期。依預設，Orchestrator 中的週期為 5 分鐘。
頻寬 (Bandwidth)	在指定的路徑之間傳輸資料的最大速率。系統會同時顯示上游和下游的頻寬詳細資料。
預先通知 (Pre-Notifications)	允許以啟用或停用已傳送給操作員的警示。按一下**編輯 (Edit)** 以修改通知設定。

選項	說明
警示	允許以啟用或停用已傳送給企業客戶的警示。按一下**編輯 (Edit)**以修改通知設定。
訊號 (Signal)	有關訊號強度的資訊。
延遲 (Latency)	封包透過網路從來源傳輸至目的地所花費的時間。系統會同時顯示上游和下游的延遲詳細資料。
抖動 (Jitter)	因網路擁塞或路由變更而導致封包接收延遲的變化。系統會同時顯示上游和下游的抖動詳細資料。
封包遺失 (Packet loss)	當一或多個封包無法到達預定目的地時，即會發生封包遺失。當路徑序號遺失，且不會在重新排序時間範圍內到達時，即會計算遺失的封包。「過度延遲」的封包會計入遺失的封包。

頻寬使用量 (Bandwidth Usage) 區段會以圖形表示下列項目的頻寬和網路使用量：應用程式、類別、作業系統以及 Edge 的來源。在各個面板中按一下箭頭，可導覽至對應的索引標籤，並檢視更多詳細資料。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

備註 連結上 SD-WAN 控制流量的最小資料耗用量為每個月 1.5 到 2 GB，視路徑數目而定。

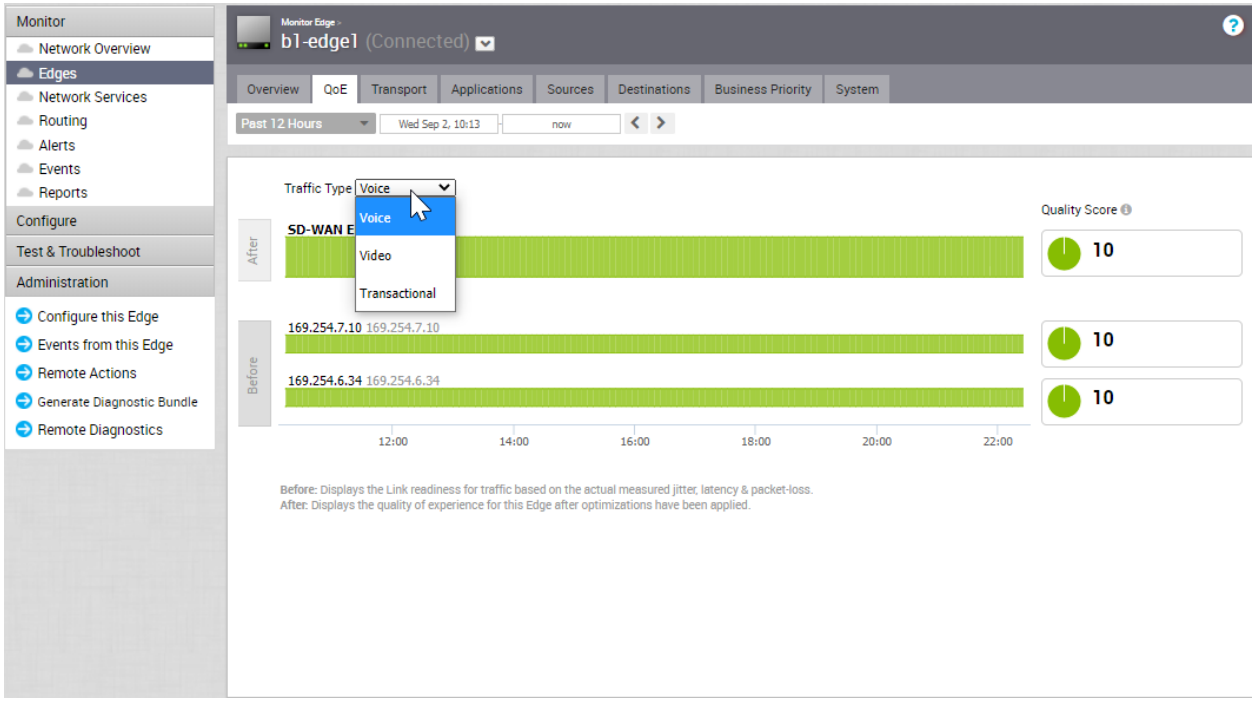
QoE 索引標籤

VMware **體驗品質 (QoE) (Quality of Experience (QoE))** 索引標籤會顯示不同應用程式的品質評分。品質評分會針對網路在一段時間內所能提供的應用程式體驗品質進行評分。

按一下**監控 (Monitor) > Edge > QoE** 索引標籤，以檢視下列詳細資料。

流量類型

在 **QoE** 索引標籤中，您可以監控三種不同的流量類型 (語音、視訊和交易式)。您可以將游標暫留在 WAN 網路連結或彙總連結上方，以顯示延遲、抖動和封包遺失的摘要。



品質評分

品質評分會針對網路在指定的時間範圍內所能提供的應用程式體驗品質進行評分。舉例來說，應用程式包括：視訊、語音和交易式。下表顯示 QoE 評等選項。

評等顏色	評等選項	定義
綠色	良好	所有度量皆優於目標臨界值。符合/超過應用程式 SLA。
黃色	尚可	部分或所有度量介於目標與最大值之間。部分符合應用程式 SLA。
紅色	不佳	部分或所有度量皆已達到或超過最大值。不符合應用程式 SLA。

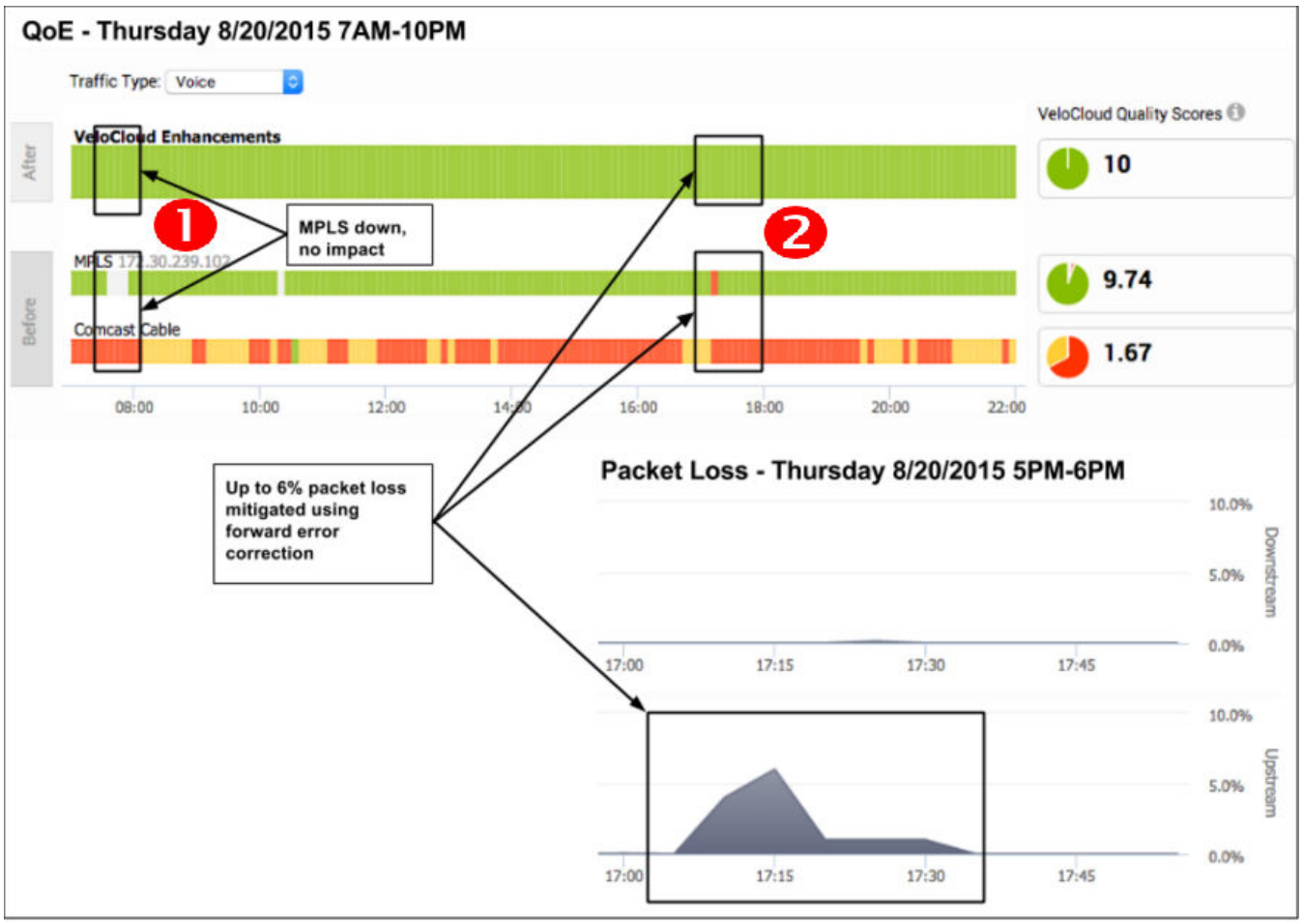
QoE 範例

下圖顯示 QoE 範例，並附上語音流量案例問題發生前後的比較，以及 VMware 如何加以解決。下圖中的紅色數字代表資料表中的案例編號。

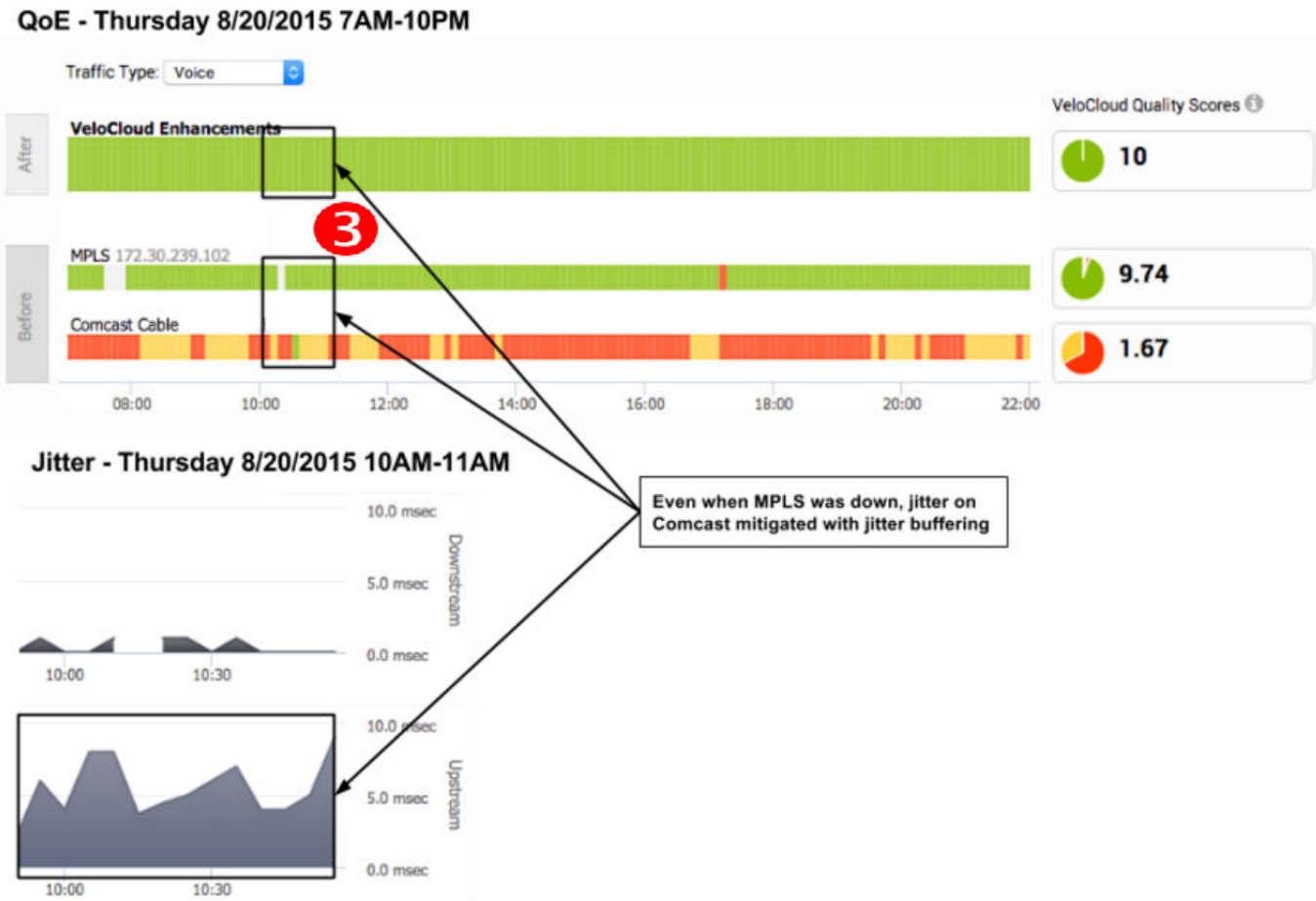
QoE 範例資料表

案例	問題	VMware 解決方案
1	MPLS 已關閉	連結操控
2	封包遺失	前饋式錯誤修正
3	MPLS 已關閉；Comcast 發生抖動	連結操控和抖動緩衝處理

案例 1 和 2：連結操控和前饋式錯誤修正解決方案範例



案例 3：連結操控和抖動緩衝處理解決方案範例



傳輸索引標籤

您可以監控連線至特定 Edge 的 WAN 連結及其狀態、介面詳細資料和其他度量。

在任何時間點，您都可以在**監控 (Monitor) > Edge > 傳輸 (Transport)** 索引標籤中檢視用於流量的連結或傳輸群組，以及傳送的資料量。

當您按一下**傳輸 (Transport)** 索引標籤時，依預設會顯示**連結 (Links)** 畫面。此畫面會針對您的連結顯示已傳送和接收的資料。與 Edge 相關聯的連結會顯示在畫面底部的 [連結 (Link)] 資料行下方，並顯示雲端、VPN、WAN 介面的狀態、應用程式詳細資料和位元組詳細資料。

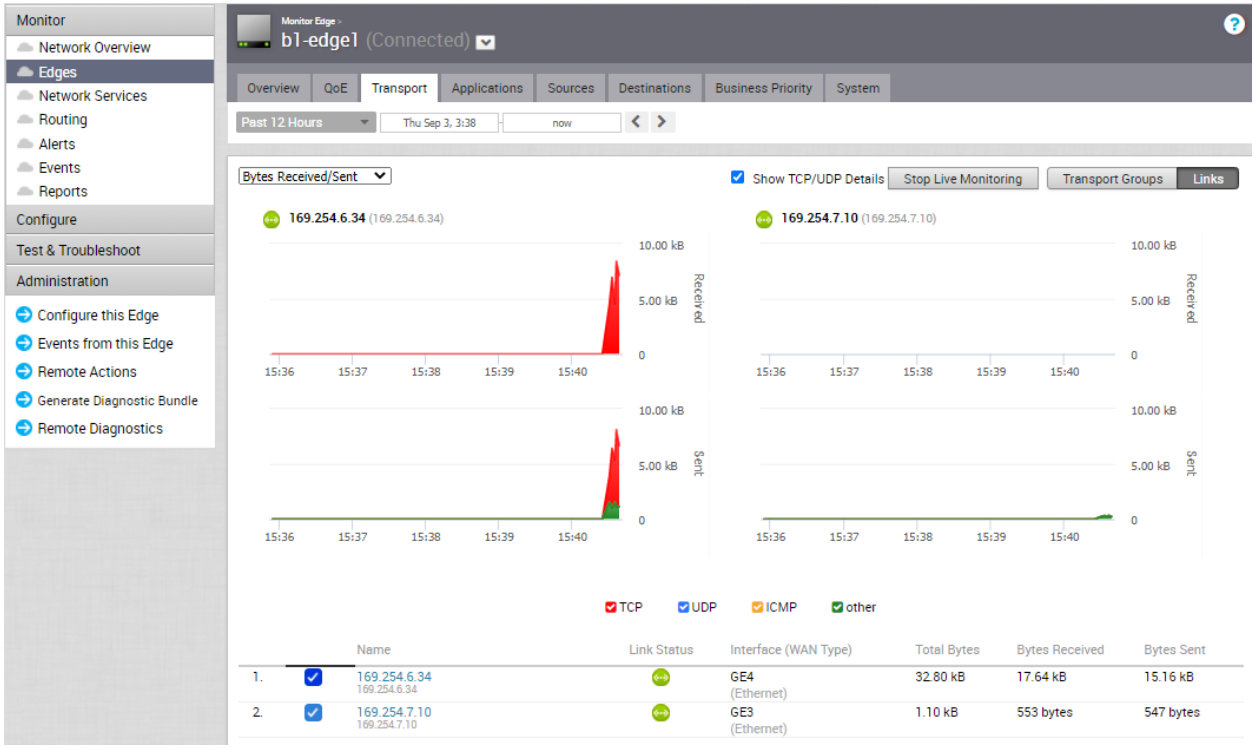
將滑鼠暫留在圖形上方，可檢視更多詳細資料。

在頁面頂端，您可以選擇特定的時段，以檢視在選取的持續時間內所使用連結的詳細資料。

按一下**傳輸群組 (Transport Groups)**，以檢視分組為下列其中一個類別的連結：公用有線 (Public Wired)、公用無線 (Public Wireless) 或私人有線 (Private Wired)。

您可以按一下**開始即時監控 (Start Live Monitoring)** 選項，以選擇即時檢視資訊。此模式啟用時，您可以檢視連結和傳輸群組的即時監控。即時監控可用來執行作用中的測試和計算平均總流量。這也有利於安全合規性的疑難排解，以及即時監控流量原則的使用情形。

在**即時監控 (Live Monitoring)** 畫面中，選取**顯示 TCP/UDP 詳細資料 (Show TCP/UDP Details)** 核取方塊，以檢視通訊協定層級的連結使用量詳細資料。

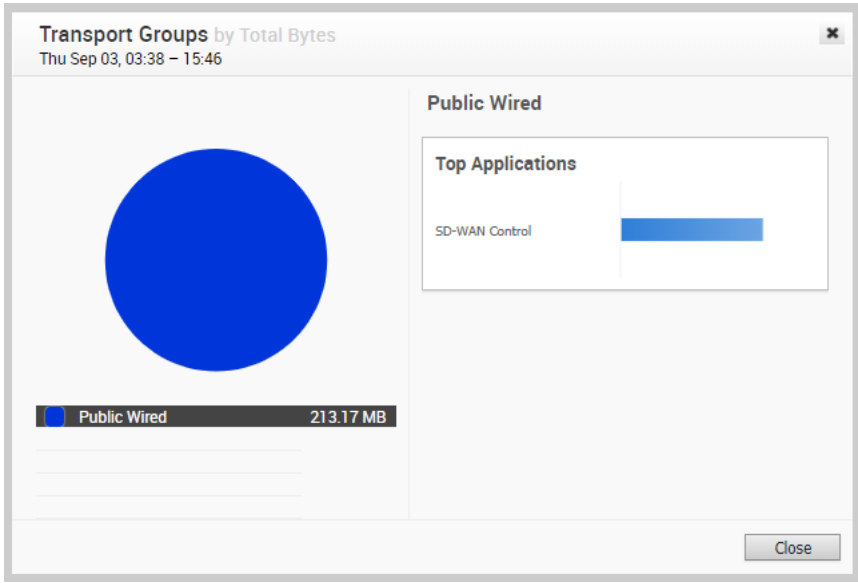


依預設會啟用**平均調整 Y 軸 (Scale Y-axis evenly)** 核取方塊。此選項會同步圖表之間的 Y 軸。如有需要，您可以停用此選項。

從下拉式功能表中選擇度量，以檢視與所選參數相關的詳細資料。底部面板會針對連結或傳輸群組顯示所選度量的詳細資料。

按一下連結名稱或傳輸群組前面的箭頭以檢視詳細資料明細。若要檢視具有更多詳細資料的深入報告，請按一下度量資料行中顯示的連結。

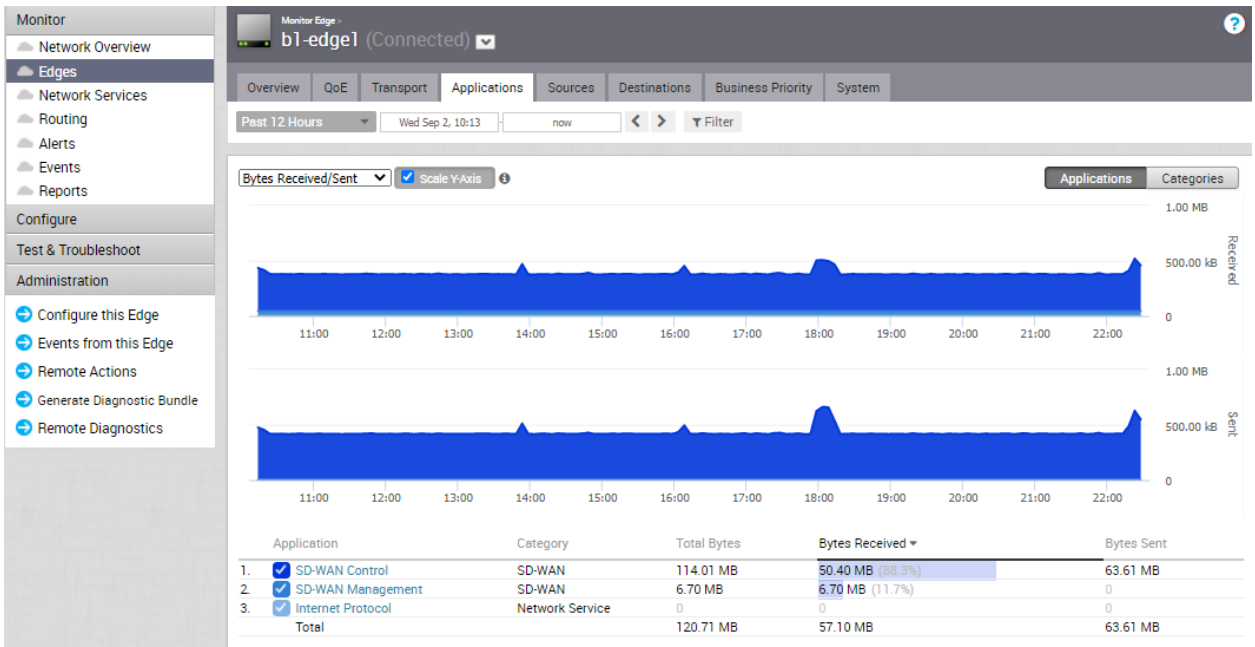
下圖顯示具有最高排名應用程式之傳輸群組的詳細報告。



應用程式索引標籤

您可以監控特定 Edge 所使用應用程式或應用程式類別的網路使用量。

按一下**監控 (Monitor) > Edge > 應用程式 (Applications)** 索引標籤，以檢視下列項目：



在頁面頂端，您可以選擇特定的時段，以檢視在選取持續時間內所使用應用程式的詳細資料。

按一下**類別 (Categories)**，以檢視分組為類別的類似應用程式。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

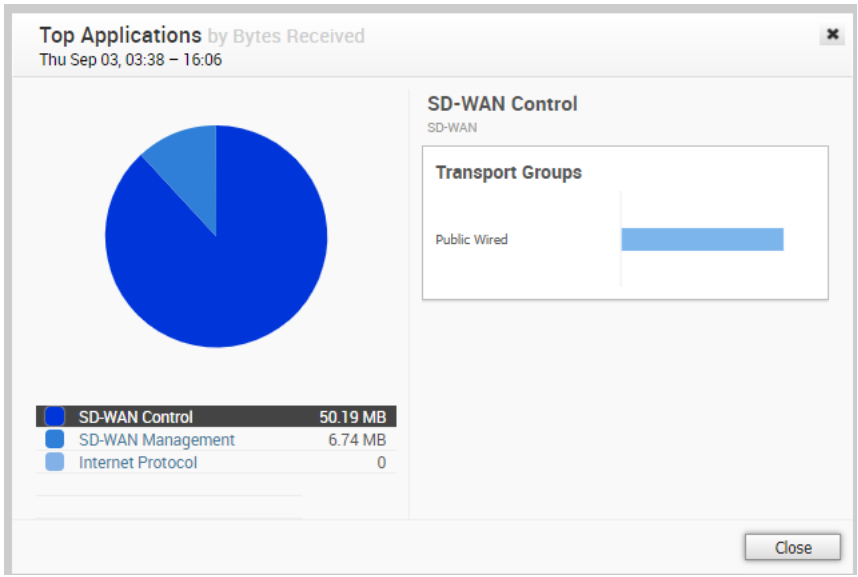
從下拉式功能表中選擇度量，以檢視與所選參數相關的詳細資料。

依預設會啟用**平均調整 Y 軸 (Scale Y-axis evenly)** 核取方塊。此選項會同步圖表之間的 Y 軸。如有需要，您可以停用此選項。

底部面板會針對應用程式或類別顯示所選度量的詳細資料。

若要檢視具有更多詳細資料的深入報告，請按一下度量資料行中顯示的連結。

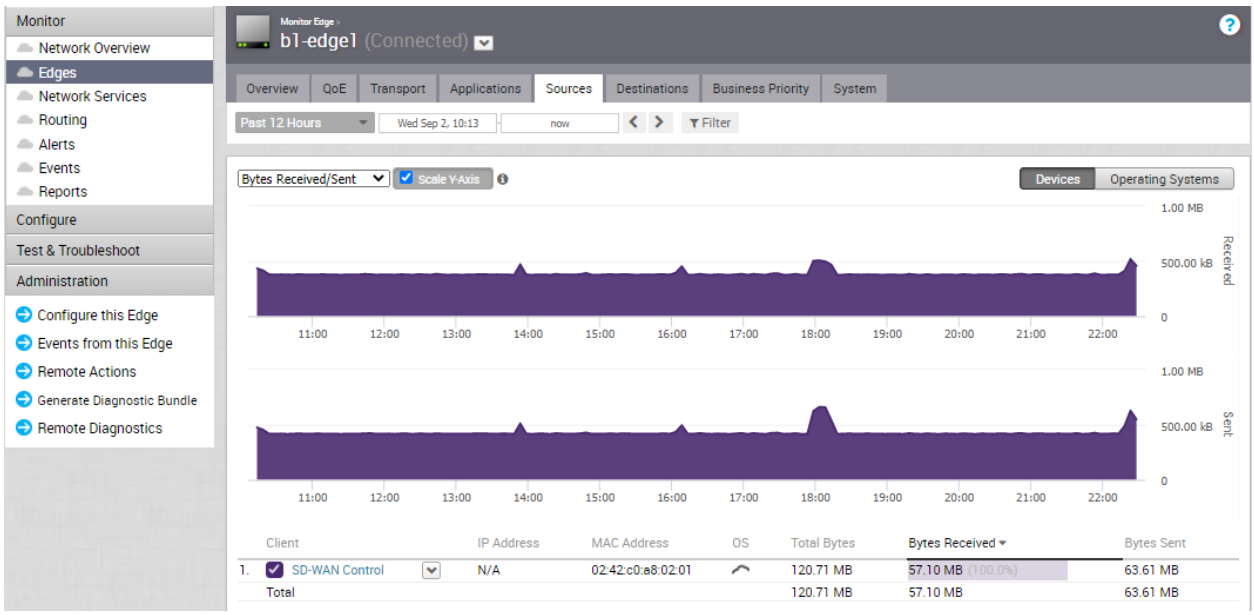
下圖顯示最高排名應用程式的詳細報告。



來源索引標籤

您可以針對特定 Edge 監控其裝置和作業系統的網路使用量。

按一下**監控 (Monitor) > Edge > 來源 (Sources)**，以檢視下列項目：



在頁面頂端，您可以選擇特定的時段，以檢視在選取的持續時間內使用之用戶端的詳細資料。

按一下**作業系統 (Operating Systems)**，以根據裝置中使用的作業系統來檢視報告。

從下拉式功能表中選擇度量，以檢視與所選參數相關的詳細資料。

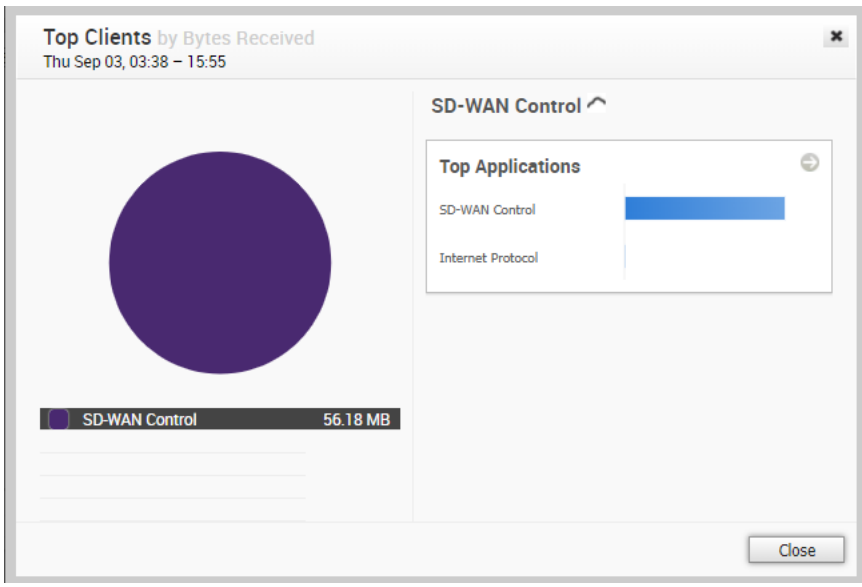
依預設會啟用**平均調整 Y 軸 (Scale Y-axis evenly)** 核取方塊。此選項會同步圖表之間的 Y 軸。如有需要，您可以停用此選項。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

底部面板會針對裝置或作業系統顯示所選度量的詳細資料。

若要檢視具有更多詳細資料的深入報告，請按一下度量資料行中顯示的連結。

下圖顯示最高排名用戶端的詳細報告。

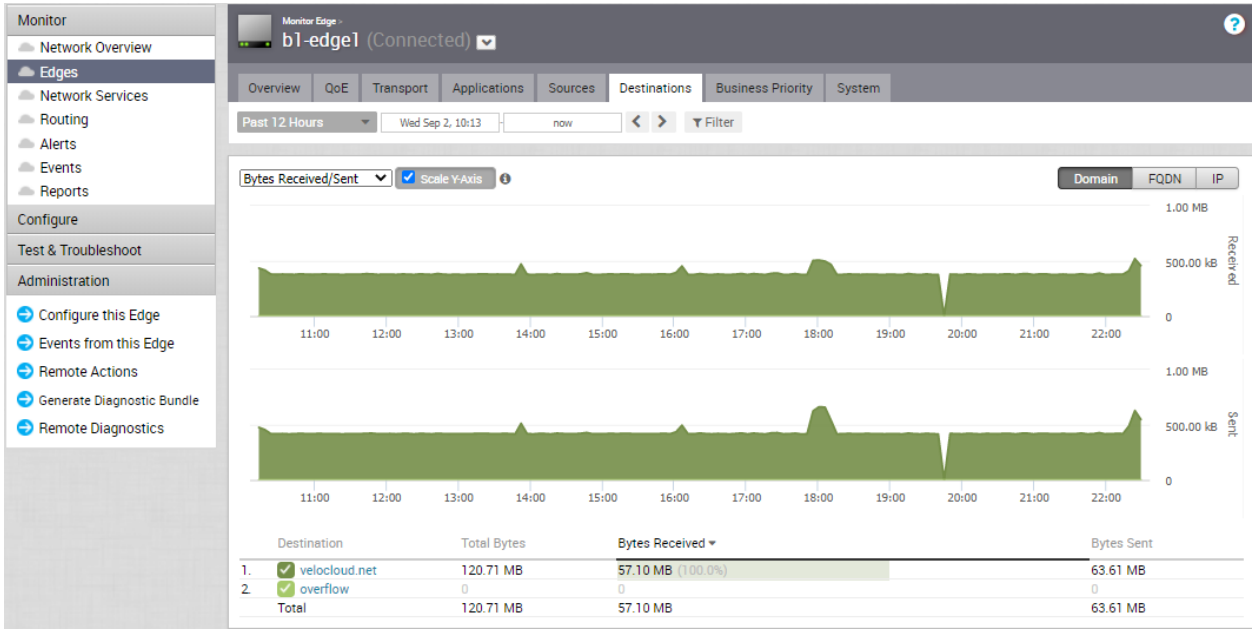


按一下**最高排名應用程式 (Top Applications)** 旁顯示的箭頭，以導覽至**應用程式 (Applications)** 索引標籤。

目的地索引標籤

您可以監控網路流量目的地的網路使用量資料。

按一下**監控 (Monitor) > Edge > 目的地(Destinations)** 索引標籤，以檢視下列項目：



在頁面頂端，您可以選擇特定的時段，以檢視在選取的持續時間內所使用目的地的詳細資料。

您可以根據**網域 (Domain)**、**FQDN** 或 **IP** 位址，來檢視目的地的報告。按一下相關類型可檢視對應的資訊。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

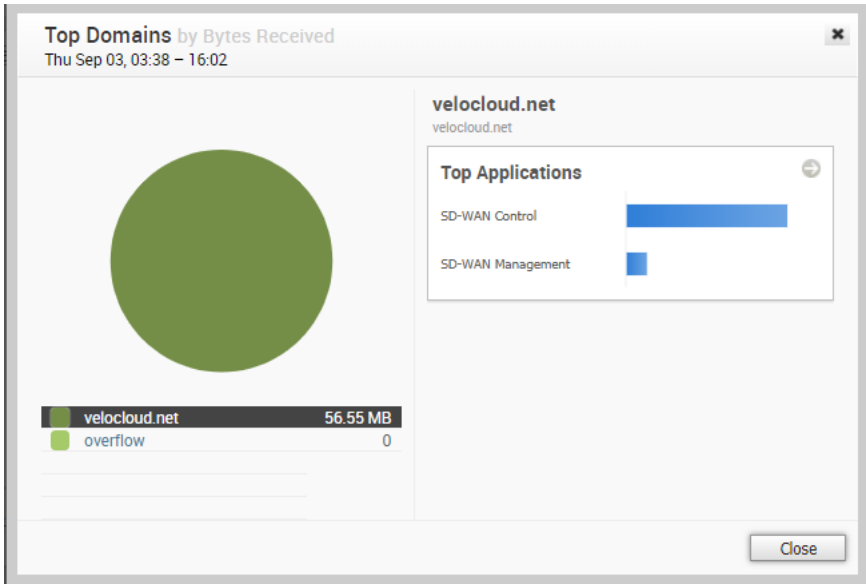
從下拉式功能表中選擇度量，以檢視與所選參數相關的詳細資料。

依預設會啟用**平均調整 Y 軸 (Scale Y-axis evenly)** 核取方塊。此選項會同步圖表之間的 Y 軸。如有需要，您可以停用此選項。

底部面板會依據選取的類型，針對目的地顯示所選度量的詳細資料。

若要檢視具有更多詳細資料的深入報告，請按一下度量資料行中顯示的連結。

下圖顯示最高排名網域的詳細報告。

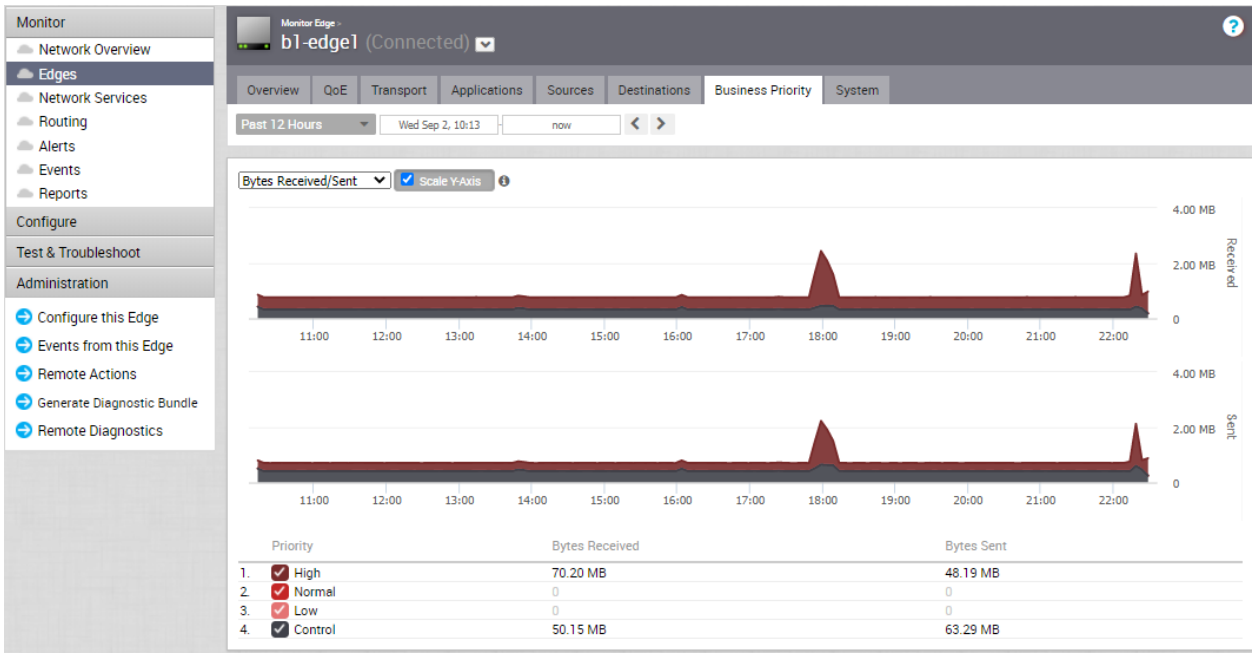


按一下**最高排名應用程式 (Top Applications)** 旁顯示的箭頭，以導覽至**應用程式 (Applications)** 索引標籤。

商務優先順序索引標籤

您可以根據特定 Edge 的優先順序和相關聯的網絡使用量資料，來監控商務原則特性。

按一下**監控 (Monitor) > Edge > 商務優先順序 (Business Priority)** 索引標籤，以檢視下列項目：



在頁面頂端，您可以選擇特定的時段，以檢視所選持續時間內的優先順序詳細資料。

從下拉式功能表中選擇度量，以檢視與所選參數相關的詳細資料。

依預設會啟用**平均調整 Y 軸 (Scale Y-axis evenly)** 核取方塊。此選項會同步圖表之間的 Y 軸。如有需要，您可以停用此選項。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

底部面板會針對商務優先順序顯示所選度量的詳細資料。

系統索引標籤

您可以針對特定 Edge 檢視系統的詳細網路使用量。

若要檢視系統資訊的詳細資料：

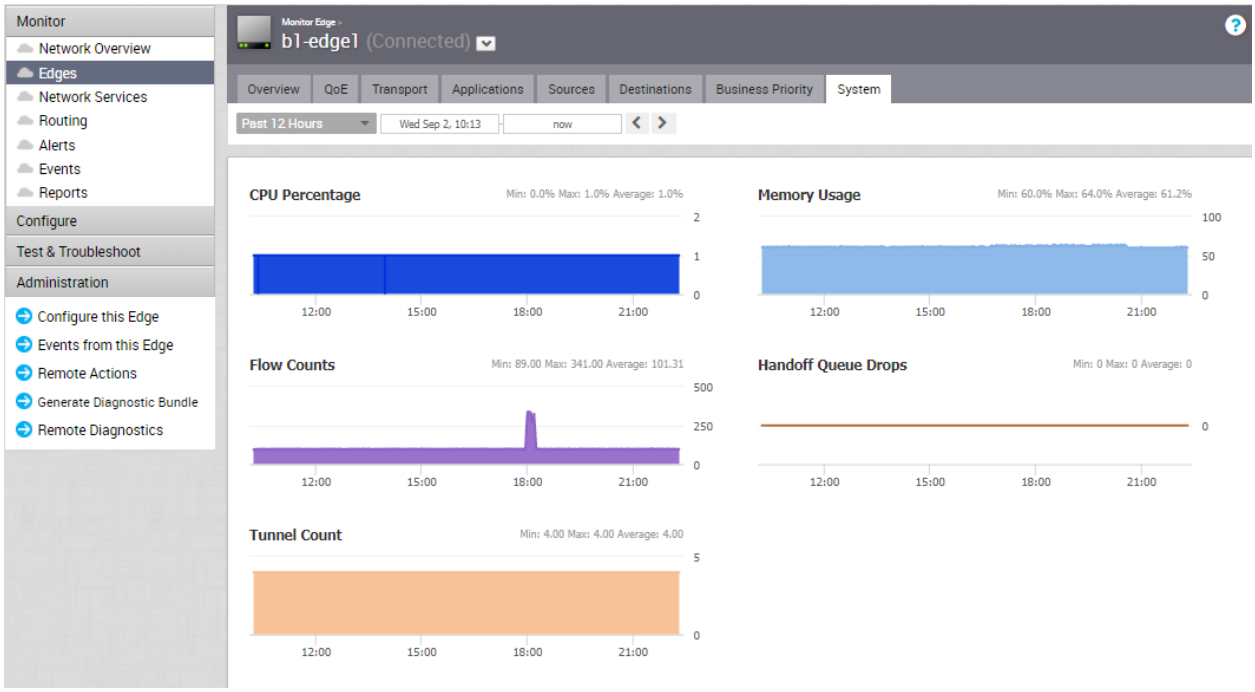
程序

1 在企業入口網站中，按一下**監控 (Monitor) > Edge**。

2 按一下 Edge 的連結，然後按一下**系統 (System)** 索引標籤。

結果

系統 (System) 索引標籤會針對選取的 Edge 顯示系統的網路使用量詳細資料。



此頁面會以圖形表示下列項目在所選持續時間內的使用量詳細資料，以及最小值、最大值和平均值。

- **CPU 百分比 (CPU Percentage)** – CPU 使用率的百分比。
- **記憶體使用量 (Memory Usage)** – 記憶體使用量的百分比。
- **流量計數 (Flow Counts)** – 流量的計數。
- **遞交佇列捨棄數 (Handoff Queue Drops)** – 因已排入佇列遞交而捨棄的封包計數。
- **通道計數 (Tunnel Count)** – 通道工作階段的計數。

將滑鼠暫留在圖形上方，可檢視更多詳細資料。

流量統計資料彙總和保留

在 3.3.0 版中，SD-WAN Orchestrator 只會儲存具有高解析度的流量統計資料，以提供可見度和疑難排解功能。從 3.3.2 版開始，SD-WAN Orchestrator 會每日彙總每個 Edge 的流量統計資料，而支援將流量統計資料保留長達一年。目前，僅支援內部部署客戶使用每日流量統計資料彙總。

彙總流量統計資料

SD-WAN Orchestrator 目前可將流量統計資料從較高的解析度 (每 5 分鐘一次) 彙總為解析度較低 (每 24 小時一次) 的可用形式。下表歸納流量統計資料彙總和保留的支援資訊。

表 6-1. 流量統計資料彙總支援

解決方案	3.3.0 前的彙總	3.3.0 後的彙總	3.3.2 後的彙總
高	5 分鐘	5 分鐘	5 分鐘
中	2 小時	已過時	不支援
低	8 小時	已過時	24 小時

表 6-2. 流量統計資料保留支援

解決方案	3.3.0 前的保留	3.3.0 後適用於內部部署裝置的保留	3.3.0 後適用於主控裝置的保留	3.3.2 後適用於內部部署裝置的保留	3.3.2 後適用於主控裝置的保留
高	6-10 週	14 天 (預設值)、31 天 (最大值)	14 天	14 天	14 天
中	10 -14 週	已過時	已過時	已過時	已過時
低	最多 1 年	已過時	已過時	最多 1 年	已過時

常見問題集

- 在完成 3.3.2 升級後如何啟用流量統計資料每日彙總？

  若要啟用流量統計資料每日彙總，請將 `flowStats.daily.rollup.enabled` 系統內容設定為 `true`。

- 每個 Edge 每天可彙總的流量數目上限為何？

  依預設，每個 Edge 每天最多可彙總一百萬個流量。即平均每 5 分鐘推送約 3500 個流量。您可以使用 `flowStats.daily.rollup.flowLimit` 系統內容，修改每個 Edge 每天可彙總的流量數目。

- 中樞流量是否會彙總？

  依預設會停用中樞流量的彙總。您可以使用 `flowStats.daily.rollup.edgeflowLimit` 系統內容來啟用中樞流量，這會使用 `<edgeId>:<numFlows>` 的索引鍵/值配對。您最多只能檢視高解析度中樞流量 15 天。

- 流量統計資料保留原則是否可設定？

彙總統計資料的保留原則可在 SD-WAN Orchestrator 上使用 `retentionWeeks.flowStats.daily` 系統內容設定。彙總流量統計資料保留可設定為在 1 到 52 週的任意期間內持續保存。

- 在啟用彙總後，UI 是否能查詢流量統計資料 15 天以上？

  否。彙總流量統計資料的保留期間較長時，不代表實際上能夠查詢這些流量統計資料。您可以使用 `session.options.maxFlowstatsRetentionDays` 系統內容來設定要查詢流量的天數。

- 開啟此功能後，是否會在資料方面產生副作用？

  雖然在彙總結果上並未發現任何副作用，但 SD-WAN Orchestrator UI 上的時間序列圖可能會因為顯示彙總序列統計資料，而失去精確度。

- 系統負載方面有何副作用？

  由於每日流量統計資料彙總會從完整解析度資料表彙總結果，並個別加以儲存，因此系統負載 (CPU/負載平均值) 必定會因為 MySQL 彙總結果所需的額外處理而增加。

- 內部部署的儲存區需求會受到什麼影響？

  由於每日流量統計資料彙總會從高解析度資料表彙總結果，並個別加以儲存，因此 VMware 預期內部部署客戶應規劃其儲存區需求，以因應彙總統計資料的需要。平均而言，彙總的流量耗用的空間將是高解析度統計資料所需的 1/8；但這在很大的程度上取決於 Edge 所傳送之每日流量的獨特性。無論如何，彙總的流量在儲存空間耗用量方面的增長速度，會比高解析度統計資料低得多。對於一開始使用較小磁碟機的客戶，VMware 建議使用邏輯磁碟區，以便在 Edge 增長時隨之擴大儲存區容量。

變更保留期間

高解析度流量統計資料保留可設定為在 1 到 31 天的任意期間內持續保存。在 3.3.0 版中，高解析度流量統計資料保留的組態細微性已從月變更為天。操作員可藉由建立系統內容來變更保留期間。若要建立系統內容以變更保留期間，請執行以下步驟。

1 在 SD-WAN Orchestrator 導覽面板中，按一下**系統內容 (System Properties)**。

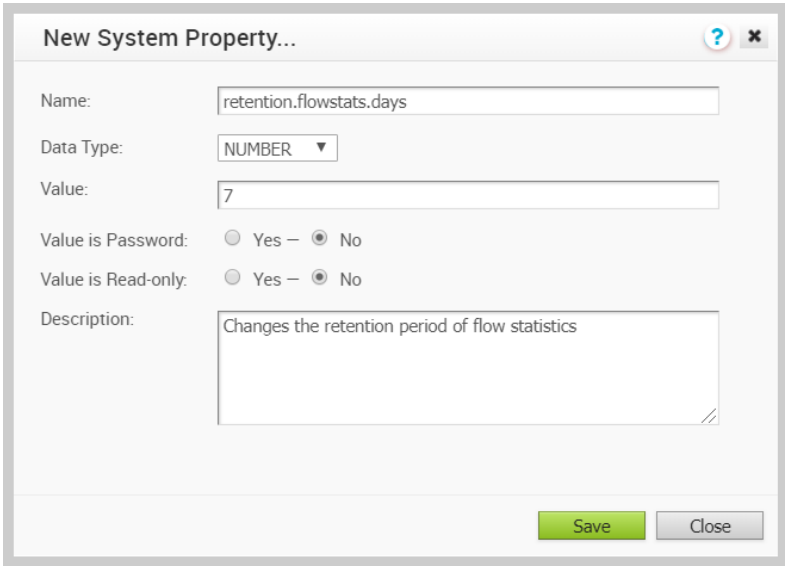
2 在**系統內容 (System Properties)** 畫面中，按一下**新增系統內容 (New System Properties)** 按鈕。

3 在**新增系統內容 (New System Property)** 對話方塊中：

   a 在**名稱 (Name)** 文字欄位中，輸入 `retention.flowstats.days`。

   b 在**資料類型 (Data Type)** 下拉式功能表中，選擇**數值 (Number)**。

   c 在**值 (Value)** 文字欄位中，輸入保留期間 (以天為單位)。



4 按一下**儲存 (Save)**。

監控網路服務

導覽面板中的**監控 (Monitor)** 選項提供網路服務，且會顯示 Non VMware SD-WAN Sites 的 VPN 通道狀態。

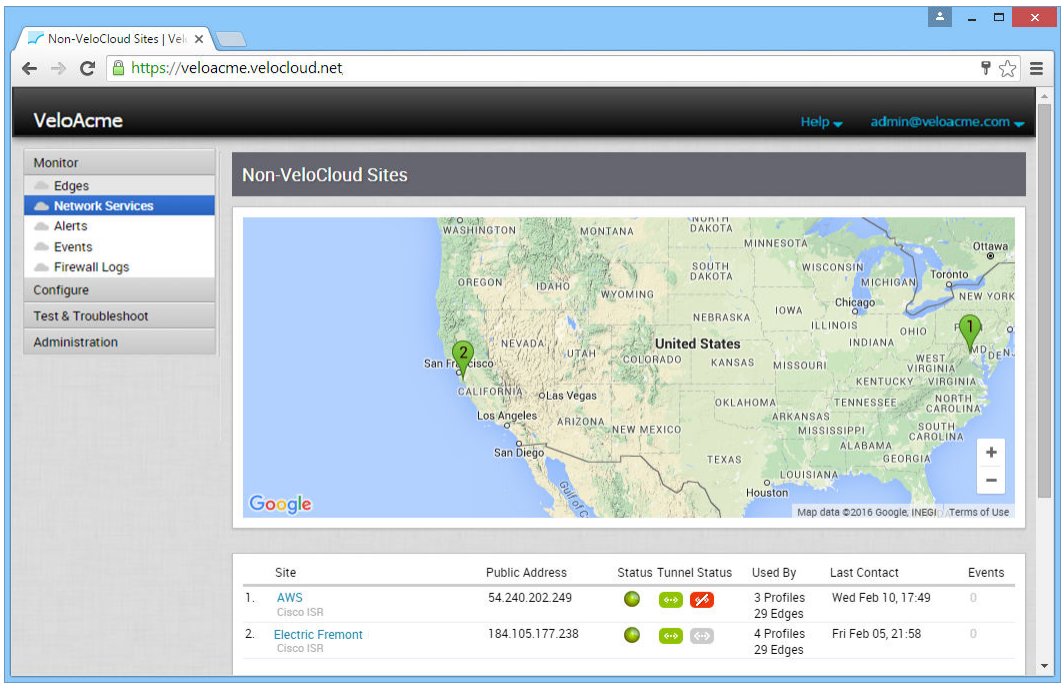
您可以按一下**站台 (Site)** 資料行中的 Non VMware SD-WAN Site 以開啟對話方塊，以變更站台的相關資訊。

Non VMware SD-WAN Sites 的類型包括：

- Iaas：AWS
- CWS：Zscaler
- Non VMware SD-WAN Site：Palo Alto、Sonic Wall
- 非 VMware SD-WAN Hub

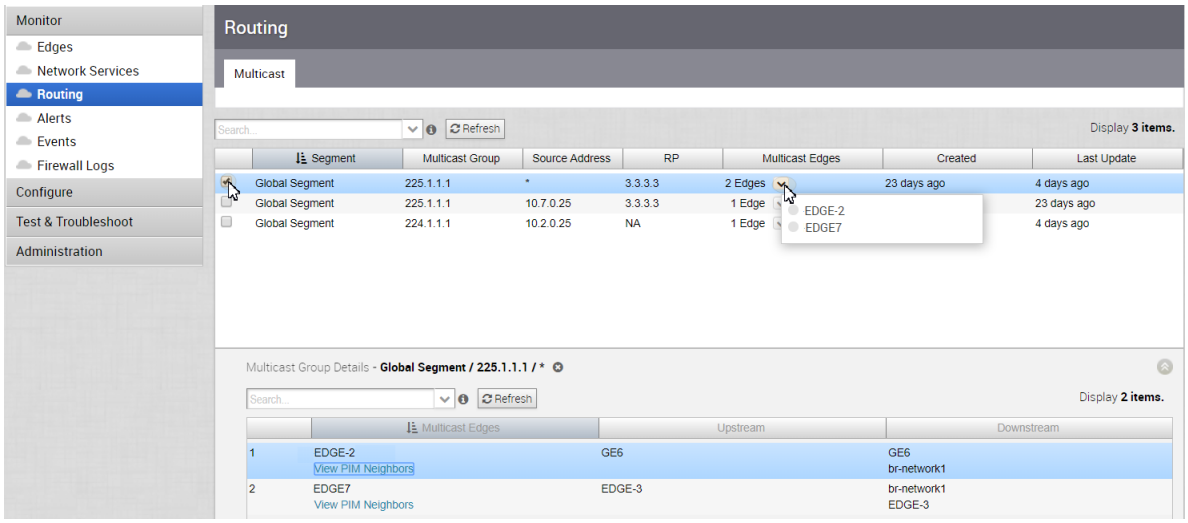
Non VMware SD-WAN Site 畫面會顯示狀態和通道狀態。以下列出狀態結果的類型：

顏色	意義
綠色	已連線
紅色	離線/已中斷連線
灰色	未啟用



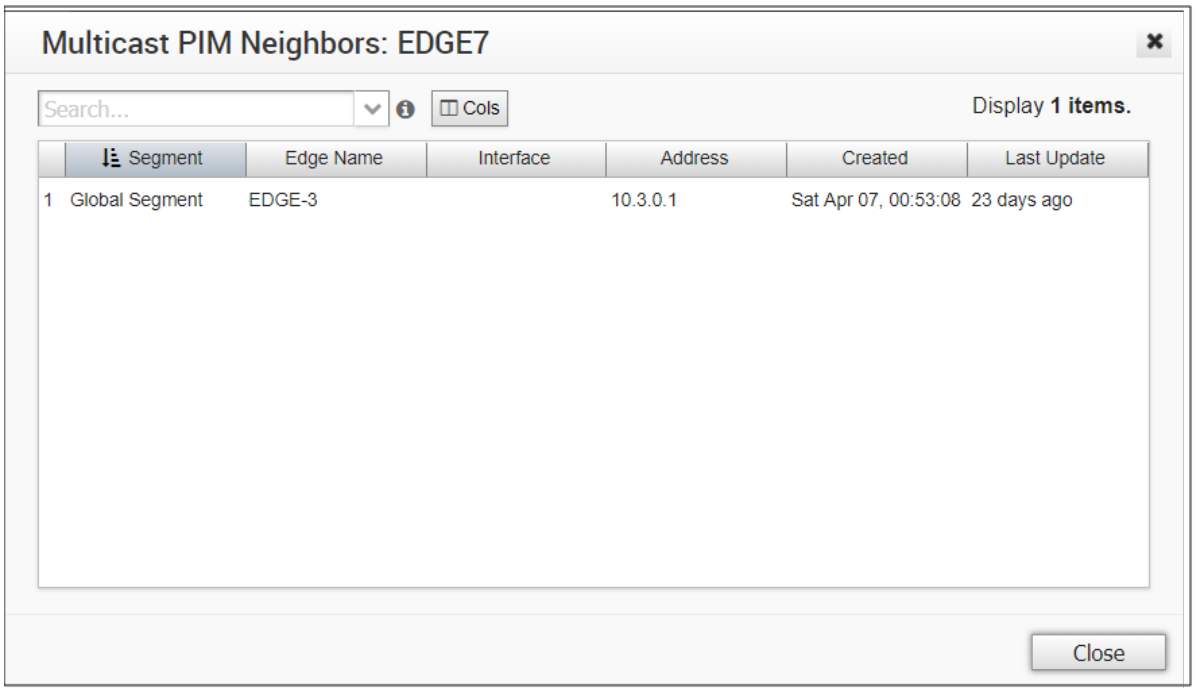
監控路由

路由功能 (**監控 (Monitor) > 路由 (Routing) > 多點傳播 (Multicast)** 索引標籤) 會顯示多點傳播群組和多點傳播 Edge 資訊。



PIM 芳鄰視圖

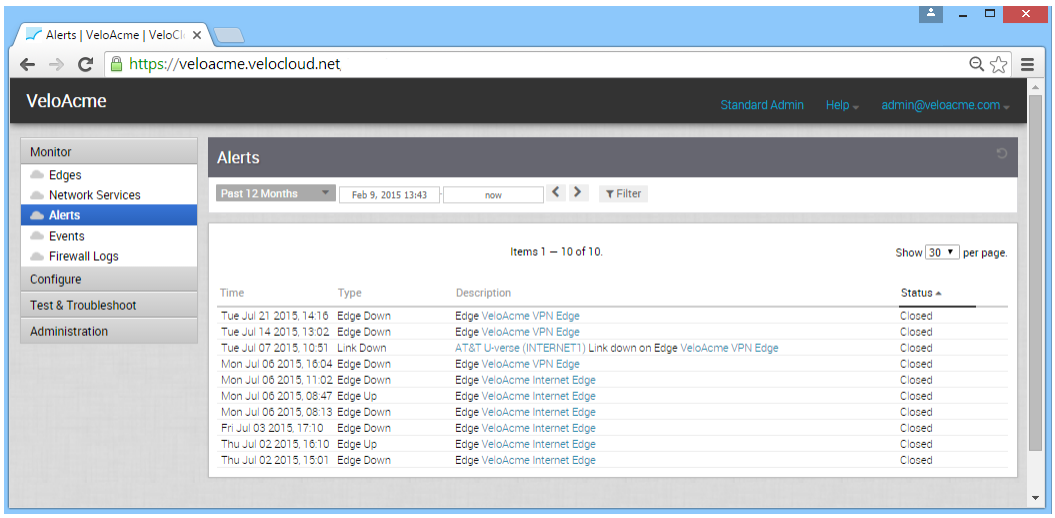
下圖顯示所選 Edge 的 PIM 芳鄰 (每個區段)、已探索到 PIM 芳鄰的介面、芳鄰 IP 位址，以及時間戳記。



監控警示

SD-WAN Orchestrator 提供警示功能，可在問題發生時通知一或多個企業管理員 (或其他支援使用者)。您可以在導覽面板中的**監控 (Monitor)** 下方按一下**警示 (Alerts)**，以存取此功能。

您可以在 SD-WAN Edge 離線或重新連線、WAN 連結失效、VPN 通道關閉或發生 Edge HA 容錯移轉時傳送警示。您可以針對每個警示類型輸入在偵測到警示後予以傳送的延遲時間。您可以在**設定 (Configure) > 警示和通知 (Alerts and Notifications)** 中設定警示。

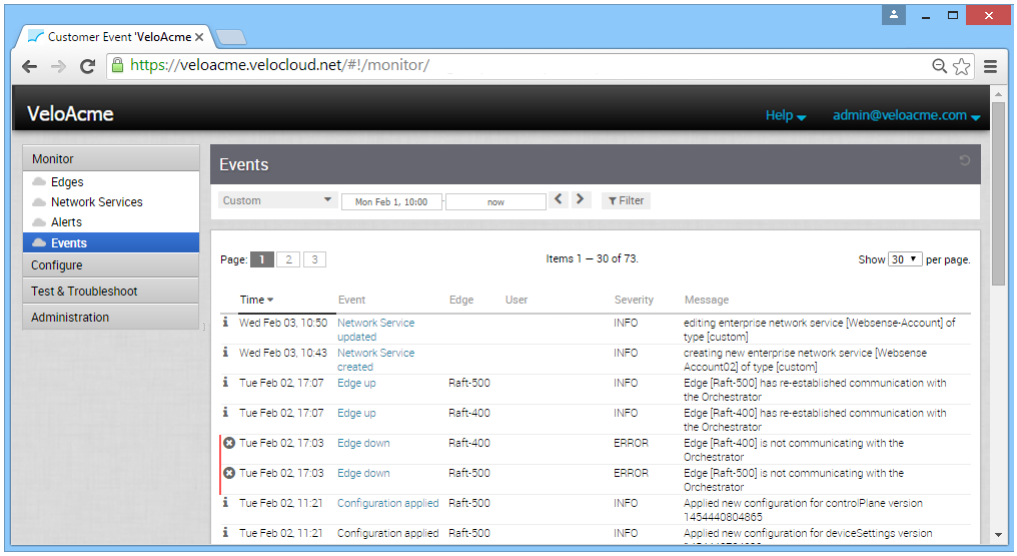


備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

監控事件

導覽面板中的**事件 (Events)** 頁面會顯示 SD-WAN Orchestrator 所產生的事件。這些事件可協助您判斷 VMware 系統的運作狀態。

您可以按一下**事件 (Events)** 頁面中顯示的 [事件 (Event)] 連結，以檢視更多詳細資料。



[事件 (Events)] 功能可用來取得下列資訊：

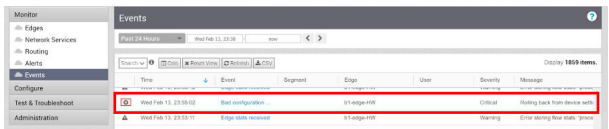
- 使用者活動的稽核線索 [依使用者篩選]
- 指定站台上活動的歷史記錄 [依站台篩選]
- 中斷和重大網路事件的記錄 [依事件篩選]
- ISP 效能降級的分析 [依時段篩選]

自動復原至上一個已知良好的組態

如果管理員變更了裝置組態而導致 Edge 與 Orchestrator 中斷連線，管理員將會看到 **Edge 關閉 (Edge Down)** 警示。Edge 在偵測到無法連線至 SD-WAN Orchestrator 時，它將會復原至上一個已知的組態，並在 Orchestrator 上產生標題為「錯誤組態」的事件。

復原時間是指對獨立 Edge 偵測到錯誤的組態，並套用先前已知「良好」的組態所需的時間，大約為 5-6 分鐘。HA Edge 的復原時間介於 10-12 分鐘之間。

備註 此功能只會復原 Edge 層級的裝置設定。如果從設定檔中推送組態而導致多個 Edge 從 Orchestrator 離線，則 Edge 會記錄「錯誤組態」事件，並復原至上一個已知良好的組態。重要：管理員應負責據以修正設定檔。設定檔組態不會自動復原。



Syslog 支援的 VMware SD-WAN Edge 事件

下表說明可匯出至 Syslog 收集器的所有可能 VMware SD-WAN Edge 事件。

事件	嚴重性	說明
BW_UNMEASURABLE	警示	在路徑頻寬不可測量時由 SD-WAN Edge 產生。
EDGE_BIOS_UPDATE_FAILED	錯誤	在 SD-WAN Edge BIOS 更新時，由 12-upgrade-bios.sh 指令碼產生。
EDGE_BIOS_UPDATED	資訊	在 SD-WAN Edge BIOS 更新失敗時，由 12-upgrade-bios.sh 指令碼產生。
EDGE_CONSOLE_LOGIN	資訊	在透過主控台連接埠登入期間由 SD-WAN Edge 產生。
EDGE_DEACTIVATED	警告	在 SD-WAN Edge 已清除其所有組態且未與客戶站台相關聯時產生。軟體組建編號會保持不變。
EDGE_DHCP_BAD_OPTION	警告	使用不正確的 DHCP 選項設定 SD-WAN Edge 時產生。
EDGE_DISK_IO_ERROR	警告	在升級/降級期間發生磁碟 IO 錯誤時，由 SD-WAN Edge 產生。
EDGE_DISK_READONLY	嚴重	當磁碟變成唯讀模式時，由 SD-WAN Edge 產生。
EDGE_DNSMASQ_FAILED	錯誤	Dnsmasq 服務失敗時產生。
EDGE_DOT1X_SERVICE_DISABLED	警告、嚴重	當 SD-WAN Edge 802.1x 服務停用時，由 vc_procmon 產生。
EDGE_DOT1X_SERVICE_FAILED	錯誤	當 SD-WAN Edge 802.1x 服務失敗時，由 vc_procmon 產生。
EDGE_HARD_RESET	警告	當使用者已起始 SD-WAN Edge 硬重設時產生。
EDGE_HEALTH_ALERT	緊急	當資料平面無法配置必要資源來處理封包時，由 SD-WAN Edge 產生。
EDGE_INTERFACE_DOWN	資訊	在介面關閉時，由熱插拔指令碼產生。
EDGE_INTERFACE_UP	資訊	在介面開啟時，由熱插拔指令碼產生。
EDGE_KERNEL_PANIC	警示	當 Edge 作業系統發生嚴重例外狀況且必須將 Edge 重新開機以進行復原時，由 SD-WAN Edge 產生。Edge 重新開機會破壞客戶的流量達 2-3 分鐘，而 Edge 會完成重新開機。
EDGE_L2_LOOP_DETECTED	錯誤	偵測到 SD-WAN Edge L2 迴圈時產生。
EDGE_LED_SERVICE_DISABLED	警告、嚴重	當 SD-WAN Edge LED 服務停用時，由 vc_procmon 產生。
EDGE_LED_SERVICE_FAILED	錯誤	當 SD-WAN Edge LED 服務失敗時，由 vc_procmon 產生。
EDGE_LOCALUI_LOGIN	資訊	使用者的本機 UI 登入成功時產生。

事件	嚴重性	說明
EDGE_MEMORY_USAGE_ERROR	錯誤	當資源監視器處理程序偵測到 Edge 記憶體使用量已超過定義的臨界值且達到 70% 臨界值時，由 SD-WAN Edge 產生。資源監視器會等待 90 秒，以允許邊緣處理程序從記憶體使用量中可能的暫時尖峰狀況復原。如果記憶體使用量在 70% 或更高的層級持續超過 90 秒，則 Edge 會產生此錯誤訊息，並將此事件傳送至 Orchestrator。
EDGE_MEMORY_USAGE_WARNING	警告	當資源監視器處理程序偵測到 Edge 記憶體使用量為 50% 或更多可用記憶體時，由 SD-WAN Edge 產生。此事件將每隔 60 分鐘傳送至 Orchestrator，直到記憶體使用量降至 50% 臨界值以下為止。
EDGE_MGD_SERVICE_DISABLED	嚴重，警告	當 mgd 無法啟動或停用而造成失敗次數過多時，由 vc_procmon 產生。
EDGE_MGD_SERVICE_FAILED	錯誤	mgd 服務失敗時，由 vc_procmon 產生。
EDGE_NEW_DEVICE	資訊	透過處理 DHCP 要求來識別新的 DHCP 用戶端時產生。
EDGE_NEW_USER	資訊	新增新的用戶端使用者時產生。
EDGE_OSPF_NSM	資訊	在 OSPF 芳鄰狀態機器 (NSM) 發生時，由 SD-WAN Edge 產生。
EDGE_REBOOTING	警告	當使用者已起始 SD-WAN Edge 重新開機時產生。
EDGE_RESTARTING	警告	當使用者已起始 SD-WAN Edge 服務重新啟動時產生。
EDGE_SERVICE_DISABLED	警告	當 SD-WAN Edge 資料平面服務停用時產生。
EDGE_SERVICE_ENABLED	警告	當 SD-WAN Edge 資料平面服務啟用時產生。
EDGE_SERVICE_FAILED	錯誤	當 SD-WAN Edge 資料平面服務失敗時產生。
EDGE_SHUTTING_DOWN	警告	當 SD-WAN Edge 關閉時產生。
EDGE_STARTUP	資訊	當 SD-WAN Edge 在僅限管理模式中執行時產生。
EDGE_SSH_LOGI	資訊	在透過 SSH 通訊協定登入期間，由 SD-WAN Edge 產生。
EDGE_TUNNEL_CAP_WARNING	警告	當 SD-WAN Edge 達到其通道容量上限時產生。
EDGE_VNFD_SERVICE_DISABLED	警告、嚴重	當 Edge VNFD 服務停用時，由 vc_procmon 產生。
EDGE_VNFD_SERVICE_FAILED	錯誤	當 Edge VNFD 服務失敗時，由 vc_procmon 產生。

事件	嚴重性	說明
FLOOD_ATTACK_DETECTED	資訊	當惡意主機對 SD-WAN Edge 湧入新連線時產生。
HA_FAILED	資訊	HA 對等狀態未知 (HA Peer State Unknown) - 當待命 Edge 尚未傳送活動訊號回應，且兩個 HA Edge 中只有一個與 Orchestrator 和閘道進行通訊時產生。
HA_GOING_ACTIVE	資訊	HA 容錯移轉。當作用中高可用性 (HA) Edge 已標記為關閉，並將待命 (Standby) 設為作用中 (Active) 時會產生。
HA_INTF_STATE_CHANGED	警示	HA 介面狀態變更為作用中 (Active) 時產生。
HA_READY	資訊	在作用中 (Active) 和待命 (Standby) Edge 均已啟動且同步時產生。
HA_STANDBY_ACTIVATED	資訊	HA 待命 Edge 已接受啟用金鑰、已下載其組態，且已更新其軟體組建編號時產生。
HA_TERMINATED	資訊	當 SD-WAN Edge 上的 HA 已停用時產生。
INVALID_JSON	嚴重	當 SD-WAN Edge 從 MGD 收到無效回應時產生。
IP_SLA_PROBE	向上 = 資訊，向下 = 警示	當 IP ICMP 探查狀態變更時產生。
IP_SLA_RESPONDER	向上 = 資訊，向下 = 警示	當 IP ICMP 回應程式狀態變更時產生。
LINK_ALIVE	資訊	當 WAN 連結不再為「無作用」時產生。
LINK_DEAD	警示	當 WAN 連結上建立的所有通道均未收到封包至少七秒時產生。
LINK_MTU	資訊	當探索到 WAN 連結 MTU 時產生。
LINK_UNUSABLE	警示	當 WAN 連結轉換為「無法使用」狀態時產生。
LINK_USABLE	資訊	當 WAN 連結轉換為「可用」狀態時產生。
MGD_ACTIVATION_ERROR	錯誤	當 SD-WAN Edge 啟用失敗時產生。啟用連結不正確，或是組態未成功下載至 Edge。
MGD_ACTIVATION_PARTIAL	資訊	當 SD-WAN Edge 部分啟用但軟體更新失敗時產生。
MGD_ACTIVATION_SUCCESS	資訊	當 SD-WAN Edge 成功啟用時產生。
MGD_CONF_APPLIED	資訊	在 Orchestrator 上所做的組態變更已推送至 SD-WAN Edge 且已成功套用時產生。
MGD_CONF_FAILED	資訊	當 SD-WAN Edge 無法套用對 Orchestrator 所做的組態變更時產生。
MGD_CONF_ROLLBACK	資訊	從 Orchestrator 傳送的組態原則因導致 SD-WAN Edge 不穩定而必須回復時產生。

事件	嚴重性	說明
MGD_CONF_UPDATE_INVALID	資訊	當指派給 SD-WAN Edge 的操作員設定檔 (Operator Profile) 具有 Edge 無法使用的無效軟體映像時產生。
MGD_DEACTIVATED	資訊	當 mgd 根據使用者要求停用 SD-WAN Edge 時產生。
MGD_DEVICE_CONFIG_WARNING/ERROR	警告，資訊	當偵測到不一致/無效的裝置設定時產生。
MGD_DIAG_REBOOT	資訊	從 Orchestrator 的遠端動作 (Remote Actions) 重新開機 SD-WAN Edge 時產生。
MGD_DIAG_RESTART	資訊	從 Orchestrator 的遠端動作 (Remote Actions) 重新啟動 SD-WAN Edge 上的資料平面服務時產生。
MGD_EMERG_REBOOT	嚴重	當 SD-WAN Edge 重新開機，以便 vc_procmon 從停滯的程序復原時產生。
MGD_ENTER_LIVE_MODE	偵錯	當 SD-WAN Edge 上的管理服務進入即時模式時產生。
MGD_EXIT_LIVE_MODE	偵錯	當 SD-WAN Edge 上的管理服務結束即時模式時產生。
MGD_EXITING	資訊	當 SD-WAN Edge 上的管理服務關閉以進行重新啟動時產生。
MGD_EXTEND_LIVE_MODE	偵錯	當即時模式已延伸時，由 SD-WAN Edge 產生。
MGD_FLOW_STATS_PUSH_FAILED	偵錯	當推送至 Orchestrator 的流量統計資料失敗時，由 SD-WAN Edge 產生。
MGD_FLOW_STATS_PUSH_SUCCEEDED	偵錯	當推送至 Orchestrator 的流量統計資料成功時，由 SD-WAN Edge 產生。
MGD_FLOW_STATS_QUEUED	資訊	當推送至 Orchestrator 的流量統計資料排入佇列時，由 SD-WAN Edge 產生。
MGD_HARD_RESET	資訊	當 SD-WAN Edge 還原為其原廠預設軟體和組態時產生。
MGD_HEALTH_STATS_PUSH_FAILED	偵錯	當推送至 Orchestrator 的健全狀況統計資料失敗時，由 SD-WAN Edge 產生。
MGD_HEALTH_STATS_PUSH_SUCCEEDED	偵錯	當推送至 Orchestrator 的健全狀況統計資料成功時，由 SD-WAN Edge 產生。
MGD_HEALTH_STATS_QUEUED	資訊	當推送至 Orchestrator 的健全狀況統計資料排入佇列時，由 SD-WAN Edge 產生。
MGD_HEARTBEAT	資訊	向 Orchestrator 產生活動訊號時，由 SD-WAN Edge 產生。
MGD_HEARTBEAT_FAILURE	資訊	當向 Orchestrator 產生的活動訊號失敗時，由 SD-WAN Edge 產生。
MGD_HEARTBEAT_SUCCESS	資訊	當向 Orchestrator 產生的活動訊號成功時，由 SD-WAN Edge 產生。

事件	嚴重性	說明
MGD_INVALID_VCO_ADDRESS	警告	在管理平面原則更新中傳送 Orchestrator 的無效位址且已忽略時產生。
MGD_LINK_STATS_PUSH_FAILED	偵錯	當推送至 Orchestrator 的連結統計資料失敗時，由 SD-WAN Edge 產生。
MGD_LINK_STATS_PUSH_SUCCEEDED	偵錯	當推送至 Orchestrator 的連結統計資料成功時，由 SD-WAN Edge 產生。
MGD_LINK_STATS_QUEUED	資訊	當推送至 Orchestrator 的連結統計資料排入佇列時，由 SD-WAN Edge 產生。
MGD_LIVE_ACTION_FAILED	偵錯	當即時動作失敗時，由 SD-WAN Edge 產生。
MGD_LIVE_ACTION_REQUEST	偵錯	當要求即時動作時，由 SD-WAN Edge 產生。
MGD_LIVE_ACTION_SUCCEEDED	偵錯	當即時動作成功時，由 SD-WAN Edge 產生。
MGD_NETWORK_MGMT_IF_BROKEN	警示	當管理網路設定不正確時產生。
MGD_NETWORK_MGMT_IF_FIXED	警告	當重新啟動網路兩次以修正管理網路不一致時產生。
MGD_NETWORK_SETTINGS_UPDATED	資訊	當新的網路設定套用至 SD-WAN Edge 時產生。
MGD_SET_CERT_FAIL	錯誤	在 SD-WAN Edge 上安裝 Orchestrator 通訊的新 PKI 憑證失敗時產生。
MGD_SET_CERT_SUCCESS	資訊	在 SD-WAN Edge 上成功安裝適用於 Orchestrator 通訊的新 PKI 憑證時產生。
MGD_SHUTDOWN	資訊	當 SD-WAN Edge 診斷根據使用者要求而關閉時產生。
MGD_START	資訊	當 SD-WAN Edge 上的管理精靈啟動時產生。
MGD_SWUP_DOWNLOAD_FAILED	錯誤	當下載 Edge 軟體更新映像失敗時產生。
MGD_SWUP_DOWNLOAD_SUCCEEDED	偵錯	當下載 Edge 軟體更新映像成功時產生。
MGD_SWUP_IGNORED_UPDATE	資訊	當軟體更新在啟用時因為 SD-WAN Edge 已執行該版本而忽略時產生。
MGD_SWUP_INSTALL_FAILED	錯誤	當軟體更新安裝失敗時產生。
MGD_SWUP_INSTALLED	資訊	當成功下載並安裝軟體更新時產生。
MGD_SWUP_INVALID_SWUPDATE	警告	從 Orchestrator 收到的軟體更新套件無效時產生。
MGD_SWUP_REBOOT	資訊	在軟體更新後將 SD-WAN Edge 重新開機時產生。
MGD_SWUP_STANDBY_UPDATE_FAILED	錯誤	當待命 HA Edge 的軟體更新失敗時產生。

事件	嚴重性	說明
MGD_SWUP_STANDBY_UPDATE_START	資訊	當 HA 待命軟體更新開始時產生。
MGD_SWUP_STANDBY_UPDATED	資訊	當待命 HA Edge 的軟體更新開始時產生。
MGD_SWUP_UNPACK_FAILED	錯誤	當 Edge 無法將已下載的軟體更新套件解壓縮時產生。
MGD_SWUP_UNPACK_SUCCEEDED	資訊	當 Edge 成功將已下載的軟體更新套件解壓縮時產生。
MGD_UNREACHABLE	緊急	當資料平面處理程序無法與管理平面 Proxy 通訊時產生。
MGD_VCO_ADDR_RESOLV_FAILED	警告	當 Orchestrator 位址的 DNS 解析失敗時產生。
MGD_WEBSOCKET_INIT	偵錯	當使用 Orchestrator 起始 WebSocket 通訊時產生。
MGD_WEBSOCKET_CLOSE	偵錯	當與 Orchestrator 的 WebSocket 通訊關閉時產生。
PEER_UNUSABLE	警示	當傳輸對等統計資料時，對等的覆疊連線關閉時產生。
PEER_USABLE	資訊	在無法使用一段時間後，對等的覆疊連線復原時產生。
PORT_SCAN_DETECTED	資訊	偵測到連接埠掃描時產生。
QOS_OVERRIDE	資訊	已產生以翻轉流量路徑 (閘道或直接)。
SLOW_START_CAP_MET	注意	在超過頻寬測量慢速啟動上限時產生。將以高載模式完成
VPN_DATACENTER_STATUS	資訊、錯誤	當 VPN 通道狀態變更時產生。
VRRP_FAIL_INFO	資訊	當 VRRP 失敗時產生。
VRRP_INTO_MASTER_STATE	資訊	當 VRRP 進入主節點狀態時產生。
VRRP_OUT_OF_MASTER_STATE	資訊	當 VRRP 離開主節點狀態時產生。

監控報告

企業入口網站中的 [監控 (Monitoring)] 儀表板可讓您產生報告，並使其包含整體網路摘要，以及 SD-WAN 流量和傳輸分佈的相關資訊。報告可讓您對網路進行分析。

備註 報告著重於說明性分析，無法用於疑難排解目的。此外，這些報告並非儀表板而反映來自網路的即時資料。

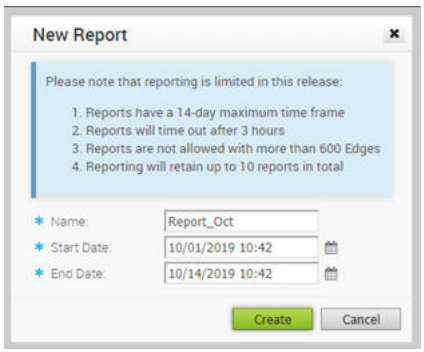
在企業入口網站中，按一下**監控 (Monitor) > 報告 (Reports)**。

若要建立新的報告：

1 在**報告 (Reports)** 視窗中，按一下**新增報告 (New Report)**。

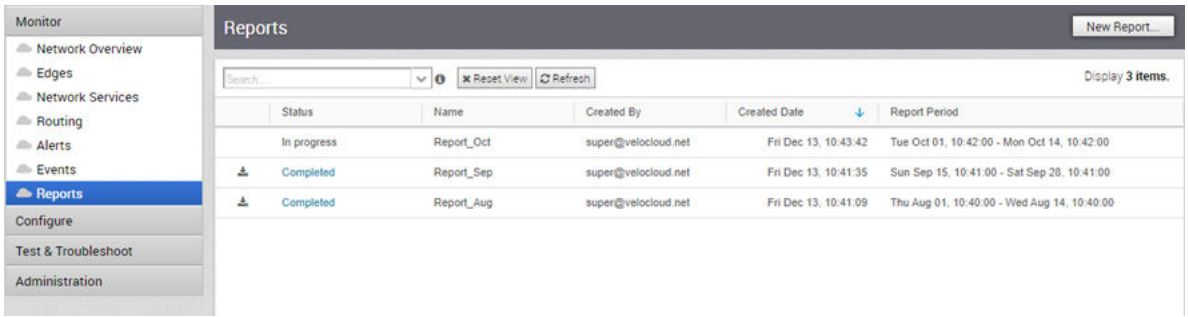
2 在**新增報告 (New Report)** 視窗中，輸入報告的描述性名稱，然後選擇開始和結束日期。

3 按一下**建立 (Create)**。

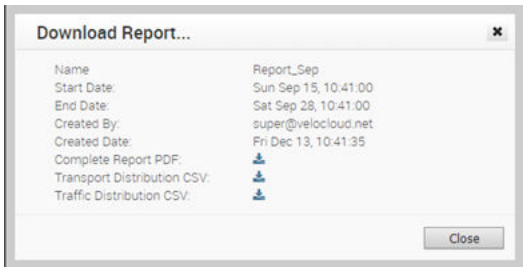


備註 您只能產生為期 14 天、最多 600 個 Edge 的報告。報告產生作業會在 3 小時後逾時。**報告 (Reports)** 資料表一次只會保留最新的 10 個報告。

報告產生的**狀態 (Status)** 會顯示在視窗中。完成後，您可以按一下**完成 (Completed)** 連結來下載報告。



下載報告 (Download Report) 視窗提供下列選項：



您可以將報告下載為 PDF，以提供流量和傳輸分佈的整體摘要 (以圓形圖表示)。此報告也會依流量和傳輸類型提供前 10 個應用程式的清單。

您可以選擇依傳輸或流量分佈以 CSV 檔案的格式下載報告。

- 傳輸分佈報告會顯示時間、傳輸類型、應用程式、Edge 的名稱和說明，以及傳送和接收的位元組等詳細資料。
- 流量分佈報告會顯示時間、流量路徑、應用程式、Edge 的名稱和說明，以及傳送和接收的位元組等詳細資料。

設定區段

7

分割這個程序是透過在轉送裝置 (例如交換器、路由器或防火牆) 上使用隔離技術，將網路分割成稱為區段的邏輯子網路。當來自不同組織和/或資料類型的流量必須隔離時，網路分割就非常重要。

在區段感知拓撲中，可以為每個區段啟用不同的虛擬私人網路 (VPN) 設定檔。例如，可以將訪客流量回傳至遠端資料中心防火牆服務：語音媒體可根據動態通道直接從「分支到分支」進行傳遞，PCI 區段可將流量回傳至資料中心，以退出 PCI 網路。

備註 您可以為每個企業客戶設定最多 16 個區段。

若要為企業設定新的區段，請執行下列步驟：

1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure) > 區段 (Segments)**。所選企業的**區段 (Segments)** 頁面隨即出現。

2 按一下 + 按鈕，然後輸入下列詳細資料以設定新的區段。

欄位	說明
區段名稱	區段名稱 (最多 256 個字元)。
說明	區段說明 (最多 256 個字元)。
類型	區段類型可以是下列其中一項： ■ **一般 (Regular)** - 標準區段類型。 ■ **私人 (Private)** - 用於需要有限可見度才能解決使用者隱私權需求的流量。 ■ **CDE** - VMware 提供經 PCI 認證的 SD-WAN 服務。持卡人資料環境 (CDE) 類型用於需要 PCI 且想要利用 VMware PCI 認證的流量。 **備註** 對於全域區段，您可以將類型設定為**一般 (Regular)** 或**私人 (Private)**。對於非全域區段，類型可以是**一般 (Regular)**、**CDE** 或**私人 (Private)**。
服務 VLAN (Service VLAN)	服務 VLAN 識別碼。如需相關資訊，請參閱安全性 VNF 中的定義區段與服務 VLAN 之間的對應 (選擇性) 區段。

欄位	說明
委派給合作夥伴 (Delegate To Partner)	依預設會選取此核取方塊。如果取消選取，合作夥伴將無法變更區段內的組態 (包括介面指派)。
委派給客戶 (Delegate To Customer)	依預設會選取此核取方塊。如果取消選取，客戶將無法變更區段內的組態 (包括介面指派)。

3 按一下**儲存變更 (Save Changes)**。

如果區段設定為**私人 (Private)**，則區段：

- 除了 VMware 控制、VMware 管理，以及在區段上傳送的所有已傳輸及已接收封包和位元組的單一 IP 流量，不會將使用者流量統計資料上傳至 Orchestrator。
- 不允許使用者在遠端診斷中檢視流量。
- 不允許傳送流量做為**網際網路多重路徑 (Internet Multipath)**，因為所有設定為**網際網路多重路徑 (Internet Multipath)** 的商務原則會由 Edge 自動覆寫為**直接 (Direct)**。

如果將區段設定為 **CDE**，則 VMware 主控的 Orchestrator 和控制器將會感知 PCI 區段，且將位於 PCI 範圍內。閘道 (標記為非 CDE 閘道) 將無法感知或傳輸 PCI 流量，且會位於 PCI 範圍外。

設定網路服務

8

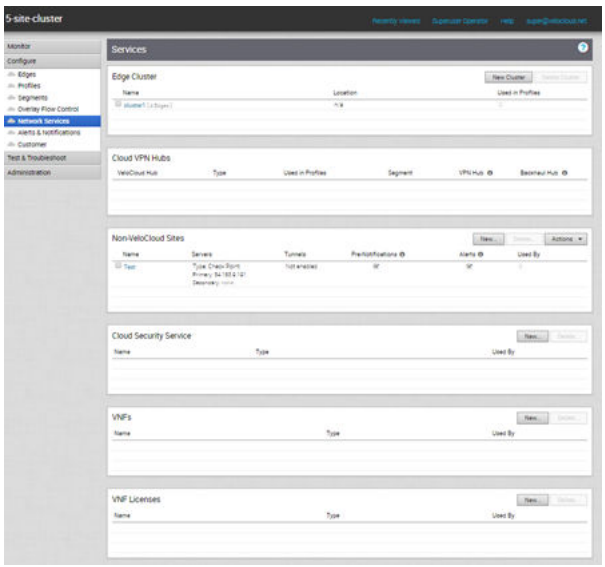
身為企業使用者，SD-WAN Orchestrator 可讓您從**設定 (Configure)** > **網路服務 (Network Services)** 設定網路服務。

備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

您可以設定下列網路服務：

- Edge 叢集
- 非 VeloCloud 站台
- 雲端安全性服務
- VNF
- VNF 授權
- DNS 服務
- Netflow 設定
- 私人網路名稱
- 驗證服務

備註 設定網路服務是選擇性作業，且可依任何順序進行設定。



備註 SD-WAN Orchestrator 不允許您從**服務 (Services)** 畫面設定雲端 VPN 中樞，但會提供所有已設定 SD-WAN Edges 的摘要。摘要資訊包括 Edge 類型、使用 Edge 的設定檔、區段、Edge 是 VPN 中樞還是/及回傳中樞。

本章節討論下列主題：

- 關於 Edge 叢集化
- 設定 Non VMware SD-WAN Site
- 設定雲端安全性服務
- 設定 DNS 服務
- 設定 Netflow 設定
- 私人網路名稱
- 設定驗證服務

關於 Edge 叢集化

具有 VMware SD-WAN Hub 的單一 VMware VPN 網路在大小方面會受限於個別中樞的規模。對於包含數千個遠端站台的大型網路，最好同時使用多個中樞來處理 Edge，以提升延展性並降低風險。但是，強制客戶管理個別的中樞來達到此目的並不務實。叢集化可讓您利用多個中樞，同時將那些中樞作為一個通用實體以簡化管理，並提供內建的復原能力。

SD-WAN Edge 叢集化可解決 SD-WAN Hub 規模的問題，因為它可用來建立 Edge 的邏輯叢集，從而輕鬆擴充中樞的通道容量動態。Edge 叢集化也能透過 SD-WAN Edges 的叢集提供的雙主動高可用性 (HA) 拓撲所提供復原能力。從其他 Edge 的角度來看，叢集在功能上被視為是個別中樞。

VMware 叢集中的中樞可以是實體或虛擬 Edge。如果是虛擬的，它們可以存在於單一 Hypervisor 上或多個 Hypervisor 間。

叢集中的每個 Edge 都會定期向 SD-WAN Gateway 報告使用量和負載統計資料。負載值會根據 Edge 的 CPU 和記憶體使用量以及連線至中樞的通道數目來計算，並以 Edge 型號的通道容量百分比來表示。叢集中的中樞不會直接通訊，也不會交換狀態資訊。Edge 叢集通常會部署為資料中心內的中樞。

備註 理論上，Edge 叢集化可用來水平調整其他向量，例如總流量。但目前的 Edge 叢集化實作已經過專門設計和測試，僅可在通道容量方面進行調整。

Edge 叢集化的運作方式

本節提供 SD-WAN Edge 叢集化功能運作方式的深入概觀。

下列的重要概念說明 SD-WAN Edge 叢集化功能：

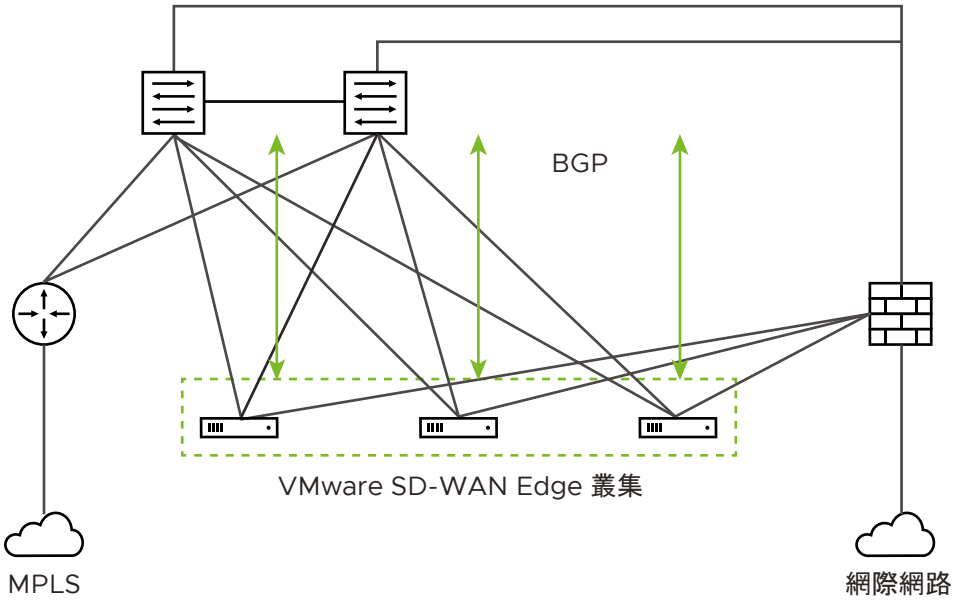
- Edge 叢集化可用於中樞上，如下所述：
  - 可讓中樞的通道容量高於作為中樞之個別 Edge 所能提供的容量。
  - 將遠端支點 Edge 散佈於多個中樞間，並減少任何可能發生事件所產生的影響。
- 叢集評分是系統整體使用量的數學計算，如下所示：

  三項使用量測量因素分別為 CPU 使用率、記憶體使用量和通道容量。
  - 每個使用量測量值都會以百分比表示，最大值為 100%。
  - 通道容量以指定硬體型號或虛擬 Edge 組態的額定容量為基礎。
  - 三個使用量百分比會在加總後平均計算，以得出整數的叢集評分 (1-100)。
  - 雖然未直接考量總流量，CPU 和記憶體使用量仍會間接反映指定中樞上的總流量和流量大小。
  - 例如，在 Edge 2000 上：
    - CPU 使用率 = 20%
    - 記憶體使用量 = 30%
    - 已連線的通道數 = 600 (容量為 6000) = 10%
    - 叢集評分：(20 + 30 + 10)/3 = 20
- 大於 70 的叢集評分會被視為「超出容量」。
- 「邏輯識別碼」是一種 128 位元的 UUID，可唯一識別 VMware 網路內的元素。
  - 例如，每個 Edge 以一個邏輯識別碼表示，而每個叢集則以另一個邏輯識別碼表示。
  - 當使用者提供 Edge 和叢集名稱時，邏輯識別碼必定是唯一的，並且用於元素的內部識別。
- 依預設，負載會平均分配到中樞之間。因此，屬於叢集一部分的所有 Edge 都必須有著相同的型號和容量。

每個叢集成員將具有自己的 WAN 和 LAN 介面的 IP 定址。中樞叢集中的所有 VMware SD-WAN Edge 都需要在 LAN 端上對第 3 層裝置執行動態路由通訊協定 (例如 eBGP)，以及為每個叢集成員提供唯一的自發系統編號 (Autonomous System Number, ASN)。在叢集 LAN 端上進行動態路由，可確保從 DC 到特定支點站台的流量會透過適當的 Edge 叢集成員進行路由。

VMware SD-WAN 閘道如何追蹤 Edge 叢集？

中樞新增至 VMware SD-WAN 叢集後，中樞會拆解其已指派之所有閘道的通道並加以重建，並且向每個閘道指出中樞已指派給叢集，同時提供叢集邏輯識別碼。



對於叢集，SD-WAN 閘道將追蹤：

- 邏輯識別碼
- 名稱
- 是否已啟用自動重新平衡
- 叢集成員的中樞物件清單

對於叢集中的每個中樞物件，閘道會追蹤：

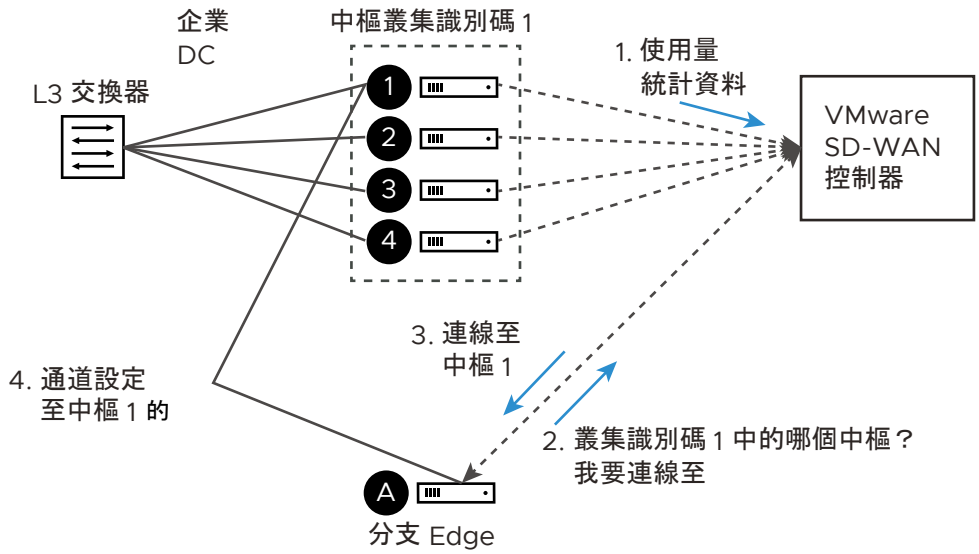
- 邏輯識別碼
- 名稱
- 一組統計資料 (透過從中樞傳送至每個已指派閘道的定期訊息每 30 秒更新一次)，其中包括：
  - 中樞目前的 CPU 使用率
  - 中樞目前的記憶體使用量
  - 中樞目前的通道計數
  - 中樞的目前 BGP 路由計數
- 根據上述公式計算的目前叢集評分。

當閘道未收到來自中樞 Edge 的任何封包達七秒以上，便會從中樞物件清單中移除中樞。

如何將 Edge 指派給叢集中的特定中樞？

在傳統的中樞和支點拓撲中，SD-WAN Orchestrator 會為 Edge 提供其必須連線之中樞的邏輯識別碼。Edge 會要求其已指派的閘道提供該中樞邏輯識別碼的連線資訊 (即 IP 位址和連接埠)，以供 Edge 用來連線至該中樞。

從 Edge 的角度來看，此行為與連線至叢集時相同。Orchestrator 會通知 Edge 其應連線之中樞的邏輯識別碼為叢集邏輯識別碼，而非個別中樞邏輯識別碼。Edge 會遵循將中樞連線要求傳送至閘道的相同程序，並預期回應中的連線資訊。



此時，基本中樞行為有兩項分歧：

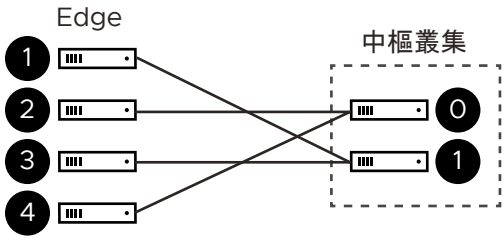
- **分歧一：**閘道必須選擇要指派的中樞。
- **分歧二：**基於分歧一，Edge 可能會從不同的閘道取得不同的指派。

分歧一最早的解決方式，是使用叢集評分將叢集中負載最輕的中樞指派給 Edge。這在理論上是可行的，但在實際環境中，這並非理想的解決方案，因為一般的重新指派事件可能涉及成千上百個 Edge，且叢集評分每 30 秒才會更新一次。換言之，如果中樞 1 的叢集評分為 20，中樞 2 的叢集評分為 21，則在 30 秒內，所有 Edge 都將選擇中樞 1，此時該中樞可能會超載，並觸發進一步的重新指派。

因此，閘道會先嘗試進行平均數學分配，而不考量叢集評分。Edge 邏輯識別碼 (由 Orchestrator 上的安全亂數產生器所產生) 將會有平均分配的值 (若提供足夠的 Edge)。這表示，使用邏輯識別碼可以計算平均分配。

- Edge 邏輯識別碼**模數**叢集中的中樞數目 = 已指派的中樞指數
- 例如：
  - 邏輯識別碼結尾分別為 1、2、3、4 的四個 Edge
  - 具有 2 個中樞的叢集
  - 1 % 2 = 1、2 % 2 = 0、3 % 2 = 1、4 % 2 = 0 (附註：「%」用來表示模數運算子)
  - 為 Edge 2 和 4 指派的中樞指數 0

- 為 Edge 1 和 3 指派的中樞指數 1



如此一致性優於循環配置資源類型指派，因為這表示 Edge 每次都會傾向於被指派相同的中樞，進而使指派和疑難排解更容易預測。

備註 中樞重新啟動 (例如，因維護或失敗) 時，將會與閘道中斷連線並從叢集中移除。這表示 Edge 在所有 Edge 重新啟動後一律會平均分配 (基於前述的邏輯)，但在任何導致其中斷連線的中樞事件發生後將不平均地分配。

當中樞超過其允許的通道容量上限時，會發生什麼情況？

Edge 指派邏輯會嘗試將 Edge 平均分配到所有可用的中樞之間。但在中樞上發生某事件 (例如重新啟動) 之後，Edge 分配將不再平均。

備註 一般而言，閘道會在初始指派時嘗試將 Edge 平均分配到中樞之間，不均勻的分配並不會被視為無效狀態。如果指派不均勻，但沒有個別中樞超過 70% 的通道容量，則會將指派視為有效。

由於中樞上的此類事件 (或將其他 Edge 新增至網路)，叢集可能會達到個別中樞已超過其允許通道容量的 70% 的臨界點。如果發生此情況，且至少另有一個中樞的通道容量低於 70%，則無論 Orchestrator 上是否啟用重新平衡，都會自動執行平均的重新分配。由於使用邏輯識別碼可預期數學指派，多數的 Edge 會保留其現有的指派，且由於容錯移轉或先前的使用量重新平衡而已指派給其他中樞的 Edge 將會重新平衡，以確保叢集會自動恢復為平均分配。

當中樞超過其允許的叢集評分上限時，會發生什麼情況？

不同於可直接對其操作的通道百分比 (容量的直接量值)，叢集評分每 30 秒才會更新一次，且在進行 Edge 重新指派後，閘道無法自動計算調整的叢集評分。在叢集組態中會提供自動重新平衡參數，以指出閘道是否應視需要動態嘗試移轉每個中樞的 Edge 負載。

如果自動重新平衡已停用，而中樞的叢集評分超過 70 (但通道容量未超過 70%)，則不會採取任何動作。

如果已啟用自動重新平衡，且有一或多個中樞的叢集評分超過 70，則閘道會每分鐘將一個 Edge 重新指派給目前叢集評分最低的中樞，直到所有中樞的評分皆低於 70 或不再可能有重新指派為止。

備註 依預設，會停用自動重新平衡。

當兩個 VMware SD-WAN 閘道提供不同的中樞指派時，會發生什麼情況？

如同分散式控制平面的本質，每個閘道對於叢集指派會進行個別判斷。在多數情況下，閘道會使用相同的數學公式，因而達成所有 Edge 的相同指派。不過，在依據叢集評分進行重新平衡的類似情況下，即無法保證達成。

如果 Edge 目前未連線至叢集中的中樞，則它將接受任何回應閘道所提供的指派。這可確保在有些閘道關閉、有些閘道啟動的情況下，Edge 絕不會未獲指派。

如果 Edge 連線至叢集中的中樞，並且收到一則訊息指出應選擇替代中樞，此訊息將會以「閘道喜好設定」的順序進行處理。例如，如果超級閘道已連線，則 Edge 將只會接受來自超級閘道的重新指派。系統將會忽略其他閘道要求的衝突指派。同樣地，如果超級閘道未連線，則 Edge 將只會接受來自替代超級閘道的重新指派。對於合作夥伴閘道 (其中不存在超級閘道)，閘道喜好設定會取決於針對該特定 Edge 所設定的合作夥伴閘道順序。

備註 當使用合作夥伴閘道時，必須將相同的閘道指派給叢集中的中樞以及支點 Edge，否則，可能會出現支點 Edge 無法收到中樞指派的情況，因為支點 Edge 所連線的閘道也未連線至叢集中的中樞。

當 VMware SD-WAN 閘道關閉時會發生什麼情況？

當 SD-WAN 閘道關閉時，如果最慣用的閘道就是已關閉的閘道，而第二慣用的閘道提供了不同的指派，則可以重新指派 Edge。例如，超級閘道將中樞 A 指派給此 Edge，而替代超級閘道將中樞 B 指派給相同的 Edge。

超級閘道的關閉將會導致 Edge 容錯移轉至中樞 B，因為替代超級閘道現在用於連線資訊最為慣用的閘道。

當超級閘道復原時，Edge 會再次從此閘道要求中樞指派。為了避免 Edge 在上述案例中再次切換回中樞 A，中樞指派要求會包含目前已指派的中樞 (如果有的話)。當閘道處理指派要求時，如果 Edge 目前被指派了叢集中的中樞，而該中樞的叢集評分低於 70，則該閘道會更新其本機指派以符合現有的指派，而不使用其指派邏輯。這可確保超級閘道在復原後將會指派目前已連線的中樞，並防止其已指派的 Edge 進行不必要的容錯移轉。

如果叢集中的中樞失去其動態路由，會發生什麼情況？

如前所述，中樞每 30 秒會向 SD-WAN 閘道報告它們透過 BGP 學習的動態路由數。如果叢集中僅有一個中樞的路由遺失，則可能是因為這些路由錯誤撤回或 BGP 芳鄰關係失敗，因此 SD WAN 閘道會將支點 Edge 容錯移轉至叢集中具有完整路由表的另一個中樞。

由於更新每 30 秒傳送一次，因此路由計數會以更新傳送至 SD-WAN 閘道的時間點為基礎。SD-WAN 閘道每 60 秒會執行一次重新平衡邏輯，這表示萬一完全失去某個 LAN 端 BGP 芳鄰時，使用者可預期容錯移轉會花費 30-60 秒。為了確保所有中樞在此情況下都有機會再次更新閘道，我們將重新平衡限制為最快每 120 秒執行一次。這表示在連續失敗第二次後，使用者可預期容錯移轉會花費 120 秒。

如何在叢集中樞上設定路由？

由於閘道可以指示支點連線至叢集中的任何成員中樞，因此，應將路由組態鏡像到所有中樞上。例如，如果支點必須連線至中樞後面的 BGP 首碼 192.168.2.1，則叢集中的所有中樞都應通告 192.168.2.1 以及完全相同的路由屬性。

叢集部署中應使用 BGP 上行社群標籤。設定叢集節點，以便將路由重新分配至 BGP 對等時，設定上行社群標籤。

如果叢集中的中樞失敗，會發生什麼情況？

SD-WAN 閘道會先等待通道被宣告為無作用 (7 秒)，之後再容錯移轉支點 Edge。這表示當 SD-WAN 中樞或及其相關聯的所有 WAN 連結失敗時，使用者可預期容錯移轉將會花費 7-10 秒 (取決於 RTT)。

設定 Edge 叢集化

您可以依照本節中的步驟來設定 Edge 叢集。

1 若要存取 **Edge 叢集 (Edge Cluster)** 區域，請移至**設定 (Configure)** > **網路服務 (Network Services)**。

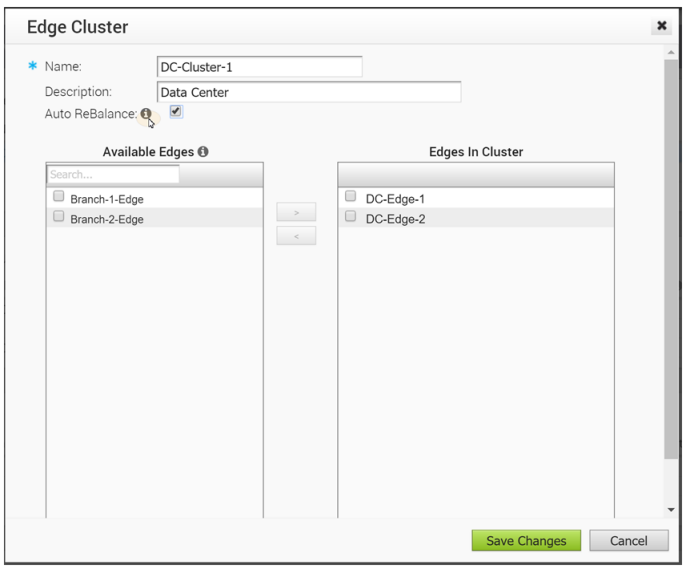
2 若要新增叢集：

a 在 **Edge 叢集 (Edge Cluster)** 區域中，按一下**新增叢集 (New Cluster)** 按鈕。

b 在 **Edge 叢集 (Edge Cluster)** 對話方塊中，在適當的文字方塊中輸入名稱和說明。

c 如有需要，請啟用**自動重新平衡 (Auto Rebalance)** (依預設不會啟用此功能)。

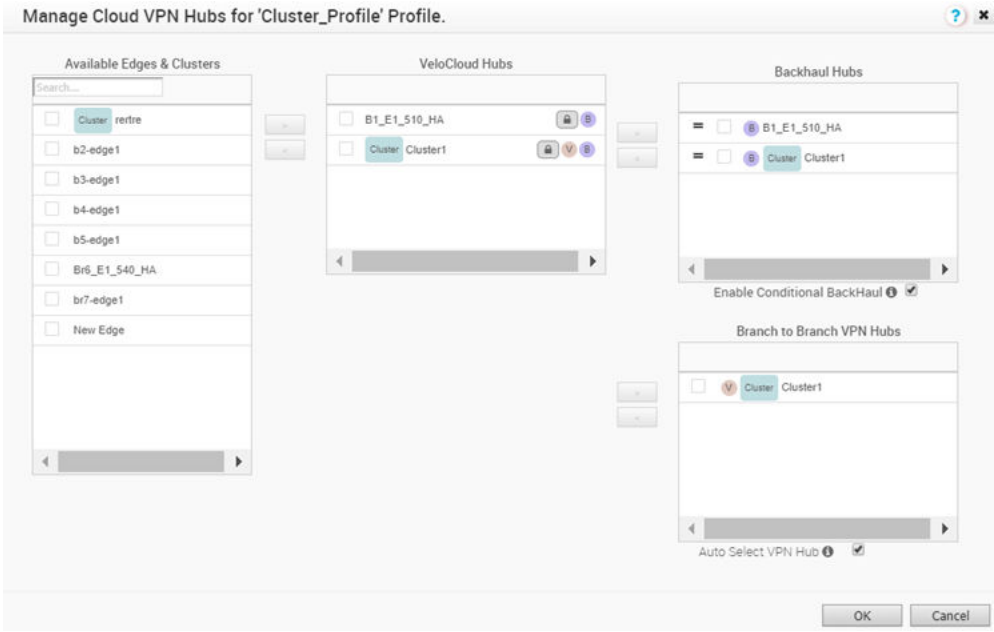
> **備註** 如果啟用此選項，當中樞叢集中的個別 Edge 超過叢集評分 70 時，支點即會以每分鐘一個支點的速率重新平衡，直到叢集評分降至 70 以下為止。將支點 Edge 重新指派給不同的中樞時，支點 Edge 的 VPN 通道將會中斷連線，且可能會有長達 6-10 秒的停機時間。如果叢集中所有中樞的叢集評分都超過 70，則不會執行重新平衡。如需叢集評分的詳細資訊，請參閱標題為 Edge 叢集化的運作方式一節。



d 在**可用的 Edge (Available Edges)** 區段中選取一個 Edge，然後使用 > 按鈕將其移至**叢集中的 Edge (Edges In Cluster)** 區段。

e 按一下**儲存變更 (Save Changes)**。已設定的 Edge 叢集將會顯示在所選設定檔之**管理雲端 VPN 中樞 (Manage Cloud VPN Hubs)** 畫面的**可用的 Edge 和叢集 (Available Edges & Clusters)** 區域下方。

備註 作為中樞或位於中樞叢集內、或設定為作用中/待命 HA 配對的 Edge，不會顯示在**可用的 Edge (Available Edges)** 清單區域中。



3 在**管理雲端 VPN 中樞 (Manage Cloud VPN Hubs)** 畫面中，您可以將 Edge 叢集和個別 Edge 同時設定為分支設定檔中的中樞。Edge 指派給叢集後，即無法指派為個別中樞。選擇 Edge 叢集作為分支設定檔中的中樞。

4 若要使用也是 Edge 叢集的中樞設定「分支到分支 VPN」，您應先從**中樞 (Hubs)** 區域中選取中樞，然後將其移至**分支到分支 VPN 中樞 (Branch to Branch VPN Hubs)** 區域。

5 您也可以將中樞叢集設定為商務原則組態中的網際網路回傳中樞，方法是先從**中樞 (Hubs)** 區域中選取中樞，然後將其移至**回傳中樞 (Backhaul Hubs)** 區域。

6 若要啟用條件式回傳，請選取**啟用條件式回傳 (Enable Conditional BackHaul)** 核取方塊。在啟用條件式回傳 (CBH) 的情況下，每當沒有公用網際網路連結可供使用時，Edge 都能夠將網際網路繫結流量 (直接網際網路流量、透過 SD-WAN Gateway 的網際網路流量，和透過 IPsec 的雲端安全性流量) 容錯移轉至 MPLS 連結。當條件式回傳啟用時，依預設，分支層級的所有商務原則規則都必須依循透過條件式回傳容錯移轉流量的準則。您可以根據所選原則的特定需求，將流量從條件式回傳中排除，只要在選取的商務原則層級停用此功能即可。如需詳細資訊，請參閱條件式回傳。

備註 必須在叢集的 LAN 端上執行動態路由通訊協定，例如 eBGP。

對 Edge 叢集化進行疑難排解

本節說明 Edge 叢集化的疑難排解增強功能。

概觀

Edge 叢集化包含疑難排解功能，可重新平衡叢集內的 VMware SD-WAN 輪輻 Edge。輪輻的平衡可對叢集內的任何中樞執行。有兩種方法可以重新平衡輪輻：

- 在叢集內的所有中樞之間平均重新平衡輪輻。
- 排除一個中樞，並在叢集中的剩餘中樞之間重新平衡輪輻。

使用 VMware SD-WAN Orchestrator 重新平衡中樞上的輪幅

管理員可以透過 VMware SD-WAN Orchestrator 上的**遠端診斷 (Remote Diagnostics)**，重新平衡叢集中的輪輻。將 SD-WAN Edge 部署為叢集中的中樞時，會出現名為**重新平衡中樞叢集 (Rebalance Hub Cluster)** 的新遠端診斷選項，而為使用者提供兩個選項。

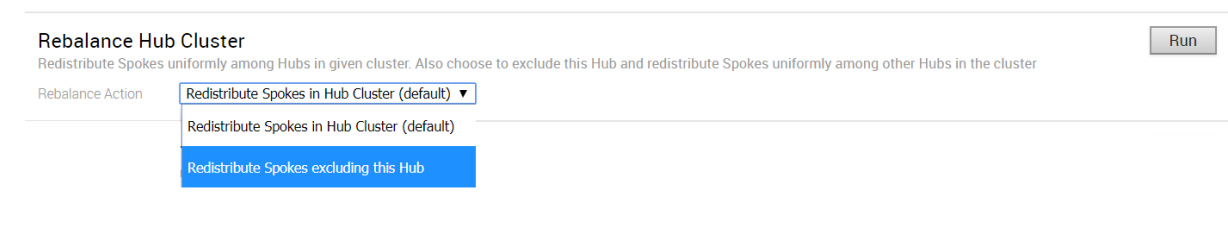
重新分配中樞叢集中的輪輻

- 此選項會嘗試將輪輻 Edge 平均地重新分配於叢集中的所有中樞 Edge 之間。

排除此中樞的重新分配輪輻

- 此選項會嘗試將輪輻 Edge 平均地重新分配於叢集中的中樞之間，但排除使用者執行「重新分配輪輻」公用程式所在的中樞 Edge。
- 此選項可用於疑難排解或維護，以移除此中樞 Edge 中的所有輪輻。

下圖顯示中樞的**遠端診斷 (Remote Diagnostics)** 區段。



備註 當輪輻移至叢集中的不同中樞時，重新平衡輪輻將會導致短暫的流量中斷。因此，強烈建議在維護時段內使用此疑難排解機制。

設定 Non VMware SD-WAN Site

VMware 支援下列 Non VMware SD-WAN Site 組態：

- 檢查點
- Cisco ASA
- Cisco ISR
- 一般 IKEv2 路由器 (以路由為基礎的 VPN)
- Microsoft Azure 虛擬中樞
- Palo Alto

- SonicWALL
- Zscaler
- 一般 IKEv1 路由器 (以路由為基礎的 VPN)
- 一般防火牆 (以原則為基礎的 VPN)

備註 VMware 現在支援一般 IKEv1 路由器 (以路由為基礎的 VPN) 和一般 IKEv2 路由器 (以路由為基礎的 VPN) Non VMware SD-WAN Site 組態。

Cisco ASA

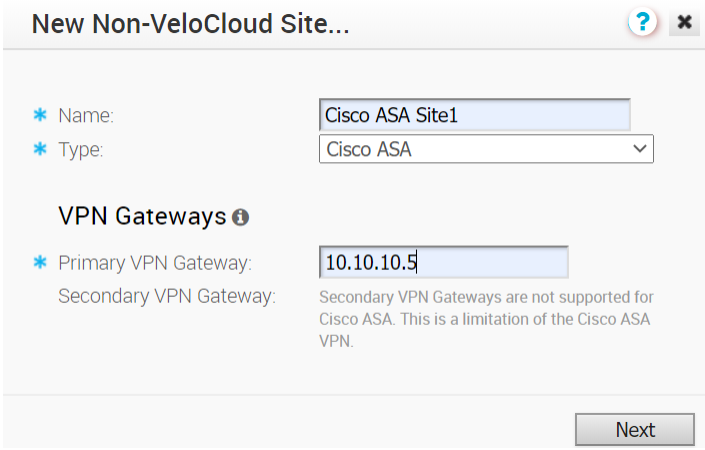
Cisco ASA 是另一個常見的第三方組態。以下說明如何在 SD-WAN Orchestrator 中使用 Cisco ASA 進行設定的指示。

若要透過 Cisco ASA 進行設定：

1 移至**設定 (Configure)** > **網路服務 (Network Services)**。

2 在**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中，按一下**新增 (New)** 按鈕。

新增非 VeloCloud 站台 (New Non-VeloCloud Site) 對話方塊隨即出現。



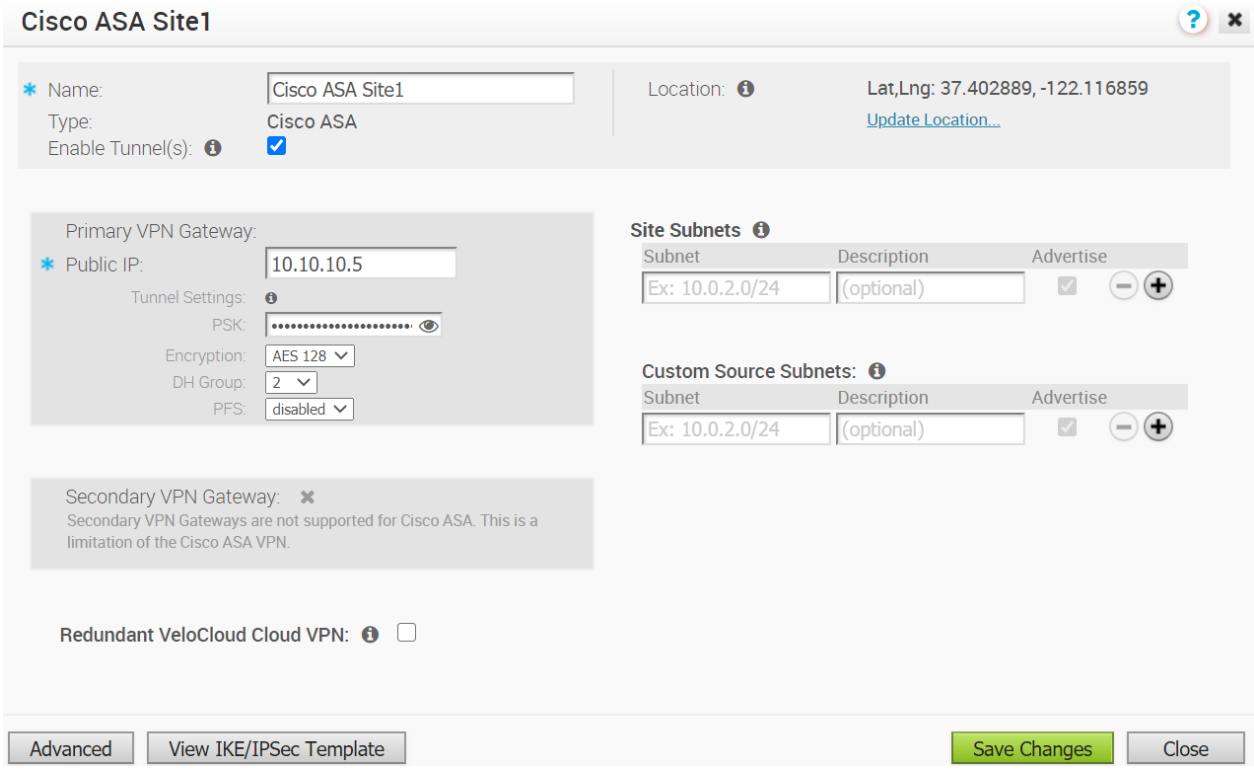
3 在**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊中：

a 在**名稱 (Name)** 文字方塊中，輸入 Non VMware SD-WAN Site 的名稱。

b 在**類型 (Type)** 下拉式功能表中，選取 **Cisco ASA**。

c 輸入主要 VPN 閘道的 IP 位址，然後按**下一步 (Next)**。

您的 Non VMware SD-WAN Site 隨即建立，並顯示 Non VMware SD-WAN Site 對話方塊。



4 在您 Non VMware SD-WAN Site 的對話方塊中：

a 若要設定 Non VMware SD-WAN Site 主要 VPN 閘道的通道設定，請按一下位於對話方塊底部的**進階 (Advanced)** 按鈕。

b 在**主要 VPN 閘道 (Primary VPN Gateway)** 區域中，您可以設定下列通道設定：

欄位	說明
PSK	預先共用金鑰 (PSK)，這是在通道間進行驗證時所使用的安全性金鑰。依預設，Orchestrator 會產生 PSK。如果您想要使用自己的 PSK 或密碼，可以在文字方塊中輸入。
加密 (Encryption)	選取 **AES 128** 或 **AES 256** 作為加密資料的演算法。預設值為 AES 128。
DH 群組 (DH Group)	選取交換預先共用金鑰時所要使用的 Diffie-Hellman (DH) 群組演算法。DH 群組會設定演算法的強度 (以位元為單位)。預設值為 2。
PFS	選取完全正向加密 (PFS) 層級以取得額外的安全性。預設值為 2。

備註 Cisco ASA 網路服務類型不支援次要 VPN 閘道。

備註 依預設，針對 Cisco ASA Non VMware SD-WAN Site 使用的本機驗證識別碼值為 SD-WAN Gateway 介面本機 IP。

c 選取**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 核取方塊，為每個 VPN 閘道新增備援通道。

對主要 VPN 閘道的加密、DH 群組或 PFS 所做的任何變更，也將套用至備援 VPN 通道 (如果已設定)。在修改主要 VPN 閘道的通道設定後儲存變更，然後按一下**檢視 IKE/IPSec 範本 (View IKE/IPSec Template)**，以檢視更新的通道組態。

d 按一下**更新位置 (Update location)** 連結，為已設定的 Non VMware SD-WAN Site 設定位置。緯度和經度詳細資料可用來判斷在網路中要連線到的最佳 Edge 或閘道。

e 在**站台子網路 (Site Subnets)** 下方，您可以按一下 **+** 按鈕以新增 Non VMware SD-WAN Site 的子網路。

f 使用**自訂來源子網路 (Custom Source Subnets)**，覆寫路由至此 VPN 裝置的來源子網路。通常，來源子網路會衍生自路由至此裝置的 Edge LAN 子網路。

g 當您準備好起始從 SD-WAN Gateway 到 Cisco ASA VPN 閘道的通道後，請勾選**啟用通道 (Enable Tunnel(s))** 核取方塊。

h 按一下**儲存變更 (Save Changes)**。

Cisco ISR

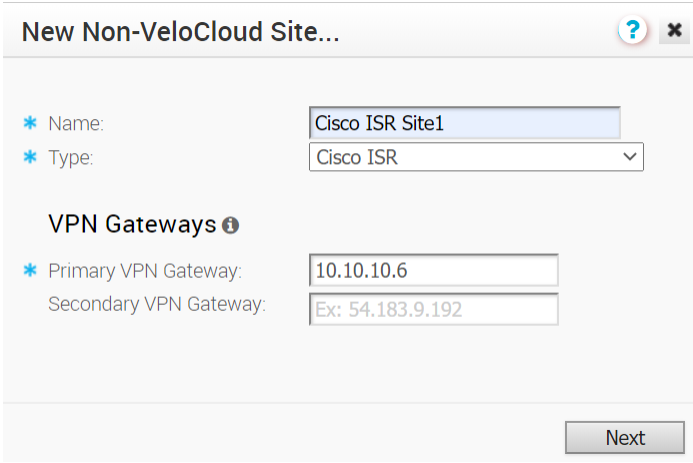
Cisco ISR 是較為常見的第三方組態之一。以下說明如何在 SD-WAN Orchestrator 中使用 Cisco ISR 進行設定的指示。

若要透過 Cisco ISR 進行設定：

1 移至**設定 (Configure) > 網路服務 (Network Services)**。

2 在**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中，按一下**新增 (New)** 按鈕。

[新增非 VeloCloud 站台 (New Non-VeloCloud Site)] 對話方塊隨即出現。



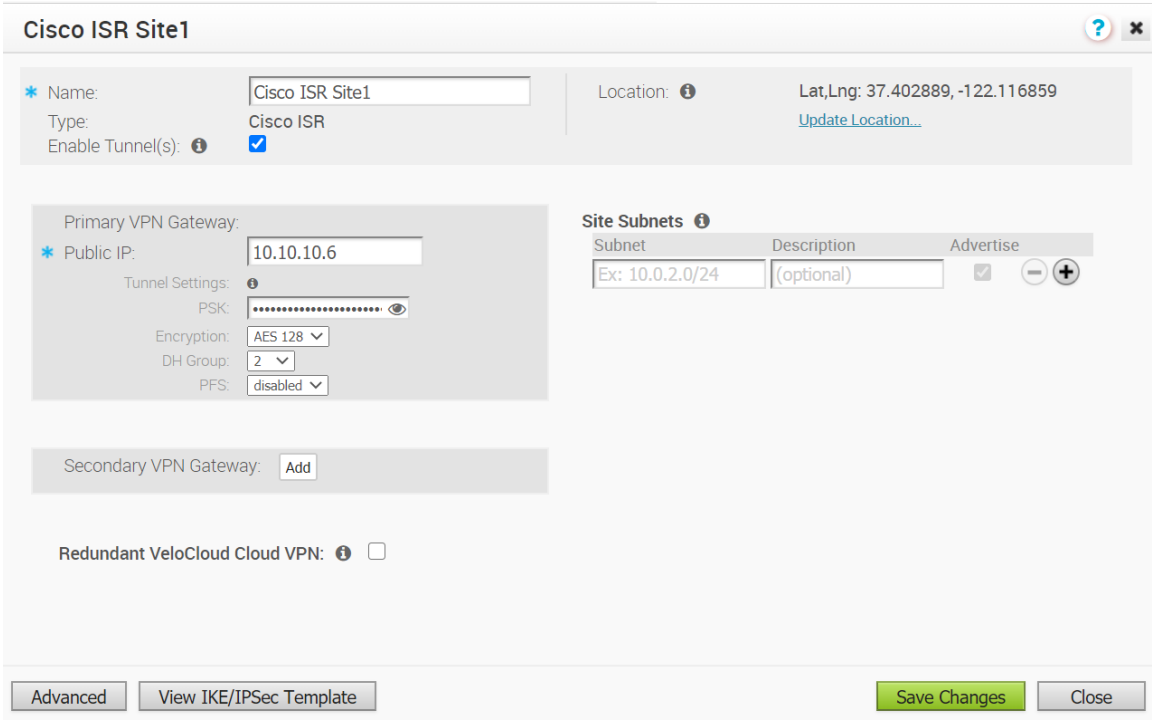
3 在**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊中：

a 在**名稱 (Name)** 文字方塊中，輸入 Non VMware SD-WAN Site 的名稱。

b 在**類型 (Type)** 下拉式功能表中，選取 **Cisco ISR**。

c 輸入主要 VPN 閘道的 IP 位址，然後按**下一步 (Next)**。

您的 Non VMware SD-WAN Site 隨即建立，並顯示 Non VMware SD-WAN Site 對話方塊。



4 在您 Non VMware SD-WAN Site 的對話方塊中：

a 若要設定 Non VMware SD-WAN Site 主要 VPN 閘道的通道設定，請按一下位於對話方塊底部的**進階 (Advanced)** 按鈕。

b 參考上表來設定通道設定，例如 PSK、加密、DH 群組和 PFS。

c 如果您想要為此站台建立次要 VPN 閘道，請按一下**次要 VPN 閘道 (Secondary VPN Gateway)** 旁的**新增 (Add)** 按鈕。在快顯視窗中，輸入次要 VPN 閘道的 IP 位址，然後按一下**儲存變更 (Save Changes)**。

系統將立即為此站台建立次要 VPN 閘道，並將 VMware VPN 通道佈建至此閘道。

備註 依預設，針對 Cisco ISR Non VMware SD-WAN Site 使用的本機驗證識別碼值為 SD-WAN Gateway 介面本機 IP。

d 選取**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 核取方塊，為每個 VPN 閘道新增備援通道。

e 在**站台子網路 (Site Subnets)** 下方，您可以按一下 **+** 按鈕以新增 Non VMware SD-WAN Site 的子網路。

f 當您準備好起始從 SD-WAN Gateway 到 Cisco ISR VPN 閘道的通道後，請勾選**啟用通道 (Enable Tunnel(s))** 核取方塊。

g 按一下**儲存變更 (Save Changes)**。

Microsoft Azure 虛擬中樞

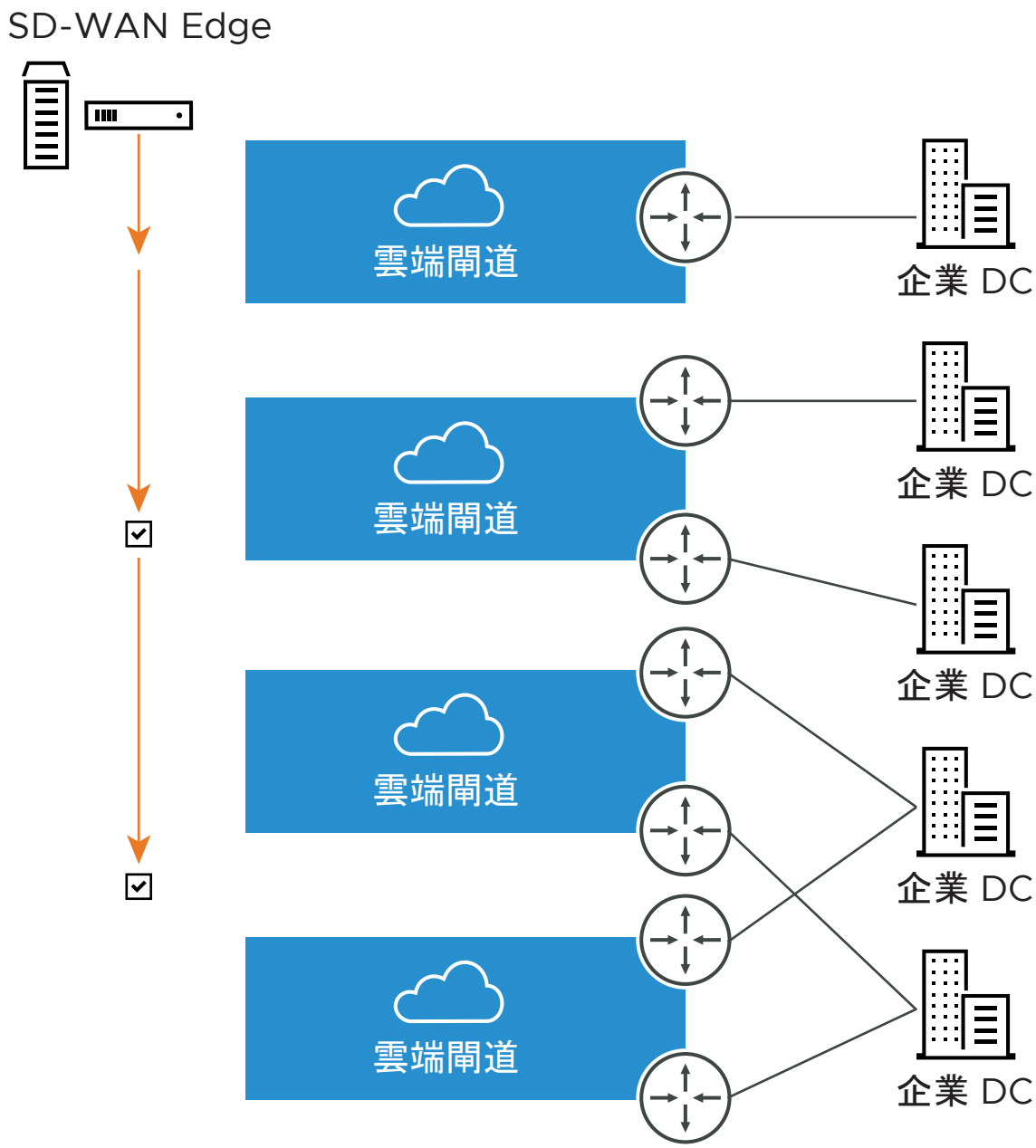
Microsoft Azure 虛擬中樞是較為常見的第三方組態之一。如需相關指示以在 SD-WAN Orchestrator 中設定 Microsoft Azure 虛擬中樞類型的 Non VMware SD-WAN Site，請參閱設定 Microsoft Azure Non VMware SD-WAN Site。

VPN 工作流程

這是一項選擇性服務，可讓您建立 VPN 通道組態，以存取一或多個 Non VMware SD-WAN Sites。VMware 提供建立通道所需的組態，包括建立 IKE IPSec 組態及產生預先共用的金鑰。

概觀

下圖說明在 VMware 和 Non VMware SD-WAN Site 之間建立的 VPN 通道的概觀。

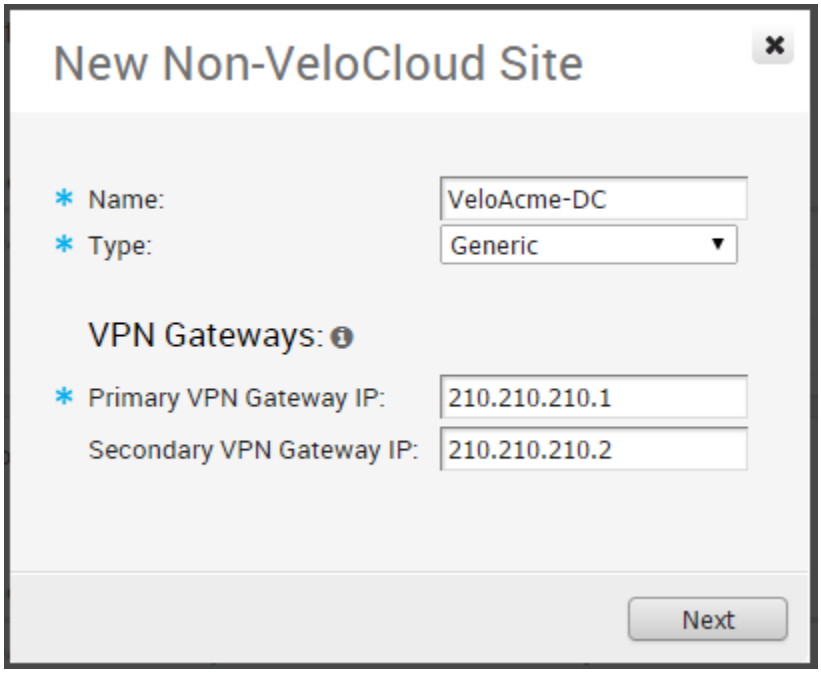


備註 您必須在 Non VMware SD-WAN Site 為主要 VPN 閘道指定 IP 位址。IP 位址會用來形成 SD-WAN Gateway 與主要 VPN 閘道之間的主要 VPN 通道。

或者，可以指定次要 VPN 閘道的 IP 位址，以形成 SD-WAN Gateway 與次要 VPN 閘道之間的次要 VPN 通道。使用進階設定，可為您建立的任何 VPN 通道指定備援 VPN 通道。

新增 Non VMware SD-WAN Site VPN 閘道

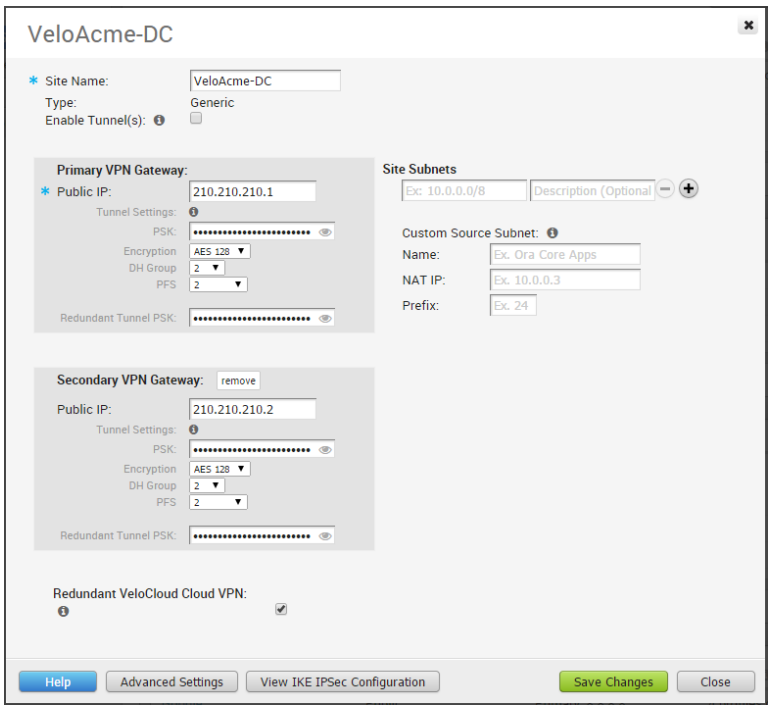
輸入名稱 (Name) 並選擇閘道類型 (Type)。指定主要 VPN 閘道的 IP 位址，並選擇性地指定次要 VPN 閘道的 IP 位址。



設定 Non VMware SD-WAN Site 子網路

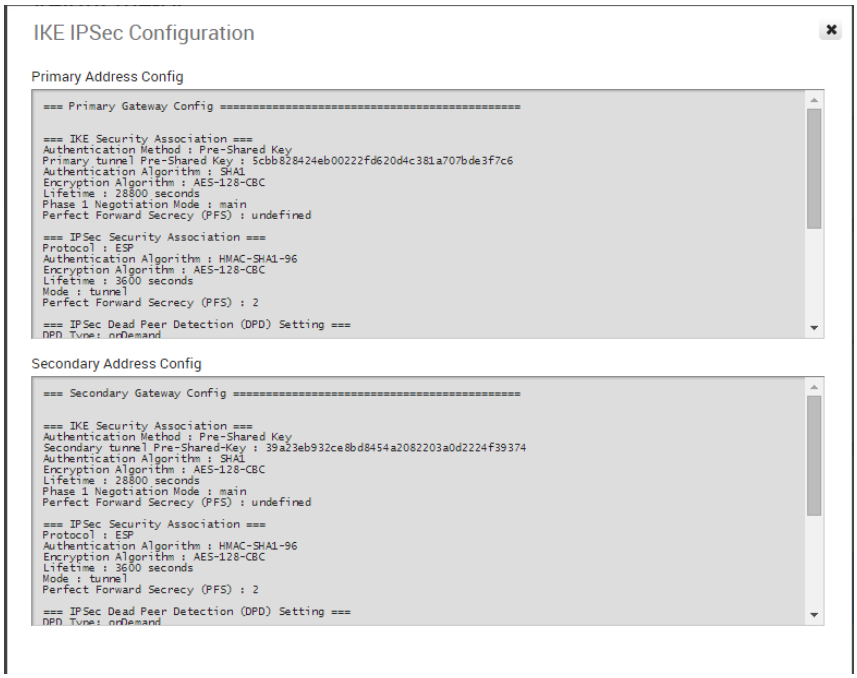
建立 Non VMware SD-WAN Site 組態後，您可以新增站台子網路並設定通道設定。

按一下**進階設定 (Advanced Settings)** 按鈕，以輸入其他子網路參數、VPN 閘道參數，以及新增備援 VPN 通道。



檢視 IKE IPSec 組態，設定 Non VMware SD-WAN Site 閘道

如果按一下 [檢視 IKE IPSec 組態 (View IKE IPSec Configuration)] 按鈕，則會顯示設定 Non VMware SD-WAN Site 閘道所需的資訊。閘道管理員應使用這項資訊來設定閘道 VPN 通道。



啟用 IPSec 通道

Non VMware SD-WAN Site VPN 通道最初會停用。您必須在設定 Non VMware SD-WAN Site 閘道之後且第一次使用「Edge 到 Non VMware SD-WAN Site VPN」之前啟用通道。

設定 Check Point

SD-WAN Gateway 會使用 IKEv1/IPsec 連線至 Check Point CloudGuard 服務。設定 Check Point 時須執行兩個步驟：設定 Checkpoint CloudGuard 服務，以及在 SD-WAN Orchestrator 上設定 Checkpoint。您將在 Check Point Infinity 入口網站上執行第一個步驟，並在 SD-WAN Orchestrator 上執行第二個步驟。

按一下下列幾節的連結，以完成設定 Check Point 的指示。

步驟 1：設定 Check Point CloudGuard Connect

步驟 2：在 SD-WAN Orchestrator 上將 Check Point 設定為 Non VMware SD-WAN Site

必要條件

您必須具有作用中的 Check Point 帳戶和登入認證，才能存取 Check Point Infinity 入口網站。

設定 Check Point CloudGuard Connect

如何設定 Check Point CloudGuard 服務的指示。

您必須具有作用中的 Check Point 帳戶和登入認證，才能存取 Check Point Infinity 入口網站。

程序

1 若要設定 Check Point CloudGuard 服務，請登入 Check Point 的 Infinity 入口網站 (https://portal.checkpoint.com/)。

2 登入後，請透過下列連結在 Check Point Infinity 入口網站上建立站台：https://sc1.checkpoint.com/documents/integrations/VeloCloud/check-point-VeloCloud-integration.html

   在 Check Point 的 Infinity 入口網站上建立站台後，在 SD-WAN Orchestrator 上將 Check Point 設定為 Non VMware SD-WAN Site

在 SD-WAN Orchestrator 上將 Check Point 設定為 Non VMware SD-WAN Site

在 Check Point Infinity 入口網站上建立站台之後，請在 SD-WAN Orchestrator 上將 Check Point 設定為 Non VMware SD-WAN Site。

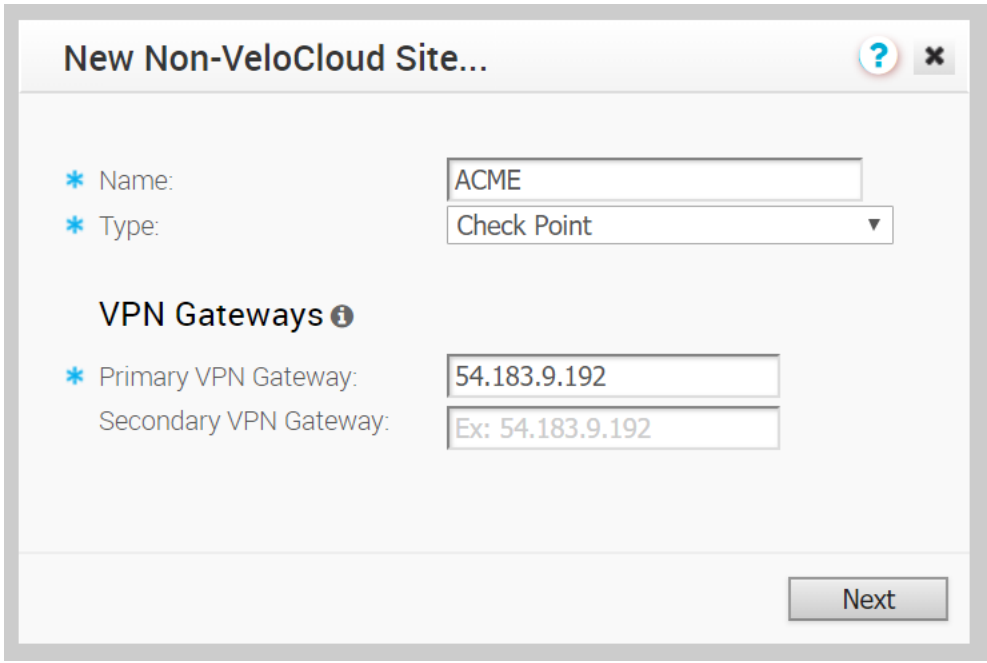
在 Check Point Infinity 入口網站上建立站台之後，請完成以下步驟：

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure) > 網路服務 (Network Services)**

2 在**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中，按一下**新增 (New)** 按鈕。

新增非 VeloCloud 站台 (New Non-VeloCloud Site) 對話方塊隨即出現。



3 在**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊中，完成下列子步驟：

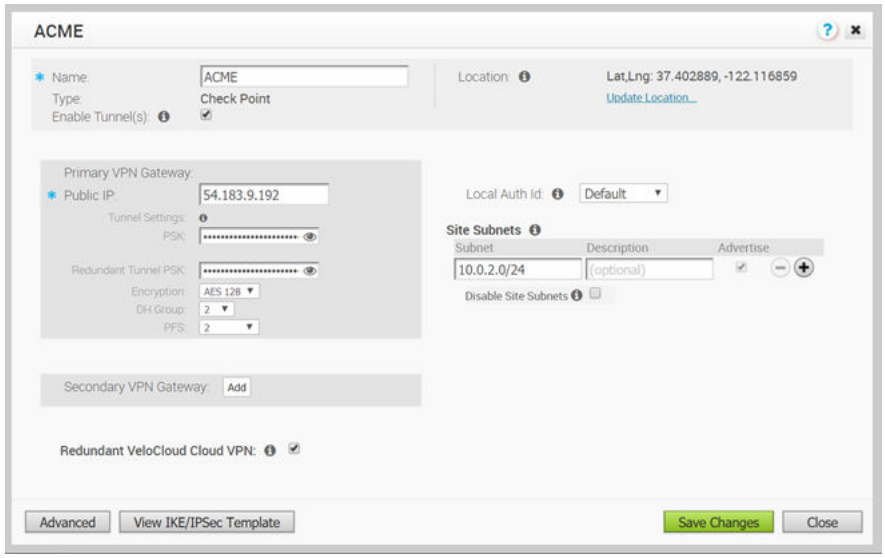
a 輸入您的站台名稱。

b 在**類型 (Type)** 下拉式功能表中，選取 Check Point。

c 輸入主要 VPN 閘道 (如有必要，請輸入次要 VPN 閘道)。

d 按**下一步 (Next)**。

Non VMware SD-WAN Site 的對話方塊隨即出現。(請見下圖)。



備註 若要設定對 Non VMware SD-WAN Site 主要 VPN 閘道的通道設定，請按一下位於對話方塊底部的 [進階 (Advanced)] 按鈕。對加密、DH 群組或 PFS 所做的任何變更，也將套用至備援通道組態。儲存變更後，請更新站台的主要 VPN 閘道裝置。按一下 [檢視 IKE/IPSec 範本 (View IKE/IPSec Template)] 按鈕，以取得詳細資料。

4 在 [主要 VPN 閘道 (Primary VPN Gateway)] 區域中，輸入下列項目：

a **PSK**：輸入在 Check Point Infinity 入口網站上設定的預先共用金鑰。請勿設定備援 IPsec 通道 (將**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 的核取方塊保留為取消勾選)。

b **加密 (Encryption)**：加密應設定為在 Check Point Infinity 入口網站上設定的相同演算法。

c **DH 群組 (DH Group)**：DH 群組應設定為在 Check Point Infinity 入口網站上設定的相同值。

d 針對此 Check Point 組態的用途，從 PFS 下拉式功能表中選擇**已停用 (disabled)**。

5 若要新增次要 VPN 閘道，請按一下**新增 (Add)** 按鈕。按一下**儲存變更 (Save Changes)** 按鈕會立即建立此站台的次要 VPN 閘道，並佈建此閘道的 VMware VPN 通道。

備註 依預設，針對 Checkpoint Non VMware SD-WAN Site 使用的本機驗證識別碼值為 SD-WAN Gateway 介面公用 IP。

6 如上述步驟 4a 所述，將**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 核取方塊取消勾選。

7 針對 Check Point 組態的用途，從 [本機驗證識別碼 (Local Auth Id)] 下拉式功能表中選擇**預設 (Default)**。

8 針對 Check Point 組態的用途，勾選**停用站台子網路 (Disable Site Subnets)** 核取方塊。

9 按一下**儲存變更 (Save Changes)**。

10 當您準備好起始從 SD-WAN Gateway 到 Check Point CloudGuard VPN 閘道的通道後，請勾選**啟用通道 (Enable Tunnel(s))** 核取方塊。

設定 Zscaler

Zscaler 設定包含四個主要步驟。您必須執行所有四個步驟才能完成此設定。

前三個主要步驟包括設定 VMware 與 Zscaler 之間的 VPN IPSec 通道閘道，而最後一個步驟則需要您設定商務規則。完成下列設定步驟：

1 建立和設定 Non VMware SD-WAN Site。

2 將 Non VMware SD-WAN Site 新增至組態設定檔。

3 Zscaler 組態：建立帳戶、新增 VPN 認證、新增位置。

4 設定商務優先順序規則。

備註 您將在 SD-WAN Orchestrator 中執行步驟 1、步驟 2 和步驟 4。您將在 Zscaler 站台上執行步驟 3。

建立和設定 Non VMware SD-WAN Site

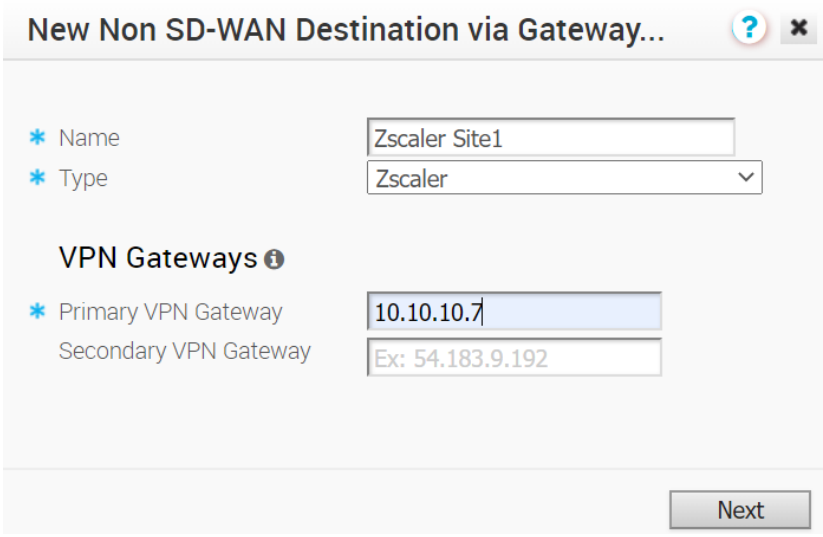
若要建立和設定 Non VMware SD-WAN Site：

1 在導覽面板中，按一下**設定 (Configure)** > **網路服務 (Network Services)**。

服務 (Services) 畫面隨即出現。

2 在**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中，按一下**新增 (New)** 按鈕。

新增非 VeloCloud 站台 (New Non-VeloCloud Site) 對話方塊隨即出現。

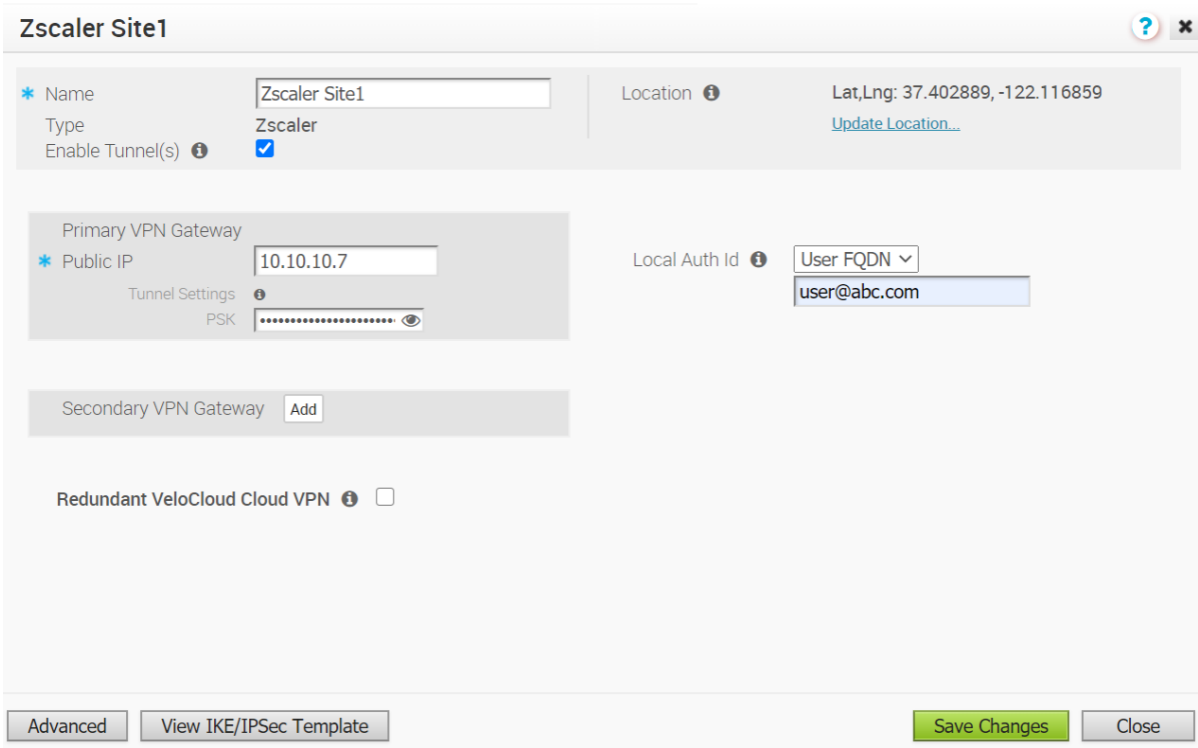


3 在**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊中：

a 在**名稱 (Name)** 文字方塊中，輸入 Non VMware SD-WAN Site 的名稱。

b 在**類型 (Type)** 下拉式功能表中，選取 **Zscaler**。

c 輸入主要 VPN 閘道的 IP 位址 (必要時也輸入次要 VPN 閘道的位址)，然後按**下一步 (Next)**。此時會建立 Zscaler 類型的 Non VMware SD-WAN Site，並顯示 Non VMware SD-WAN Site 的對話方塊。



4 在您 Non VMware SD-WAN Site 的對話方塊中：

a 若要設定 Non VMware SD-WAN Site 主要 VPN 閘道的通道設定，請按一下**進階 (Advanced)** 按鈕。

b 在**主要 VPN 閘道 (Primary VPN Gateway)** 區域中的**通道設定 (Tunnel Settings)** 下方，您可以設定預先共用金鑰 (PSK)，這是在通道間進行驗證時所使用的安全性金鑰。依預設，Orchestrator 會產生 PSK。如果您想要使用自己的 PSK 或密碼，可以在文字方塊中輸入。

c 如果您想要為此站台建立次要 VPN 閘道，請按一下**次要 VPN 閘道 (Secondary VPN Gateway)** 旁的**新增 (Add)** 按鈕。在快顯視窗中，輸入次要 VPN 閘道的 IP 位址，然後按一下**儲存變更 (Save Changes)**。系統將立即為此站台建立次要 VPN 閘道，並將 VMware VPN 通道佈建至此閘道。

d 選取**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 核取方塊，為每個 VPN 閘道新增備援通道。對主要 VPN 閘道的 PSK 所做的任何變更，也將套用至備援 VPN 通道 (如果已設定)。在修改主要 VPN 閘道的通道設定後儲存變更，然後按一下**檢視 IKE/IPSec 範本 (View IKE/IPSec Template)**，以檢視更新的通道組態。

e 按一下**更新位置 (Update location)** 連結，為已設定的 Non VMware SD-WAN Site 設定位置。緯度和經度詳細資料可用來判斷在網路中要連線到的最佳 Edge 或閘道。

f 本機驗證識別碼會定義本機閘道的格式和識別。從**本機驗證識別碼 (Local Auth Id)** 下拉式功能表中，選擇下列其中一種類型，然後輸入您決定的值：

- **FQDN** - 完整網域名稱或主機名稱。例如 google.com。
- **使用者 FQDN (User FQDN)** - 電子郵件地址形式的使用者完整網域名稱。例如 user@google.com。
- **IPv4** - 用來與本機閘道進行通訊的 IP 位址。

備註 對於 Zscaler Non VMware SD-WAN Site，**建議使用 FQDN 或使用者 FQDN 作為本機驗證識別碼**。

複製本機驗證詳細資料和 PSK 密碼。(在 Zscaler 帳戶中設定 VPN 認證時，將需要這項資訊)。

g 當您準備好起始從 SD-WAN Gateway 到 Zscaler VPN 閘道的通道後，請勾選**啟用通道 (Enable Tunnel(s))** 核取方塊。

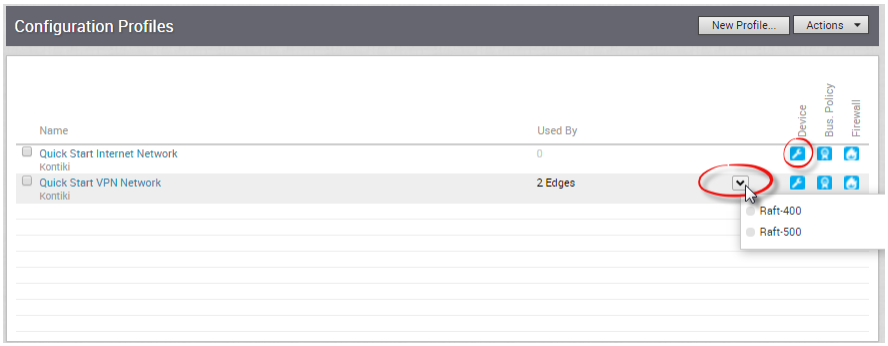
h 按一下**儲存變更 (Save Changes)**。

將 NVS 與組態設定檔相關聯

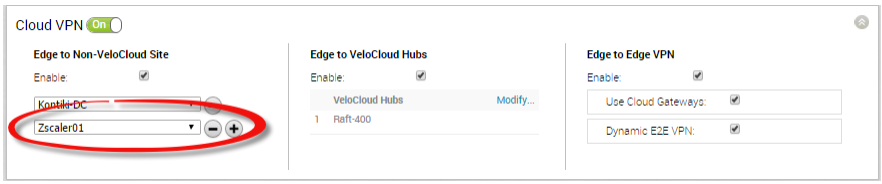
若要將 NVS 與組態設定檔相關聯：

1 在導覽面板中，按一下**設定 (Configure) > 設定檔 (Profiles)**。

2 在**設定設定檔 (Configure Profiles)** 畫面中，按一下設定檔右側的**裝置 (Devices)** 圖示 。(如有多個 Edge，請使用下拉式功能表選取 Edge，然後按一下**裝置 (Device)** 索引標籤)。



3 在**雲端 VPN (Cloud VPN)** 區域中，按一下 ⊕ 符號，然後從下拉式功能表中選擇您的 Non VMware SD-WAN Site。



備註 您也可以從 [雲端 VPN (Cloud VPN)] 區域建立新的 Non VMware SD-WAN Site。在按一下 ⊕ 符號後，請從下拉式功能表中選取**新增非 VeloCloud 站台 (New Non-VeloCloud Site)**。

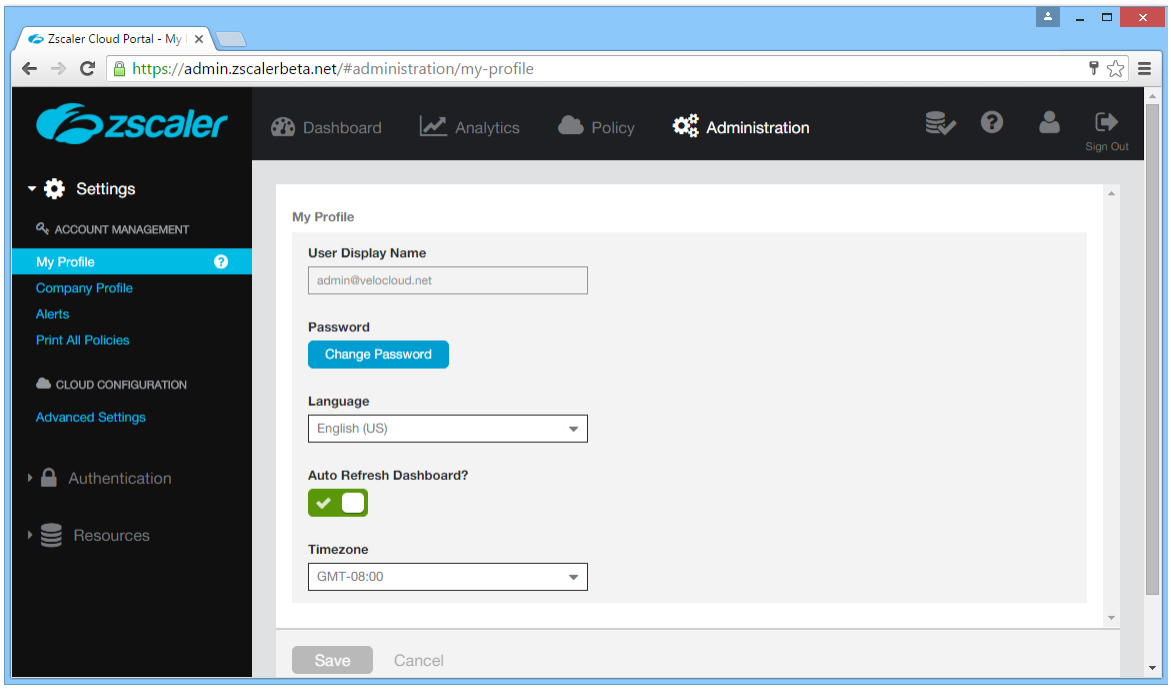
4 按一下**儲存變更 (Save Changes)**。

設定 Zscaler

本節說明 Zscaler 組態。

請在 Zscaler 網站上完成下列步驟。您將在該處建立 Zscaler 帳戶、新增 VPN 認證，以及新增位置。

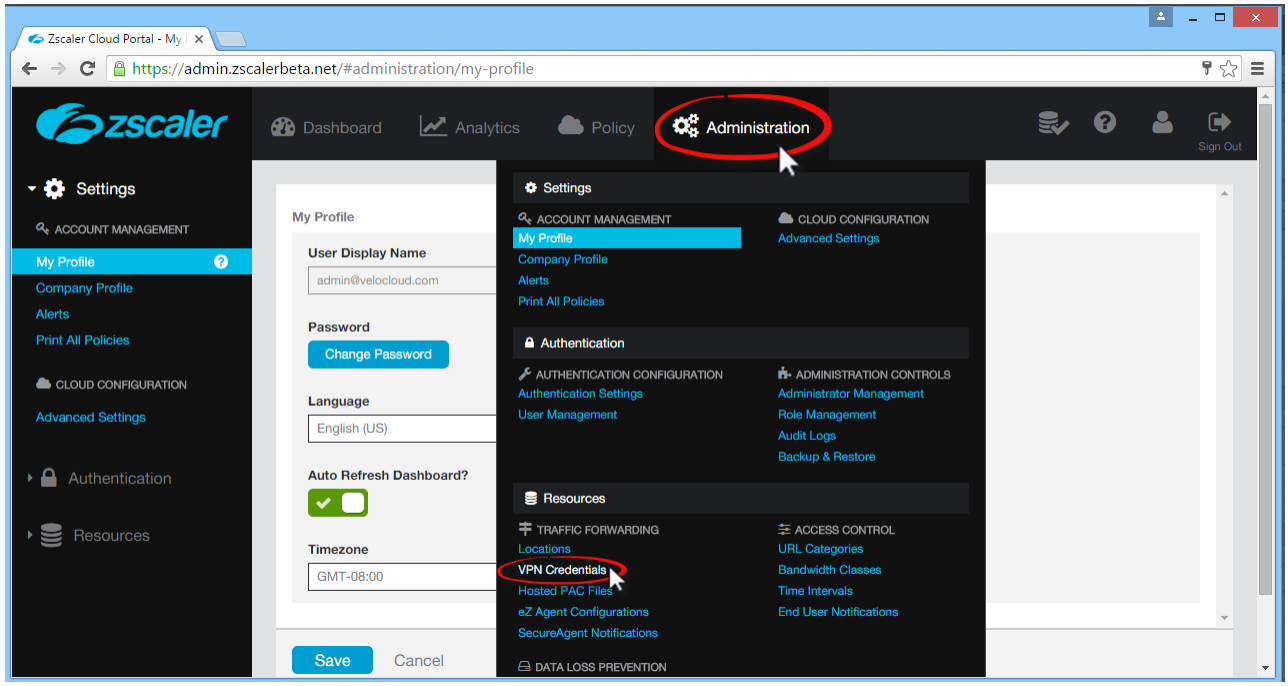
1 在 Zscaler 網站中，建立 Zscaler Web 安全性帳戶。



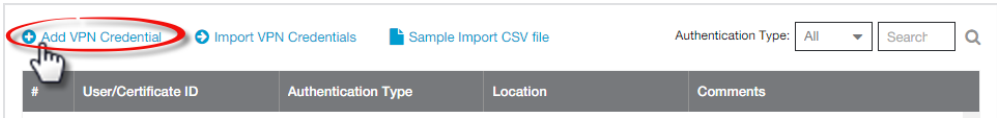
2 設定您的 VPN 認證：

a 在 Zscaler 畫面頂端，將游標暫留在**管理 (Administration)** 選項上方，以顯示下拉式功能表。(請參閱下圖)。

b 在**資源 (Resources)** 下，按一下 **VPN 認證 (VPN Credentials)**。



c 按一下左上角的**新增 VPN 認證 (Add VPN Credentials)**。

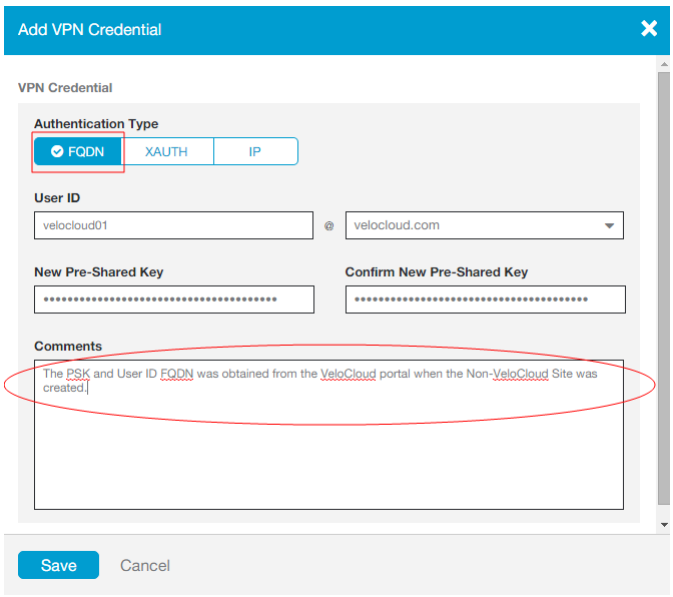


d 在**新增 VPN 認證 (Add VPN Credential)** 對話方塊中：

1 選擇 **FQDN** 作為驗證類型。

2 輸入使用者識別碼和預先共用金鑰 (PSK)。您已從 SD-WAN Orchestrator 的 Non VMware SD-WAN Site 對話方塊中取得這項資訊。

3 如有必要，請在**註解 (Comments)** 區段中輸入任何註解。



4 按一下**儲存 (Save)**。

3 指派位置：

a 在 Zscaler 畫面頂端，將游標暫留在**管理 (Administration)** 選項上方，以顯示下拉式功能表。

b 在**資源 (Resources)** 下，按一下**位置 (Locations)**。

c 按一下左上角的**新增位置 (Add Location)**。

d 在**新增位置 (Add Location)** 對話方塊中 (請參閱下圖)：

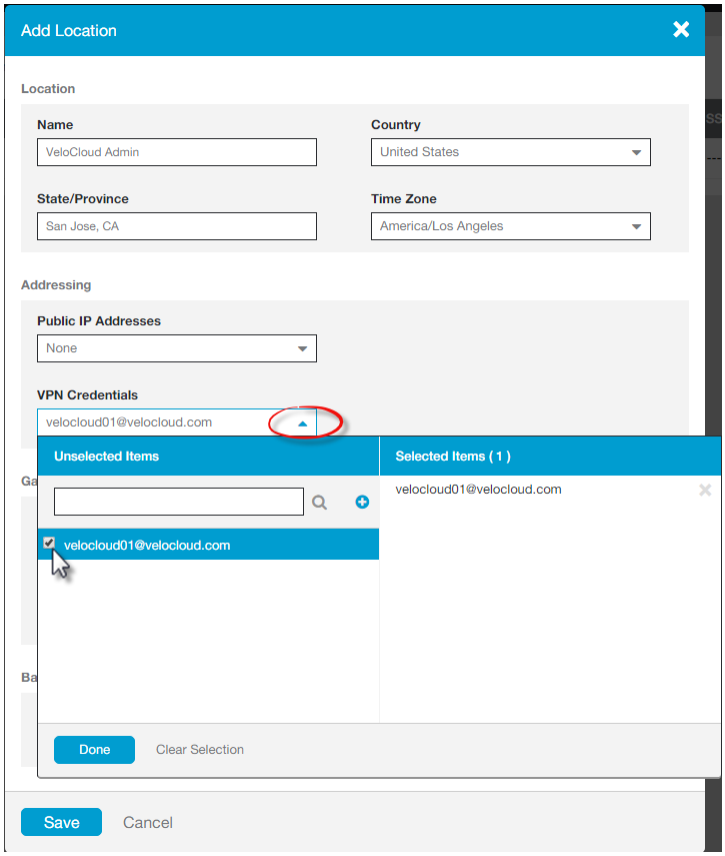
1 填寫 [位置 (Location)] 區域中的文字方塊 (名稱、國家/地區、州/省、時區)。

2 在**公用 IP 位址 (Public IP Addresses)** 下拉式功能表中，選擇**無 (None)**。

3 在 **VPN 認證 (VPN Credentials)** 下拉式功能表中，選取您剛才建立的認證。(請參閱下圖)。

4 按一下**完成 (Done)**。

5 按一下**儲存 (Save)**。



設定商務優先順序規則

在您的 SD-WAN Orchestrator 中定義商務原則，以指定 Web 安全性篩選。

1 在 SD-WAN Orchestrator 的導覽面板中，移至**設定 (Configure) > Edge**。

2 在 **Edge** 畫面中，針對您的 Edge 按一下**商務原則 (Bus. Policy)** 圖示。

3 按一下**新增規則 (New Rule)** 按鈕。

   a 在**規則 (Rule)** 對話方塊中：

      1 在**規則名稱 (Rule Name)** 文字方塊中輸入規則的名稱。

      2 在**比對 (Match)** 區段的**目的地 (Destination)** 區域中，選擇您的選項。(範例選項如下所示)：

         a 按一下**定義 (Define)** 按鈕。

         b 選擇**網際網路 (Internet)**。

         c 在**通訊協定 (Protocol)** 下拉式功能表中，選擇 **TCP**。

         d 在**連接埠 (Ports)** 文字方塊中輸入您的連接埠。下圖顯示使用連接埠 80 選項的範例。VMware 建議使用連接埠 80 或連接埠 443。如需詳細資訊，請參閱本節結尾處的附註。

      3 在**動作 (Action)** 區域中，選擇您的選項。(範例選項如下所示)：

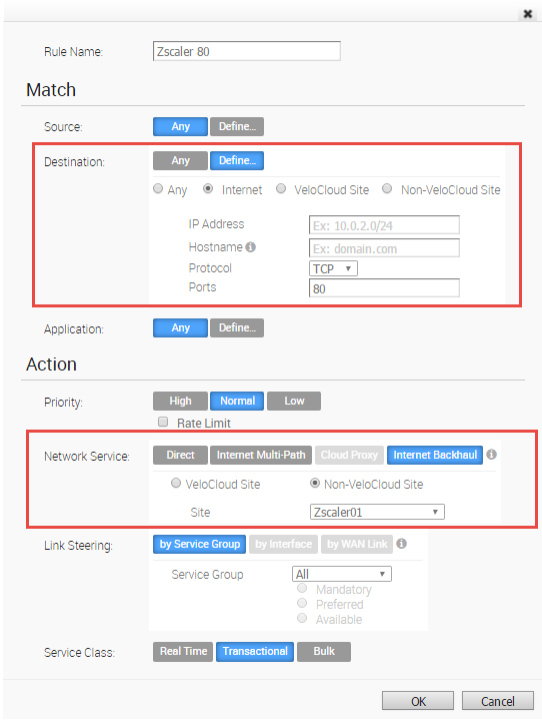
         a 針對**優先順序 (Priority)**，選擇**一般 (Normal)**。

b 針對**網路服務 (Network Service)**，按一下**網際網路回傳 (Internet Backhaul)**，然後從下拉式功能表中選擇您的 Non VMware SD-WAN Site。

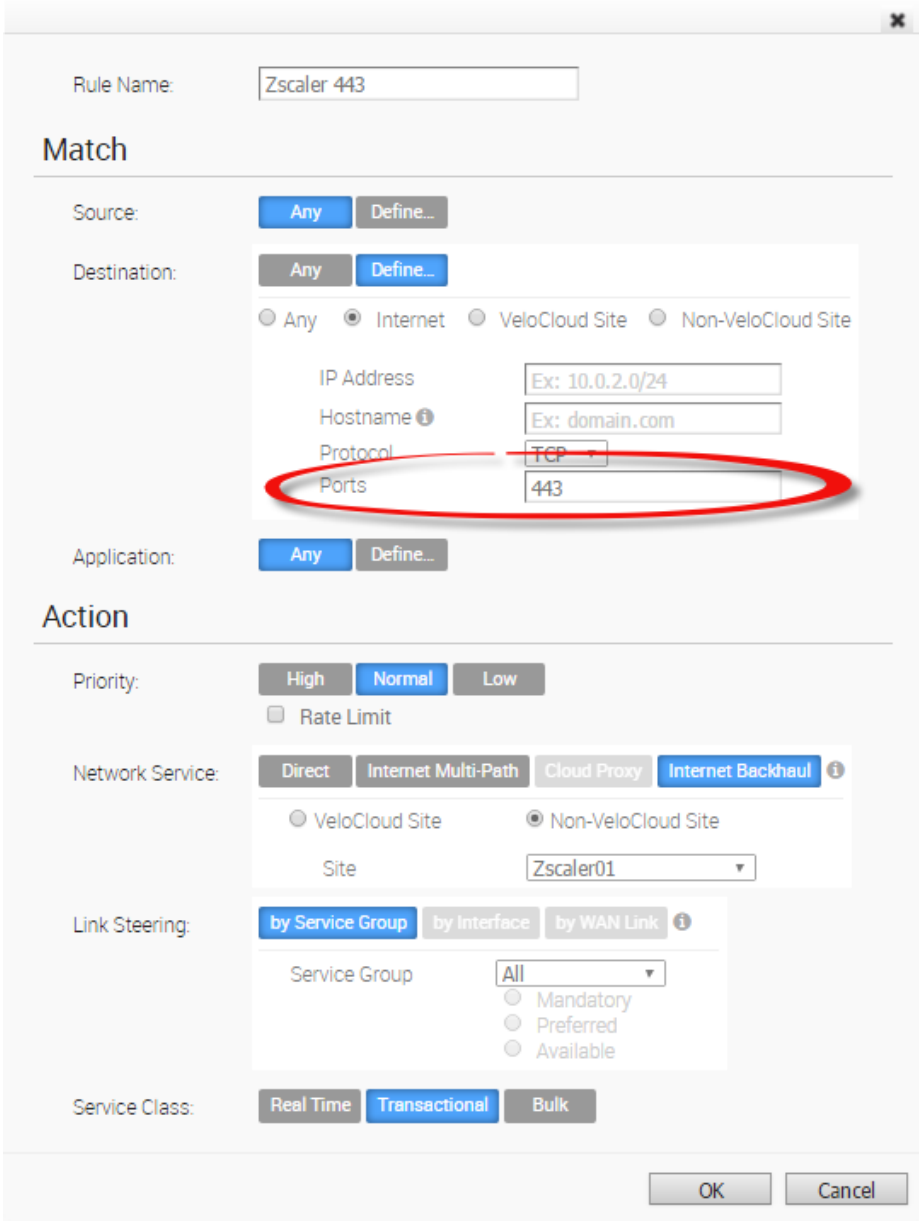
c 針對**連結操控 (Link Steering)** 選擇一個選項 (例如，**依服務群組 (by Service Group)**)。

d 針對**服務類別 (Service Class)**，選擇**交易式 (Transactional)**。

b 按一下**確定 (OK)**。



備註 VMware 建議對回傳 Web 流量使用商務原則規則，尤其是連接埠 80 和 443。您可以將所有網際網路流量傳送至回傳 Zscaler。使用連接埠 443 的影像範例如下所示。



設定 Amazon Web Services

VMware 支援在 Non VMware SD-WAN Site 中設定 Amazon Web Services (AWS)。

依照下列方式設定 Amazon Web Services (AWS)：

1 從 Amazon Web Services 網站中取得公用 IP、內部 IP 和 PSK 詳細資料。

2 將您從 AWS 網站取得的詳細資料輸入至 VMware Orchestrator 中的非 VMware 網路服務。

若要使用 Amazon Web Services 進行設定，請完成下一節中的指示。

取得 Amazon Web Services 組態詳細資料

本節說明如何取得 Amazon Web Services 組態詳細資料。

對您的組態使用 Amazon Web Services 時，請參閱 Amazon 說明文件 (Amazon Virtual Private Cloud Network Administrator Guide) 中的指示，位置如下：http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-nag.pdf。請參閱第 79 頁的〈範例：不具邊界閘道的通用客戶閘道〉一節，以取得特定的組態指示。

1 從 Amazon Web Services 建立 VPC 和 VPN 連線。(請參閱上述章節，以透過相關連結瞭解如何存取 Amazon Web Services 以完成此步驟)。

2 記下與 SD-WAN Orchestrator 中的企業帳戶相關聯的 SD-WAN Gateways，在 Amazon Web Services 中建立虛擬私人閘道時可能需要用到。

3 記下與虛擬私人閘道相關聯的公用 IP、內部 IP 和 PSK 詳細資料。您在建立 Non VMware SD-WAN Site 時將在 SD-WAN Orchestrator 中輸入這項資訊。

建立和設定 Non VMware SD-WAN Site

在您從 Amazon Web Services (AWS) 網站取得公用 IP、內部 IP 和 PSK 資訊之後，您可以設定 Non VMware SD-WAN Site。

若要設定 Non VMware SD-WAN Site：

1 移至**設定 (Configure) > 網路服務 (Network Services)**。

2 在**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中，按一下**新增 (New)** 按鈕。

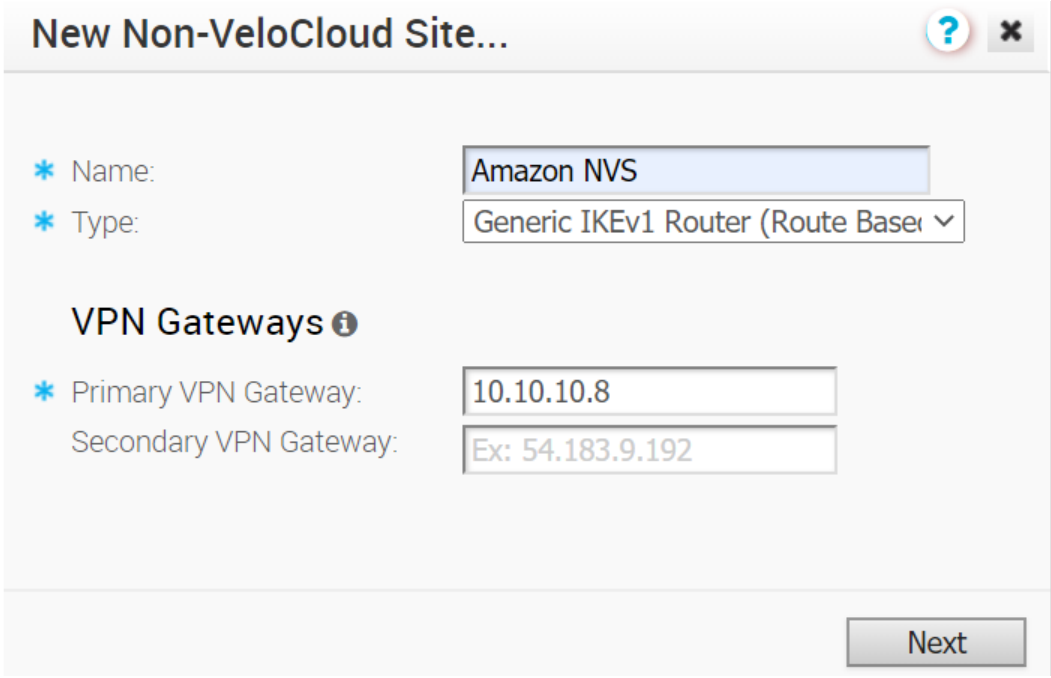
3 在**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊中：

   a 輸入您的站台名稱。

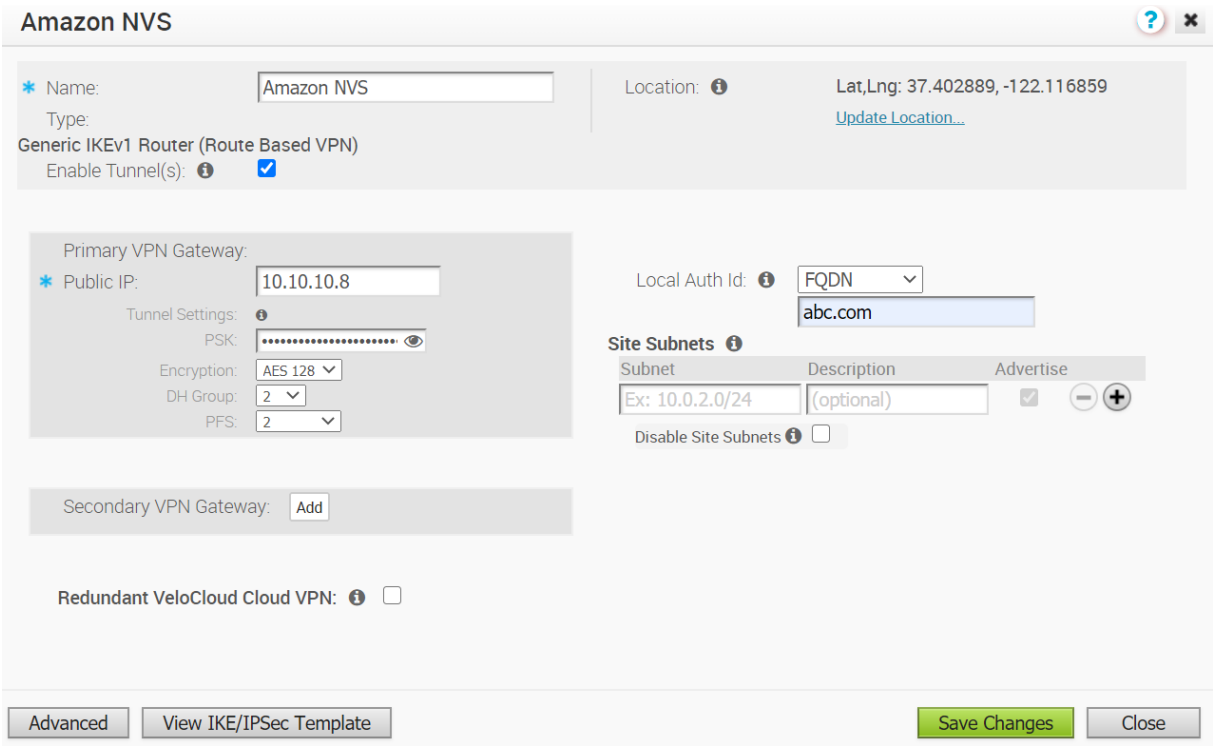
   b 從**類型 (Type)** 下拉式功能表中，選取**一般 IKEv1 路由器 (以路由為基礎的 VPN) (Generic IKEv1 Router (Route Based VPN))** 或 **一般 IKEv2 路由器 (以路由為基礎的 VPN) (Generic IKEv2 Router (Route Based VPN))**。

   c 輸入主要 VPN 閘道 (如有必要，請輸入次要 VPN 閘道)。

   d 按**下一步 (Next)**。



以路由為基礎的 Non VMware SD-WAN Site 隨即建立，並顯示 Non VMware SD-WAN Site 對話方塊。



4 若要設定 Non VMware SD-WAN Site 主要 VPN 閘道的通道設定，請按一下**進階 (Advanced)** 按鈕。

5 在**主要 VPN 閘道 (Primary VPN Gateway)** 區域中，您可以設定下列通道設定：

欄位	說明
PSK	預先共用金鑰 (PSK)，這是在通道間進行驗證時所使用的安全性金鑰。依預設，Orchestrator 會產生 PSK。如果您想要使用自己的 PSK 或密碼，可以在文字方塊中輸入。
加密 (Encryption)	選取 **AES 128** 或 **AES 256** 作為加密資料的演算法。預設值為 AES 128。
DH 群組 (DH Group)	選取交換預先共用金鑰時所要使用的 Diffie-Hellman (DH) 群組演算法。DH 群組會設定演算法的強度 (以位元為單位)。預設值為 2。
PFS	選取完全正向加密 (PFS) 層級以取得額外的安全性。預設值為 2。

6 如果您想要為此站台建立次要 VPN 閘道，請按一下**次要 VPN 閘道 (Secondary VPN Gateway)** 旁的**新增 (Add)** 按鈕。在快顯視窗中，輸入次要 VPN 閘道的 IP 位址，然後按一下**儲存變更 (Save Changes)**。

系統將立即為此站台建立次要 VPN 閘道，並將 VMware VPN 通道佈建至此閘道。

7 選取**備援 VeloCloud 雲端 VPN (Redundant VeloCloud Cloud VPN)** 核取方塊，為每個 VPN 閘道新增備援通道。

對主要 VPN 閘道的加密、DH 群組或 PFS 所做的任何變更，也將套用至備援 VPN 通道 (如果已設定)。在修改主要 VPN 閘道的通道設定後儲存變更，然後按一下**檢視 IKE/IPSec 範本 (View IKE/IPSec Template)**，以檢視更新的通道組態。

8 按一下**更新位置 (Update location)** 連結，為已設定的 Non VMware SD-WAN Site 設定位置。緯度和經度詳細資料可用來判斷在網路中要連線到的最佳 Edge 或閘道。

9 本機驗證識別碼會定義本機閘道的格式和識別。從**本機驗證識別碼 (Local Auth Id)** 下拉式功能表中，選擇下列其中一種類型，然後輸入您決定的值：

- **FQDN** - 完整網域名稱或主機名稱。例如 google.com。
- **使用者 FQDN (User FQDN)** - 電子郵件地址形式的使用者完整網域名稱。例如 user@google.com。
- **IPv4** - 用來與本機閘道進行通訊的 IP 位址。

備註 對於一般以路由為基礎的 VPN，若使用者未指定任何值，則會使用**預設值 (Default)** 作為本機驗證識別碼。預設的本機驗證識別碼值將是 SD-WAN Gateway 介面公用 IP。

10 在**站台子網路 (Site Subnets)** 下方，您可以按一下 **+** 按鈕以新增 Non VMware SD-WAN Site 的子網路。如果您不需要站台的子網路，請選取**停用站台子網路 (Disable Site Subnets)** 核取方塊。

11 當您準備好起始從 SD-WAN Gateway 到一般路由器 VPN 閘道的通道後，請選取**啟用通道 (Enable Tunnel(s))** 核取方塊。

12 按一下**儲存變更 (Save Changes)**。

設定雲端安全性服務

雲端安全性服務是雲端主控的安全性服務 (例如防火牆、URL 篩選等)，可保護企業的分支和/或資料中心。以下幾節說明如何定義和設定雲端安全性服務執行個體，以及如何建立直接從 Edge 連至雲端安全性服務的安全通道。

雲端安全性服務概觀

本節提供雲端安全性服務的概觀。

目前，從分支 Edge 到雲端服務或 Non VMware SD-WAN Site 的連線是透過 SD-WAN Gateway 建立的。在此模式中，SD-WAN Gateway 會彙總來自多個分支 Edge 的流量，並安全地將流量轉送至 Non VMware SD-WAN Site。

您也可以設定分支 Edge，以建立直接連至雲端服務 POP 的通道。此選項具有下列優點：

- 您可以將非企業流量卸載至網際網路，以節省連結頻寬成本。
- 藉由將網際網路流量重新導向至雲端安全性服務，您可以確保分支站台不受惡意流量入侵。
- 簡化的組態。

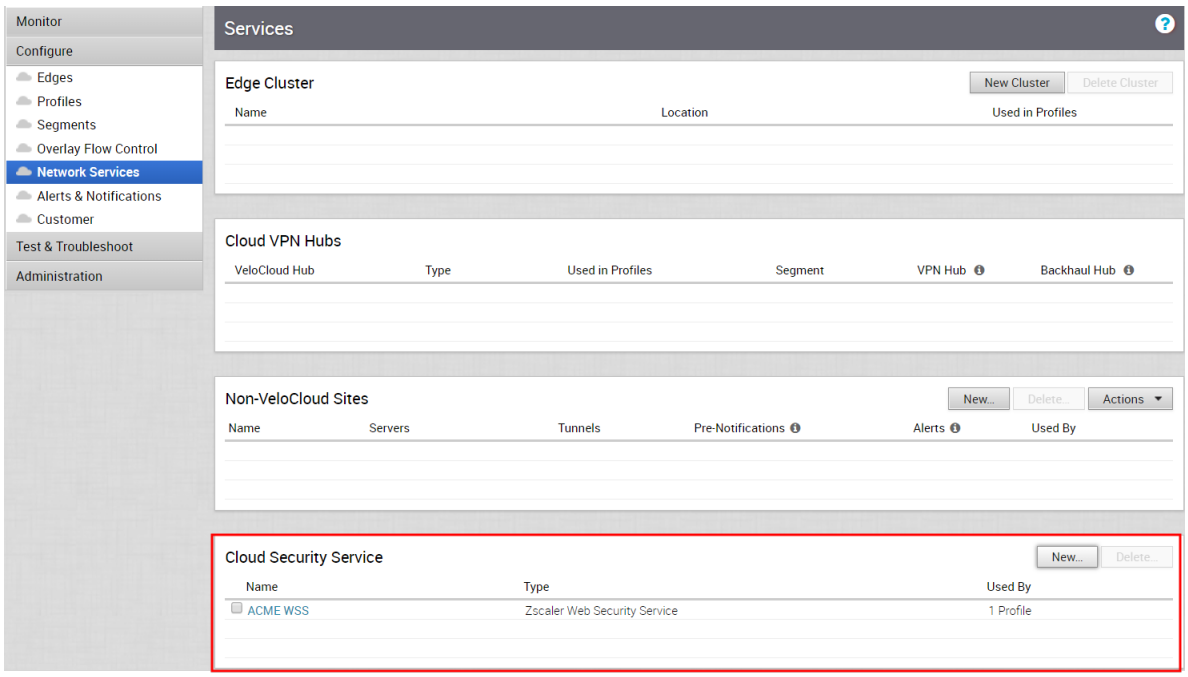
本文件說明如何定義和設定雲端安全性服務執行個體，以及如何建立直接從 Edge 連至雲端安全性服務的安全通道。此設定分成三個部分：

- 設定雲端安全性服務
- 為設定檔設定雲端安全性服務
- 為 Edge 設定雲端安全性服務

設定雲端安全性服務

您可以在 [網路服務 (Network Services)] 視窗中設定雲端安全性服務。

在企業入口網站中，導覽至**設定 (Configure) > 網路服務 (Network Services)**。若要從 Edge 建立通往雲端安全性服務站台的安全通道，您可以在**雲端安全性服務 (Cloud Security Service)** 區域中定義服務執行個體。



新增和設定雲端安全性提供者

雲端安全服務會建立從 Edge 到雲端安全性服務站台的安全通道。這可確保通往雲端安全性服務的流量安全無虞。

1 在 [客戶 (Customer)] 面板中，按一下**設定 (Configure) > 網路服務 (Network Services)**。

2 在**雲端安全性服務 (Cloud Security Service)** 面板中，按一下**新增 (New)**。

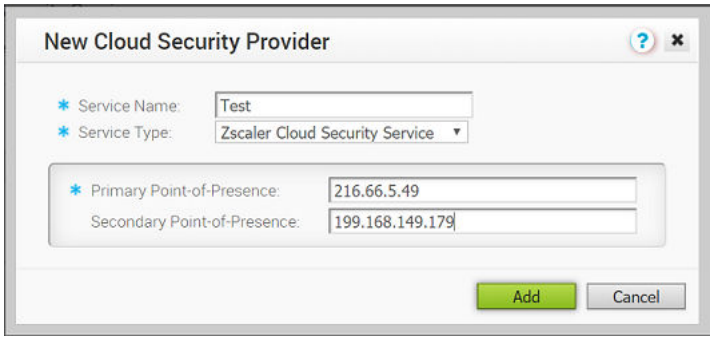
3 在**新增雲端安全性提供者 (New Cloud Security Provider)** 對話方塊中，選取雲端服務的**服務類型 (Service Type)**。

4 在**服務名稱 (Service Name)** 旁輸入描述性名稱。

5 輸入**主要存在點/伺服器 (Primary Point-of-Presence/Server)** 和**次要存在點/伺服器 (Secondary Point-of-Presence/Server)** 的 IP 位址。

> **備註** 如果您已選取 **Zscaler 雲端安全性服務 (Zscaler Cloud Security Service)** 作為服務類型並計劃指派 GRE 通道，則建議您僅輸入 IP 位址作為存在點，而不使用主機名稱，因為 GRE 不支援主機名稱。

6 若要儲存您的組態，請按一下**新增 (Add)**。



備註 您必須為每個 Edge 設定通道屬性。請參閱為 Edge 設定雲端安全性服務一節。

為設定檔設定雲端安全性服務

您必須啟用雲端安全性，才能建立從 Edge 到雲端安全性服務站台的安全通道。這可讓流量安全地重新導向至第三方雲端安全性站台。

開始之前：

- 確定您具有設定網路服務的權限。
- 確定您的 SD-WAN Orchestrator 具有 3.3.x 版或更高版本。
- 您應具有第三方 CSS 中設定的雲端安全性服務閘道端點 IP 和 FQDN 認證。

1 在企業入口網站中，按一下**設定 (Configure) > 設定檔 (Profiles)**。

2 按一下設定檔旁的裝置圖示，或按一下設定檔的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在**雲端安全性 (Cloud Security)** 區段中，將開關從**關閉 (Off)** 位置切換至**開啟 (On)** 位置。

4 進行下列設定：

選項	說明
雲端安全性服務 (Cloud Security Service)	從下拉式功能表中選取雲端安全性服務。您也可以從下拉式功能表中按一下**新增雲端安全性服務 (New Cloud Security Service)**，以建立新的服務類型。
通道通訊協定 (Tunneling Protocol)	此選項僅適用於 Zscaler 雲端安全性服務。請選擇 IPsec 或 GRE。依預設會選取 IPsec。
雜湊 (Hash)	從下拉式清單中選取雜湊函數 SHA 1 或 SHA 256。依預設會選取 SHA 1。 **備註** VMware 不支援 MD5，建議不要選擇 MD5 做為雜湊功能。

選項	說明
加密 (Encryption)	從下拉式清單中選取加密演算法 AES 128 或 AES 256。依預設會選取 [無 (None)]。
金鑰交換通訊協定 (Key Exchange Protocol)	此選項不適用於 Symantec 雲端安全性服務。 選取金鑰交換方法，如 IKEv1 或 IKEv2。依預設會選取 IKEv2。

5 按一下**儲存變更 (Save Changes)**。

當您在設定檔中啟用雲端安全性服務並加以設定時，該設定將會自動套用至與設定檔相關聯的 Edge。如有需要，您可以覆寫特定 Edge 的組態。請參閱為 Edge 設定雲端安全性服務。

若設定檔是透過 3.3.1 版之前所啟用並設定的雲端安全性服務而建立，則您可以選擇以下列方式重新導向流量：

- 僅將 Web 流量重新導向至雲端安全性服務
- 將所有網際網路繫結流量重新導向至雲端安全性服務
- 根據商務原則設定重新導向流量 – 此選項只能從 3.3.1 版使用。如果您選擇此選項，則其他兩個選項將不再提供使用。

備註 對於您為 3.3.1 版或更新版本建立的新設定檔，依預設會根據商務原則設定來重新導向流量。

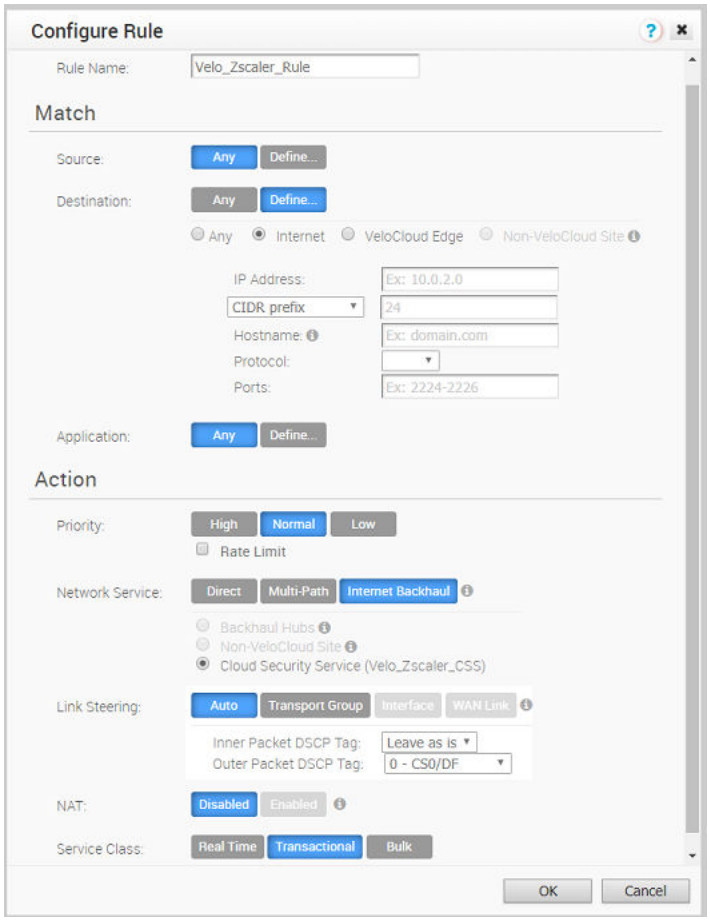
您可以在商務原則中建立規則，以將流量重新導向至雲端安全性服務。

1 在設定檔的**商務原則 (Business Policy)** 索引標籤中按一下**新增規則 (New Rule)**，或在**動作 (Actions)** 下拉式功能表中選擇**新增 (New)**，以建立新的規則。

設定規則 (Configure Rule) 對話方塊隨即出現。

2 輸入**規則名稱 (Rule Name)** 的唯一名稱。

3 在**動作 (Action)** 區域中，按一下**網際網路回傳 (Internet Backhaul)** 按鈕，然後選擇**雲端安全性服務 (Cloud Security Service)**。



4 按一下**確定 (OK)**。

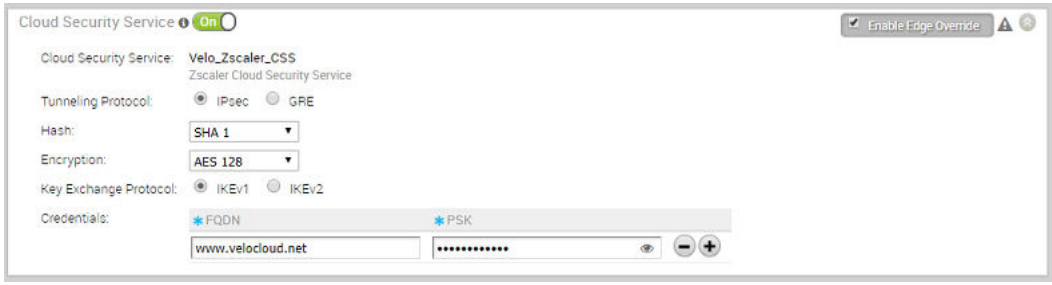
新規則會顯示在**商務原則 (Business Policy)** 畫面中。

為 Edge 設定雲端安全性服務

當您將設定檔指派給 Edge 後，裝置會自動繼承與該設定檔相關聯的雲端安全性服務。您可以覆寫設定，以修改每個 Edge 的屬性。

1 在企業入口網站中，按一下**設定 (Configure)** > **Edge**。

2 在**雲端安全性服務 (Cloud Security Service)** 區段中，會顯示相關聯設定檔的雲端安全性服務參數。選取**啟用 Edge 覆寫 (Enable Edge Override)**，以修改屬性。如需屬性的詳細資訊，請參閱為設定檔設定雲端安全性服務。



除了現有屬性之外，您還可以為 Edge 設定下列其他參數：

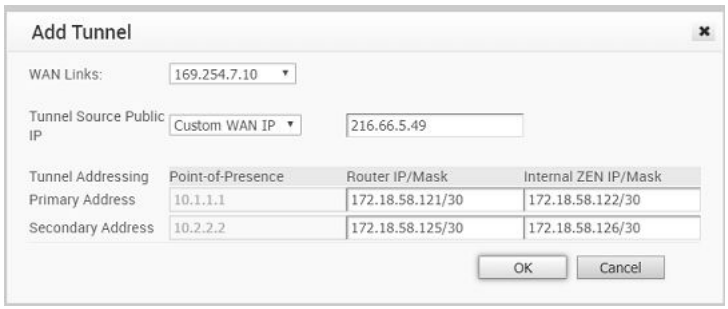
- **FQDN** – 輸入 IPsec 通訊協定的完整網域名稱。
- **PSK** – 輸入 IPsec 通訊協定的預先共用金鑰。

備註 以上選項不適用於 Symantec 雲端安全性服務。

如果您針對 Zscaler 雲端安全性服務選擇 GRE 通道通訊協定，請新增 GRE 通道參數。

1 按一下**新增通道 (Add Tunnel)**。

2 在**新增通道 (Add Tunnel)** 視窗中，設定下列項目：



選項	說明
WAN 連結 (WAN Links)	選取要由 GRE 通道用作來源的 WAN 介面。
通道來源公用 IP (Tunnel Source Public IP)	選擇要由通道用作公用 IP 位址的 IP 位址。您可以選擇 WAN 連結 IP 或自訂 WAN IP。如果您選擇自訂 WAN IP，請輸入要用作公用 IP 的 IP 位址。
主要路由器 IP/遮罩 (Primary Router IP/Mask)	輸入路由器的主要 IP 位址。
次要路由器 IP/遮罩 (Secondary Router IP/Mask)	輸入路由器的次要 IP 位址。
主要 ZEN IP/遮罩 (Primary ZEN IP/Mask)	輸入內部 Zscaler 公用服務 Edge 的主要 IP 位址。
次要 ZEN IP/遮罩 (Secondary ZEN IP/Mask)	輸入內部 Zscaler 公用服務 Edge 的次要 IP 位址。

備註 路由器 IP/遮罩和 ZEN IP/遮罩是由 Zscaler 提供。

3 按一下**確定 (OK)**，通道詳細資料隨即顯示在雲端安全性服務 (Cloud Security Services) 區段中。

在 **Edge** 視窗中，按一下**儲存變更 (Save Changes)**，以儲存修改的設定。

若設定檔是透過 3.3.1 版之前所啟用並設定的雲端安全性服務而建立，則您可以選擇以下列方式重新導向流量：

- 僅將 Web 流量重新導向至雲端安全性服務
- 將所有網際網路繫結流量重新導向至雲端安全性服務

- 根據商務原則設定重新導向流量 – 此選項只能從 3.3.1 版使用。如果您選擇此選項，則其他兩個選項將不再提供使用。

備註 對於您為 3.3.1 版或更新版本建立的新設定檔，依預設會根據商務原則設定來重新導向流量。

您可以在商務原則中建立規則，以建立雲端安全性服務的關聯。

1 在 Edge 的**商務原則 (Business Policy)** 索引標籤中按一下**新增規則 (New Rule)**，或在**動作 (Actions)** 下拉式功能表中選擇**新增規則 (New Rule)**，以建立新的規則。

設定規則 (Configure Rule) 對話方塊隨即出現。

2 輸入**規則名稱 (Rule Name)** 的唯一名稱。

3 在**動作 (Action)** 區域中，按一下**網際網路回傳 (Internet Backhaul)** 按鈕，然後選擇**雲端安全性服務 (Cloud Security Service)**。

4 按一下**確定 (OK)**。

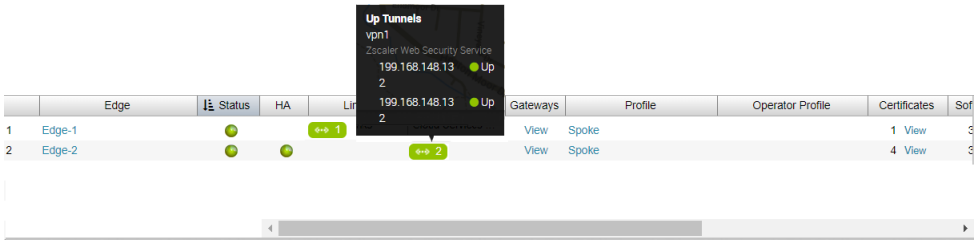
新規則會顯示在**商務原則 (Business Policy)** 畫面中。

監控雲端安全性服務

在導覽面板中，有兩處可讓您監控雲端安全性服務，即 Edge 畫面 (**監控 (Monitor)**> Edge) 和**網路服務 (Network Services)** 畫面 (**監控 (Monitor)** > **網路服務 (Network Services)**)。以下幾節將提供更多資訊。

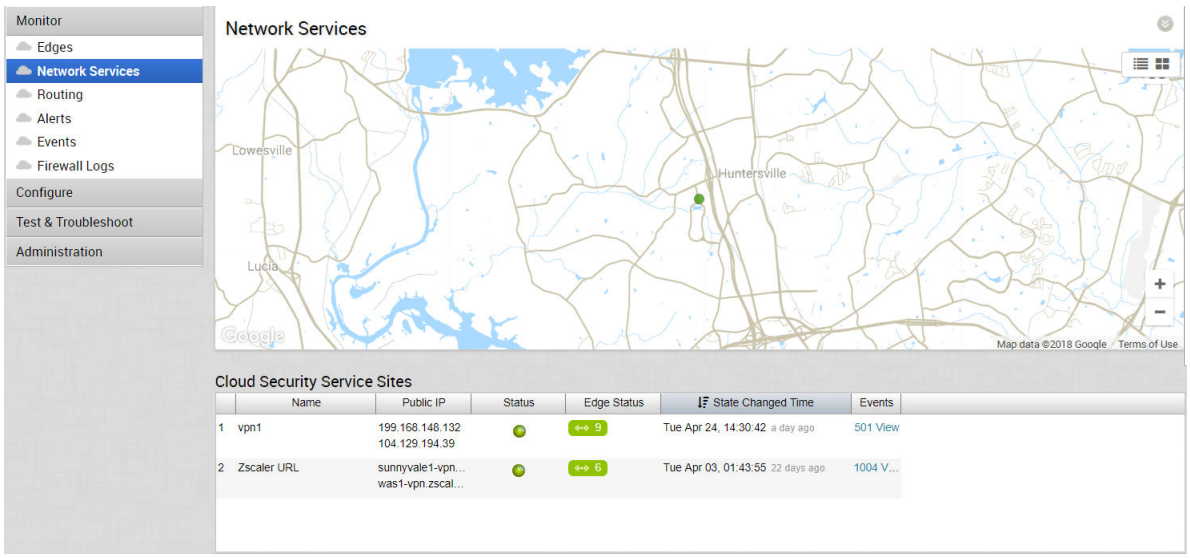
Edge 畫面

若要從 Edge 畫面監控您的雲端服務，請移至**監控 (Monitor)** > **Edge**。此視圖會顯示啟動的通道數目以及關閉的通道數目。



網路服務畫面

若要從**網路服務 (Network Services)** 畫面監控您的雲端安全性服務，請移至**監控 (Monitor)** > **網路服務 (Network Services)** > **雲端安全性通道狀態 (Cloud Security Tunnel State)**。



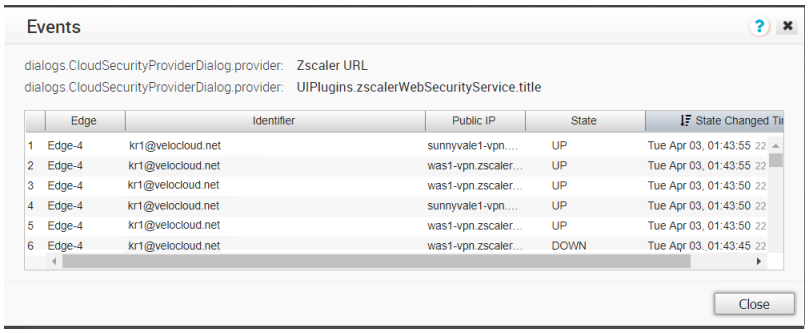
[雲端安全性通道狀態 (Cloud Security Tunnel State)] 區域中的 [Edge 狀態 (Edge Status)] 資料行會顯示完全連線和中斷連線的 Edge 數目。

狀態資料行

狀態 (Status) 資料行會顯示特定雲端安全性服務的整體連線狀態。如果所有 Edge 都完全連線，圖示的顏色將是綠色。如果有些 Edge 已連線，而有些已中斷連線，則圖示的而色將是黃色。如果所有 Edge 皆已中斷連線，圖示的顏色將是紅色。

事件

若要檢視雲端安全性服務的事件，請按一下**雲端安全性服務站台 (Cloud Security Service Sites)** 區域中的**事件 (Events)** 連結。

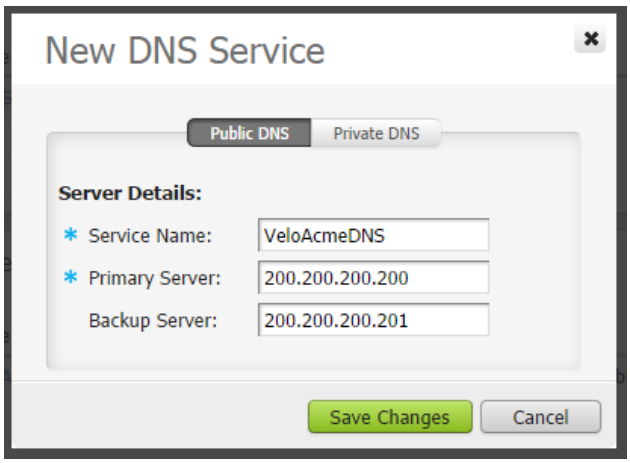


設定 DNS 服務

這是一項選用服務，可讓您建立 DNS 的組態。

DNS 服務可用於公用 DNS 服務，或是您的公司所提供的私人 DNS 服務。您可以指定**主要伺服器 (Primary Server)** 和**備份伺服器 (Backup Server)**。此服務已預先設定為使用 Google 和 Open DNS 伺服器。

下圖顯示公用 DNS 的範例組態。



對於私人服務，您也可以指定一或多個**私人網域 (Private Domains)**。

設定 Netflow 設定

在企業網路中，Netflow 會監控流經 SD-WAN Edges 的流量，並直接從 SD-WAN Edges 將網際網路通訊協定流量資訊匯出 (IPFIX) 資訊匯出至一或多個 Netflow 收集器。SD-WAN Orchestrator 可讓您在設定檔、Edge 和區段層級將 Netflow 收集器和篩選器設定為網路服務。每個區段最多可設定兩個收集器，每個設定檔和 Edge 最多可設定八個收集器。此外，您最多可為每個收集器設定 16 個篩選器。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **網路服務 (Network Services)**。

服務 (Services) 頁面隨即出現。

2 若要設定收集器，請移至 **Netflow 設定 (Netflow Settings)** 區域，然後按一下 [收集器 (Collector)] 資料表右側的**新增 (New)** 按鈕。**新增收集器 (Add New Collector)** 對話方塊隨即出現。

a 在**收集器名稱 (Collector Name)** 文字方塊中，輸入收集器的唯一名稱。

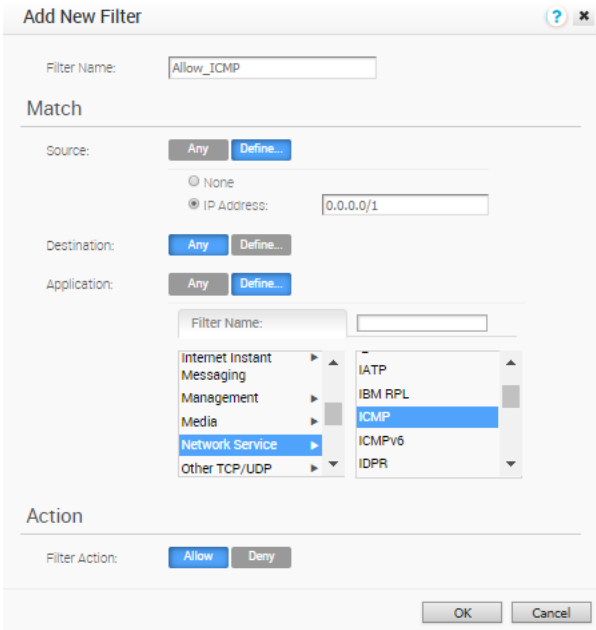
b 在**收集器 IP (Collector IP)** 文字方塊中，輸入收集器的 IP 位址。

c 在**收集器連接埠 (Collector Port)** 文字方塊中，輸入收集器的連接埠識別碼。

d 按一下**儲存變更 (Save Changes)**。

在**網路服務 (Network Services)** 下，新增的收集器會顯示在 [收集器 (Collector)] 資料表中。

3 SD-WAN Orchestrator 可讓您依來源 IP、目的地 IP 以及與流量相關聯的應用程式識別碼來篩選流量記錄。若要設定篩選器，請移至 **Netflow 設定 (Netflow Settings)** 區域，然後按一下 [篩選器 (Filter)] 資料表右側的**新增 (New)** 按鈕。**新增篩選器 (Add New Filter)** 對話方塊隨即出現。



a 在**篩選器名稱 (Filter Name)** 文字方塊中，輸入篩選器的唯一名稱。

b 在**比對 (Match)** 區域下方按一下**定義 (Define)**，以定義要以來源 IP、目的地 IP 或與流量相關聯的應用程式比對的個別收集器篩選規則，或按一下**任何 (Any)**，以使用任何來源 IP、目的地 IP 或與流量相關聯的應用程式作為 Netflow 篩選的比對準則。

c 在**動作 (Action)** 區域下，選取**允許 (Allow)** 或**拒絕 (Deny)** 作為流量的篩選動作，然後按一下**確定 (OK)**。

在**網路服務 (Network Services)** 下，新增的篩選器會顯示在 [篩選器 (Filter)] 資料表中。

結果

在設定檔和 Edge 層級上，已設定的收集器和篩選器會在**裝置 (Device)** 索引標籤中的 **Netflow 設定 (Netflow Settings)** 區域下顯示為清單。

- 設定設定檔或 Edge 時，您可以從可用清單中選取收集器和篩選器，或新增收集器和篩選器。如需相關步驟，請參閱在設定檔層級設定 Netflow 設定。
- 若要覆寫 Edge 層級的 Netflow 設定，請參閱在 Edge 層級設定 Netflow 設定。

私人網路名稱

您可以定義多個私人網路，並將其指派給個別的私人 WAN 覆疊。

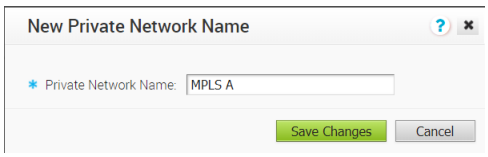
設定私人網路

若要設定私人網路：

1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure) > 網路服務 (Network Services)**。

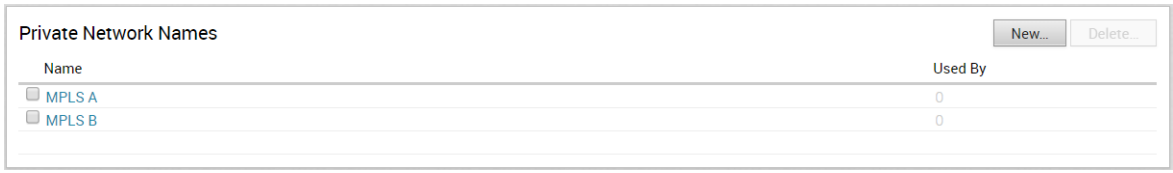
2 在**私人網路名稱 (Private Network Names)** 區域中，按一下**新增 (New)** 按鈕。

3 在**新增私人網路名稱 (New Private Network Name)** 對話方塊中，在適當的文字方塊中輸入唯一名稱。



4 按一下**儲存變更 (Save Changes)**。

私人網路名稱會顯示在**私人網路名稱 (Private Network Name)** 區域中。



刪除私人網路名稱

僅能刪除 Edge 裝置未使用的私人網路名稱。

若要刪除 Edge 裝置未使用的私人網路名稱：

1 按一下名稱的核取方塊以選取名稱，然後按一下**刪除 (Delete)** 按鈕。

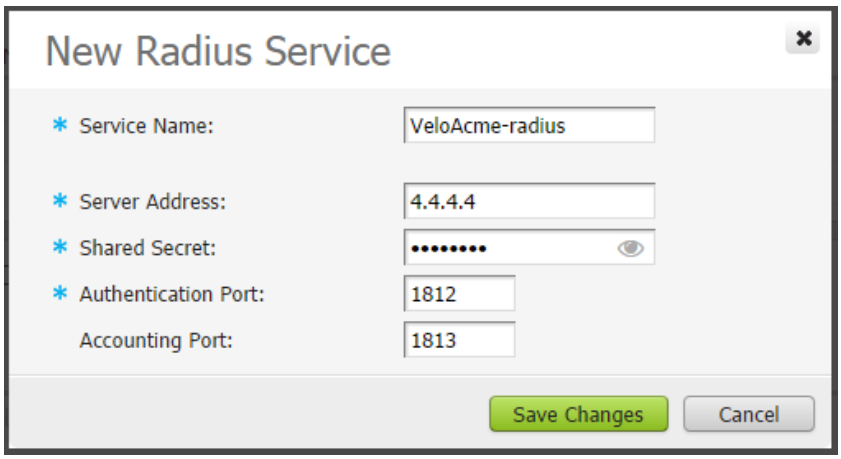
2 在**確認刪除 (Confirm Deletion)** 對話方塊中，按一下**確定 (OK)**。

在定義使用者定義的覆疊時，您可以選取私人連結標籤。請參閱標題為「選取私人網路名稱」一節。

設定驗證服務

驗證服務是選擇性的組態。如果您的組織使用服務進行驗證或帳戶處理，您可以建立網路服務，以指定用於服務的 IP 位址和連接埠。這是 802.1 x 設定程序的一部分，設定於設定檔中。

下圖顯示範例組態。



備註 僅在 Edge 層級設定來源介面。

設定設定檔

9

設定檔會提供在網路和網路服務中建立的複合組態。此外也會新增商務原則和防火牆規則的組態。

備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

設定檔有四個索引標籤頁面：**設定檔概觀 (Profile Overview)**、**裝置 (Device)**、**商務原則 (Business Policy)** 和**防火牆 (Firewall)**。

本章節討論下列主題：

- 建立設定檔
- 修改設定檔
- 設定檔概觀畫面
- 網路到區段的移轉
- 設定本機認證

建立設定檔

全新安裝後，SD-WAN Orchestrator 會具有下列預先定義的設定檔：網際網路設定檔、VPN 設定檔，和 3.0 版所導入區段型設定檔。

備註 透過 3.0 版中導入的分割功能，若 Edge 執行 3.0 之前的軟體，則可以使用以網路為基礎的組態或以分割為基礎的組態。**基於此轉換，您必須將以網路為基礎的設定檔移轉/轉換為區段型設定檔。

建立新的設定檔時通常應遵循下列步驟：

1 建立設定檔

2 設定裝置

   a 選取網路

   b 指派驗證/DNS

   c 設定介面設定

3 啟用雲端 VPN

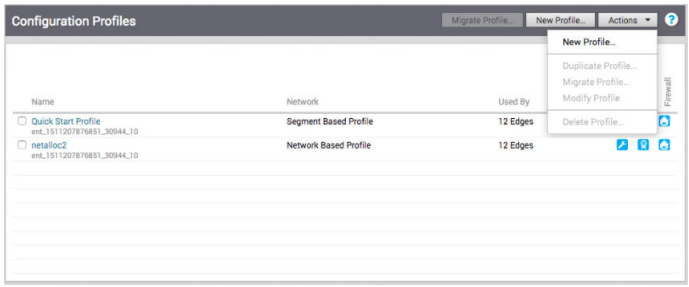
4 設定商務原則

5 設定防火牆

6 檢閱設定檔概觀

若要建立新的設定檔：

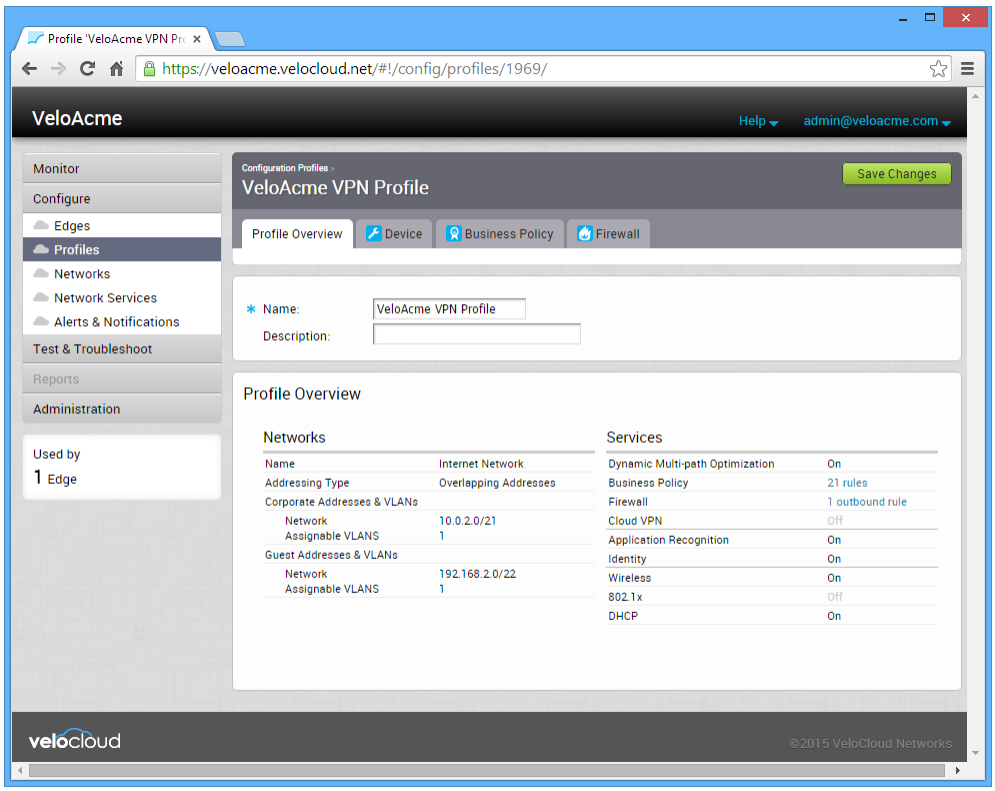
1 移至 [設定 (Configure)] -> [設定檔 (Profiles)]，然後按一下**新增設定檔 (New Profile)** 按鈕。



2 在**新增設定檔 (New Profile)** 對話方塊中，在適當的文字方塊中輸入設定檔名稱和說明。

3 按一下**建立 (Create)** 按鈕。

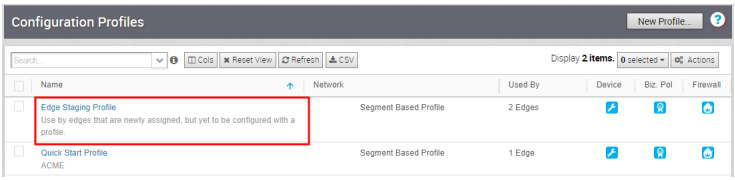
設定檔概觀 (Profile Overview) 索引標籤頁面會重新整理。如需詳細資訊，請參閱下方的**設定檔概觀畫面 (Profile Overview Screen)** 區段。



修改設定檔

企業管理員也可以手動將設定檔指派給 Edge。

需要進行此變更的案例之一，是處理 Edge 預備設定檔時。在此情況下，依預設會因為推送啟用而根據預備設定檔啟動 Edge。企業管理員必須手動將最終生產設定檔指派給 Edge。如需如何手動指派設定檔的指示，請參閱《指派設定檔 (變更設定檔)》中的〈佈建 Edge〉。



設定檔概觀畫面

設定檔概觀 (Profile Overview) 畫面提供設定檔中所定義所有網路和服務的快速摘要。

此概觀分為兩個類別：

類別	說明
網路	具有已使用的網路組態名稱、定址類型，以及指派給公司和客體網路的網路位址和 VLAN。
服務	具有 VMware 系統所提供之服務的摘要。

輸入設定檔裝置、商務原則和防火牆索引標籤畫面的所有設定後，**設定檔概觀 (Profile Overview)** 畫面應會反映您所執行的設定。

網路到區段的移轉

在 3.2 版中導入了設定檔移轉功能，以利簡化 Edge 升級 (從以網路為基礎的設定檔到區段型設定檔) 的工作流程。本文件提供如何將 2.X Edge (使用以網路為基礎的設定檔) 升級至 3.X (使用區段型設定檔) 的相關工作流程和詳細資料。

Edge 從 2.X 升級至 3.X 的必要條件

若要從 2.X 版升級至 3.X 版，Edge 必須符合下列必要條件：

- 支援從 2.4 版和 2.5 版升級至 3.X。
- 確定 SD-WAN Orchestrator 和 SD-WAN Gateway 的版本相同，或版本高於 Edge。

對部署作為中樞和輪輻的 Edge 進行升級的最佳做法

對中樞和輪輻組態中部署的 Edge 執行升級時：

- 在升級設定為輪輻的 Edge 之前，應先將設定為中樞的 Edge 升級至 3.X。
- 如果中樞採用 3.X 的設定檔，而所有輪輻皆以 2.X 的設定檔執行，則不會進行通道形成。
- 若要克服上述的限制，每個輪輻設定檔應至少有一個輪輻以 3.2.1 的設定檔執行。

對部署於 HA 中的 Edge 進行升級的最佳做法

一般軟體升級步驟適用於將一組高可用性 Edge 升級至版本 3.3.x 或更早版本的客戶 (例如 3.3.2 P2)。但是，將 HA 中部署的 Edge 升級至 3.4.x 版分支或更新版本的客戶，必須在將其 HA Edge 升級至所需的 3.4.x 或更新版本之前，執行至 3.3.x 的中繼升級。支援將單一獨立 Edge 直接從 2.x 版本升級至 3.4.x 或更新版本，且沒有任何已知問題。

將網路移轉至區段

本節說明從網路到區段的移轉。

開始之前

- 升級 Edge 之前，請確定 SD-WAN Orchestrator 和 SD-WAN Gateway 的版本相同，或版本高於 Edge。

  備註 由於 3.X Edge 只能辨識區段型設定檔，因此，只有在 Edge 已獲指派區段設定檔時，3.2 映像更新才會推送至 Edge。區段型設定檔在指派給 Edge 後，將無法重新指派給以網路為基礎的設定檔。以網路為基礎的設定檔可以轉換為區段型設定檔，但區段型設定檔則無法轉換為以網路為基礎的設定檔。

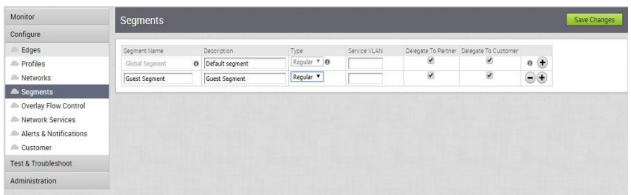
- 在移轉設定檔之前請確定已啟用分割。

  備註 依預設會啟用分割。

步驟 1：建立用來配置客體網路的非全域區段

由於依預設會在以網路為基礎的設定檔中建立客體網路，因此您必須建立非全域區段，以在進行移轉期間將客體網路對應至個別的區段。

1 從 SD-WAN Orchestrator，移至**設定 (Configure) > 區段 (Segments)**。**區段 (Segments)** 畫面隨即出現。請注意，全域區段無法刪除。



2 按一下新增符號 ⊕ 以建立新區段。

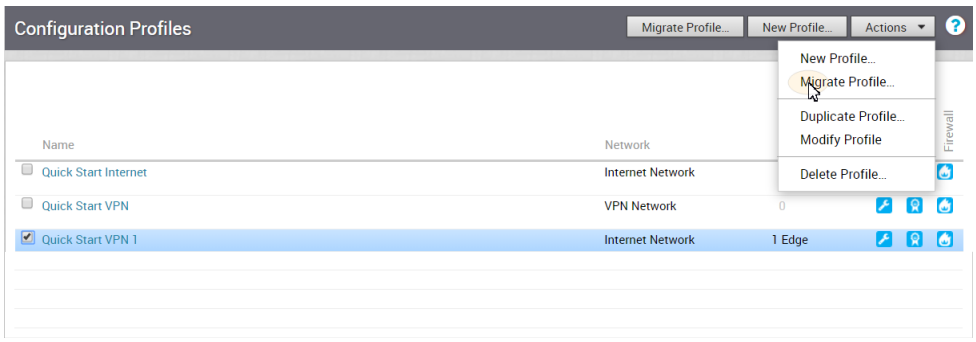
3 按一下**儲存變更 (Save Changes)**。

步驟 2：從網路設定檔建立已移轉的設定檔

1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure) > 設定檔 (Profiles)**。

2 選取組態設定檔名稱旁邊的核取方塊，以選取以網路為基礎的設定檔。

3 在**動作 (Actions)** 下拉式功能表中，選擇**移轉設定檔 (Migrate Profile)**。



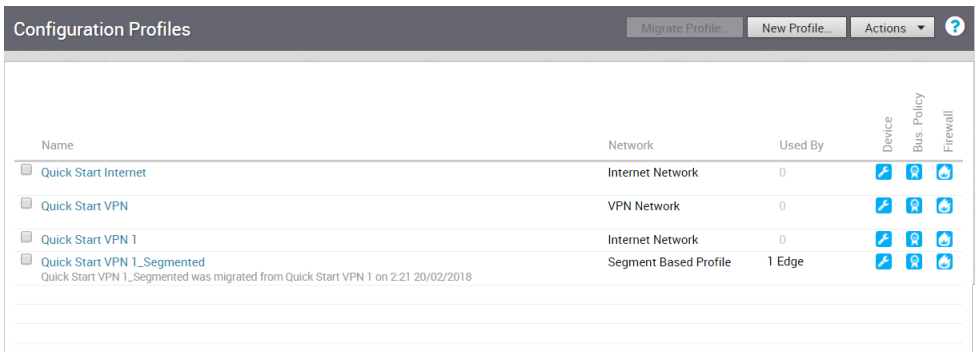
4 在**移轉設定檔 (Migrate Profile)** 對話方塊中，輸入設定檔的名稱和說明。

5 選取客體網路所將對應到的區段 (請參閱步驟 4)。

公司區段組態將會移轉至全域區段。

6 按一下**建立 (Create)** 按鈕。

此時將會建立新的區段設定檔，且其在全域區段中的設定與以網路為基礎的舊設定檔相同。請參閱下圖。請注意，沒有任何 Edge 指派給此設定檔。



步驟 3：將已移轉的設定檔指派給 Edge (請參閱以下重要附註)

在此步驟中，當 Edge 報告的軟體映像 < 3.0 時，將不會有任何組態更新推送至 Edge。處於此狀態的 Edge 基本上會處於「組態凍結」狀態，直到對其佈建 3.X 映像為止。

若要將區段型設定檔指派給以網路為基礎的 Edge：

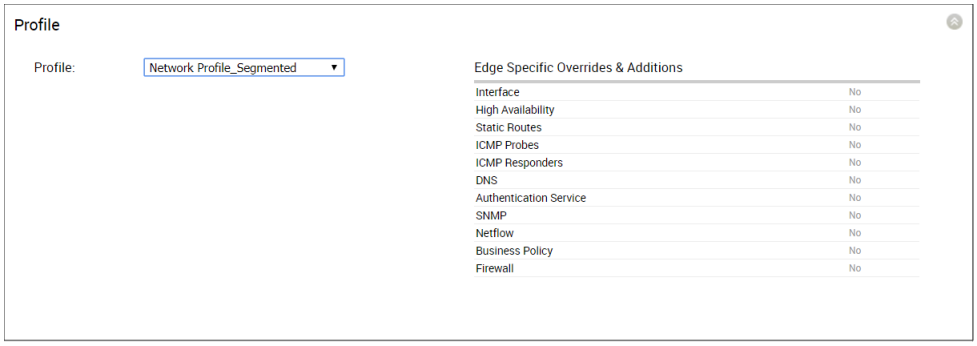
1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure) > Edge**。

2 在 **Edge** 畫面中，選取您要為其指派區段設定檔的 Edge。

3 在 **Edge 概觀 (Edge Overview)** 索引標籤中，移至**設定檔 (Profile)** 區域。

4 在**設定檔 (Profile)** 下拉式功能表中，選擇**區段型設定檔 (Segment Based Profile)**。

只有在 Edge 升級至 3.2.X 之後，才會套用區段型設定檔。



備註 移轉設定檔時所要執行的兩個額外步驟：「使用 3.2 Edge 映像建立新的操作員設定檔」和「將以區段為基礎的操作員設定檔指派給 Edge」。所有層級的企業管理員使用者都無法執行這些額外的步驟，而必須與操作員連絡。其操作員必須使用 3.X 映像建立新的操作員設定檔，並將操作員設定檔指派給企業使用量。指派 3.X 的操作員設定檔和區段設定檔後，Edge 將會接收到軟體映像更新。如需詳細資訊，請連絡您的操作員。

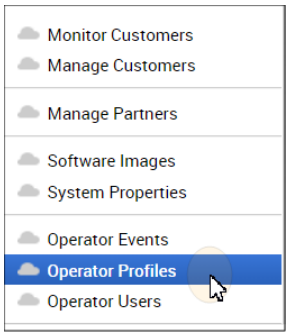
備註 下一個步驟「使用 3.2 Edge 映像建立新的操作員設定檔」是僅適用於操作員層級的步驟，必須先完成才能移轉設定檔。合作夥伴無法存取此步驟的功能，而必須與操作員連絡。

步驟 4：使用 3.2 Edge 映像建立新的操作員設定檔 (僅適用於操作員層級的步驟)

操作員必須使用 3.2 Edge 映像建立新的操作員設定檔，才能移轉設定檔。企業和合作夥伴層級使用者無法存取此步驟中的功能。

步驟 5 是僅適用於操作員層級的步驟。操作員必須使用 3.2 Edge 映像建立新的操作員設定檔。

1 從 SD-WAN Orchestrator，選擇**操作員設定檔 (Operator Profiles)**。請參閱下圖。



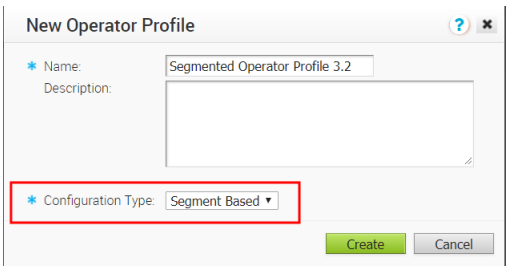
2 從**操作員設定檔 (Operator Profile)** 畫面中，按一下**新增設定檔 (New Profile)** 按鈕。

3 在**新增操作員設定檔 (New Operator Profile)** 對話方塊中：

a 輸入設定檔的名稱和說明。

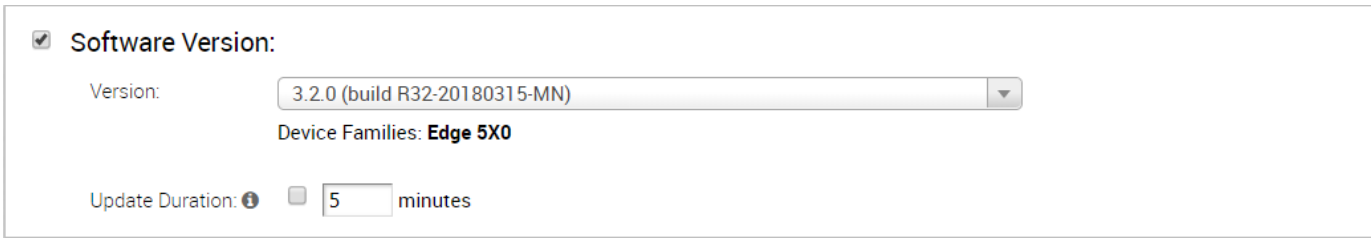
b 在**組態類型 (Configuration Type)** 下拉式功能表中，選擇**以區段為基礎的 (Segment Based)**。

c 按一下**建立 (Create)** 按鈕。



4 在新建立的 **操作員設定檔 (Operator Profile)** 畫面中，移至**軟體版本 (Software Version)** 區域。

5 在**軟體版本 (Software Version)** 區域中，從**版本 (Version)** 下拉式功能表中選擇軟體版本。(請參閱下圖)。



6 按一下 SD-WAN Orchestrator 畫面頂端的**儲存變更 (Save Changes)** 按鈕。

步驟 6：將以區段為基礎的操作員設定檔指派給 Edge

3.3.0 軟體版本的這個步驟中新增了一個重要附註 (請參閱以下附註) (An Important Note has been added to this step for the 3.3.0 software release (see note below))。

備註 操作員和合作夥伴可以指派軟體映像，但所有層級的企業管理員皆無此功能的存取權。

具有區段設定檔的 Edge 將透過操作員設定檔接收軟體映像更新。為此，可以切換客戶的操作員設定檔，或將新的操作員設定檔指派給選取的 Edge。以下步驟說明如何將新的操作員設定檔指派給選取的 Edge。

備註 建議您先對一個 Edge 執行設定檔指派，並驗證 Edge 可正常運作，再繼續處理其他 Edge。第一個被指派設定檔的 Edge 將會分類為中樞 (因為中樞必須在輪輻之前進行移轉)。

若要指派新的操作員設定檔：

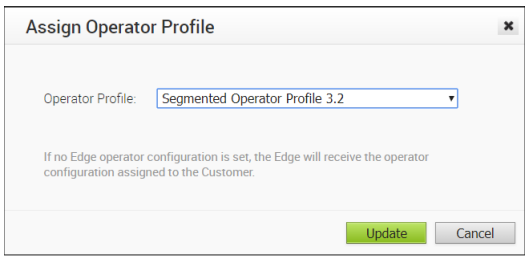
1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure) > Edge**。

2 在 **Edge** 畫面中，選取您要為其指派操作員設定檔的 Edge。

3 在**動作 (Actions)** 下拉式功能表中，選擇**指派操作員設定檔 (Assign Operator Profile)** 或**指派軟體映像 (Assign Software Image)**。(附註：只有操作員超級使用者才會在**動作 (Actions)** 下拉式功能表中看到**指派操作員設定檔 (Assign Operator Profile)**，其他所有可存取此功能的使用者，將會在**動作 (Actions)** 下拉式功能表中看到**指派軟體映像 (Assign Software Image)**)。

4 在適當的對話方塊 (**指派操作員設定檔 (Assign Operator Profile)** 對話方塊或**指派軟體映像 (Assign Software Image)** 對話方塊) 中，選擇在步驟 3 中所建立以區段為基礎的操作員設定檔。(**附註**：如有必要，請將操作員設定檔指派給客戶或合作夥伴)。

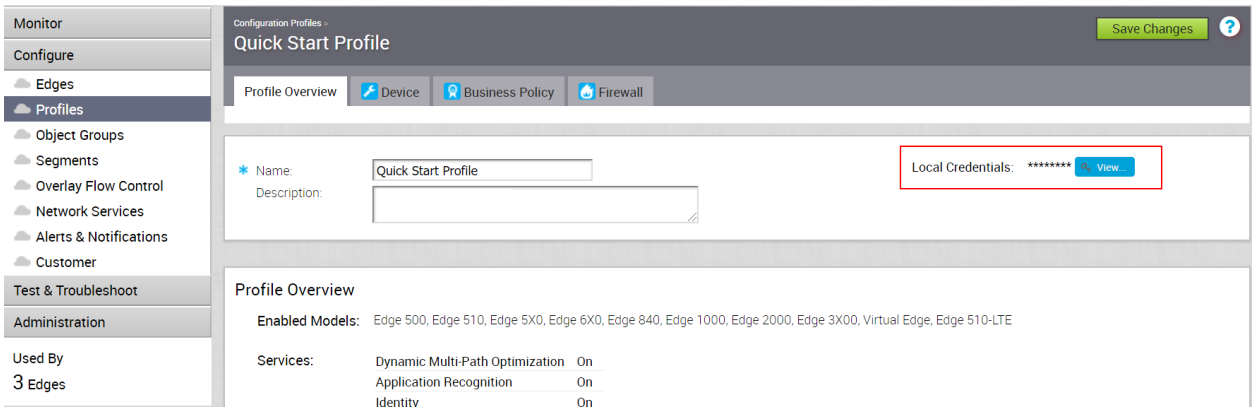
5 按一下**更新 (Update)** 按鈕。



執行此作業後，Edge 將會收到 3.2 軟體映像更新，而在映像更新程序完成後，Edge 將會開始與 SD-WAN Orchestrator 進行通訊。

設定本機認證

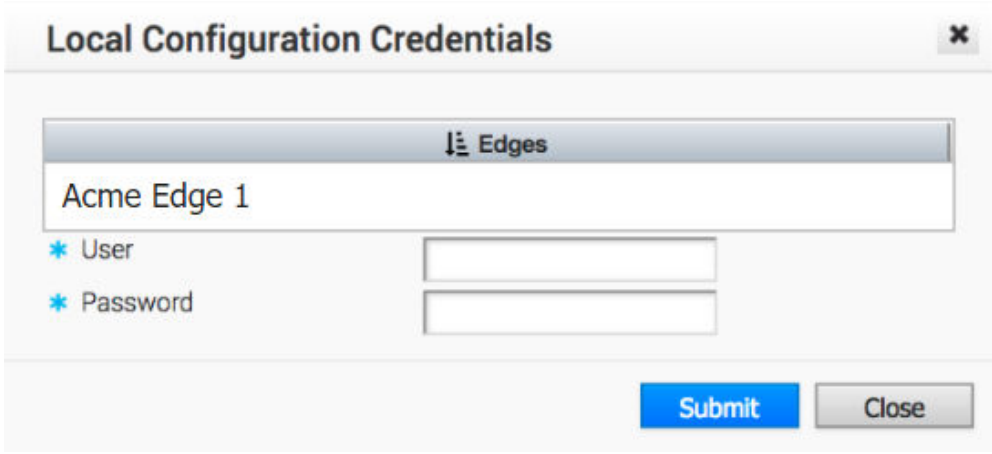
您可以在**設定 (Configure)** > **設定檔 (Profiles)** > **設定檔概觀 (Profile Overview)** 索引標籤中，在設定檔層級變更本機認證。認證更新時，系統會將認證傳送至所有以設定檔作為 Edge 動作的 Edge。



新增認證

本節說明如何新增認證。

按一下**檢視 (View)** 按鈕，以開啟**本機組態認證 (Local Configuration Credentials)** 對話方塊。輸入**使用者 (User)** 名稱和**密碼 (Password)**，然後按一下**提交 (Submit)** 按鈕。


Local Configuration Credentials
Edges
Acme Edge 1
* User
* Password
Submit
Close

設定設定檔裝置

10

本節說明如何設定設定檔裝置。

備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

VMware 可讓您使用設定檔中的**裝置 (Device)** 索引標籤 (**設定 (Configure) > 設定檔 (Profiles) > 裝置 (Device)**) 來提供裝置設定。**裝置設定 (Device Settings)** 索引標籤可用來指派區段、建立 VLAN、設定介面、設定 DNS 設定以及設定驗證設定。如需分割的詳細資訊，請參閱第 7 章 設定區段。

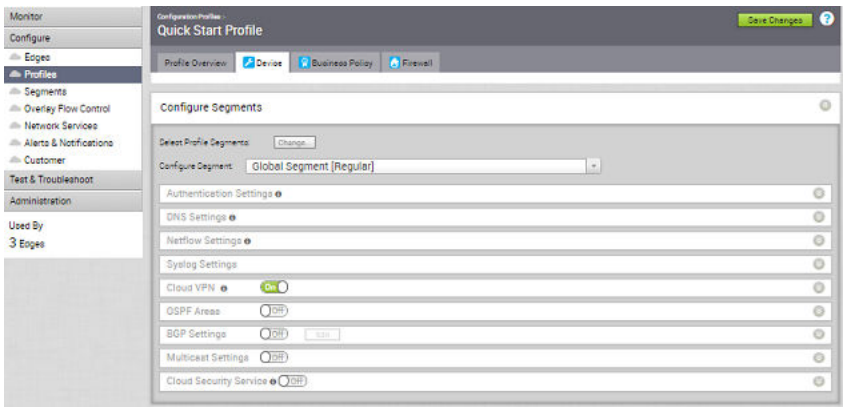
本章節討論下列主題：

設定裝置

裝置組態可讓您將區段指派給設定檔，並設定要與設定檔相關聯的介面。

在區段感知設定檔中，UI 有兩個區段：

組態類型	說明
區段感知組態	**裝置 (Device)** 索引標籤畫面的**設定區段 (Configure Segments)** 區域。客戶可以從下拉式功能表中選擇區段，接著選取區段，該區段的組態就會顯示在**設定區段 (Configure Segments)** 區域中。
一般組態	**裝置 (Device)** 索引標籤畫面的下半部。適用於多個區段的功能和組態，包括 VLAN 組態、裝置設定、Wi-Fi 和多重來源 QoS。



您可以為裝置組態執行下列步驟：

區段感知組態

- 驗證設定
- DNS 設定
- Netflow 設定
- Syslog 設定
- 雲端 VPN (Cloud VPN)
- OSPF 區域 (OSPF Areas)
- BGP 設定
- 多點傳播設定
- 雲端安全服務

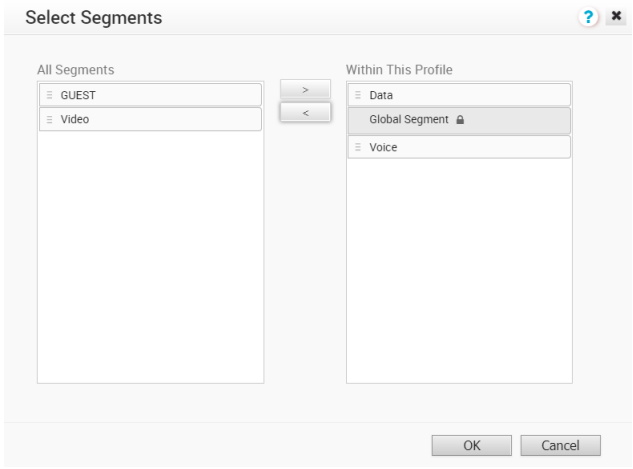
一般組態：

- VLAN
- 裝置設定
- Wi-Fi 無線電設定
- 多重來源 QoS
- SNMP 設定
- NTP 伺服器
- 可見度模式 (Visibility Mode)

在設定檔中指派區段

建立設定檔後，您可以藉由按一下**設定區段 (Configure Segments)** 視窗中的**變更 (Change)** 按鈕來選取設定檔區段。

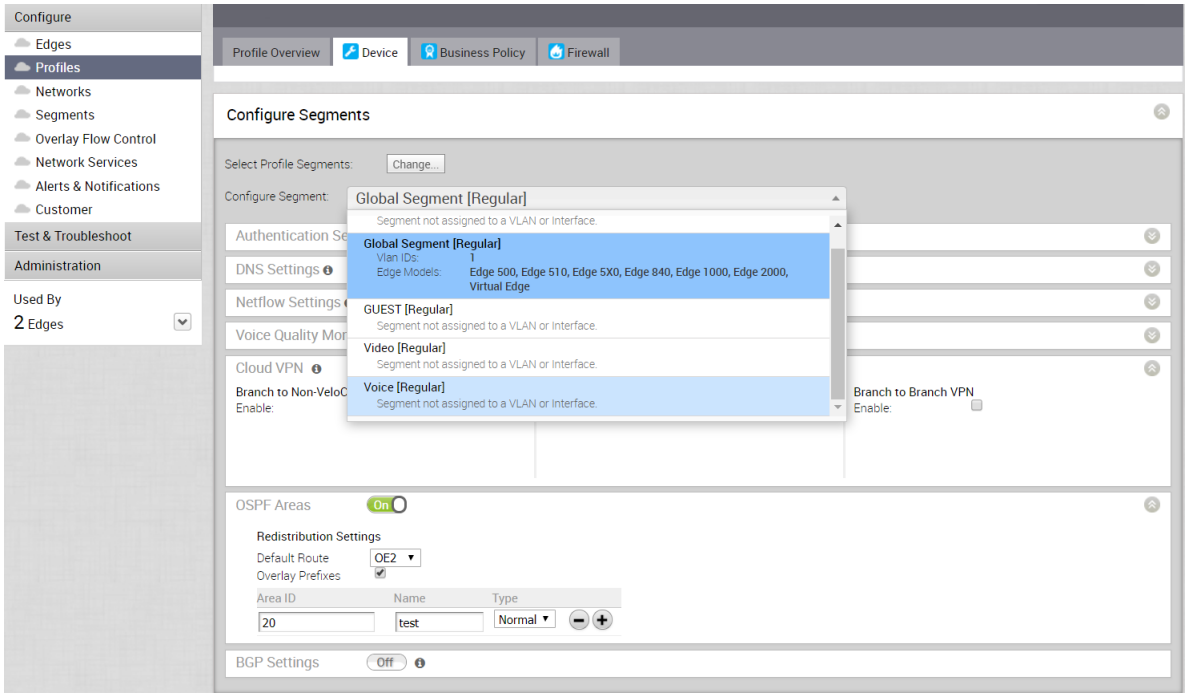
按一下**變更 (Change)** 按鈕即會開啟**選取區段 (Select Segments)** 對話方塊。



在此對話方塊中，您可以選取要包含在設定檔中的區段。旁邊有鎖定符號的區段，表示該區段正用於設定檔內，因此無法移除。可供使用的區段會顯示在對話方塊左側的**所有區段 (All Segments)** 底下。

選取區段之後，您可以透過**設定區段 (Configure Segment)** 下拉式功能表來設定區段。所有可用於設定的區段皆會在**設定區段 (Configure Segment)** 下拉式功能表中列出。如果將區段指派給 VLAN 或介面，該區段將會顯示 VLAN 識別碼及其相關聯的 Edge 型號。

當您從**設定區段 (Configure Segment)** 下拉式功能表中選擇要設定的區段時，視區段的選項而定，與該區段相關聯的設定將會顯示在**設定區段 (Configure Segments)** 區域中。



設定驗證設定

裝置驗證設定 (Device Authentication Settings) 可讓您指定所要使用的網路服務 DNS 服務。

設定 DNS 設定

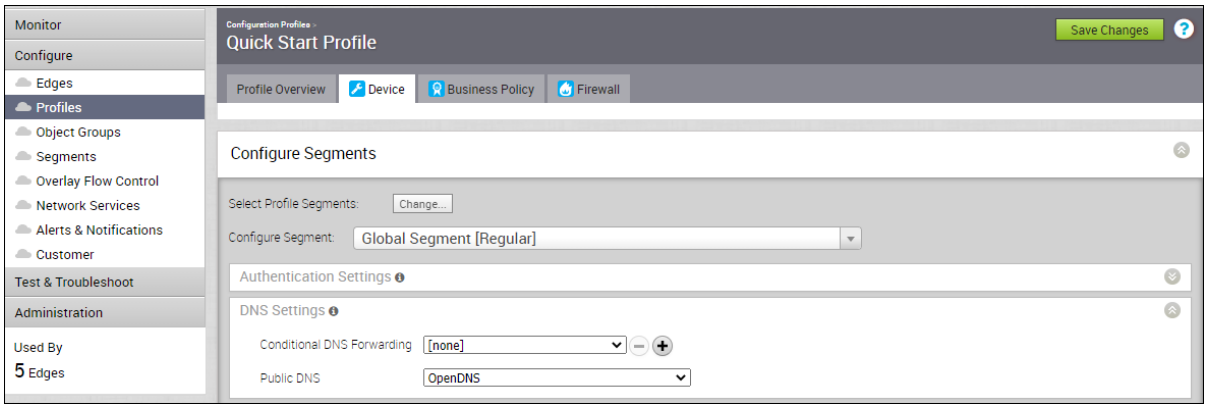
DNS 設定 (DNS Settings) 可用於透過私人 DNS 服務設定條件式 DNS 轉送，以及指定要用於查詢用途的公用 DNS 服務。

若要設定 DNS 設定：

1 在企業入口網站中，按一下**設定 (Configure) > 設定檔 (Profiles)**。

2 按一下設定檔旁的裝置圖示，或按一下設定檔的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 索引標籤中，於 **DNS 設定 (DNS Settings)** 區段中進行下列設定：



- **條件式 DNS 轉送 (Conditional DNS Forwarding)** – 從下拉式清單中選取私人 DNS 服務，以轉送與網域名稱相關的 DNS 要求。您也可以按一下**新增私人 DNS 服務 (New Private DNS Service)**，以建立新的私人 DNS 服務。
- **公用 DNS (Public DNS)** – 從下拉式清單中選取要用於查詢網域名稱的公用 DNS 服務。您也可以按一下**新增 DNS 服務 (New DNS Service)**，以建立新的公用 DNS 服務。

  備註 只有當在 VLAN 或路由介面上啟用了 DHCP 服務時，才會在該 VLAN 或路由介面上啟用公用 DNS 服務。如需指示，請參閱在路由介面上設定 DHCP 伺服器。

如需建立新 DNS 服務的詳細資訊，請參閱設定 DNS 服務。

4 在**裝置 (Device)** 索引標籤上，按一下**儲存變更 (Save Changes)**。

備註 DNS 的全域區段組態會套用至所有客戶建立的區段。來源 IP 是在**設定 VLAN (Configure VLAN)** 區段中設定的管理 IP。請參閱設定設定檔的 VLAN。

在設定檔層級設定 Netflow 設定

身為企業管理員，您可以在設定檔層級設定 Netflow 設定。

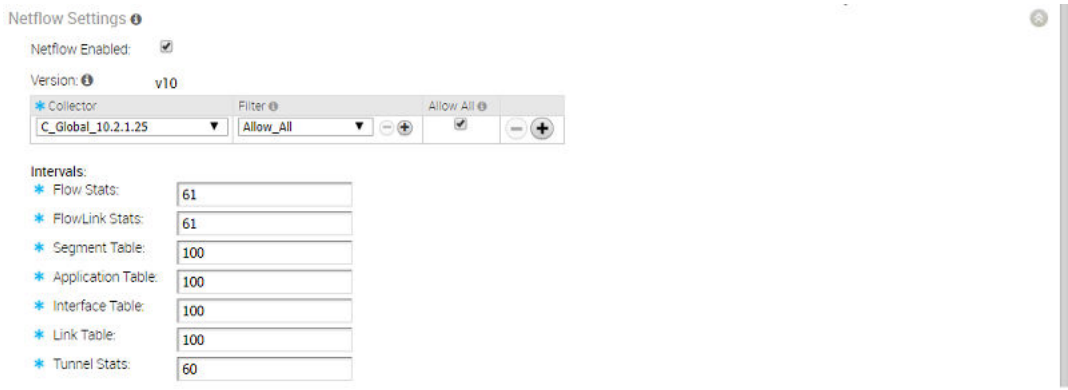
程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

2 選取要設定 Netflow 設定的設定檔，然後按一下**裝置 (Device)** 資料行下的圖示。

所選設定檔的 [裝置設定 (Device Setting)] 頁面隨即出現。



3 在**設定區段 (Configure Segment)** 下拉式功能表中，選取設定檔區段以設定 Netflow 設定。

4 移至 **Netflow 設定 (Netflow Settings)** 區域，然後設定下列詳細資料。

a 選取**已啟用 Netflow (Netflow Enabled)** 核取方塊。

SD-WAN Orchestrator 支援 IP 流量資訊匯出 (IPFIX) 通訊協定第 10 版。

b 在**收集器 (Collector)** 下拉式功能表中選取現有的 Netflow 收集器，以直接從 SD-WAN Edges 匯出 IPFIX 資訊，或按一下**新增收集器 (New Collector)** 以設定新的 Netflow 收集器。

如需如何新增收集器的詳細資訊，請參閱設定 Netflow 設定。

備註 您可以透過按一下 **+** 按鈕，為每個區段設定最多兩個收集器，以及為每個設定檔設定最多八個收集器。當已設定的收集器數目達到允許的限制上限時，就會停用 **+** 按鈕。

c 在**篩選器 (Filter)** 下拉式功能表中，選取現有的 Netflow 篩選器用於來自 SD-WAN Edges 的流量，或按一下**新增篩選器 (New Filter)** 以設定新的 Netflow 篩選器。

如需如何新增篩選器的詳細資訊，請參閱設定 Netflow 設定。

備註 您可以透過按一下**+** 按鈕為每個收集器設定最多 16 個篩選器。不過，對於每個收集器，都會有 [全部允許 (Allow all)] 篩選規則隱含地新增於已定義的篩選器清單結尾。

d 啟用與收集器相對應的**全部允許 (Allow All)** 核取方塊，以允許所有通往該收集器的區段流量。

e 在**間隔 (Intervals)** 下方，設定下列 Netflow 匯出間隔：

- **流量統計資料** - 流量統計資料範本的匯出間隔，會將流量統計資料匯出至收集器。依預設，此範本的 Netflow 記錄會每 60 秒匯出一次。允許的匯出間隔範圍為 60 秒到 300 秒。
- **流量統計資料 (FlowLink Stats)** - 流量連結統計資料範本的匯出間隔，會將每個連結的流量統計資料匯出至收集器。依預設，此範本的 Netflow 記錄會每 60 秒匯出一次。允許的匯出間隔範圍為 60 秒到 300 秒。
- **VRF 資料表 (VRF Table)** - VRF 選項範本的匯出間隔，會將區段相關資訊匯出至收集器。預設匯出間隔為 300 秒。允許的匯出間隔範圍為 60 秒到 300 秒。
- **應用程式資料表 (Application Table)** - 應用程式選項範本的匯出間隔，會將應用程式資訊匯出至收集器。預設匯出間隔為 300 秒。允許的匯出間隔範圍為 60 秒到 300 秒。
- **介面資料表 (Interface Table)** - 介面選項範本的匯出間隔，會將介面資訊匯出至收集器。預設匯出間隔為 300 秒。允許的匯出間隔範圍為 60 秒到 300 秒。
- **連結資料表 (Link Table)** - 連結選項範本的匯出間隔，會將連結資訊匯出至收集器。預設匯出間隔為 300 秒。允許的匯出間隔範圍為 60 秒到 300 秒。
- **通道統計資料 (Tunnel Stats)** - 通道統計資料範本的匯出間隔。依預設，Edge 中作用中通道的統計資料會每 60 秒匯出一次。允許的匯出間隔範圍為 60 秒到 300 秒。

備註 在企業中，您只能在全域區段為每個範本設定 Netflow 間隔。已設定的 Netflow 匯出間隔適用於 Edge 上所有區段的所有收集器。

5 按一下**儲存變更 (Save Changes)**。

在設定檔層級設定 Syslog 設定

在企業網路中，SD-WAN Orchestrator 可用來將源自企業 SD-WAN Edges 的 SD-WAN Orchestrator 繫結事件和防火牆記錄，以原生 Syslog 格式收集到一或多個集中式遠端 Syslog 收集器 (伺服器)。若要讓 Syslog 收集器從企業中已設定 Edge 接收 SD-WAN Orchestrator 繫結事件和防火牆記錄，請在設定檔層級上執行此程序的步驟，以設定 SD-WAN Orchestrator 中每個區段的 Syslog 收集器詳細資料。

必要條件

- 確定已為 SD-WAN Edge (此為產生 SD-WAN Orchestrator 繫結事件之處) 設定雲端虛擬私人網路 (分支到分支 VPN 設定)，以建立 SD-WAN Edge 與 Syslog 收集器之間的路徑。如需詳細資訊，請參閱設定雲端 VPN。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

2 選取要設定 Syslog 設定的設定檔，然後按一下**裝置 (Device)** 資料行下的圖示。

所選設定檔的 [裝置設定 (Device Settings)] 頁面隨即出現。

3 在**設定區段 (Configure Segment)** 下拉式功能表中，選取設定檔區段以設定 Syslog 設定。依預設會選取**全域區段 [一般] (Global Segment [Regular])**。

4 移至 **Syslog 設定 (Syslog Settings)** 區域，然後設定下列詳細資料。

a 在**設施代碼 (Facility Code)** 下拉式功能表中選取一個 Syslog 標準值，而此值對應於您 Syslog 伺服器如何使用設施欄位對所有來自 SD-WAN Edges 的事件進行訊息管理。允許的值介於 **local0** 到 **local7** 之間。

備註 無論是否在設定檔中啟用 Syslog 設定，都只能在**全域區段 (Global Segment)** 設定**設施代碼 (Facility Code)** 欄位。其他區段將繼承全域區段中的設施代碼值。

b 選取**已啟用 Syslog (Syslog Enabled)** 核取方塊。

c 在 **IP** 文字方塊中，輸入 Syslog 收集器的目的地 IP 位址。

d 在**通訊協定 (Protocol)** 下拉式功能表中，選取 **TCP** 或 **UDP** 作為 Syslog 通訊協定。

e 在**連接埠 (Port)** 文字方塊中，輸入 Syslog 收集器的連接埠號碼。預設值為 514。

f 由於 Edge 介面在設定檔層級無法使用，**來源介面 (Source Interface)** 欄位會設定為**自動 (Auto)**。Edge 會自動選取已將 [通告 (Advertise)] 欄位設定為來源介面的介面。

g 在**角色 (Role)** 下拉式功能表中，選取下列其中一項：

- **EDGE 事件**
- **防火牆事件**
- **EDGE 和防火牆事件**

h 在 **Syslog 層級 (Syslog Level)** 下拉式功能表中，選取需要設定的 Syslog 嚴重性層級。例如，如果已設定**嚴重 (CRITICAL)**，則 SD-WAN Edge 會傳送所有設定為 [嚴重] 或 [警示] 或 [緊急] 的事件。

備註 依預設，會使用 Syslog 嚴重性層級**資訊 (INFO)** 來轉送防火牆事件記錄。

允許的 Syslog 嚴重性層級為：

- **緊急 (EMERGENCY)**
- **警示 (ALERT)**
- **嚴重 (CRITICAL)**
- **錯誤 (ERROR)**
- **警告 (WARNING)**
- **注意 (NOTICE)**
- **資訊 (INFO)**
- **偵錯 (DEBUG)**

i 或者，在**標籤 (Tag)** 文字方塊中，輸入 Syslog 的標籤。Syslog 標籤可在 Syslog 收集器上用來區分不同類型的事件。允許的字元長度上限為 32，以句號分隔。

j 使用**防火牆事件 (FIREWALL EVENT)** 或 **EDGE 和防火牆事件 (EDGE AND FIREWALL EVENT)** 角色設定 Syslog 收集器時，如果要 Syslog 收集器接收來自所有區段的防火牆記錄，請選取**所有區段 (All Segments)** 核取方塊。如果停用此核取方塊，Syslog 收集器將僅從已設定收集器的特定區段接收防火牆記錄。

備註 當角色為 **EDGE 事件 (EDGE EVENT)** 時，任何區段中設定的 Syslog 收集器依預設會接收 Edge 事件記錄。

5 按一下 **+** 按鈕以新增另一個 Syslog 收集器，或按一下**儲存變更 (Save Changes)**。遠端 Syslog 收集器會設定於 SD-WAN Orchestrator 中。

備註 每個區段最多可設定兩個 Syslog 收集器，每個 Edge 可設定 10 個 Syslog 收集器。當已設定的收集器數目達到允許的限制上限時，就會停用 **+** 按鈕。

備註 根據選取的角色，Edge 會將指定嚴重性層級的對應記錄匯出至遠端 Syslog 收集器。如果您想要在 Syslog 收集器上接收 SD-WAN Orchestrator 自動產生的本機事件，則必須使用 `log.syslog.backend` 和 `log.syslog.upload` 系統內容在 SD-WAN Orchestrator 層級上設定 Syslog。

若要瞭解防火牆記錄的 Syslog 訊息格式，請參閱防火牆記錄的 Syslog 訊息格式。

後續步驟

SD-WAN Orchestrator 可讓您在設定檔和 Edge 層級啟用 Syslog 轉送功能。在設定檔組態的**防火牆 (Firewall)** 頁面上，如果您想要將源自企業 SD-WAN Edges 的防火牆記錄轉送至已設定的 Syslog 收集器，請啟用 **Syslog 轉送 (Syslog Forwarding)** 按鈕。

備註 依預設，**Syslog 轉送 (Syslog Forwarding)** 按鈕會在設定檔或 Edge 組態的**防火牆 (Firewall)** 頁面上顯示並停用。

如需設定檔層級上防火牆設定的詳細資訊，請參閱設定設定檔的防火牆。

防火牆記錄的 Syslog 訊息格式

說明防火牆記錄的 Syslog 訊息格式，並提供範例。

範例： IETF Syslog 訊息格式 (RFC 3164)

```
<%PRI%>%timegenerated% %HOSTNAME% %syslogtag%%msg
```

以下是 Syslog 訊息的範例。

```
<158>Dec 17 07:21:16 b1-edge1 velocloud.sdwan: VCF Open xR6FveSQT220kZiTmoYJHA SID=12278
SEGMENT=0 IN="IFNAME" PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x DEST_NAME=Internet-via-gateway-3
```

該訊息包含下列部分：

- 優先順序 - 設施 * 8 + 嚴重性 (local3 & info) - 158
- 日期 - Dec 17
- 時間 - 07:21:16
- 主機名稱 - b1-edge1
- Syslog 標籤 - velocloud.sdwan
- 訊息 - VCF Open xR6FveSQT220kZiTmoYJHA SID=12278 SEGMENT=0 IN="IFNAME" PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x DEST_NAME=Internet-via-gateway-3

VMware 支援下列防火牆記錄訊息：

- 啟用可設定狀態的防火牆：
  - 開啟 (Open) - 流量工作階段已啟動。
  - 關閉 (Close) - 由於工作階段逾時或透過 Orchestrator 排清工作階段，流量工作階段已結束。
  - 拒絕 (Deny) - 如果工作階段符合拒絕規則，則會出現拒絕記錄訊息，並且會捨棄封包。在此情況下的 TCP，重設將會傳送至來源。
  - 更新 (Update) - 對於所有進行中的工作階段，如果透過 Orchestrator 新增或修改防火牆規則，則會顯示更新記錄訊息。
- 停用可設定狀態的防火牆：
  - 允許
  - 拒絕

表 10-1. 防火牆記錄訊息欄位

欄位	說明
SID	套用至每個工作階段的唯一識別編號。
SVLAN	來源裝置的 VLAN 識別碼。
DVLAN	目的地裝置的 VLAN 識別碼。
區段	工作階段所屬的區段。允許的範圍為 0 到 255。
傳入	已接收工作階段之第一個封包的介面名稱。如果是覆疊接收的封包，此欄位將包含 **VPN**。若是任何其他封包 (透過底層接收)，此欄位將顯示 Edge 中的介面名稱。

表 10-1. 防火牆記錄訊息欄位 (續)

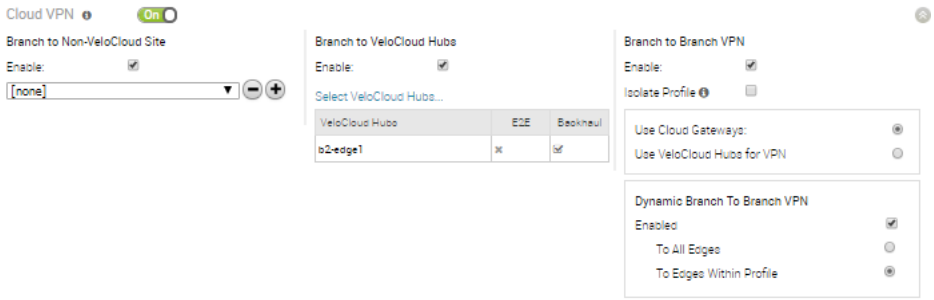
欄位	說明
PROTO	工作階段所使用的 IP 通訊協定類型。可能的值包括 TCP、UDP、GRE、ESP 和 ICMP。
SRC	工作階段的來源 IP 位址 (採用小數點十進位表示法)。
DST	工作階段的目的地 IP 位址 (採用小數點十進位表示法)。
SPT	工作階段的來源連接埠號碼。只有在基礎傳輸為 UDP/TCP 時，此欄位才適用。
DPT	工作階段的目的地連接埠號碼。只有在基礎傳輸為 UDP/TCP 時，此欄位才適用。
DEST_NAME	工作階段的遠端裝置名稱。可能的值為： ■ CSS-Backhaul - 用於從 Edge 到雲端安全性服務的流量。 ■ Internet-via-<*egress-iface-name*> - 用於使用商務原則直接來自 Edge 的雲端流量。 ■ Internet-BH-via-<*backhaul hub name*> - 用於使用商務原則透過回傳中樞進入網際網路的雲端繫結流量。 ■ <*Remote edge name*>-via-Hub - 用於流經中樞的 VPN 流量。 ■ <*Remote edge name*>-via-DE2E - 用於透過直接 VCMP 通道在 Edge 之間流動的 VPN 流量。 ■ <*Remote edge name*>-via-Gateway - 用於流經雲端閘道的 VPN 流量。 ■ NVS-via-<*gateway name*> - 用於流經雲端閘道的 Non VMware SD-WAN Site 流量。 ■ Internet-via-<*gateway name*> - 用於流經雲端閘道的網際網路流量。
NAT_SRC	用於將直接網際網路流量進行來源 NAT 的來源 IP 位址。
NAT_SPT	用於將直接網際網路流量進行 PAT 的來源連接埠。
APPLICATION	工作階段被 DPI 引擎分類到的應用程式名稱。此欄位僅適用於「關閉」記錄訊息。
BYTES_SENT	工作階段中傳送的資料量 (以位元組為單位)。此欄位僅適用於「關閉」記錄訊息。
BYTES_RECEIVED	工作階段中接收的資料量 (以位元組為單位)。此欄位僅適用於「關閉」記錄訊息。

表 10-1. 防火牆記錄訊息欄位 (續)

欄位	說明
DURATION_SECS	工作階段處於作用中狀態的持續時間。此欄位僅適用於「關閉」記錄訊息。
REASON	結束或拒絕工作階段的原因。可能的值為： ■ 狀態違規 ■ 重設 ■ 已清除 ■ 已逾期 ■ 已接收 Fin ■ 已接收 RST ■ 錯誤 此欄位可用於「關閉」和「拒絕」記錄訊息。

設定雲端 VPN

在設定檔層級，SD-WAN Orchestrator 可讓您設定雲端虛擬私人網路 (VPN)。若要起始和回應 VPN 連線要求，您必須啟用雲端 VPN。您可以從**設定 (Configure)** > **設定檔 (Profiles)** > **裝置 (Device)** 頁面設定雲端 VPN。



在啟用設定檔的雲端 VPN 時，您可以設定下列雲端 VPN 類型：

- 設定分支到 Non VMware SD-WAN Site VPN
- 設定分支與 SD-WAN Hubs VPN 之間的通道
- 設定分支到分支 VPN

備註 您應為每個區段設定雲端 VPN。

如需拓撲和使用案例，請參閱雲端 VPN 概觀。

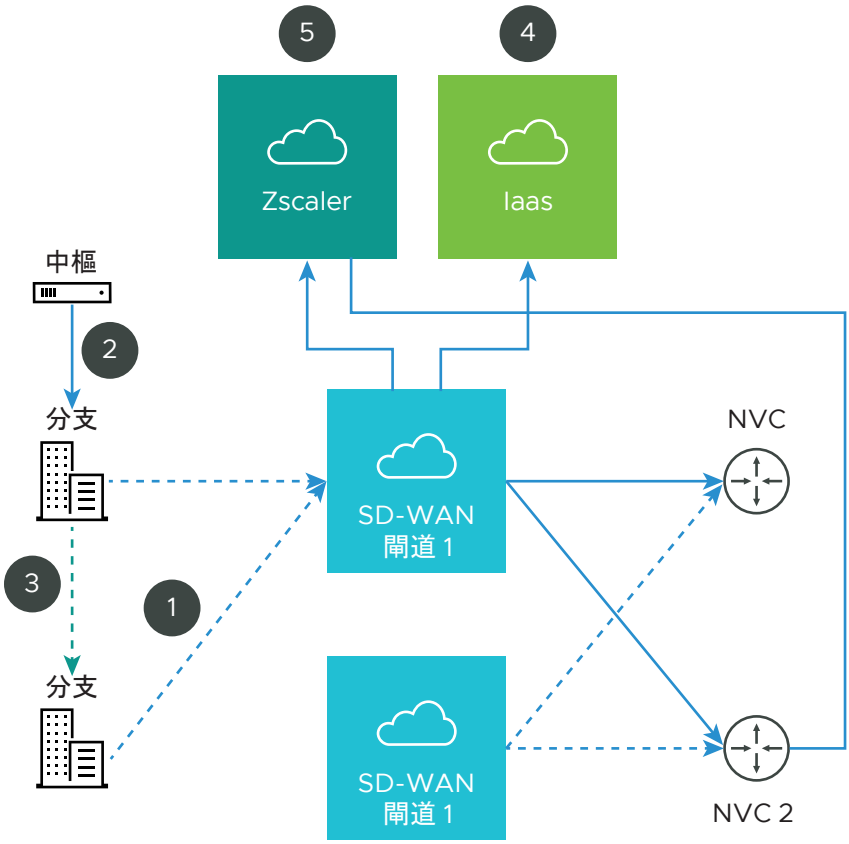
雲端 VPN 概觀

雲端虛擬私人網路 (VPN) 可讓與 VPNC 相容的 IPSec VPN 連線 (連線 VMware 與 Non VMware SD-WAN Sites)。其還會指出站台的健全狀況 (啟動或關閉狀態)，並提供站台的即時狀態。

雲端 VPN 支援下列流量：

- 分支到 Non VMware SD-WAN Site
- 分支到 SD-WAN Hub
- 分支到分支 VPN

下圖顯示雲端 VPN 所有的三個分支。圖中的數字代表每個分支，並對應至後續表格中的說明。



數字 (取自上圖)	說明
1	Non VMware SD-WAN Site
2	分支到 SD-WAN Hub
3	分支到分支 VPN
4	分支到 Non VMware SD-WAN Site
5	分支到 Non VMware SD-WAN Site

分支到 Non VMware SD-WAN Site

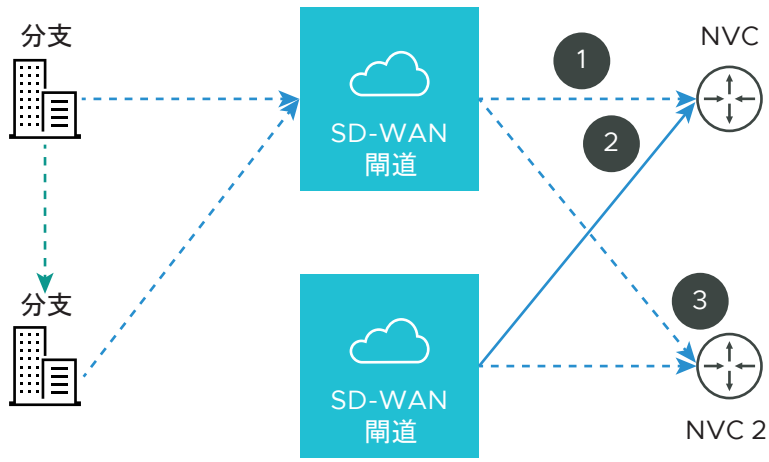
「分支到 Non VMware SD-WAN Site」支援下列組態：

- 透過現有的防火牆 VPN 路由器連線至客戶資料中心
- Iaas
- 連線至 CWS (Zscaler)

透過現有的防火牆 VPN 路由器連線至客戶資料中心

VMware 閘道與資料中心防火牆 (任何 VPN 路由器) 之間的 VPN 連線可提供分支 (已安裝 SD-WAN Edges) 與 Non VMware SD-WAN Sites 之間的連線，從而簡化插入作業，換言之，無須安裝客戶資料中心。

下圖顯示 VPN 組態：



數字 (取自上圖)	說明
1	主要通道
2	備援通道
3	次要 VPN 閘道

VMware 支援對下列第三方防火牆的 VPN 連線：

- Cisco ASA
- Cisco ISR
- PaloAlto
- SonicWall
- 一般路由器 (以路由器為基礎的 VPN)

- 一般防火牆 (以原則為基礎的 VPN)

如需如何設定「分支到 Non VMware SD-WAN Site」的相關資訊，請參閱設定 Non VMware SD-WAN Site。

Iaas

使用 Amazon Web Services (AWS) 進行設定時，請使用 Non VMware SD-WAN Site 對話方塊中的 [一般防火牆 (以原則為基礎的 VPN)] 選項。

使用第三方防火牆進行設定，可獲得下列幾方面的好處：

- 消除網格
- 成本
- 效能

VMware 雲端 VPN 很容易設定 (SD-WAN Gateways 的全域網路免除了 VPC 的網格通道需求)、有集中式原則可控制分支 VPC 存取、可確保效能，且相較於傳統 VPC 的 WAN 更能保護連線。

如需如何使用 Amazon Web Services (AWS) 進行設定的相關資訊，請參閱設定 Amazon Web Services 一節。

連線至 CWS (Zscaler)

Zscaler Web Security 可提供安全性、可見度和控制。Zscaler 提供於雲端中，其功能包括威脅防護、即時分析和鑑識，可提供網路安全性。

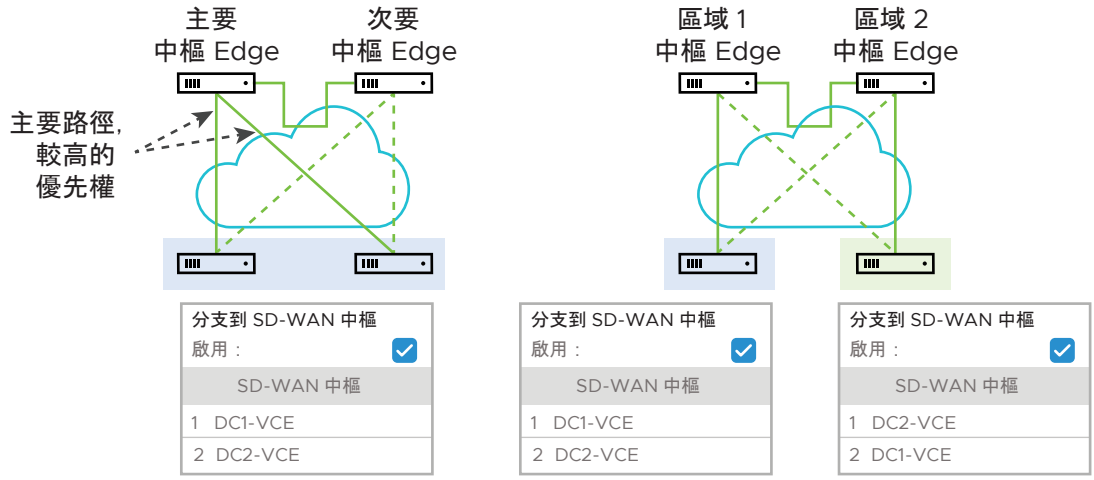
使用 Zscaler 進行設定可提供下列優點：

- **效能：**導向至 Zscaler (透過閘道的 Zscaler)
- **管理 Proxy 是複雜的作業：**按一下即可啟用原則感知 Zscaler

分支到 SD-WAN Hub

SD-WAN Hub 是部署於資料中心的 Edge，可供分支用來存取資料中心資源。您必須在 SD-WAN Orchestrator 中設定 SD-WAN Hub。SD-WAN Orchestrator 向所有 SD-WAN Edges 發出關於中樞的通知，而 SD-WAN Edges 會建置連往中樞的安全覆疊多重路徑通道。

下圖顯示同時支援主動備用和雙主動的情形。



分支到分支 VPN

「分支到分支 VPN」支援在分支之間建立 VPN 連線以改善效能和延展性的組態。

「分支到分支 VPN」支援兩種組態：

- 雲端閘道
- VPN 的 SD-WAN Hubs

下圖顯示雲端閘道和 SD-WAN Hub 的「分支到分支」流量。

您也可以為雲端閘道和中樞啟用動態「分支到分支 VPN」。

您可以從**雲端 VPN (Cloud VPN)** 區域中的**設定 (Configure)** > **設定檔 (Profiles)** > **裝置索引標籤 (Device Tab)**，存取 SD-WAN Orchestrator 中的單鍵式雲端 VPN 功能。

備註 如需設定雲端 VPN 的逐步指示，請參閱設定雲端 VPN。

設定分支到 Non VMware SD-WAN Site VPN

設定「分支到 Non VMware SD-WAN Site VPN」，以建立分支與 Non VMware SD-WAN Site 之間的 VPN 連線。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

2 選取您想要設定雲端 VPN 的設定檔，然後按一下**裝置 (Device)** 資料行下方的圖示。

所選設定檔的**裝置設定 (Device Settings)** 頁面隨即出現。

3 移至**雲端 VPN (Cloud VPN)** 區域，並藉由**開啟**切換按鈕來啟用雲端 VPN。

4 若要設定「分支到 Non VMware SD-WAN Site」，請在**分支到非 VeloCloud 站台 (Branch to Non-VeloCloud Site)** 下，選取**啟用 (Enable)** 核取方塊。

5 從下拉式功能表中選取 Non VMware SD-WAN Site 以建立 VPN 連線。按一下 **+** (加號) 按鈕，以新增其他 Non VMware SD-WAN Sites。

6 您也可以從下拉式功能表中選取**新增非 VeloCloud 站台 (New Non-VeloCloud Site)**，以建立 VPN 連線。**新增非 VeloCloud 站台 (New Non-VeloCloud Site)** 對話方塊隨即出現。

a 在**名稱 (Name)** 文字方塊中，輸入 Non VMware SD-WAN Site 的名稱。

b 在**類型 (Type)** 下拉式功能表中，選取 Non VMware SD-WAN Site。

c 在**主要 VPN 閘道 (Primary VPN Gateway)** 文字方塊中，輸入您想要為所選 Non VMware SD-WAN Site 設定為主要 VPN 閘道的 IP 位址。

d 按**下一步 (Next)**。新的 Non VMware SD-WAN Site 隨即建立，並新增至 Non VMware SD-WAN Site 下拉式功能表。

如需設定 Non VMware SD-WAN Site 的詳細資訊，請參閱設定 Non VMware SD-WAN Site。

7 按一下**儲存變更 (Save Changes)**。

備註 在企業資料中心管理員設定企業資料中心的閘道，且資料中心 VPN 通道啟用之前，不應啟用「分支到 Non VMware SD-WAN Site VPN」。

設定分支與 SD-WAN Hubs VPN 之間的通道

設定「分支到 SD-WAN Hubs VPN」，以建立分支與中樞之間的 VPN 連線。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

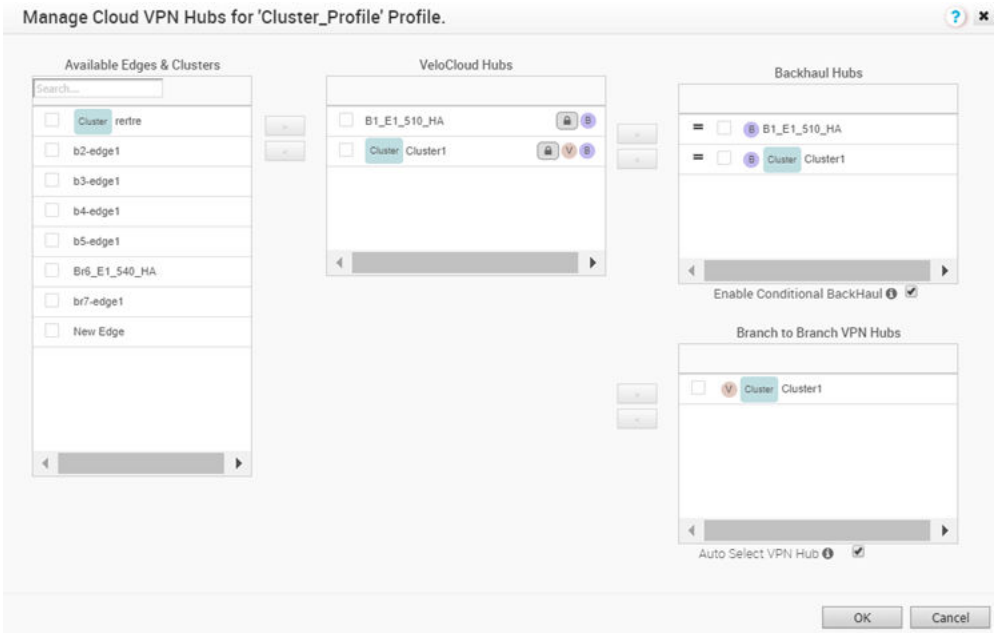
2 選取您想要設定雲端 VPN 的設定檔，然後按一下**裝置 (Device)** 資料行下方的圖示。

所選設定檔的**裝置設定 (Device Settings)** 頁面隨即出現。

3 移至**雲端 VPN (Cloud VPN)** 區域，並藉由**開啟**切換按鈕來啟用雲端 VPN。

4 若要設定「分支到 SD-WAN Hubs」，請在**分支到中樞 (Branch to Hubs)** 下方，選取**啟用 (Enable)** 核取方塊。

5 按一下**選取中樞 (Select Hubs)** 連結。所選設定檔的**管理雲端 VPN 中樞 (Manage Cloud VPN Hubs)** 頁面隨即出現。



6 在**可用的 Edge 和叢集 (Available Edges & Clusters)** 中，您可以使用 > 或 < 箭頭，在分支設定檔中選取並設定 Edge 以做為 SD-WAN Hubs、回傳中樞，或分支到分支 VPN 中樞。

備註 Edge 叢集和個別 Edge 可同時設定為分支設定檔中的中樞。Edge 指派給叢集後，即無法指派為個別中樞。

備註 無論中樞是叢集還是個別 Edge，使用中樞的分支到分支 VPN 的功能都相同。若要使用也是 Edge 叢集的中樞設定「分支到分支 VPN」，您可以從**中樞 (Hubs)** 區域中選取中樞，然後將其移至**分支到分支 VPN 中樞 (Branch to Branch VPN Hubs)** 區域。建議選取**自動選取 VPN 中樞 (Auto Select VPN Hub)** 核取方塊，使 Edge 會選取最佳中樞來建立分支到分支 VPN 中樞的連線。

7 若要啟用條件式回傳，請選取**啟用條件式回傳 (Enable Conditional BackHaul)** 核取方塊。

在啟用條件式回傳 (CBH) 的情況下，每當沒有公用網際網路連結可供使用時，Edge 都能夠將網際網路繫結流量 (直接網際網路流量、透過 SD-WAN Gateway 的網際網路流量，和透過 IPsec 的雲端安全性流量) 容錯移轉至 MPLS 連結。當條件式回傳啟用時，依預設，分支層級的所有商務原則規則都必須依循透過條件式回傳容錯移轉流量的準則。您可以根據所選原則的特定需求，將流量從條件式回傳中排除，只要在選取的商務原則層級停用此功能即可。如需詳細資訊，請參閱條件式回傳。

8 按一下**儲存變更 (Save Changes)**。

條件式回傳

條件式回傳 (CBH) 是專為至少具有一個公用和一個私人連結的混合 SD-WAN 分支部署而設計的功能。當 VMware SD-WAN Edge 發生公用網際網路連結失敗時，將不會建立 VMware SD-WAN Gateway、雲端安全性服務 (CSS) 和直接分流至網際網路的通道。在此案例中，如果啟用了條件式回傳功能，則會透過

私人連結連線至指定的回傳中樞，讓 SD-WAN Edge 能夠透過私人覆疊將網際網路繫結流量容錯移轉至中樞，並提供對網際網路目的地的可連線性。

當公用網際網路連結失敗，而條件式回傳已啟用時，Edge 可以容錯移轉下列網際網路繫結流量類型：

1 直接導向網際網路

2 透過 SD-WAN Gateway 導向網際網路

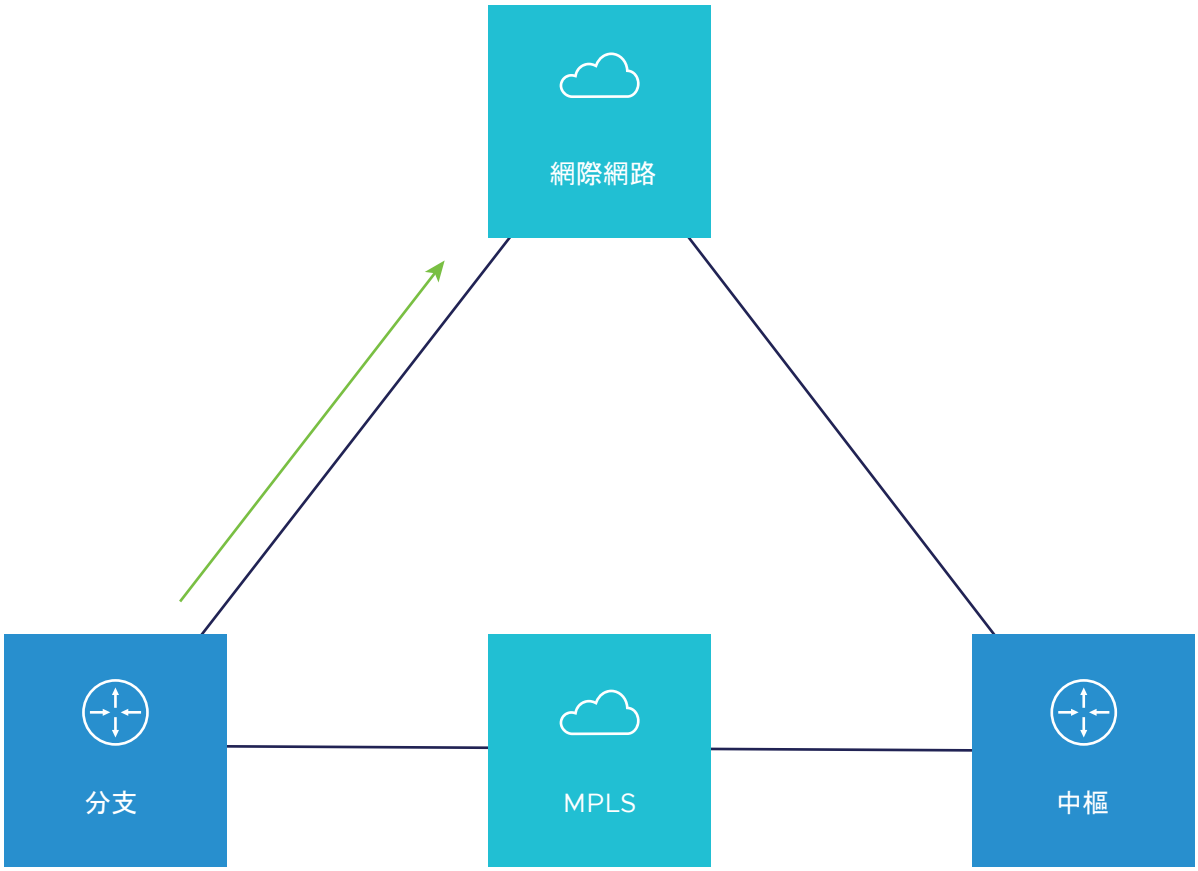
3 雲端安全性服務流量

條件式回傳的行為特性

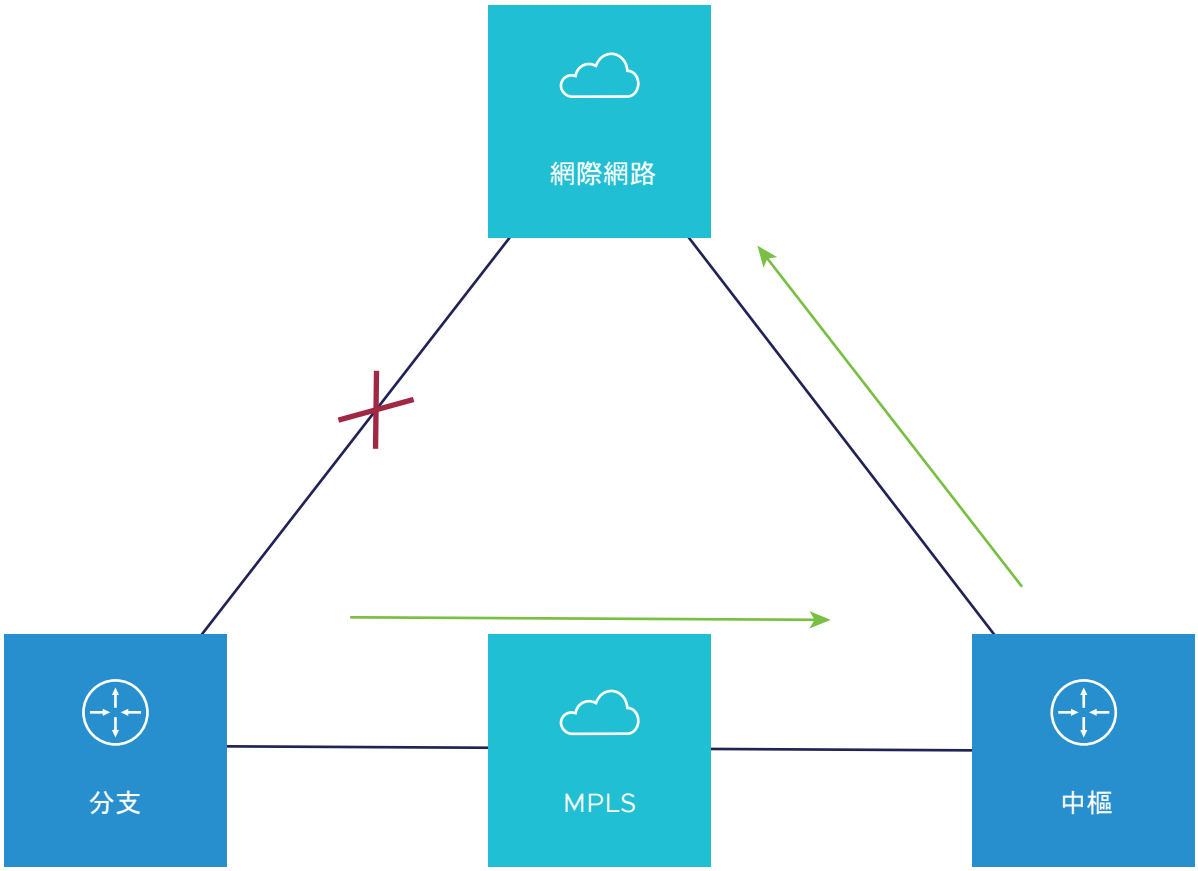
- 當條件式回傳啟用時，依預設，分支層級的所有商務原則規則都必須依循透過 CBH 容錯移轉流量的準則。您可以根據所選原則的特定需求，將流量從條件式回傳中排除，只要在選取的商務原則層級停用此功能即可。
- 條件式回傳並不會影響在公用連結已關閉的情況下正在回傳至中樞的現有流量。現有的流量仍將使用相同的中樞轉送資料。
- 如果某個分支位置具有備份公用連結，則備份公用連結的優先順序將高於 CBH。只有在主要和備份連結皆無法運作時才會觸發 CBH 並使用私人連結。
- 如果以私人連結作為備份，當作用中的公用連結失敗，且私人備份連結進入作用中狀態時，流量將會使用 CBH 功能容錯移轉至私人連結。
- 若要讓此功能正常運作，分支和條件式回傳中樞必須將相同的私人網路名稱指派給其私人連結。(否則，私人通道將不會啟動。)

操作流程

在一般作業下，公用連結會啟動，而網際網路繫結流量會根據已設定的商務原則直接或透過 SD-WAN Gateway 進行傳輸。



當公用網際網路連結關閉，或 SD-WAN 覆疊路徑進入安靜狀態時 (在 7 個活動訊號後未收到來自閘道的封包)，網際網路繫結流量將會以動態方式回傳至中樞。

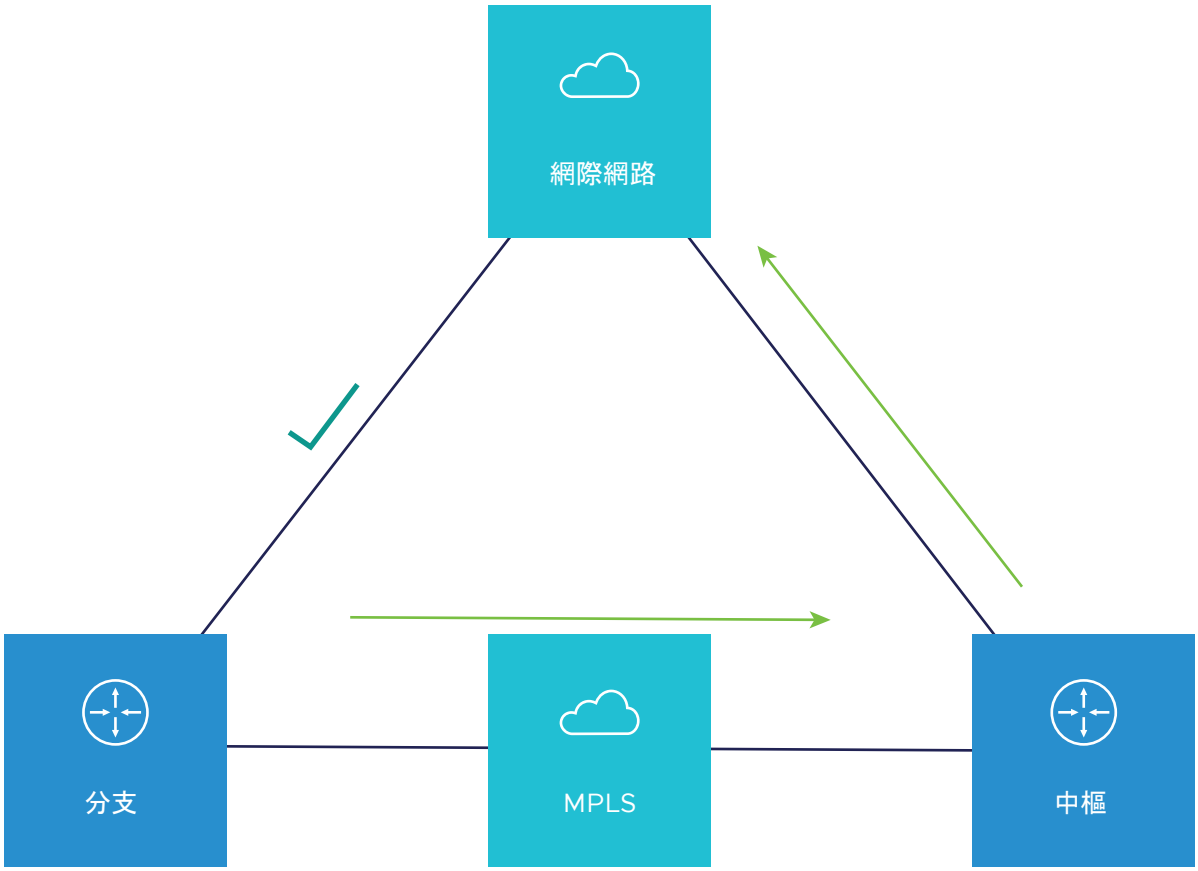


在中樞上設定的商務原則將決定此流量在到達中樞後的轉送方式。選項包括：

- 直接從中樞
- 從中樞到閘道，然後從閘道分流

當公用網際網路連結連回時，CBH 會嘗試將流量移回至公用連結。為了避免不穩定的連結導致流量在公用與私人連結之間翻動，CBH 提供了預設 30 秒的延遲計時器。在延遲計時器結束後，流量將會容錯回復至公用網際網路連結。

。



設定條件式回傳

若要在設定檔層級設定條件式回傳，您應啟用雲端 VPN，然後執行下列步驟，在分支與 SD-WAN Hubs 之間建立 VPN 連線：

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。**組態設定檔 (Configuration Profiles)** 頁面隨即出現。

2 選取您想要設定雲端 VPN 的設定檔，然後按一下 [裝置 (Device)] 資料行下方的圖示。所選設定檔的 [裝置設定 (Device Settings)] 頁面隨即出現。

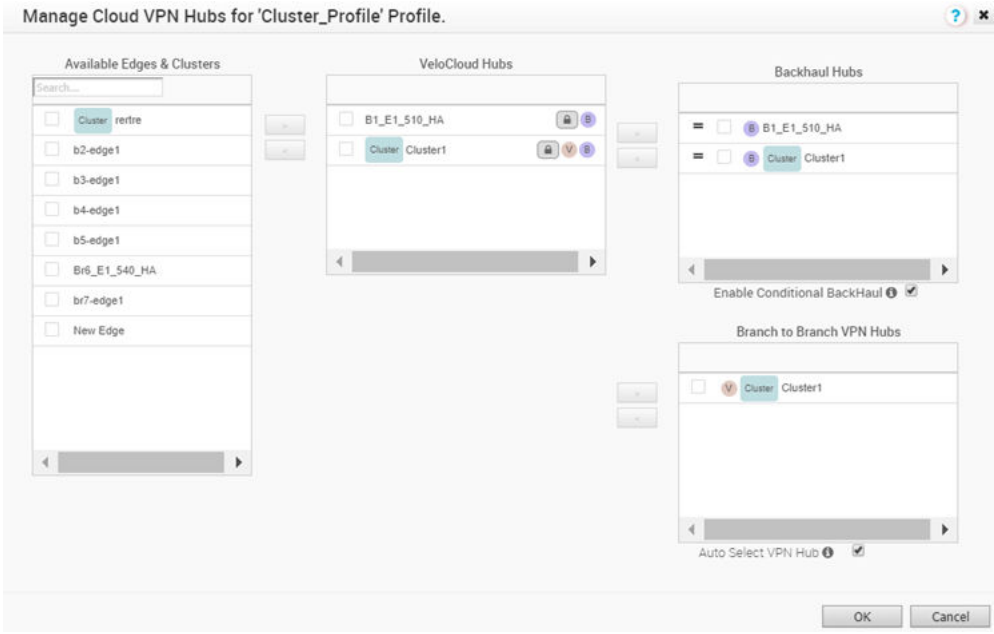
3 在**設定區段 (Configure Segment)** 下拉式功能表中，選取設定檔區段以設定條件式回傳。依預設會選取**全域區段 [一般] (Global Segment [Regular])**。

備註 條件式回傳功能是區段感知的，因此必須在預期要執行該功能的每個區段上加以啟用。

4 移至**雲端 VPN (Cloud VPN)** 區域，並藉由**開啟**切換按鈕來啟用雲端 VPN。

5 若要設定「分支到 SD-WAN Hubs」，請在**分支到中樞 (Branch to Hubs)** 下方，選取**啟用 (Enable)** 核取方塊。

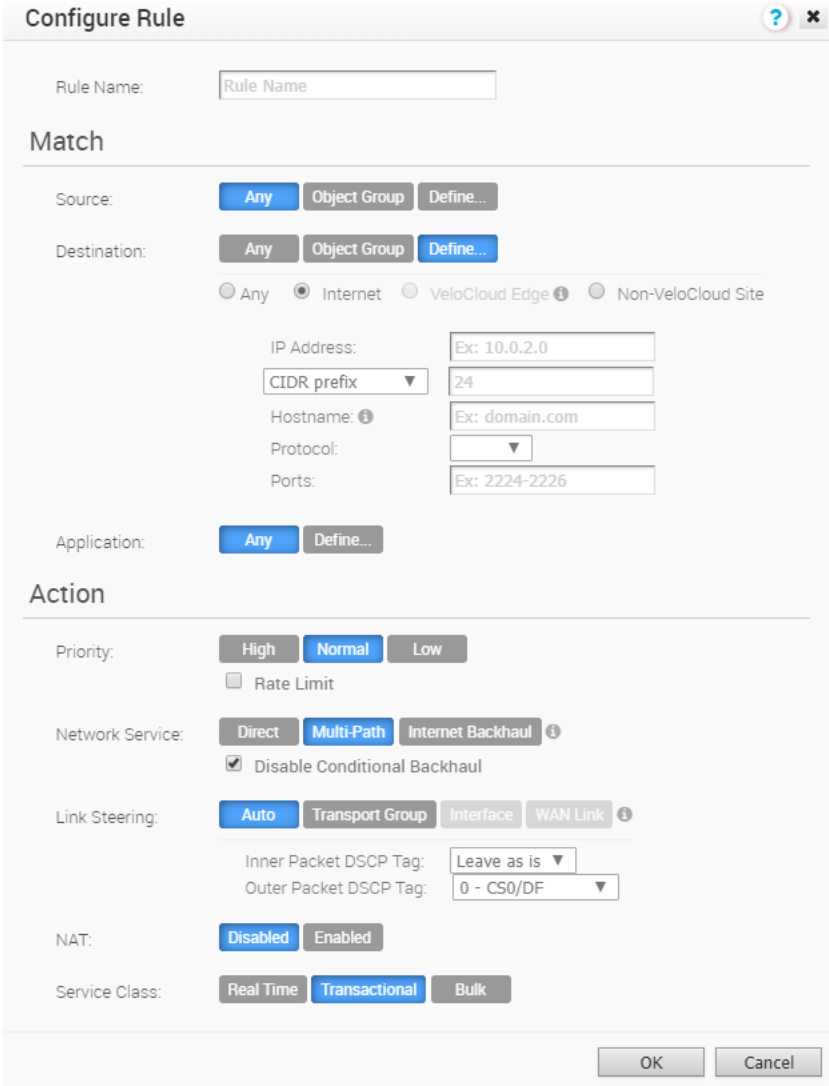
6 按一下**選取中樞 (Select Hubs)** 連結。所選設定檔的**管理雲端 VPN 中樞 (Manage Cloud VPN Hubs)** 頁面隨即出現。



在**中樞 (Hubs)** 區域中，選取要作為回傳中樞的中樞，並使用 > 箭頭將其移至**回傳中樞 (Backhaul Hubs)** 區域。

7 若要啟用條件式回傳，請選取**啟用條件式回傳 (Enable Conditional BackHaul)** 核取方塊。

在啟用條件式回傳的情況下，每當沒有公用網際網路連結可供使用時，Edge 都能夠將網際網路繫結流量 (直接網際網路流量、透過 SD-WAN Gateway 的網際網路流量，和透過 IPsec 的雲端安全性流量) 容錯移轉至 MPLS 連結。依預設，條件式回傳在啟用時將會套用至所有商務原則。如果您要根據特定需求將流量從條件式回傳中排除，則可以停用所選原則的條件式回傳，將選取的流量排除於此行為外，方法是在所取商務原則的**設定規則 (Configure Rule)** 畫面中，選取**動作 (Action)** 區域中的**停用條件式回傳 (Disable Conditional Backhaul)** 核取方塊。



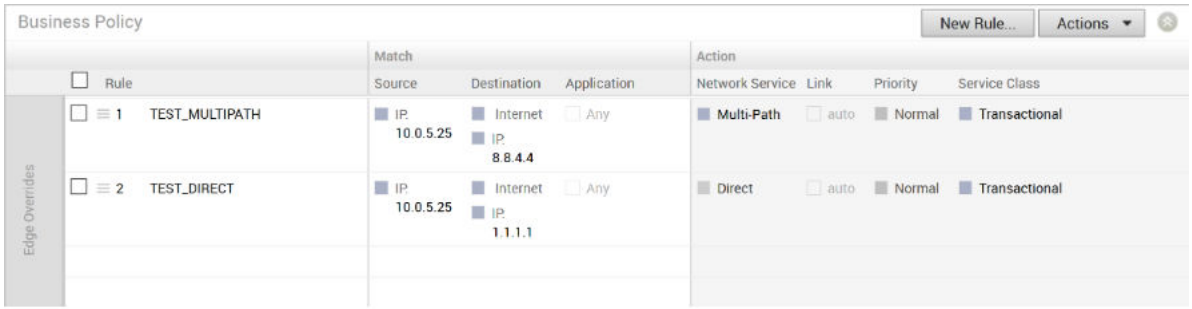
備註

- 條件式回傳和 SD-WAN 可連線性可在相同的 Edge 中搭配運作。在 Edge 上的公用網際網路關閉時，條件式回傳和 SD-WAN 可連線性支援將雲端繫結閘道流量容錯移轉至 MPLS。如果已啟用條件式回傳且沒有閘道的路徑，而有透過 MPLS 通往中樞的路徑，則直接和閘道繫結流量都將套用條件式回傳。如需 SD-WAN 可連線性的詳細資訊，請參閱透過 MPLS 的 SD-WAN 服務可連線性。
- 有多個候選中樞時，條件式回傳將會使用清單中的第一個中樞，除非中樞與閘道的連線已中斷。

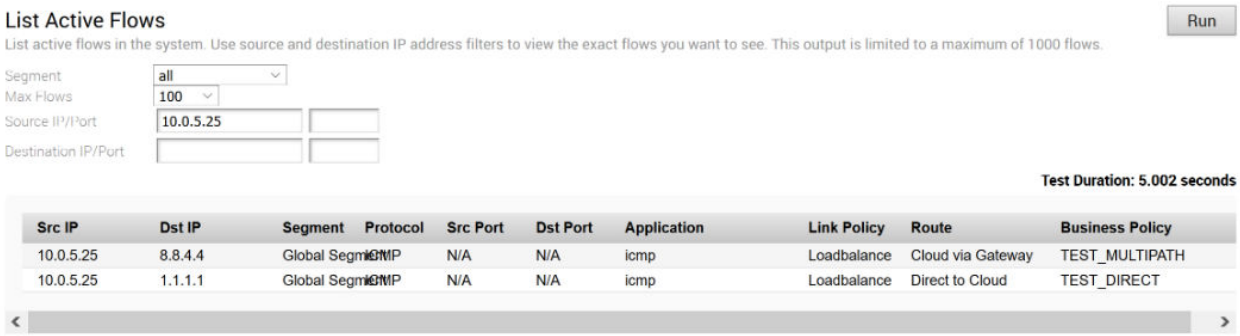
8 按一下**儲存變更 (Save Changes)**。

對條件式回傳進行疑難排解

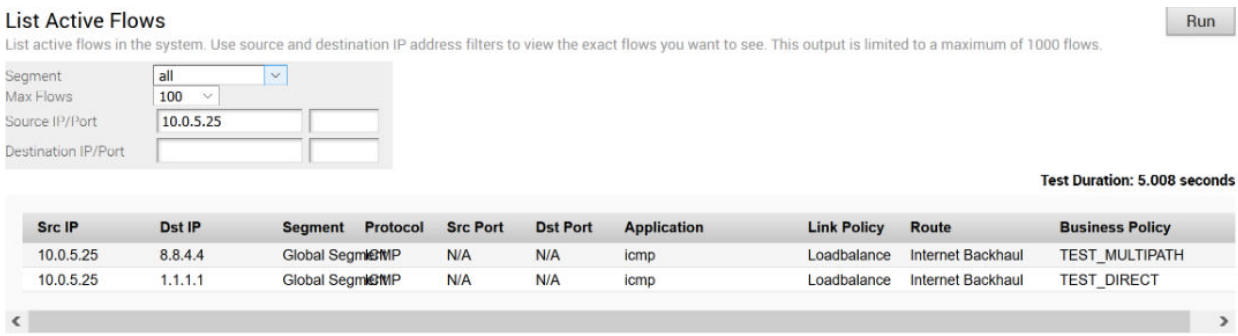
假設某個使用者在分支層級上建立了下列兩個商務原則規則。



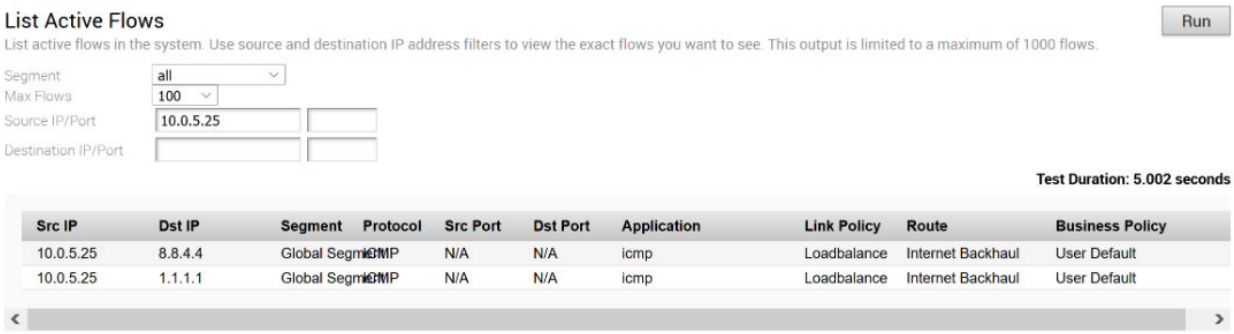
您可以從 [遠端診斷 (Remote Diagnostics)] 區段執行**列出作用中流量 (List Active Flows)** 命令，以檢查分支對於每個目的地 IP 位址的持續 Ping 是否都處於作用中狀態。



如果在分支的公用連結中發生極端封包遺失，且連結已關閉，則相同的流量將會切換至位於分支的網際網路回傳。



請注意，中樞上的商務原則會決定中樞轉送流量的方式。由於中樞對於這些流量沒有特定規則，因此會將其分類為預設流量。在此案例中，可以在中樞層級建立商務原則規則以符合所需的 IP 或子網路範圍，從而定義在 CBH 開始運作時如何處理來自特定分支的流量。



設定分支到分支 VPN

設定「分支到分支 VPN」，以建立分支之間的 VPN 連線。

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

2 選取您想要設定雲端 VPN 的設定檔，然後按一下**裝置 (Device)** 資料行下方的圖示。

所選設定檔的**裝置設定 (Device Settings)** 頁面隨即出現。

3 移至**雲端 VPN (Cloud VPN)** 區域，並藉由**開啟**切換按鈕來啟用雲端 VPN。

4 若要設定「分支到分支 VPN」，請在**分支到分支 VPN (Branch to Branch VPN)** 下，選取**啟用 (Enable)** 核取方塊。

「分支到分支 VPN」支援兩個在分支之間建立 VPN 連線的組態：

組態	說明
使用 SD-WAN Gateway	在此選項中，Edge 與最近的閘道建立 VPN 通道，而 Edge 之間的連線將經過該閘道。SD-WAN Gateway 可能會有來自其他客戶的流量。
使用 SD-WAN Hub	在此選項中，系統會選取一或多個 Edge 作為可與分支建立 VPN 連線的中樞。分支 Edge 之間的連線將經過中樞。中樞是保存您的公司資料的唯一資產，從而提高整體的安全性。

5 若要啟用設定檔隔離，請選取**隔離設定檔 (Isolate Profile)** 核取方塊。

如果已啟用設定檔隔離，則設定檔中的 Edge 將不會透過 SD-WAN 覆疊從設定檔外部的其他 Edge 學習路由。

您可以對所有 Edge 或設定檔中的 Edge 啟用「動態分支到分支 VPN」。在選取**已啟用 (Enabled)** 核取方塊時，依預設會為所有 Edge 設定「動態分支到分支 VPN」。若要依設定檔設定「動態分支到分支 VPN」，請確定**隔離設定檔 (Isolate Profile)** 核取方塊已取消選取。

備註 設定檔隔離啟用時，只能對設定檔內的 Edge 啟用「動態分支到分支 VPN」。

當您啟用「動態分支到分支 VPN」時，第一個封包會經過雲端閘道 (或中樞)。如果起始 Edge 決定流量可透過安全覆疊多重路徑通道進行路由，且如果已啟用「動態分支到分支 VPN」，則會在這些分支之間建立直接通道。

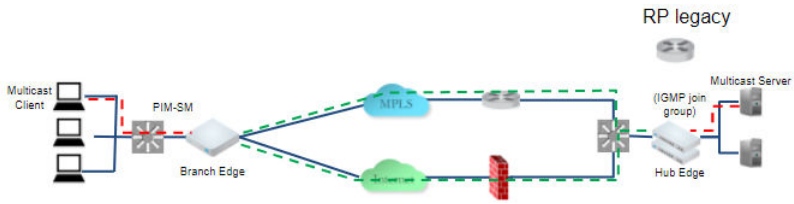
建立通道後，流量會開始流經分支之間的安全覆疊多重路徑通道。流量靜音 (從分支任一端的正向或反向) 180 秒之後，起始 Edge 會移除通道。

6 按一下**儲存變更 (Save Changes)**。

設定多點傳播設定

多點傳播提供一種僅需來源中一份資料即可傳送至一組相關接收器的高效方式，也就是讓網路中的中繼多點傳播路由器複寫封包，以根據群組訂閱到達多個接收器。

多點傳播用戶端可使用網際網路群組管理通訊協定 (IGMP) 將成員資格資訊從主機傳播到已啟用多點傳播的路由器和 PIM，以透過多點傳播路由器將群組成員資格資訊傳播到多點傳播伺服器。



多點傳播支援包括：

- 覆疊和底層上的多點傳播支援
- SD-WAN Edge 上的通訊協定通用多點傳播 - 稀疏模式 (PIM-SM)
- SD-WAN Edge 上的網際網路群組管理通訊協定 (IGMP) 第 2 版
- 第三方路由器上啟用 RP 的靜態集合點 (RP) 組態。

全域設定多點傳播

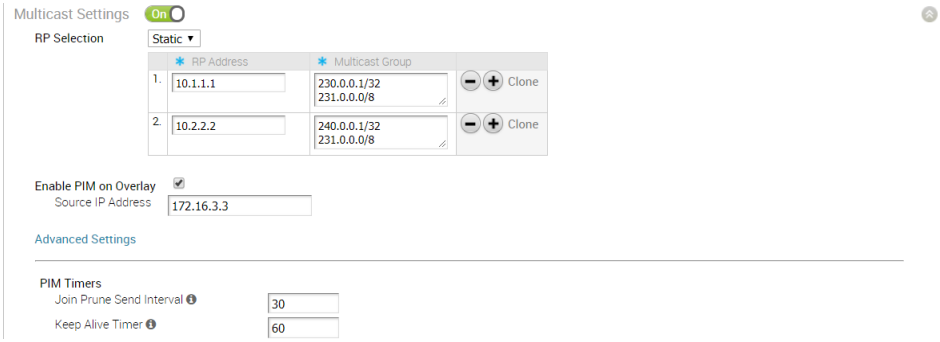
啟用和設定多點傳播時須執行兩個步驟 (全域和介面層級)，而這兩個層級的設定皆可在 Edge 層級上覆寫。下列步驟提供如何全域啟用多點傳播的相關指示。

若要全域設定多點傳播：

1 從**設定 (Configure) > 設定檔 (Profile) > 裝置 (Device)**，移至**多點傳播設定 (Multicast Settings)** 區域。

2 如果**多點傳播設定 (Multicast Settings)** 按鈕位於**關閉 (Off)** 位置，請按一下**關閉 (Off)** 按鈕，以**開啟**多點傳播設定。

依預設會將 RP 選項設為**靜態 (Static)**。



3 在 RP 選取的適當文字方塊中，輸入 RP 位址和多點傳播群組。(請參閱下表，以取得 **RP 位址 (RP Address)** 和**多點傳播群組 (Multicast Group)** 的說明)。

4 如果適用，請選取**在覆疊上啟用 PIM (Enable PIM on Overlay)** 核取方塊，然後輸入 IP 來源位址。

5 如有必要，請設定**進階設定 (Advanced Settings)**。請參閱下表，以取得每個設定的說明。在適當的文字方塊中，輸入**加入/剪除/傳送間隔 (Join Prune Send Interval)** 的 PIM 計時器 (預設為 60 秒)，以及**保持運作計時器 (Keep Alive Timer)** (預設為 60 秒)。

多點傳播設定

下表說明多點傳播設定。

多點傳播設定	說明
RP 選取 (RP Selection)	為多點傳播群組設定 RP。**靜態 RP (Static RP)** 是 3.2 版中的預設和支援機制。
在覆疊上啟用 PIM (Enable PIM on Overlay)	在 SD-WAN 覆疊上啟用 PIM 對等。例如，它們同時在分支 SD-WAN Edge 和中樞 SD-WAN Edge 上啟用時，將會形成 PIM 對等。依預設，覆疊的來源 IP 位址衍生自任何交換介面 (如果存在的話)，或停用了 WAN 覆疊的靜態類型的路由介面。使用者可以選擇指定**來源 IP 位址 (Source IP Address)** 來變更來源 IP；這將是一個虛擬位址，且將會自動在覆疊上通告。
PIM 計時器 (PIM Timers)	
加入/剪除/傳送間隔 (Join Prune Send Interval)	加入/剪除間隔計時器。預設值為 60 秒。
保持運作計時器 (Keep Alive Timer)	PIM 保持運作計時器。預設值為 60 秒。

在介面層級設定多點傳播設定

您可以在介面層級為每個 Edge 型號設定多點傳播設定。

若要在介面層級啟用和設定多點傳播：

1 在企業入口網站中，移至 [設定 (Configure)] > [設定檔 (Profiles)] > [裝置 (Device)]，然後選取一個目標 Edge 型號，以設定多點傳播。

2 在**介面設定 (Interfaces Settings)** 區域中，選取您要啟用多點傳播的介面，然後按一下**編輯 (Edit)** 按鈕。

3 在所選 Edge 的**介面 (Interface)** 對話方塊中：

a 依預設，會啟用**已啟用介面 (Interface Enabled)** 核取方塊。如有需要，您可以停用介面。停用時，將無法使用介面進行任何通訊。

b 在**功能 (Capability)** 下拉式功能表中選擇**已路由 (Routed)**，以便能夠使用多點傳播設定。依預設，對於 [交換器連接埠 (Switch Port)]，會選取**已交換 (Switched)** 選項。

c 在**定址類型 (Addressing Type)** 下拉式功能表中，選擇 DHCP、PPPoE 或 [靜態 (Static)]。

d 如果適用，請選取 **WAN 覆疊 (WAN Overlay)** 核取方塊。依預設會使用自動偵測覆疊啟用此選項。您可以選擇使用者定義的覆疊，並設定覆疊設定。如需詳細資訊，請參閱設定 Edge WAN 覆疊設定。

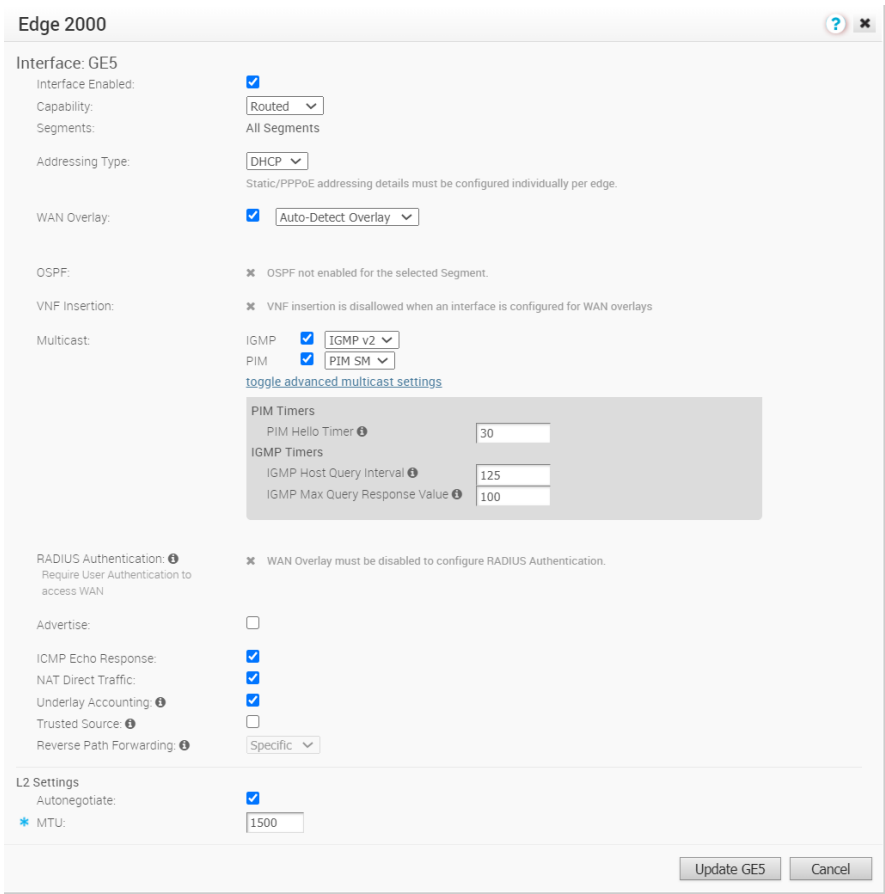
e 如果適用，請選取 **OSPF** 核取方塊。

f 在**多點傳播 (Multicast)** 區段中：

1 如果適用，請選取 **IGMP** 核取方塊，然後選取唯一的可用選項 IGMP v2。

2 如果適用，請選取 **PIM** 核取方塊，然後選取唯一可用的選項 PIM SM。

3 按一下**切換進階多點傳播設定 (toggle advanced multicast settings)** 連結，以設定 IGMP 計時器和 PIM 計時器。



- **PIM 問詢計時器 (PIM Hello Timer)** - 預設值為 30 秒，允許的範圍是 1 到 180 秒。

- **IGMP 主機查詢間隔 (IGMP Host Query Interval)**：預設值為 125 秒，允許的範圍是 1 到 1800。
- **IGMP 最大查詢回應值 (IGMP Max Query Response Value)**：預設值為 100 分秒，允許的範圍是 10 到 250 分秒。

g 您必須停用 WAN 覆疊，才能設定 RADIUS 驗證。選取此核取方塊可在介面上啟用 RADIUS 驗證，並新增不應轉送至 RADIUS 進行重新驗證的 MAC 位址。如需詳細資訊，請參閱在路由介面上啟用 RADIUS 。

h 如果適用，請選取以下核取方塊：

- **通告 (Advertise)** - 選取此核取方塊，以將介面通告至網路中的其他分支。
- **ICMP 回應回覆 (ICMP Echo Response)** - 選取此核取方塊，以便讓介面能夠回覆 ICMP 回應訊息。基於安全考量，您可以為介面停用此選項。
- **NAT 直接流量 (NAT Direct Traffic)** - 選取此核取方塊，以將 NAT 套用至介面所傳來的網路流量。
- **底層計量 (Underlay Accounting)** - 依預設，會啟用此選項。如果在介面上定義了私人 WAN 覆疊，則周遊介面的所有底層流量都將根據 WAN 連結的測量速率計數，以防止過度訂閱。如果您不想要此行為 (例如，在使用單臂部署時)，請停用此選項。
- **信任的來源 (Trusted Source)** - 選取此核取方塊，以將介面設定為信任的來源。

i 從**反向路徑轉送 (Reverse Path Forwarding)** 下拉式功能表的下拉式清單中，選取下列其中一個選項：

- **已停用 (Disabled)** - 即使路由表中沒有相符的路由仍允許傳入流量。
- **特定 (Specific)** - 即使已停用信任的來源 (Trusted Source) 選項，依預設仍會選取此選項。傳入流量應符合傳入介面上的特定傳回路由。如果找不到特定的相符項，則會捨棄傳入的封包。這是設定了公用覆疊和 NAT 的介面上常用的模式。
- **寬鬆 (Loose)** - 傳入流量應符合路由表中的任何路由 (已連線/靜態/已路由)。這會允許非對稱路由，通常用於未設定下一個躍點的介面。

備註 只有在已啟用信任的來源時，才能選擇反向路徑轉送 (RPF) 的選項。如果停用了 [信任的來源 (Trusted Source)]，則 RPF 會預設為 [特定 (Specific)] 模式。

j 在 **L2 設定 (L2 Settings)** 區域中，依預設，會啟用**自動交涉 (Autonegotiate)** 核取方塊。自動交涉可讓連接埠與連結另一端的裝置進行通訊，以判斷連線的最佳雙工模式和速度。

k 如果未選取 [自動交涉 (Autonegotiate)]，請輸入以下詳細資料：

- **速度 (Speed)** - 只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取連接埠與其他連結通訊時所需的速度。依預設會選取 100 Mbps。
- **雙工 (Duplex)** - 只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取全雙工或半雙工作為連線模式。依預設會選取全雙工。
- **MTU** - 在所有交換器介面上接收和傳送之框架的預設 MTU 大小為 1500 個位元組。您可以變更介面的 MTU 大小。

- 按一下**更新 (Update)** 以儲存設定。

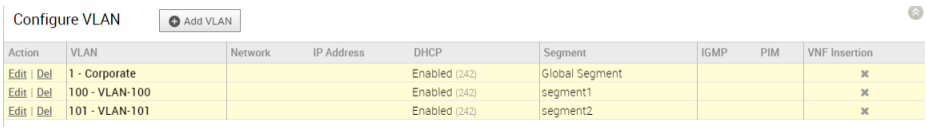
備註 移至**監控 (Monitor)** > **路由 (Routing)** > **多點傳播 (Multicast)** 索引標籤，以檢視多點傳播路由資訊。如需詳細資訊，請參閱監控路由。

設定設定檔的 VLAN

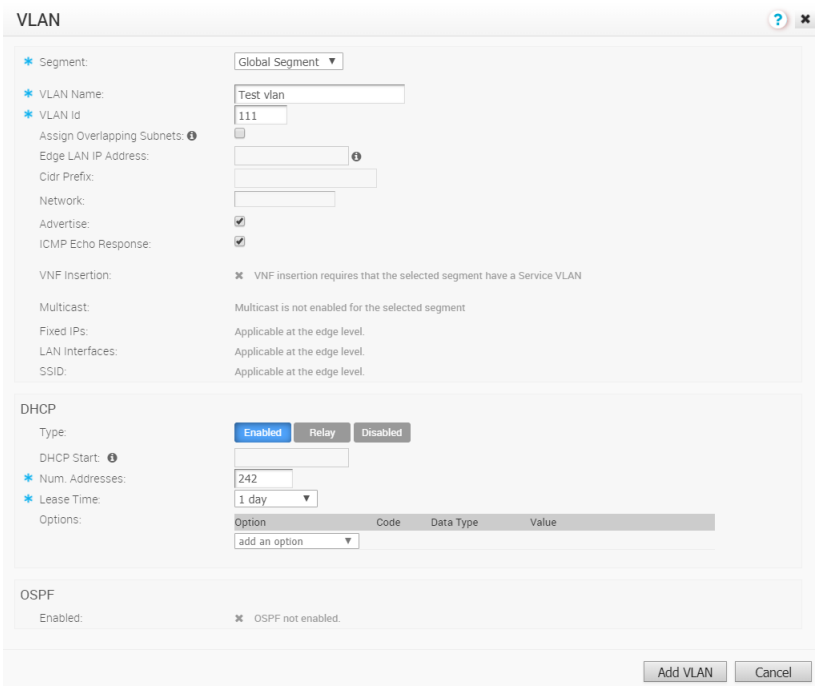
身為企業管理員，您可以在設定檔層級設定 VLAN。

若要在設定檔層級新增 VLAN，請執行下列步驟：

1. 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)**。**組態設定檔 (Configuration Profiles)** 頁面隨即出現。
2. 選取要設定 VLAN 的設定檔，然後按一下**裝置 (Device)** 資料行下的圖示。所選設定檔的 [裝置設定 (Device Setting)] 頁面隨即出現。



3. 移至**設定 VLAN (Configure VLAN)** 區域，按一下**新增 VLAN (Add VLAN)**。



4. 在 **VLAN** 對話方塊中，設定下列詳細資料：
   a. 在**區段 (Segment)** 下拉式功能表中，選取設定檔區段以設定 VLAN。
   b. 在 **VLAN 名稱 (VLAN Name)** 文字方塊中，輸入 VLAN 的唯一名稱。
   c. 在 **VLAN 識別碼 (VLAN ID)** 文字方塊中，輸入 VLAN 的唯一識別碼。

d 如果您要將 VLAN 的相同子網路指派給設定檔中的每個 Edge，請選取**指派重疊的子網路 (Assign Overlapping Subnets)** 核取方塊。啟用此核取方塊可讓您定義設定檔中要用於每個 Edge 的子網路，方法是使用 **Edge LAN IP 位址 (Edge LAN IP Address)** 和 **CIDR 首碼 (CIDR Prefix)** 欄位。將根據子網路遮罩和 CIDR 值自動設定**網路 (Network)** 位址。

備註 如果您想要將不同的子網路指派給每個 Edge (例如，針對 VPN 網路)，請勿在設定檔層級上啟用**指派重疊的子網路 (Assign Overlapping Subnets)** 核取方塊，但是您可以個別設定每個 Edge 上的子網路。

e 選取**通告 (Advertise)** 核取方塊，將 VLAN 通告至網路中的其他分支。

f 選取 **ICMP 回顯回應 (ICMP Echo Response)** 核取方塊，以啟用 VLAN 來回應 ICMP 回顯訊息。

g 選取 **VNF 插入 (VNF Insertion)** 核取方塊，以啟用 Edge 虛擬網路功能 (VNF) 插入。

備註 VNF 插入需要選取的區段具有服務 VLAN。如需 VNF 的詳細資訊，請參閱安全性 VNF。

h 如果為所選區段啟用了多點傳播功能，則可以透過啟用 **IGMP** 和 **PIM** 核取方塊來設定**多點傳播 (Multicast)** 設定。

i 在 **DHCP** 區域下，選擇下列其中一項做為 DHCP 類型：

- **已啟用 (Enabled)** - 使用 Edge 啟用 DHCP 做為 DHCP 伺服器。選擇此選項時，您必須提供下列詳細資料：
  - **DHCP 啟動 (DHCP Start)** - 輸入子網路內可用的有效 IP 位址做為 DHCP 啟動 IP。
  - **位址數目 (Num Addresses)** - 輸入 DHCP 伺服器子網路上可用的 IP 位址數目。
  - **租用時間 (Lease Time)** - 從下拉式功能表中，選取允許 VLAN 使用由 DHCP 伺服器動態指派之 IP 位址的時段。

  此外，您可以新增一或多個 DHCP 選項，用以指定預先定義的選項或新增自訂選項。
- **轉送 (Relay)** - 使用在遠端位置安裝的 DHCP 轉送代理程式來啟用 DHCP。如果您選擇此選項，則可以指定一或多個轉送代理程式的 IP 位址。
- **已停用 (Disabled)** - 停用 DHCP。

j 如果已針對選取的區段啟用 OSPF 功能，請設定 **OSPF** 設定。

5 按一下**新增 VLAN (Add VLAN)**。已針對設定檔設定 VLAN。您可以按一下**動作 (Actions)** 資料行下的**編輯 (Edit)** 連結來變更 VLAN 設定。

若要在 Edge 層級設定 VLAN，請參閱 設定 Edge 的 VLAN。

設定管理 IP 位址

您可以在設定檔層級設定管理 IP 位址，並選擇在 Edge 層級覆寫該位址。

從 3.4 版開始，Edge 不會以管理 IP 位址作為指向 Orchestrator 的流量來源。相反地，Edge 會選擇區段上的第一個「已啟動並已通告的」介面，來啟動流量。如果找不到這類 LAN 介面，則會使用啟用了 NAT 的 WAN 連結，直接將流量輸出至網際網路。目前，如果您透過全域區段中的 VPN 來傳送源自管理 IP 的流量，且在全域區段中沒有任何已啟動並已通告的 LAN 介面，則當您將 Edge 和 Orchestrator 升級至 3.4 版時，會遇到可連線性問題。請連絡 VMware 客戶支援，以還原 3.4 之前的行為，以便繼續以管理 IP 位址作為流量來源。

以下是您可以使用管理 IP 位址的各種案例，但前提是 Edge 和 Orchestrator 是 3.3 或更舊版本：

- 此位址用來作為從 Edge 指向 Orchestrator 的管理流量來源。在此案例中，您可以使用預設管理 IP 位址 (192.168.1.1)，或使用您在設定檔層級設定的所選 IP 位址，以便讓所有連結至設定檔的 Edge，以相同的 IP 位址作為指向 Orchestrator 的流量來源。

  備註 如果您在 WAN 連接埠上啟用了「NAT 直接」，或者來自 Edge 的流量會經由閘道路由至 Orchestrator，則可以選擇忽略管理 IP 組態。

- 如果您選擇設定 DNS、NTP、Netflow、BGP 等服務，則必須在 Edge 層級覆寫管理 IP 位址組態，以便讓每個 Edge 具有唯一的 IP 位址，以作為這些服務的來源位址。
- 當在 Edge 層級設定此位址時，此位址還作為診斷測試用的目的地 IP 位址。

若要為設定檔設定管理 IP 位址，請執行以下動作：

1 在企業入口網站中，移至**設定 (Configure) > 設定檔 (Profiles)**。

2 在您要設定管理 IP 位址的設定檔旁，按一下 [裝置 (Device)] 圖示，或按一下指向設定檔的連結，然後移至**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 頁面中，向下捲動至**管理 IP (Management IP)** 區段，然後輸入所需的管理 IP 位址。

4 按一下**儲存變更 (Save Changes)**。

您可以選擇覆寫 Edge 的管理 IP 位址組態：

1 在企業入口網站中，移至**設定 (Configure) > Edge**。

2 在您要覆寫管理 IP 位址組態的 Edge 旁，按一下 [裝置 (Device)] 圖示，或按一下指向 Edge 的連結，然後移至**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 頁面中，向下捲動至**管理 IP (Management IP)** 區段，然後選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。

4 輸入所需的管理 IP 位址。

5 按一下**儲存變更 (Save Changes)**。

設定裝置設定

裝置設定可讓您在設定檔中設定一或多個 Edge 型號的介面設定。

根據 Edge 型號，每個介面可以是交換器連接埠 (LAN) 介面或路由 (WAN) 介面。根據分支型號，連線連接埠會是專用的 LAN 或 WAN 連接埠，或連接埠可以設定為 LAN 或 WAN 連接埠。分支連接埠可以是乙太網路或 SFP 連接埠。某些 Edge 型號可能也支援無線 LAN 介面。

在此假設有單一公用 WAN 連結連結至僅用來處理 WAN 流量的單一介面。若未針對支援 WAN 的路由介面設定 WAN 連結，則會假設應自動探索單一公用 WAN 連結。如果探索到連結，則會向 SD-WAN Orchestrator 報告。然後，這個自動探索的 WAN 連結可透過 SD-WAN Orchestrator 進行修改，而新的組態會推送回分支。

備註

- 如果路由介面已啟用 WAN 覆疊，並且與 WAN 連結連結，則介面將可用於所有區段。
- 如果介面設定為 PPPoE，則只會支援單一自動探索的 WAN 連結。無法將其他連結指派給介面。

如果不應或無法自動探索連結，必須明確加以設定。有多個支援的組態無法執行自動探索，包括：

- 私人 WAN 連結
- 單一介面上的多個 WAN 連結。範例：具有 2 個 MPLS 連線的資料中心中樞
- 可透過多個介面存取的單一 WAN 連結。範例：用於作用中/作用中 HA 拓撲

自動探索到的連結一律為公用連結。使用者定義的連結可以是公用或私人的，且會根據選取的類型而有不同的組態選項。

備註 即便是自動探索到的連結，覆寫自動偵測到的參數 (例如服務提供者和頻寬) 後，仍可由 Edge 組態覆寫。

公用 WAN 連結

公用 WAN 連結是可用來存取公用網際網路 (如纜線、DSL 等) 的任何傳統連結。公用 WAN 連結不需要對等組態。它們會自動連線至 SD-WAN Gateway，由其處理對等連線所需資訊的散佈。

私人 (MPLS) WAN 連結

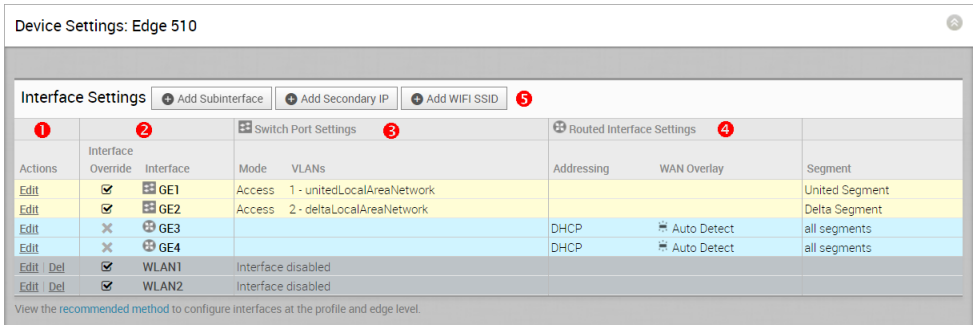
私人 WAN 連結屬於私人網路，只能連線至相同私人網路內的其他 WAN 連結。由於可能會有多個 MPLS 網路，例如在單一企業內，使用者必須識別哪個連結屬於哪個網路。SD-WAN Gateway 將會使用這項資訊來散佈 WAN 連結的連線資訊。

您可以選擇將 MPLS 連結視為單一連結。但是，若要區分服務不同的 MPLS 類別，您可以為每個 WAN 連結指派不同的 DSCP 標籤來定義多個 WAN 連結，以對應至服務的不同 MPLS 類別。

此外，您也可以決定為私人 WAN 連結定義靜態 SLA。如此，對等就不再需要交換路徑統計資料並減少連結上的頻寬耗用量。由於探查間隔會影響裝置進行容錯移轉的速度，因此靜態 SLA 定義是否應自動縮短探查間隔並不明確。

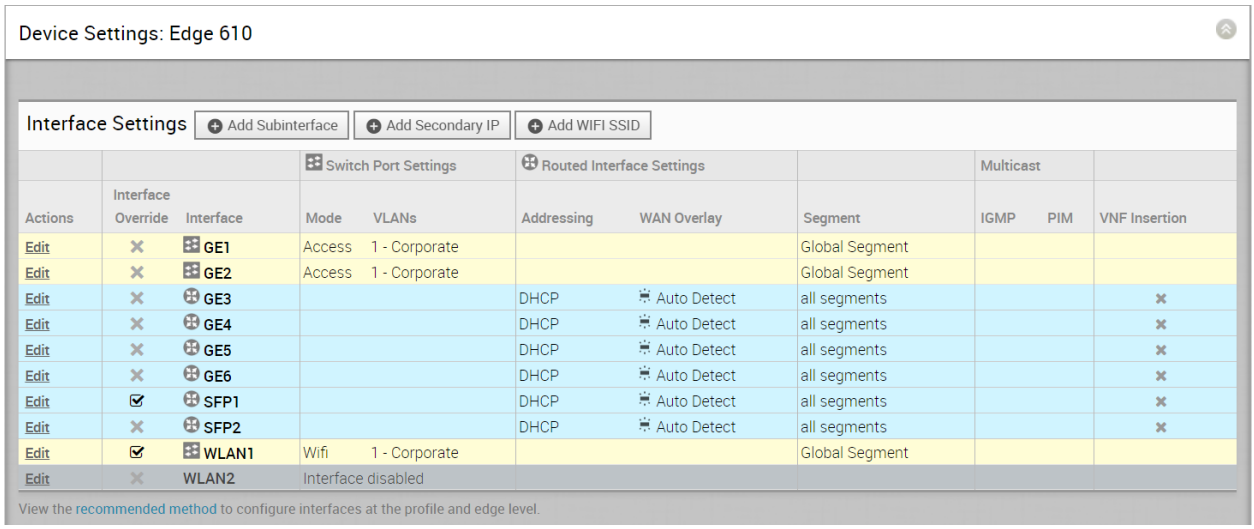
裝置設定

下列螢幕擷取畫面說明 SD-WAN Edge 500、SD-WAN Edge 1000 的最上層使用者介面，並介紹 3.4 版的 SD-WAN Edge 610。下表說明 UI 的主要功能 (表格中的號碼對應於後續螢幕擷取畫面中的號碼)。

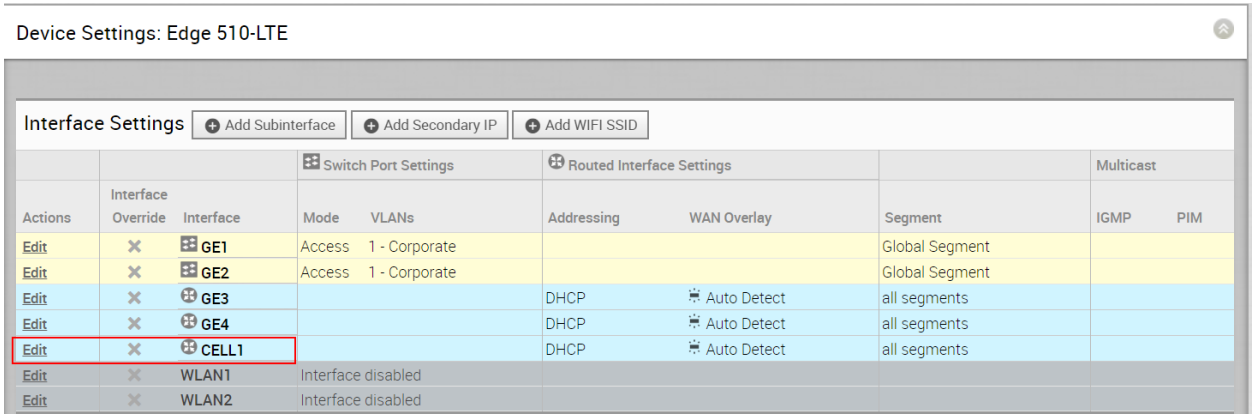


1. 您可以在網路介面上執行的動作，例如編輯或**刪除**。
2. 介面名稱。此名稱與 Edge 裝置上的 Edge 連接埠標籤相符，或已針對無線 LAN 預先決定。
3. 交換器連接埠的清單，其中包含其部分設定的摘要 (例如存取或主幹模式，以及介面的 VLAN)。交換器連接埠會以淺黃色背景反白顯示。
4. 路由介面的清單，其中包含其設定的摘要 (例如定址類型，以及介面是自動偵測到的，還是具有自動偵測或使用者定義的 WAN 覆疊)。路由介面會以淺藍色背景反白顯示。
5. 無線介面清單 (如果在 Edge 裝置上可供使用)。您可以按一下**新增 Wi-Fi SSID (Add Wi-Fi SSID)** 按鈕，以新增其他無線網路。無線介面會以淺灰色背景反白顯示。
5.
   - 您可以按一下**新增 Wi-Fi SSID (Add Wi-Fi SSID)** 按鈕，以新增其他無線網路。無線介面會以淺灰色背景反白顯示。
   - 您可以按一下**新增子介面 (Add Sub Interfaces)** 按鈕，以新增子介面。子介面會在介面旁顯示「SIF」。不支援 PPPoE 介面的子介面。
   - 您可以按一下**新增次要 IP (Add Secondary IP)** 按鈕，以新增次要 IP。次要 IP 會在介面旁顯示「SIP」。

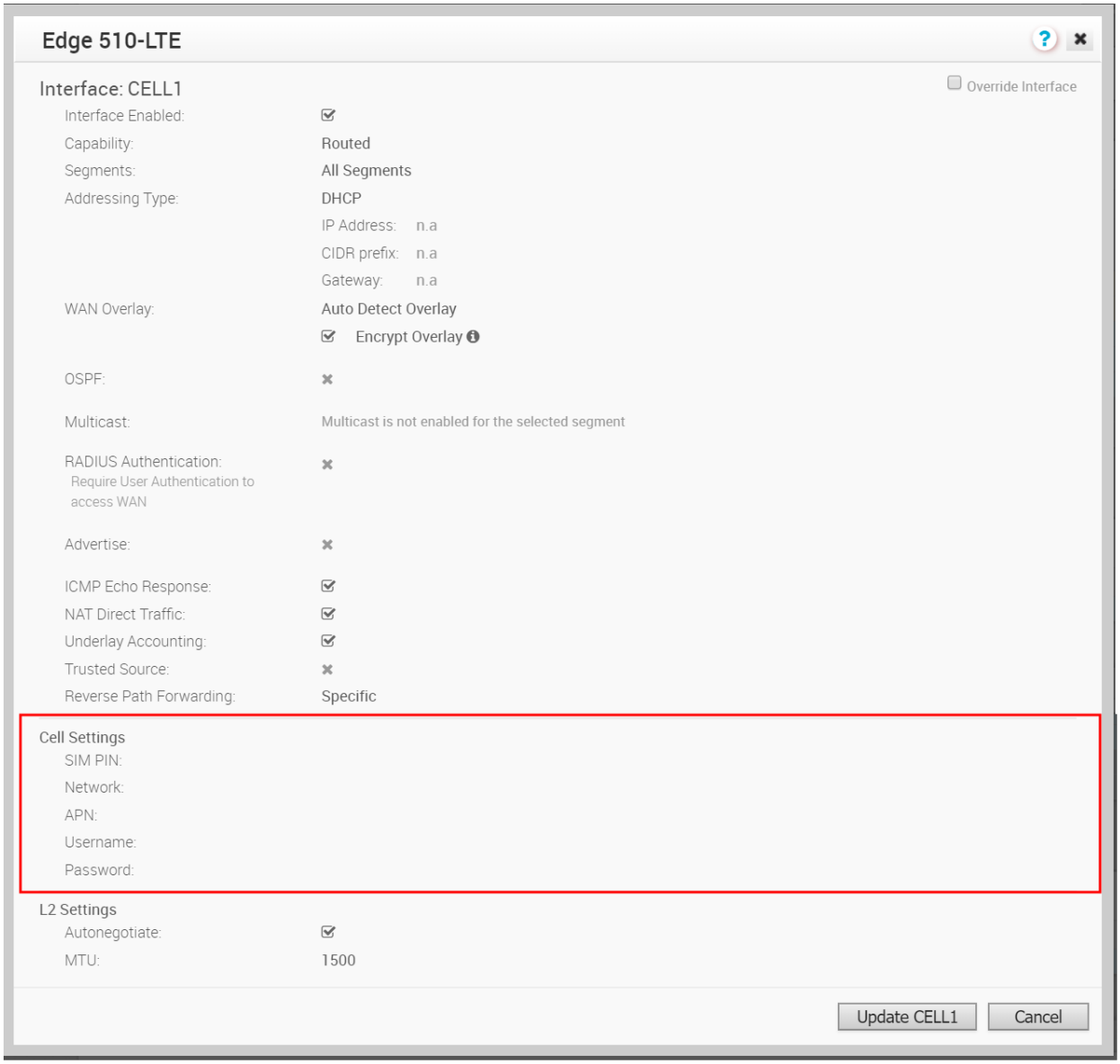
3.4 版本導入了 Edge 610。



3.4 版中新增了新的路由介面 (CELL1)，如果使用者選擇 Edge 510-LTE 作為型號，將會顯示在**介面設定 (Interface Settings)** 區域中 (請參閱下圖)。

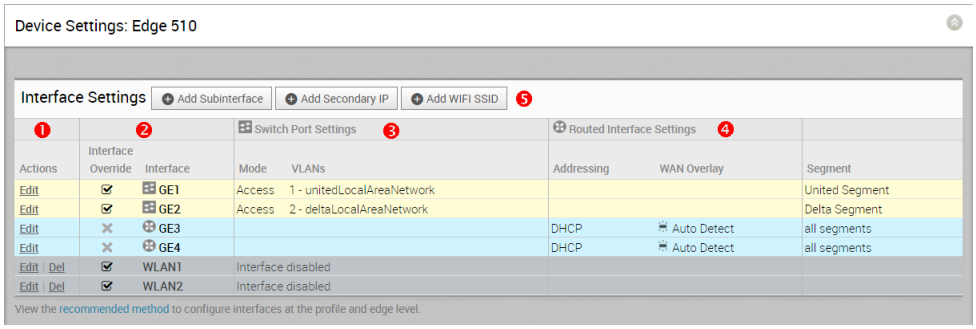


按一下**編輯 (Edit)** 連結 (如上圖所示)，使用者即可編輯**儲存格設定 (Cell Settings)** 區段。(請參閱下圖)。



備註　510 LTE 數據機資訊診斷測試：在 3.4 版中，如果已設定 Edge 510 LTE 裝置，則可以使用「LTE 數據機資訊」診斷測試。LTE 數據機資訊診斷測試將會擷取診斷資訊，例如訊號強度、連線資訊等。如需如何執行診斷測試的相關資訊，請參閱標題為遠端診斷一節

子介面和次要 IP

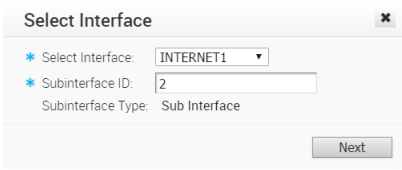


新增子介面

將子介面新增至路由介面時，子介面會取得提供給父系介面的組態選項子集。

1 按一下**新增子介面 (Add Sub Interface)** 按鈕。

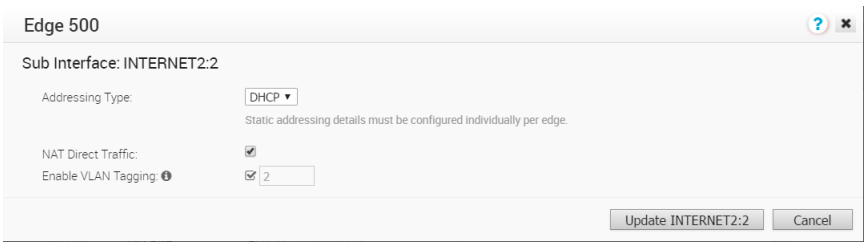
2 從下拉式功能表中選取介面，然後選取文字方塊中的**子介面識別碼 (Sub Interface ID)**，如下方的**選取介面 (Select Interface)** 對話方塊所示。



3 按**下一步 (Next)**。

4 在**子介面 (Sub Interface)** 對話方塊中，選擇您的定址類型 (DHCP 或**靜態 (Static)**)。

a 如果您選擇定址類型 DHCP，則依預設會選取**啟用 VLAN 標記 (Enable VLAN Tagging)** 核取方塊，且在先前的對話方塊中選擇的子介面識別碼會顯示在文字方塊中。



b 如果您選擇定址類型**靜態 (Static)**，您可以選擇藉由選取**啟用 VLAN 標記 (Enable VLAN Tagging)** 核取方塊來啟用 VLAN。您在先前的對話方塊中選擇的子介面識別碼會顯示在文字方塊中。

5 如有必要，請勾選 **NAT 直接流量 (NAT Direct Traffic)** 核取方塊。

6 按一下**更新 (Update)** 按鈕。

介面 (Interface) 資料行會重新整理，並顯示新建立的子介面。

新增次要 IP 位址

1 按一下**新增次要 IP (Add Secondary IP)** 按鈕。

2 從下拉式功能表中選取介面，然後選取文字方塊中的**子介面識別碼 (Sub Interface ID)**，如下方的**選取介面 (Select Interface)** 對話方塊所示。請注意，子介面類型為次要 IP。

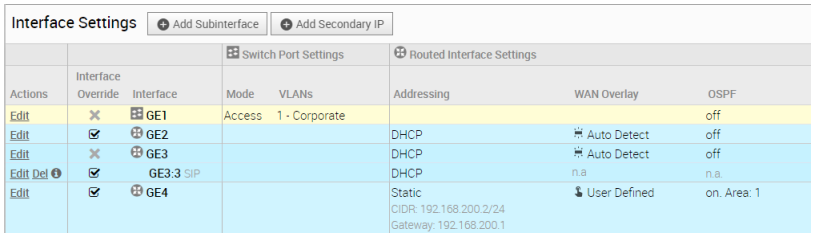
3 按**下一步 (Next)**。

4 在**次要 IP (Secondary IP)** 對話方塊中，選擇您的定址類型 (DHCP 或**靜態 (Static)**)。

5 在**次要 IP (Secondary IP)** 對話方塊中，選擇您的定址類型 (DHCP 或**靜態 (Static)**)。

6 按一下**更新 (Update)** 按鈕。

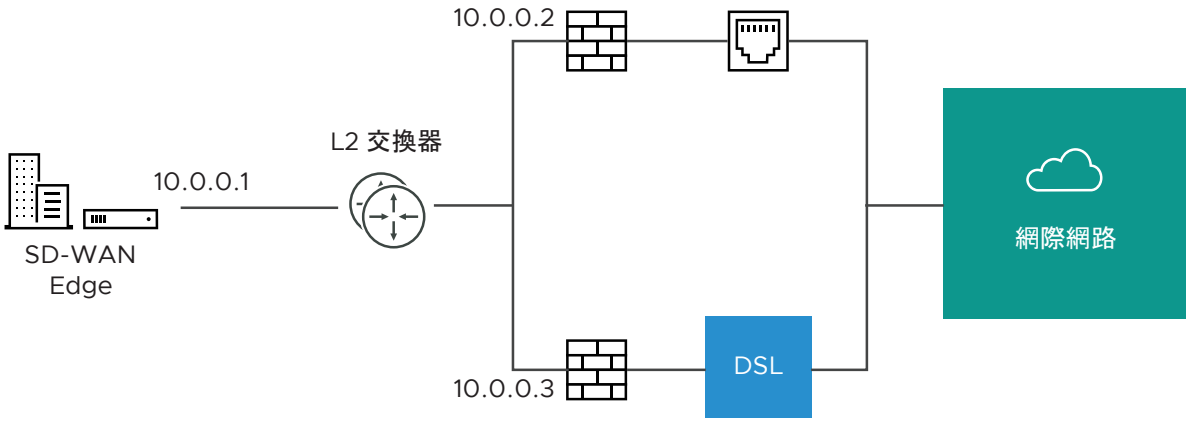
介面 (Interface) 資料行會重新整理，並顯示新建立的次要 IP (請參閱下方的**介面設定 (Interface Settings)** 影像)。



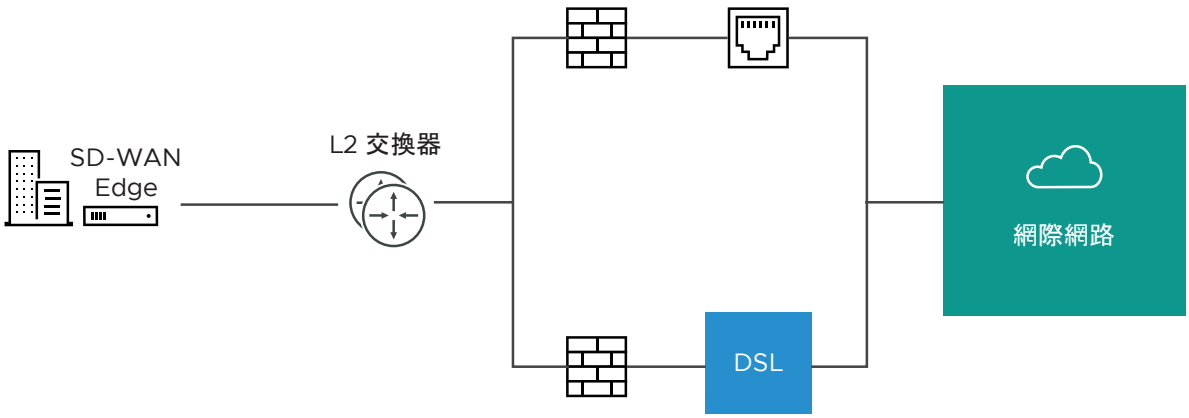
使用者定義的 WAN 覆疊使用案例

在此會先列出可運用此組態的案例，然後列出組態本身的規格。

1 **使用案例 1：兩個 WAN 連結連線至 L2 交換器** - 假設有一個傳統資料中心拓撲，其中的 SD-WAN Edge 連線至 DMZ 中的 L2 交換器，而該交換器連線至多個防火牆，且每個防火牆分別連線至不同的上游 WAN 連結。



在此拓撲中，VMware 介面可能已將 FW1 設定為下一個躍點。不過，若要使用 DSL 連結，則必須為其佈建替代的下一個躍點以將封包轉送至該處，因為 FW1 無法連線至 DSL。定義 DSL 連結時，使用者必須將自訂的下一個躍點 IP 位址設定為 FW2 的 IP 位址，以確保封包可以連線至 DSL 數據機。此外，使用者必須為此 WAN 連結設定自訂來源 IP 位址，以允許 Edge 識別傳回介面。最終組態會如下圖所示：

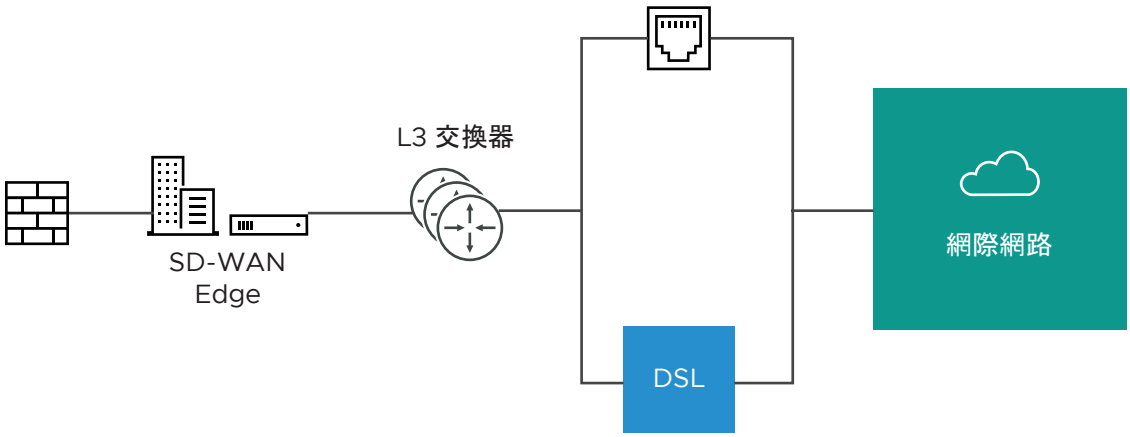


下一段說明如何定義最終組態。

- 為介面定義 IP 位址 10.0.0.1 和下一個躍點 10.0.0.2。由於有多個 WAN 連結連結至介面，因此連結會設定為「使用者定義」。
- 定義纜線連結，並繼承 IP 位址 10.0.0.1 和下一個躍點 10.0.0.2。不需要進行變更。需要將封包傳送至纜線連結時，封包會從來源 10.0.0.1 轉送至針對 10.0.0.2 回應 ARP 的裝置 (FW1)。傳回封包的目的地為 10.0.0.1，並識別為已到達纜線連結。

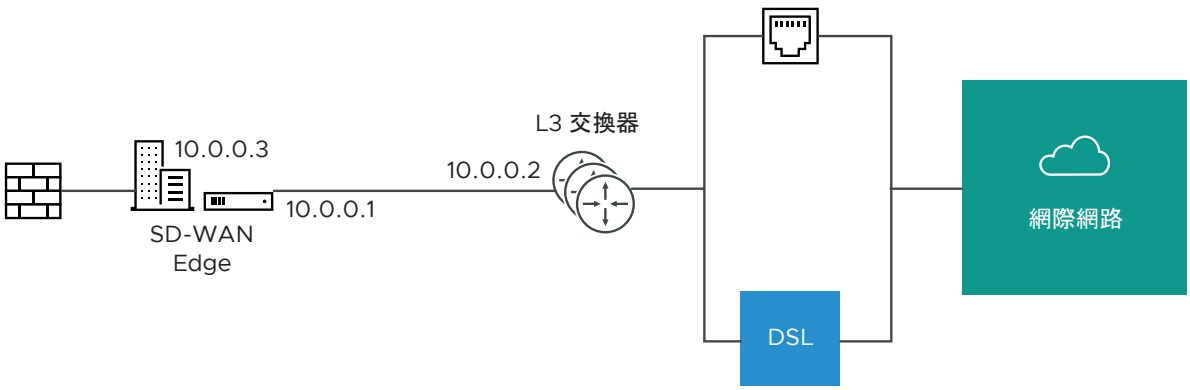
- 定義 DSL 連結，且由於這是第二個 WAN 連結，SD-WAN Orchestrator 會將 IP 位址和下一個躍點標示為必要的組態項目。使用者會指定自訂虛擬 IP (例如 10.0.0.4) 作為來源 IP，並將下一個躍點指定為 10.0.0.3。需要將封包傳送至 DSL 連結時，封包會從來源 10.0.0.4 轉送至針對 10.0.0.3 回應 ARP 的裝置 (FW2)。傳回封包的目的地為 10.0.0.4，並識別為已到達 DSL 連結。

2 **案例 2：兩個 WAN 連結連線至 L3 交換器/路由器：**或者，上游裝置可以是 L3 交換器或路由器。在此情況下，兩個 WAN 連結的下一個躍點裝置是相同的 (交換器)，而非上一個範例中的不同裝置 (防火牆)。此方式通常用於防火牆位於 SD-WAN Edge 的 LAN 端時。



在此拓撲中，將使用以原則為基礎的路由將封包導向至適當的 WAN 連結。此操控可由 IP 位址或 VLAN 標籤執行，因此我們同時支援這兩個選項。

依 IP 操控：如果 L3 裝置能夠依來源 IP 位址進行以原則為基礎的路由，則兩個裝置可以位於相同的 VLAN 上。在此情況下，所需的組態只有用來區分裝置的自訂來源 IP。

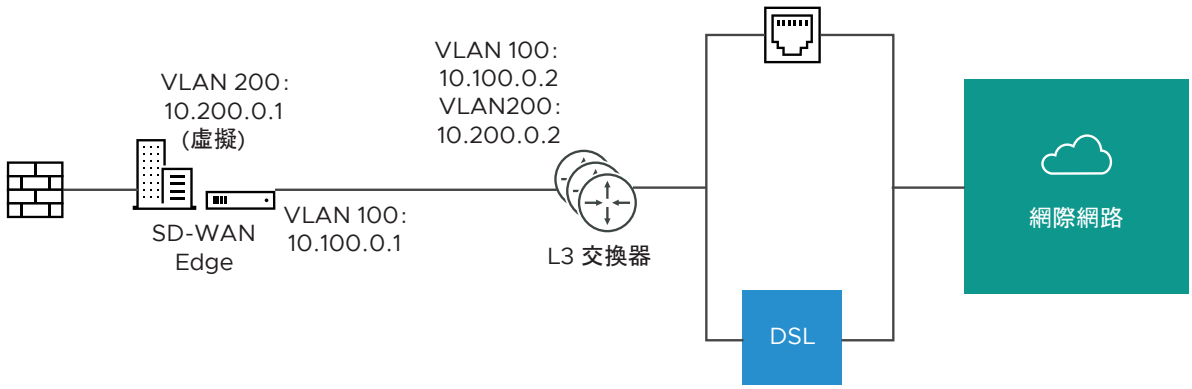


下一段說明如何定義最終組態。

- 為介面定義 IP 位址 10.0.0.1 和下一個躍點 10.0.0.2。由於有多個 WAN 連結連結至介面，因此連結會設定為「使用者定義」。
- 定義纜線連結，並繼承 IP 位址 10.0.0.1 和下一個躍點 10.0.0.2。不需要進行變更。需要將封包傳送至纜線連結時，封包會從來源 10.0.0.1 轉送至針對 10.0.0.2 回應 ARP 的裝置 (L3 交換器)。傳回封包的目的地為 10.0.0.1，並識別為已到達纜線連結。

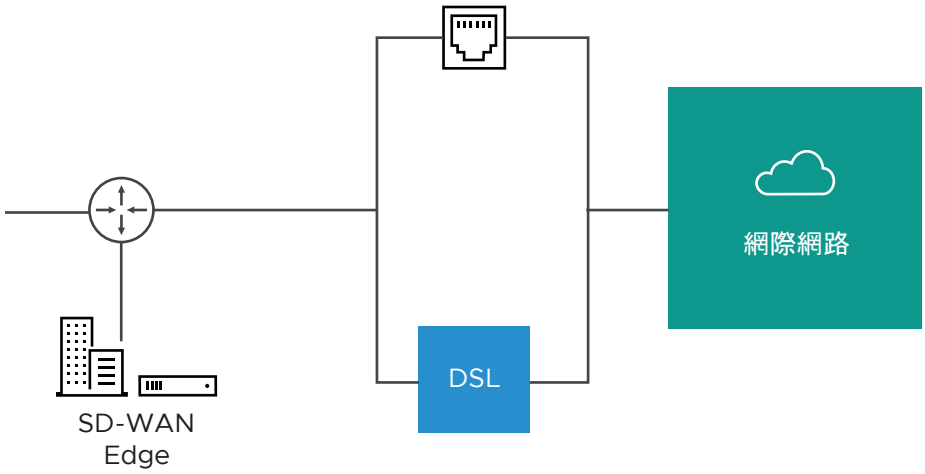
- 定義 DSL 連結，且由於這是第二個 WAN 連結，SD-WAN Orchestrator 會將 IP 位址和下一個躍點標示為必要的組態項目。使用者會指定自訂虛擬 IP (例如 10.0.0.3) 作為來源 IP，並將下一個躍點同樣指定為 10.0.0.2。需要將封包傳送至 DSL 連結時，封包會從來源 10.0.0.3 轉送至針對 10.0.0.2 回應 ARP 的裝置 (L3 交換器)。傳回封包的目的地為 10.0.0.3，並識別為已到達 DSL 連結。

依 VLAN 操控：如果 L3 裝置無法進行來源路由，或使用者基於其他原因選擇將不同的 VLAN 指派給纜線和 DSL 連結，則必須進行此設定。



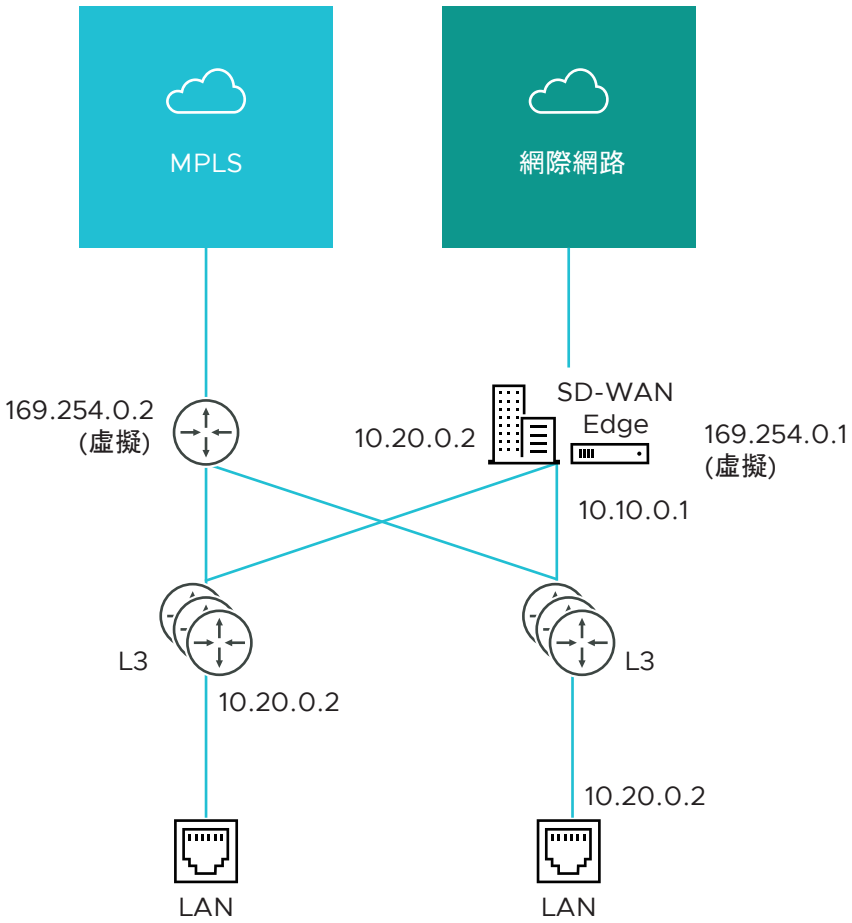
- 為介面定義 VLAN 100 上的 IP 位址 10.100.0.1 和下一個躍點 10.100.0.2。由於有多個 WAN 連結連結至介面，因此連結會設定為「使用者定義」。
- 定義纜線連結，並繼承 VLAN 100 以及 IP 位址 10.100.0.1 和下一個躍點 10.100.0.2。不需要進行變更。需要將封包傳送至纜線連結時，標記為 VLAN 100 的封包會從來源 10.100.0.1 轉送至針對 VLAN 100 上 10.100.0.2 回應 ARP 的裝置 (L3 交換器)。傳回封包的目的地為 10.100.0.1/VLAN 100，並識別為已到達纜線連結。
- 定義 DSL 連結，且由於這是第二個 WAN 連結，SD-WAN Orchestrator 會將 IP 位址和下一個躍點標示為必要的組態項目。使用者會指定自訂 VLAN 識別碼 (200) 和虛擬 IP (例如 10.200.0.1) 作為來源 IP，並將下一個躍點指定為 10.200.0.2。需要將封包傳送至 DSL 連結時，標記為 VLAN 200 的封包會從來源 10.200.0.1 轉送至針對 VLAN 200 上 10.200.0.2 回應 ARP 的裝置 (L3 交換器)。傳回封包的目的地為 10.200.0.1/VLAN 200，並識別為已到達 DSL 連結。

3 **案例 3：單臂部署**：單臂部署最終與其他 L3 部署非常類似。



同樣地，SD-WAN Edge 會讓兩個 WAN 連結共用相同的下一個躍點。您可以完成以原則為基礎的路由，以確保流量會依照上述定義轉送至適當的目的地。或者，VMware 中的 WAN 連結物件的來源 IP 和 VLAN 可以與纜線和 DSL 連結的 VLAN 相同，以自動進行路由。

4 **案例 4：透過多個介面連線至一個 WAN 連結**：請考量可透過兩個替代路徑連線至 MPLS 的傳統金級站台拓撲。在此情況下，我們必須定義無論使用哪個介面進行通訊都可共用的自訂來源 IP 位址和下一個躍點。



- 為 GE1 定義 IP 位址 10.10.0.1 和下一個躍點 10.10.0.2。
- 為 GE2 定義 IP 位址 10.20.0.1 和下一個躍點 10.20.0.2。
- 定義 MPLS，並將其設定為可透過任一介面進行連線。這會使來源 IP 和下一個躍點 IP 位址成為無預設值的必要項目。
- 定義無論使用哪個介面皆可用於通訊的來源 IP 和目的地。需要將封包傳送至 MPLS 連結時，標記為已設定 VLAN 的封包會從來源 169.254.0.1 轉送至針對已設定 VLAN 上 169.254.0.2 回應 ARP 的裝置 (CE 路由器)。傳回封包的目的地為 169.254.0.1，並識別為已到達 MPLS 連結。

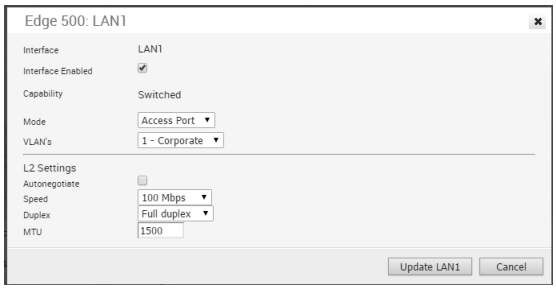
備註 若未啟用 OSPF 或 BGP ，您可能必須在兩個交換器上設定相同的傳送 VLAN，以啟用此虛擬 IP 的連線。

介面組態

按一下**編輯 (Edit)** 連結會顯示一個對話方塊，供您更新特定介面的設定。以下幾節將簡短說明針對 Edge 型號和介面類型顯示的各種對話方塊。

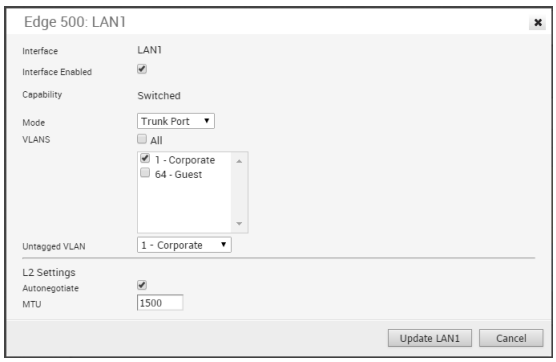
Edge 500 LAN 存取

以下說明設定為存取連接埠的 Edge 500 LAN 介面的參數。針對連接埠您可以選擇 VLAN，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。



Edge 500 LAN 主幹

以下說明設定為主幹連接埠的 Edge 500 LAN 介面的參數。針對連接埠您可以選擇 VLAN，以及選擇如何處理未標記的 VLAN 資料 (路由至特定 VLAN 或捨棄)，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。

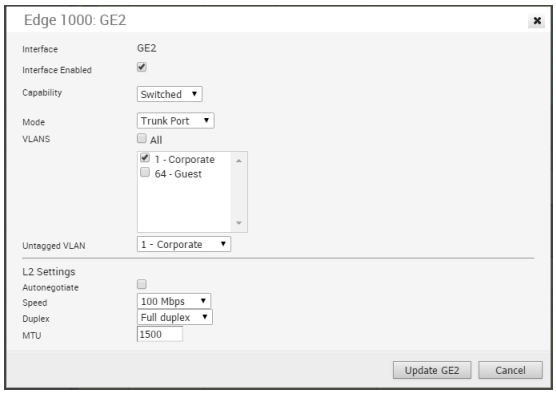


Edge 1000 LAN 存取

以下說明設定為已交換存取連接埠之 Edge 1000 LAN 介面的參數。針對連接埠您可以選擇 VLAN，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。

Edge 1000 LAN 主幹

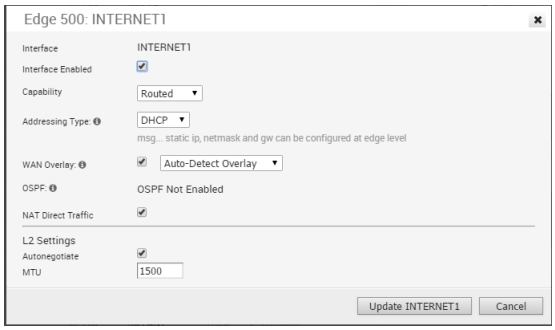
以下說明設定為主幹連接埠的 Edge 1000 LAN 介面的參數。針對連接埠您可以選擇 VLAN，以及選擇如何處理未標記的 VLAN 資料 (路由至特定 VLAN 或捨棄)，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。



Edge 500 WAN

以下說明將 [功能 (Capability)] 設為 [路由 (Routed)] 的 Edge 500 WAN 介面的參數。您可以選擇 [定址類型 (Addressing Type)] (DHCP、PPPoE 或靜態)、[WAN 覆疊 (WAN Overlay)] (自動偵測或使用者定義)、啟用 OSPF、啟用 NAT 直接流量，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。

備註 連接埠也可以設定為已交換介面。



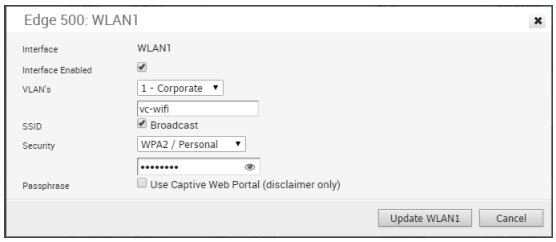
Edge 1000 WAN

以下說明將 [功能 (Capability)] 設為**路由 (Routed)** 的 Edge 1000 WAN 介面的參數。您可以選擇 [定址類型 (Addressing Type)] (DHCP、PPPoE 或靜態)、[WAN 覆疊 (WAN Overlay)] (自動偵測或使用者定義)、啟用 OSPF、啟用 NAT 直接流量，並選取 [L2 設定 (L2 Settings)] 以設定 [自動交涉 (Autonegotiate)] (依預設已選取)、[速度 (Speed)]、[雙工類型 (Duplex type)] 和 MTU 大小 (預設值為 1500)。

備註 連接埠也可以設定為已交換介面。

Edge 500 WLAN

一開始會為 SD-WAN Edge 500 定義兩個 Wi-Fi 網路；一個作為公司網路，另一個作為已初始停用的客體網路。您可以定義其他無線網路，並使其分別具有特定的 VLAN、SSID 和安全性組態。



Wi-Fi 連線的安全性

Wi-Fi 連線的安全性可以是下列三種類型之一：

類型	說明
開放 (Open)	不強制執行安全性。
WPA2/個人 (WPA2 / Personal)	使用密碼來驗證使用者。
WPA2/企業 (WPA2 / Enterprise)	使用 Radius 伺服器來驗證使用者。在此情況下，必須在 [網路服務 (Network Services)] 中設定 Radius 伺服器，且必須在**裝置 (Device)** 頁面的**設定檔驗證設定 (Profile Authentication Settings)** 中選取 Radius 伺服器。您也可以在 **Edge 裝置 (Edge Device)** 頁面上覆寫安全性的預設設定。

設定介面設定

您可以設定每個 Edge 型號的介面設定。Edge 上的各個介面可以是交換器連接埠 (LAN) 或路由 (WAN) 介面。

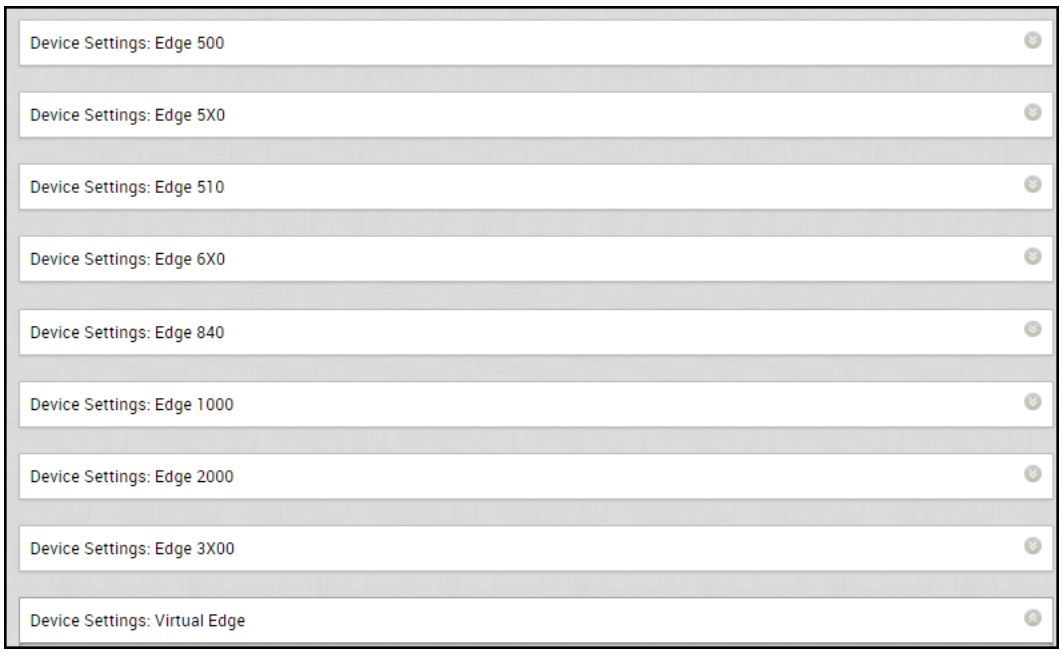
介面設定選項會根據 Edge 型號而有所不同。如需關於不同 Edge 型號和部署的詳細資訊，請參閱設定裝置設定。

程序

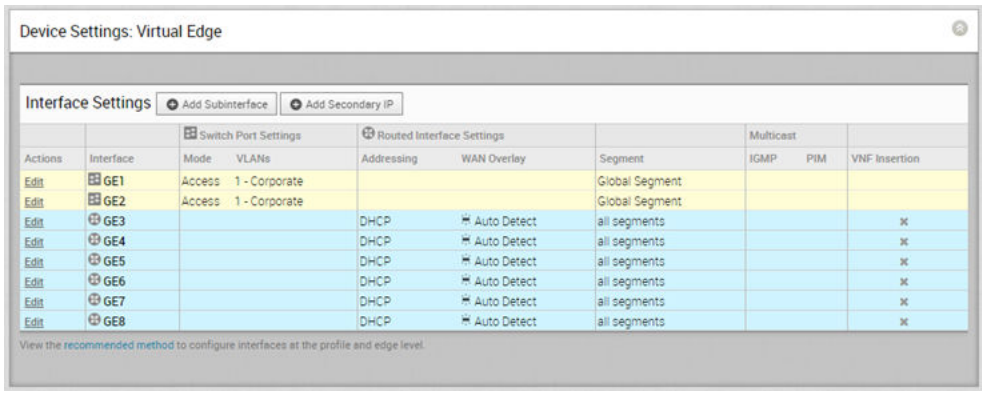
1 在企業入口網站中，按一下**設定 (Configure) > 設定檔 (Profiles)**。

2 按一下設定檔旁的裝置圖示，或按一下設定檔的連結，然後按一下**裝置 (Device)** 索引標籤。

3 向下捲動至**裝置設定 (Device Settings)** 區段，此處會顯示企業中的現有 Edge 型號。



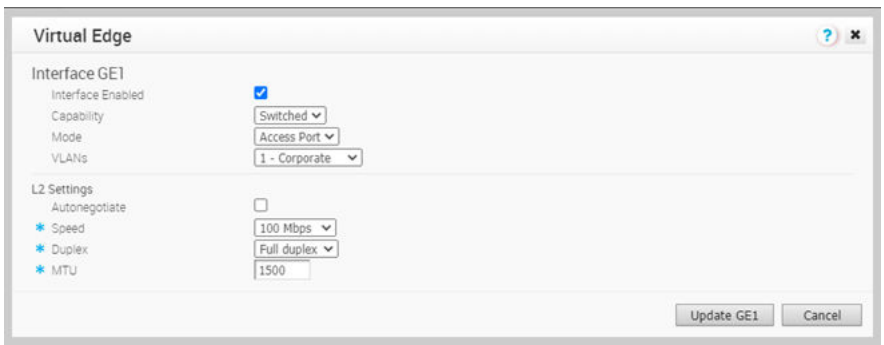
4 按一下 Edge 型號旁的向下箭頭，以檢視 Edge 的**介面設定 (Interface Settings)**。



介面設定 (Interface Settings) 區段會顯示所選 Edge 型號中可用的現有介面。

5 按一下介面的**編輯 (Edit)** 選項，以檢視和修改設定。

6 下圖顯示介面的交換器連接埠設定。

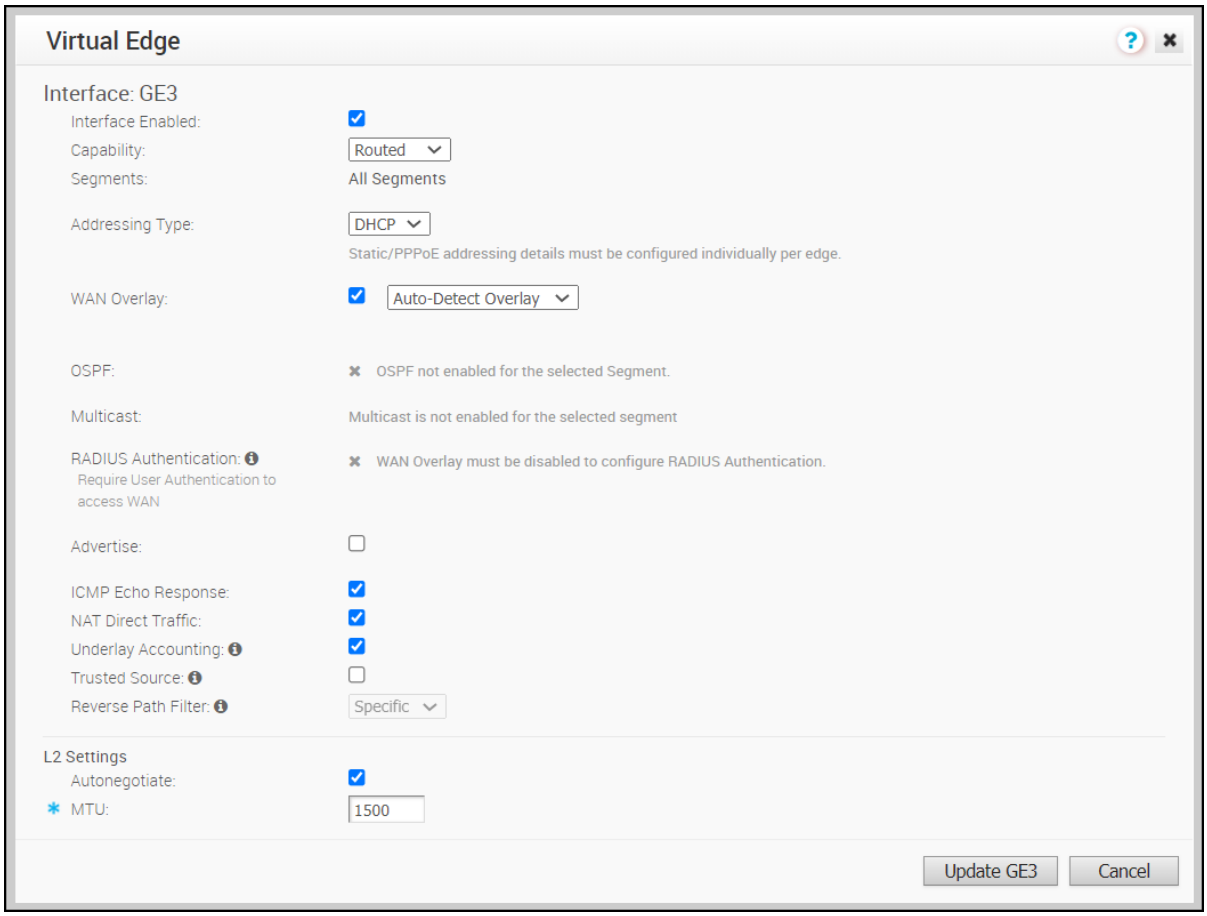


您可以修改現有設定，如下所示：

選項	說明
已啟用介面 (Interface Enabled)	此選項依預設為啟用。如有需要，您可以停用介面。停用時，將無法使用介面進行任何通訊。
功能 (Capability)	對於 [交換器連接埠 (Switch Port)]，依預設會選取**已交換 (Switched)** 選項。您可以從下拉式清單中選取**路由式 (Routed)** 選項，以選擇將連接埠轉換為路由介面。
模式 (Mode)	選取存取或主幹連接埠作為連接埠的模式。
VLAN	針對存取連接埠，請從下拉式清單中選取現有的 VLAN。 針對主幹連接埠，您可以選取多個 VLAN，然後選取未標記的 VLAN。
L2 設定	
自動交涉 (Autonegotiate)	此選項依預設為啟用。啟用時，自動交涉可讓連接埠與連結另一端的裝置進行通訊，以判斷連線的最佳雙工模式和速度。
速度 (Speed)	只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取連接埠與其他連結通訊時所需的速度。依預設會選取 100 Mbps。
雙工 (Duplex)	只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取全雙工或半雙工作為連線模式。依預設會選取全雙工。
MTU	在所有交換器介面上接收和傳送之框架的預設 MTU 大小為 1500 個位元組。您可以變更介面的 MTU 大小。

按一下**更新 (Update)** 以儲存設定。

7 下圖顯示路由介面設定。



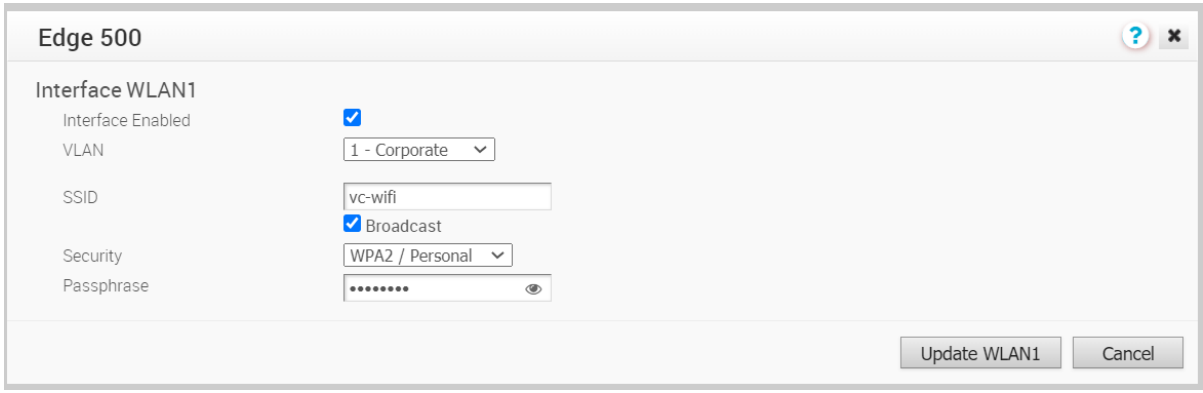
您可以修改現有設定，如下所示：

選項	說明
已啟用介面 (Interface Enabled)	此選項依預設為啟用。如有需要，您可以停用介面。停用時，將無法使用介面進行任何通訊。
功能 (Capability)	對於 [路由介面 (Routed Interface)]，依預設會選取**路由式 (Routed)** 選項。您可以從下拉式清單中選取**已交換 (Switched)** 選項，以選擇將介面轉換為交換器連接埠。
區段 (Segments)	依預設會將組態設定套用至所有區段。
定址類型 (Addressing Type)	依預設會選取動態指派 IP 位址的 DHCP。如果您選取靜態或 PPPoE，則應為每個 Edge 設定定址詳細資料。
WAN 覆疊 (WAN Overlay)	依預設會使用自動偵測覆疊啟用此選項。您可以選擇使用者定義的覆疊，並設定覆疊設定。如需詳細資訊，請參閱設定 Edge WAN 覆疊設定。
OSPF	只有在已為設定檔設定 OSPF 時，才會啟用此選項。選取核取方塊，然後從下拉式清單中選擇 OSPF。按一下**切換進階 OSPF 設定 (toggle advance ospf settings)**，以設定所選 OSPF 的介面設定。如需 OSPF 設定的詳細資訊，請參閱啟用 OSPF。

選項	說明
VNF 插入 (VNF Insertion)	您必須停用 WAN 覆疊並啟用信任的來源，才能允許 VNF 插入。當您將 VNF 插入第 3 層介面或子介面時，系統會將來自第 3 層介面或子介面的流量重新導向至 VNF。
多點傳播 (Multicast)	只有在已為設定檔設定多點傳播設定時，才會啟用此選項。您可以為選取的介面設定多點傳播設定。如需詳細資訊，請參閱在介面層級設定多點傳播設定。
RADIUS 驗證 (RADIUS Authentication)	您必須停用 WAN 覆疊，才能設定 RADIUS 驗證。選取此核取方塊可在介面上啟用 RADIUS 驗證，並新增不應轉送至 RADIUS 進行重新驗證的 MAC 位址。如需詳細資訊，請參閱在路由介面上啟用 RADIUS 。
通告 (Advertise)	選取將介面通告至網路中其他分支的核取方塊。
ICMP 回應回覆 (ICMP Echo Response)	選取讓介面能夠回覆 ICMP 回應訊息的核取方塊。基於安全考量，您可以為介面停用此選項。
NAT 直接流量 (NAT Direct Traffic)	選取此核取方塊，可將 NAT 套用至從介面傳送的網路流量。
底層計量 (Underlay Accounting)	此選項依預設為啟用。如果在介面上定義了私人 WAN 覆疊，則周遊介面的所有底層流量都將根據 WAN 連結的測量速率計數，以防止過度訂閱。如果您不想要此行為 (例如，在使用單臂部署時)，請停用此選項。
信任的來源 (Trusted Source)	選取此核取方塊，可將介面設定為信任的來源。
反向路徑轉送 (Reverse Path Forwarding)	只有在已啟用信任的來源時，才能選擇反向路徑轉送的選項。只有在可於相同的介面上轉送傳回流量時，此選項才會允許介面上的流量。這有助於防止企業網路上來自不明來源的流量 (惡意流量)。如果傳入來源不明，則會在入口捨棄封包，而不會建立流量。從下拉式清單中選取下列其中一個選項： ■ **已停用 (Disabled)** - 即使路由表中沒有相符的路由仍允許傳入流量。 ■ **特定 (Specific)** – 依預設會選取此選項。傳入流量應符合傳入介面上的特定傳回路由。如果找不到特定的相符項，則會捨棄傳入的封包。這是設定了公用覆疊和 NAT 的介面上常用的模式。 ■ **寬鬆 (Loose)** - 傳入流量應符合路由表中的任何路由 (已連線/靜態/已路由)。這會允許非對稱路由，通常用於未設定下一個躍點的介面。
VLAN	輸入介面的 VLAN 識別碼，以支援透過連接埠的 VLAN 標記。如果您選擇 DHCP 作為**定址類型 (Addressing Type)**，則無法使用此選項。
L2 設定	
自動交涉 (Autonegotiate)	此選項依預設為啟用。啟用時，自動交涉可讓連接埠與連結另一端的裝置進行通訊，以判斷連線的最佳雙工模式和速度。
速度 (Speed)	只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取連接埠與其他連結通訊時所需的速度。依預設會選取 100 Mbps。

選項	說明
雙工 (Duplex)	只有在停用**自動交涉 (Autonegotiate)** 時，才能使用此選項。選取全雙工或半雙工作為連線模式。依預設會選取全雙工。
MTU	在所有路由介面上接收和傳送之框架的預設 MTU 大小為 1500 個位元組。您可以變更介面的 MTU 大小。
SFP 設定 (SFP Settings) – 此選項僅適用於支援 SFP 連接埠的 Edge 型號。	
SFP 模組 (SFP Module)	依預設會選取 [標準 (Standard)]。您可以選取 DSL 作為模組，以將 SFP 連接埠用於頻寬較高的服務。
DSL 設定 (DSL Settings) – 設定數位用戶線路 (DSL) 設定的選項，在您選取 SFP 模組作為 **DSL** 時可供使用。	
模式 (Mode)	從下列選項中選擇 DSL 模式： ■ **VDSL2** - 依預設會選取此選項。高位元率數位用戶線路 (VDSL) 技術可提供更快速的資料傳輸。VDSL 線路可將服務提供者網路與客戶站台連線，以透過單一連線提供高頻寬應用程式。 當您選擇 VDSL2 時，請從下拉式清單中選取**設定檔 (Profile)**。設定檔是預先設定的 VDSL2 設定清單。支援的設定檔如下：17a 和 30a。 ■ **ADSL2/2 +** - 非對稱數位用戶線路 (ADSL) 技術是 xDSL 系列的一部分，用來傳輸高頻寬資料。ADSL2 可改善資料速率，並達到 ADSL 數據機的效能、診斷、待命模式和互通性。ADSL2+ 會加倍可能的下游資料頻寬。 如果您選擇 ADSL2/2+，請設定下列設定： ■ **PVC** - 永久虛擬線路 (PVC) 是網路中軟體定義的邏輯連線，例如框架轉送網路。從下拉式清單中選擇 PVC。範圍從 0 到 7。 ■ **VPI** - 虛擬路徑識別碼 (VPI) 可用來識別路由資訊封包的路徑。輸入 VPI 號碼，範圍介於 0 到 255 之間。 ■ **VCI** - 虛擬通道識別碼 (VCI) 會定義用來傳送資訊封包的固定通道。輸入 VCI 號碼，範圍介於 35 到 65535 之間。 ■ **PVC VLAN** - 將 VLAN 設定為透過 ATM 模組上的 PVC 執行。輸入 VLAN 識別碼，範圍介於 1 到 4094 之間。

8 部分 Edge 型號支援無線 LAN。下圖顯示 WLAN 介面設定。



您可以修改這些設定，如下所示：

選項	說明
已啟用介面 (Interface Enabled)	此選項依預設為啟用。如有需要，您可以停用介面。停用時，將無法使用介面進行任何通訊。
VLAN	選擇介面所將使用的 VLAN。
SSID	輸入無線網路名稱。 選取**廣播 (Broadcast)** 核取方塊，以將 SSID 名稱廣播至周圍的裝置。
安全性 (Security)	從下拉式清單中選取 Wi-Fi 連線的安全性類型。可用選項如下： ■ **開放 (Open)** - 不強制執行安全性。 ■ **WPA2/個人 (WPA2 / Personal)** - 驗證需要密碼。請在**複雜密碼 (Passphrase)** 欄位中輸入密碼。 ■ **WPA2/企業 (WPA2 / Enterprise)** - 使用 RADIUS 伺服器進行驗證。您應已設定 RADIUS 伺服器，並且已為設定檔和 Edge 選取該伺服器。 若要設定 RADIUS 伺服器，請參閱設定驗證服務。 若要選取設定檔的 RADIUS 伺服器，請參閱設定驗證設定。

後續步驟

當您為設定檔設定了介面設定時，這些設定將會自動套用至與設定檔相關聯的 Edge。如有需要，您可以覆寫特定 Edge 的組態，如下所示：

1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 按一下 Edge 旁的裝置圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 索引標籤中，向下捲動至**介面設定 (Interface Settings)** 區段，此處會顯示所選 Edge 中可用的介面。

4 按一下介面的**編輯 (Edit)** 選項，以檢視和修改設定。

5 選取**覆寫介面 (Override Interface)** 核取方塊，以修改所選介面的組態設定。

設定 Wi-Fi 無線電設定

在設定檔層級上，您可以啟用/停用 Wi-Fi 無線電並設定無線電頻率的頻帶。

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

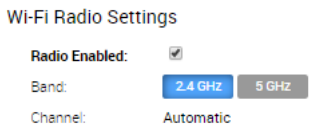
2 選取要設定 Wi-Fi 無線電設定的設定檔，然後按一下**裝置 (Device)** 資料行下的圖示。

所選設定檔的**裝置設定 (Device Settings)** 頁面隨即出現。

3 在 **Wi-Fi 無線電設定 (WI-FI Radio Settings)** 區域中，依預設會啟用**已啟用無線電 (Radio Enabled)** 核取方塊，且**通道 (Channel)** 會設定為**自動 (Automatic)**。

4 選取無線電頻帶。這可以是 **2.4 GHz** 或 **5 GHz**。

5 按一下**儲存變更 (Save Changes)**。



在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 Wi-Fi 無線電設定。如需詳細資訊，請參閱設定 Wi-Fi 無線電覆寫。

設定設定檔的 SNMP 設定

SNMP 是網路監控常用的通訊協定，而 MIB 是與 SNMP 相關聯以管理實體的資料庫。若要啟用 SNMP，請選取所需的 SNMP 版本，如下列步驟中所述。

開始之前：

- 若要下載 SD-WAN Edge MIB：請移至**遠端診斷 (Remote Diagnostics)** 畫面 (**測試和疑難排解 (Test & Troubleshooting)** > **遠端診斷 (Remote Diagnostics)**)，然後針對 SD-WAN Edge 執行 MIB。將結果複製並貼到本機電腦上。
- 在用戶端主機上安裝 VELOCLOUD-EDGE-MIB 所需的所有 MIB，包括 SNMPv2-SMI、SNMPv2-CONF、SNMPv2-TC、INET-ADDRESS-MIB、IF-MIB、UUID-TC-MIB 和 VELOCLOUD-MIB。上述所有的 MIB 皆可從 [遠端診斷 (Remote Diagnostics)] 頁面取得。

支援的 MIB

- SNMP MIB-2 系統
- SNMP MIB-2 介面
- VELOCLOUD-EDGE-MIB
- HOST-RESOURCES-MIB，來自 RFC 1514

在設定檔層級設定 SNMP 設定的程序：

1 從**遠端診斷 (Remote Diagnostics)** 取得 VELOCLOUD-EDGE-MIB。

2 安裝 VELOCLOUD-EDGE-MIB 所需的所有 MIB。請參閱「開始之前」以取得更多資訊。

3 從 SD-WAN Orchestrator，移至**設定 (Configure) > 設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 畫面隨即出現。

4 選取您要為其設定 SNMP 設定的設定檔，然後按一下 [裝置 (Device)] 資料行下的**裝置 (Device)** 圖示。

所選設定檔的**組態設定檔 (Configuration Profiles)** 畫面隨即出現。

5 向下捲動至 **SNMP 設定 (SNMP Settings)** 區域。您有兩個版本可供選擇：v2c 或 v3。

6 若要設定 SNMP v2c，請依照下列步驟操作：

a 勾選 **v2c** 核取方塊。

b 在**連接埠 (Port)** 文字方塊中輸入連接埠。預設設定為 161。

c 在**社群 (Community)** 文字方塊中輸入文字或數字序列，這將作為讓您存取 SNMP 代理程式的「密碼」。

d 針對允許的 IP：

- 勾選**任何 (Any)** 核取方塊，以允許任何 IP 存取 SNMP 代理程式。
- 若要限制對 SNMP 代理程式的存取，請取消選取**任何 (Any)** 核取方塊，然後輸入將可存取 SNMP 代理程式的 IP 位址。

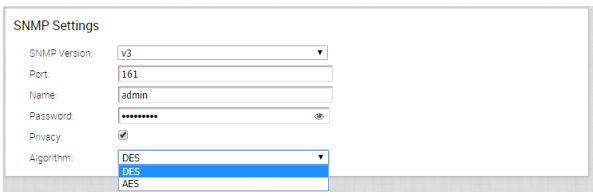
7 針對提供更高安全性支援的 SNMP v3 組態，請依照下列步驟操作：

a 在**連接埠 (Port)** 文字方塊中輸入連接埠。161 是預設設定。

b 在適當的文字方塊中輸入使用者名稱和密碼。

c 如果您要讓封包傳輸加密，請勾選**隱私權 (Privacy)** 核取方塊。

d 如果您已勾選**隱私權 (Privacy)** 核取方塊，請從 **演算法 (Algorithm)** 下拉式功能表中選擇 DES 或 AES。



8 設定防火牆設定。設定 SNMP 設定後，請移至防火牆設定 (**設定 (Configure) > 設定檔 (Profiles) > 防火牆 (Firewall)**)，以設定將啟用 SNMP 設定的防火牆設定。

備註 已啟用 DPDK 的介面支援 3.3.0 及更新版本的 SNMP 介面監控。

設定可見度模式

本節說明如何設定可見度模式。

關於可見度模式

即使依 MAC 位址進行追蹤是理想的方式 (提供全域唯一識別碼)，但當 L3 交換器位於用戶端與 Edge 之間時會缺乏可見度，因為 Edge 可得知交換器 MAC，但無法得知裝置 MAC。因此，可用的追蹤模式有兩種 (MAC 位址和目前的 IP 位址)。無法依 MAC 位址追蹤時，將會改用 IP 位址。

選擇可見度模式

若要選擇**可見度模式 (Visibility Mode)**，請移至**設定 (Configure) > 設定檔 (Profile) > 裝置 (Devices)** 索引標籤。選取下列其中一項：

- **依 MAC 位址的可見度 (Visibility by MAC address)**
- **依 IP 位址的可見度 (Visibility by IP address)**

使用可見度模式的注意事項

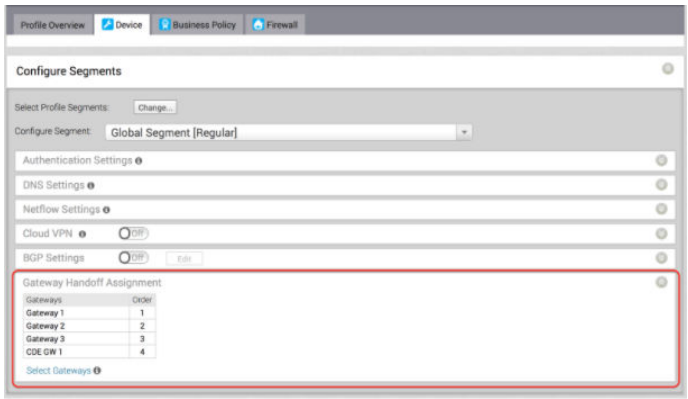
選擇可見度模式時，請留意下列事項：

- 如果選擇**依 MAC 位址的可見度 (Visibility by MAC address)**：
  - 用戶端會位於 L2 SW 後方
  - 將會顯示用戶端 MAC、IP 和主機名稱 (如果適用)
  - 將會根據 MAC 收集統計資料
- 如果選擇**依 IP 位址的可見度 (Visibility by IP address)**：
  - 用戶端會位於 L3 SW 後方
  - 將會顯示 SW MAC、用戶端 IP 和主機名稱 (如果適用)
  - 將會根據 IP 收集統計資料

指派合作夥伴閘道

若要讓客戶能夠使用合作夥伴閘道，操作員必須選取閘道的**啟用合作夥伴遞交 (Enable Partner Handoff)** 核取方塊，以啟用此功能。如果此功能可供您使用，您會在**設定 (Configure) > 設定檔 (Profiles) > 裝置 (Device)** 索引標籤畫面中看到**合作夥伴閘道指派 (Partner Gateway Assignment)** 區域。

備註 合作夥伴閘道指派功能已強化，也支援以區段為基礎的組態。您可以在設定檔層級上設定多個合作夥伴閘道，和/或在 Edge 層級上覆寫。



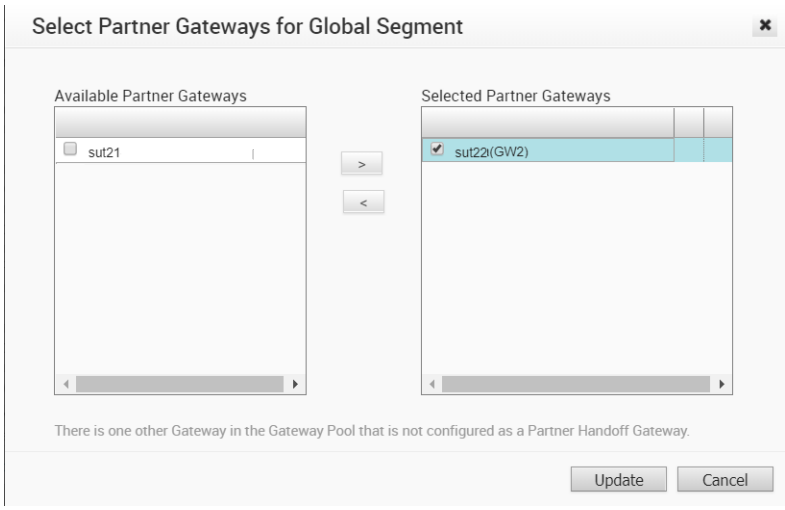
選取閘道

若要完成此區段，您必須啟用此功能。如需詳細資訊，請洽詢操作員。

如果**閘道遞交指派 (Gateway Handoff Assignment)** 區域中未列出任何閘道：

1 按一下**選取閘道 (Select Gateways)** 連結以選取合作夥伴閘道。

2 在**選取全域區段的合作夥伴閘道 (Select Partner Gateways for Global Segment)** 對話方塊中，從**可用的合作夥伴閘道 (Available Partner Gateway)** 區域中選取可用的合作夥伴閘道，然後將其移至**選取的合作夥伴閘道 (Selected Partner Gateway)** 區域 (使用適當的箭頭)。



請注意，只有設定為「合作夥伴遞交閘道」的閘道，才會顯示在**可用的合作夥伴閘道 (Available Partner Gateway)** 區域中。如果有其他閘道未設定為合作夥伴遞交閘道，則對話方塊中會出現下列訊息：**閘道集區中還有一個閘道未設定為合作夥伴遞交閘道 (There is one other Gateway in the Gateway Pool that is not configured as a Partner Handoff Gateway)**。

選取 CDE 閘道

在一般情況下，當 PCI 流量遞交至 PCI 網路，而閘道超出 PCI 範圍時，PCI 流量便會在客戶分支和資料中心之間傳遞。(操作員可取消選取 CDE 角色，將閘道設定為排除 PCI 區段)。

在閘道可遞交至 PCI 網路且位於 PCI 範圍內的特定情況下，操作員可為合作夥伴閘道啟用 CDE 角色，而這些閘道 (CDE 閘道) 將可供使用者在 PCI 區段 (CDE 類型) 中進行指派。

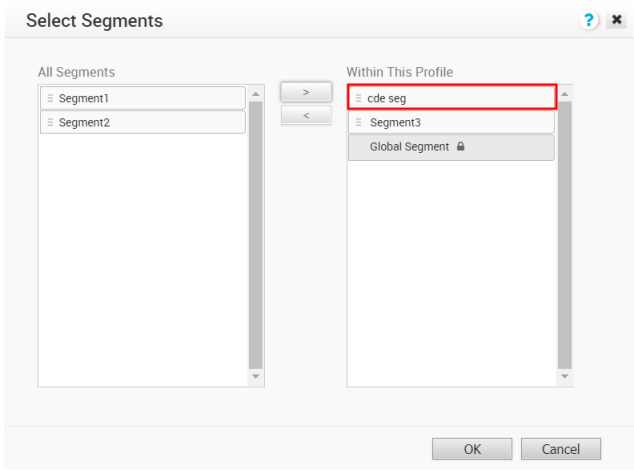
若要完成此區段，您必須啟用此功能。如需詳細資訊，請洽詢操作員。

指派 CDE 閘道

若要指派 CDE 閘道：

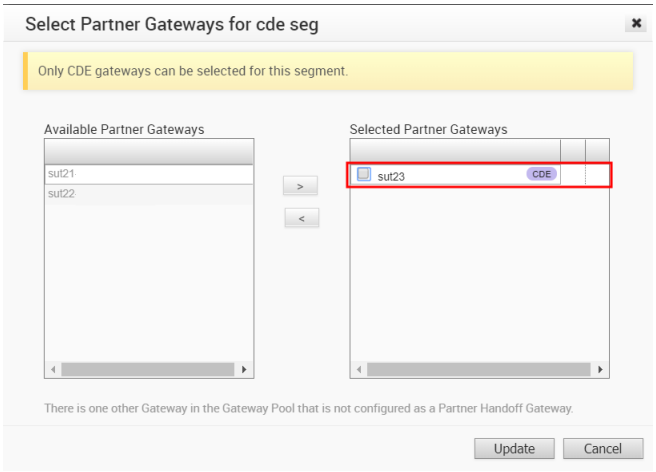
1 在**設定區段 (Configure Segments)** 視窗中，按一下**選取設定檔區段 (Select Profile Segments) 變更 (Change)** 按鈕。

2 在**選取區段 (Select Segments)** 對話方塊中，將可用的 CDE 區段從**可用的區段 (Available Segments)** 區域移至**在此設定檔中 (Within This Profile)** 區域 (使用適當的箭頭)。



3 在**閘道遞交指派 (Gateway Handoff Assignment)** 區域中，按一下**選取閘道 (Select Gateways)** 連結。

4 在**選取 CDE 區段的合作夥伴閘道 (Select Partner Gateways for cde seg)** 對話方塊中，從**可用的合作夥伴閘道 (Available Partner Gateway)** 區域中選取可用的 CDE 合作夥伴閘道，然後將其移至**選取的合作夥伴閘道 (Selected Partner Gateway)** 區域。



5 按一下**更新 (Update)** 按鈕。

閘道遞交指派 (Gateway Handoff Assignment) 區域會以選取的閘道重新整理。

備註 如**選取 CDE 區段的合作夥伴閘道 (Select Partner Gateways for cde seg)** 對話方塊中所示，您只能為區段選取 CDE 閘道。

指派合作夥伴閘道時的考量事項：

指派合作夥伴閘道時，請考量下列注意事項：

- 合作夥伴閘道可在設定檔或 Edge 層級上指派。
- 可將兩個以上的合作夥伴閘道指派給 Edge (最多 16 個)。
- 可就個別區段指派合作夥伴閘道。

備註 若未在**設定區段 (Configure Segments)** 視窗中看到**閘道遞交指派 (Gateway Handoff Assignment)** 區域，請連絡操作員以啟用此功能。

指派控制器

SD-WAN Gateway 可同時支援資料和控制平面。在 3.2 版中，VMware 導入了僅限控制器的功能 (控制器閘道指派)。

在多個使用案例中，SD-WAN Gateway 都必須僅以控制器的形式運作 (也就是移除資料平面功能)。此外，因為通常專用於封包處理的資源可能會改用於支援控制平面處理，如此將可讓閘道以不同的方式進行調整。例如，這可讓控制器所支援的並行通道數目比傳統閘道更多。請參閱下一節中的一般使用案例。

使用案例：經由不同合作夥伴閘道的動態分支到分支

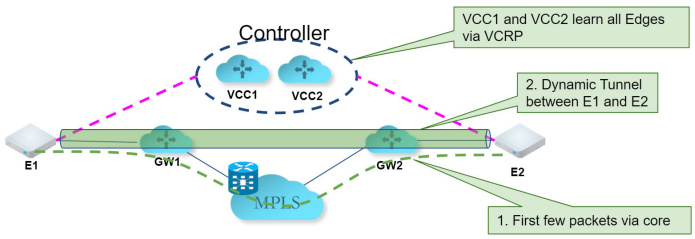
在此案例中，圖中所示的 Edge 1 (E1) 和 Edge 2 (E2) 屬於 Orchestrator 中的相同企業。但是，兩者連線至不同的合作夥伴閘道 (通常是因為位於不同區域)。因此，在 E1 與 E2 之間無法進行「動態分支到分支」，但藉由控制器的運用，就變得可行了。

初始流量

如下圖所示，當 E1 和 E2 嘗試直接通訊時，流量一開始會周遊私人網路，如同在舊版程式碼中一樣。同時，這些 Edge 也會通知控制器它們正在進行通訊，並要求直接連線。

動態通道

控制器會向 Edge 發出訊號，藉由將 E1 連線資訊提供給 E2 (反之亦然) 來建立動態通道。該流量在建立時會順暢地移至新的動態通道。



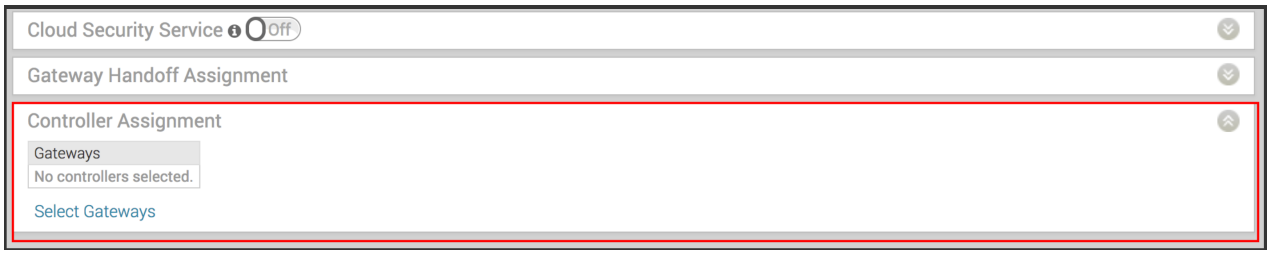
將閘道設定為控制器

若要讓客戶能夠使用合作夥伴閘道，操作員必須選取閘道的**啟用合作夥伴遞交 (Enable Partner Handoff)** 核取方塊，以啟用此功能。如果此功能可供您使用，您會在**設定 (Configure) > 設定檔 (Profiles) > 裝置 (Device)** 索引標籤畫面中看到**控制器指派 (Controller Assignment)** 區域。

備註 閘道集區中至少要有一個閘道應為「僅限控制器」閘道。

1 移至**設定 (Configure) > 設定檔 (Profiles) > 裝置 (Device)** 索引標籤。

2 向下捲動至**控制器指派 (Controller Assignment)** 區域。



3 在**控制器指派 (Controller Assignment)** 區域中，按一下**選取閘道 (Select Gateways)** 連結。

4 在**選取全域區段的控制器 (Select Controllers for Global Segment)** 對話方塊中，將控制器從**可用的 (Available)** 區域移至**選取的 (Selected)** 區域。

5 按一下**更新 (Update)**。

控制器指派 (Controller Assignment) 區域會重新整理。

設定設定檔商務原則

11

VMware 提供了增強的服務品質功能，名為商務原則。此功能可使用設定檔中的**商務原則 (Business Policy)** 索引標籤定義，或在 Edge 覆寫層級定義。

備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

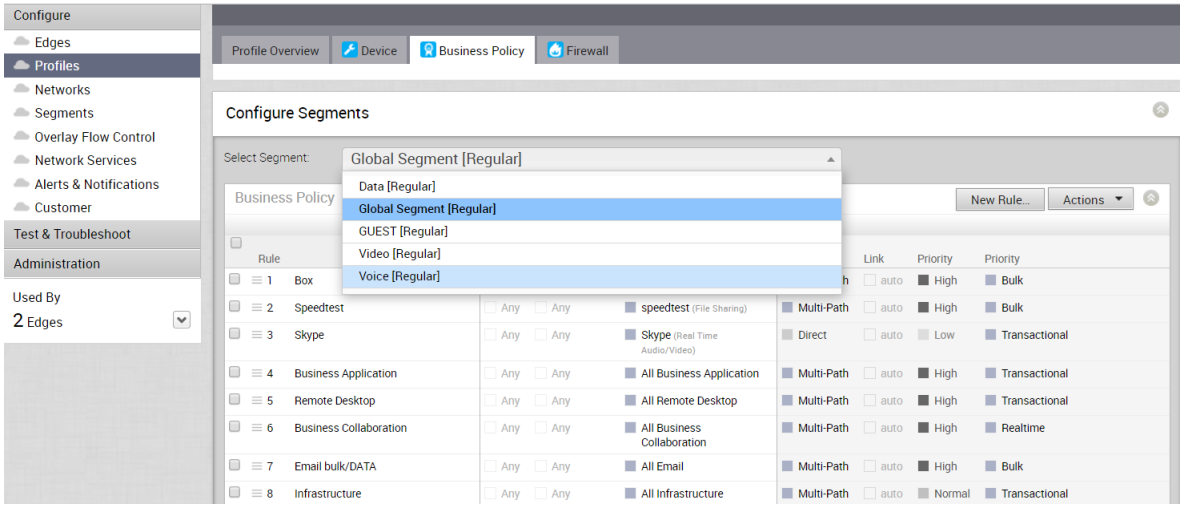
根據商務原則組態，VMware 會檢查正在使用的流量，並且識別應用程式行為、指定應用程式所需的商務服務目標 (高、中或低)，以及 Edge WAN 連結的情況。據此，商務原則可最佳化應用程式行為驅動佇列、頻寬使用量、連結操控的效能，以及減少網路錯誤。

下方的螢幕擷取畫面會顯示部分商務原則規則。您可以使用預先定義的多個規則，也可以自行新增規則以自訂網路作業。規則會依優先順序由高至低列出。網路流量的管理方式是先識別其特性，然後將這些特性與優先順序最高的規則進行比對。

如下圖所示，商務原則規則現在能夠感知區段。所有可用於設定的區段皆會在**設定區段 (Configure Segment)** 下拉式功能表中列出。

當您從**設定區段 (Configure Segment)** 下拉式功能表中選擇要設定的區段時，與該區段相關聯的設定和選項將會顯示在**設定區段 (Configure Segments)** 區域中。**全域區段 [一般] (Global Segment [Regular])** 是預設區段。

如需分割的詳細資訊，請參閱第 7 章 設定區段和第 10 章 設定設定檔裝置。



備註 您可以將已設定的規則在規則清單中向上或向下移動，以建立優先順序，方法是將游標暫留在規則左側的數值上方，然後將該規則上移或下移。 如果您將游標暫留在規則右側，則可以按一下規則旁邊的 **– (減號)** 以將其從清單中移除，或按一下 **+ (加號)** 以新增規則。

本章節討論下列主題：

建立商務原則規則

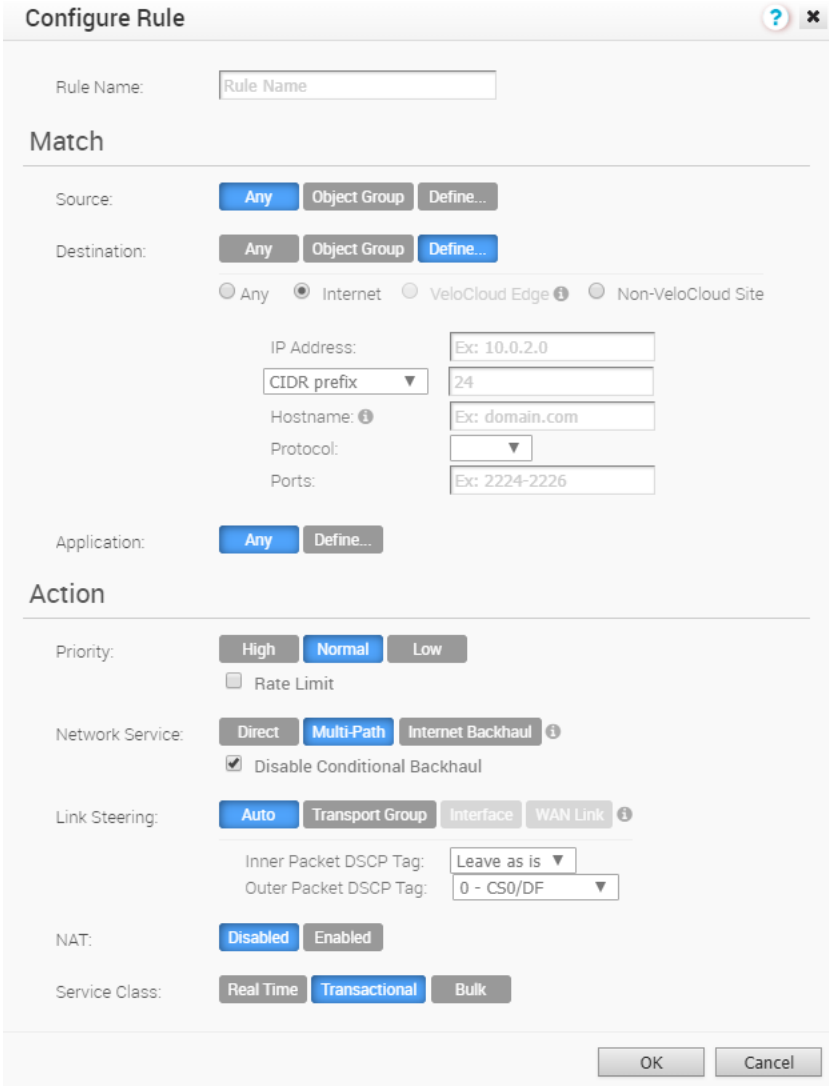
SD-WAN Orchestrator 可讓您在設定檔和 Edge 層級設定商務原則規則。所有層級的操作員、合作夥伴和管理員都可以建立商務原則。商務原則會比對參數，例如 IP 位址、連接埠、VLAN 識別碼、介面、網域名稱、通訊協定、作業系統、物件群組、應用程式和 DSCP 標籤。當資料封包符合相符條件時，會採取相關聯的一或多個動作。如果封包不符合任何參數，則會在封包上採取預設動作。

開始之前：瞭解裝置的 IP 位址，並瞭解設定萬用字元遮罩的影響。

若要建立商務原則：

1 從 SD-WAN Orchestrator 移至**設定 (Configure)** > **設定檔 (Profiles)** > **商務原則 (Business Policy)**。

2 在**商務原則 (Business Policy)** 區域中，按一下**新增規則 (New Rule)**。**設定規則 (Configure Rule)** 對話方塊隨即出現。



3 在**規則名稱 (Rule Name)** 方塊中，輸入規則的唯一名稱。

4 在**比對 (Match)** 區域下，設定流量的比對條件。您選擇的選項可能會變更對話方塊中的欄位：

設定	說明
來源 (Source)	允許指定來源流量的比對準則。請選取下列任一選項： ■ **任何 (Any)** - 依預設會比對所有來源流量。 ■ **物件群組 (Object Group)** - 可讓您選取要為來源比對的位址群組和連接埠群組的組合。如需詳細資訊，請參閱第 16 章 物件群組和使用物件群組設定商務原則。 **備註** 如果所選位址群組包含任何網域名稱，則會在與來源相符時忽略這些網域名稱。 ■ **定義 (Define)** - 可讓您為來自特定 VLAN、介面、IP 位址、連接埠或作業系統的來源流量定義比對準則。選取下列其中一個選項，依預設會選取**無 (None)**： ■ VLAN - 比對來自指定 VLAN (從下拉式功能表中選取) 的流量。 ■ 介面 (Interface) - 比對來自指定介面 (從下拉式功能表中選取) 的流量。 **備註** 如果無法選取介面，則介面會停用或不指派給此區段。 ■ IP 位址 (IP Address) - 比對來自指定 IP 位址的流量。除了 IP 位址，您還可以指定下列其中一個選項以比對來源流量： ■ CIDR 首碼 (CIDR prefix) - 如果您想要將網路定義為 CIDR 值 (例如：`172.10.0.0 /16`)，請選擇此選項。 ■ 子網路遮罩 (Subnet mask) - 如果您想要根據子網路遮罩定義網路 (例如 `172.10.0.0 255.255.0.0`)，請選擇此選項。 ■ 萬用字元遮罩 (Wildcard mask) - 如果您想要能夠將強制執行原則的範圍縮小到共用相符主機 IP 位址值的不同 IP 子網路間的一組裝置，請選擇此選項。萬用字元遮罩會根據反向的子網路遮罩比對 IP 或一組 IP 位址。遮罩的二進位值中若包含「0」，表示值是固定的，遮罩的二進位值中若包含「1」，則表示值是萬用字元 (可以是 1 或 0)。以 IP 位址為 172.0.0 的萬用字元遮罩 0.0.0.255 (二進位對等項目 = 00000000.00000000.00000000.11111111) 為例，前三個八位元數字是固定值，最後一個八位元數字是變數值。 ■ 連接埠 (Port) - 比對來自指定的來源連接埠或連接埠範圍的流量。 ■ 作業系統 (Operating System) - 比對來自指定作業系統 (從下拉式功能表中選取) 的流量。
目的地 (Destination)	允許指定目的地流量的比對準則。請選取下列任一選項： ■ **任何 (Any)** - 依預設會比對所有目的地流量。 ■ **物件群組 (Object Group)** - 可讓您選取要為目的地比對之位址群組和連接埠群組的組合。如需詳細資訊，請參閱第 16 章 物件群組和使用物件群組設定商務原則。

設定	說明
	■ **定義 (Define)** - 可讓您為傳至特定 IP 位址、網域名稱、通訊協定或連接埠的目的地流量定義比對準則。選取下列其中一個選項，依預設會選取**任何 (Any)**： ■ 任何 (Any) - 比對所有目的地流量。 ■ 網際網路 (Internet) - 比對連往目的地的所有網際網路流量 (不符合 SD-WAN 路由的流量)。 ■ Edge - 比對傳至 Edge 的所有流量。 ■ 透過閘道的非 SD-WAN 目的地 (Non SD-WAN Destination via Gateway) - 比對透過與設定檔相關聯之閘道傳輸至指定 Non VMware SD-WAN Site 的所有流量。請確定您已在設定檔層級將透過閘道的非 SD-WAN 站台相關聯。 ■ 透過 Edge 的非 SD-WAN 目的地 (Non SD-WAN Destination via Edge) - 比對透過與 Edge 或設定檔相關聯之 Edge 傳輸至指定 Non VMware SD-WAN Site 的所有流量。請確定您已在設定檔或 Edge 層級將透過 Edge 的非 SD-WAN 站台相關聯。 通訊協定 (Protocol) - 比對指定的通訊協定 (從下拉式功能表中選取) 的流量。支援的通訊協定為：GRE、ICMP、TCP 和 UDP。 網域 (Domain) - 比對整個網域名稱的流量，或**網域名稱 (Domain Name)** 欄位中指定之部分網域名稱的流量。例如，「salesforce」將會比對「www.salesforce.com」的流量。
應用程式 (Application)	請選取下列任一選項： ■ **任何 (Any)** - 依預設會將商務原則規則套用至任何應用程式。 ■ **定義 (Define)** - 允許選取要套用商務原則規則的特定應用程式。此外也可以指定 DSCP 值，以比對具有預設 DSCP/TOS 標籤的傳入流量。 **備註** 當建立僅符合某應用程式的商務原則規則時，若要對此類應用程式套用網路服務動作，Edge 可能需要使用 DPI (深度封包檢查) 引擎。通常，DPI 將無法根據第一個封包來判斷應用程式。DPI 引擎通常需要使用流量中的前 5-10 個封包，才能識別應用程式。僅就收到的第一個封包而言，流量可能會採用不同的路徑，即 [直接 (Direct)] 而不是 [多重路徑 (Multipath)] 或 [網際網路回傳 (Internet Backhaul)]，具體取決於商務原則組態。

根據您的**比對 (Match)** 選項，某些動作可能無法使用。

5 在**動作 (Action)** 區域下，設定規則的動作：

設定	說明
優先順序 (Priority)	指定下列其中一個規則優先順序： ■ **高 (High)** ■ **一般 (Normal)** ■ **低 (Low)** 選取**速率限制 (Rate Limit)** 核取方塊，以設定輸入和輸出流量方向的限制。
網路服務 (Network Service)	將**網路服務 (Network Service)** 設定為下列其中一個選項： ■ **直接 (Direct)** - 繞過 SD-WAN Gateway，直接將 WAN 線路的輸出流量傳送至目的地。 **備註** 依預設，Edge 偏好安全路由，而不是商務原則。實際上，這意味著 Edge 將透過 MultiPath (分支到分支或透過閘道的雲端，具體取決於路由) 轉送流量，即使商務原則設定成透過直接路徑來傳送該流量也是如此，但前提是 Edge 已從合作夥伴閘道或其他 Edge 收到安全預設路由或更具體的安全路由。 ■ **多重路徑 (Multi-Path)** - 將流量從一個 SD-WAN Edge 傳送至另一個 SD-WAN Edge。 ■ **網際網路回傳 (Internet Backhaul)** - 只有在**目的地 (Destination)** 設定為**網際網路 (Internet)** 時，才會啟用此網路服務。 **備註** **網際網路回傳 (Internet Backhaul)** 網路服務只會套用至網際網路流量 (以不符合已知本機路由或 VPN 路由而已網路首碼為目的地的 WAN 流量)。 如需這些選項的相關資訊，請參閱設定動作網路服務。 如果在設定檔層級啟用了條件式回傳，則依預設會將其套用至針對該設定檔而設定的所有商務原則。您可以停用所選原則的條件式回傳，將選取的流量 (直接、多重路徑和 CSS) 排除於此行為外，方法是選取**停用條件式回傳 (disable conditional backhaul)** 核取方塊。 如需有關如何啟用和疑難排解條件式回傳功能的詳細資訊，請參閱條件式回傳。

設定	說明
連結操控 (Link Steering)	選取下列其中一個連結操控模式： ■ **自動 (Auto)** - 依預設，所有應用程式都會設定為自動連結操控模式。當應用程式處於自動連結操控模式時，DMPO 會根據應用程式類型自動選擇最佳的連結，並在必要時自動啟用隨選修復。從下拉式功能表中輸入內部封包 DSCP 標籤，然後從下拉式功能表中輸入外部封包 DSCP 標籤。 ■ **傳輸群組 (Transport Group)** - 在操控原則中指定下列任一傳輸群組選項，以便在不同的裝置類型或位置之間套用相同的商務原則組態，這可能會有完全不同的 WAN 電信業者和 WAN 介面： ■ **公用有線 (Public Wired)** ■ **公用無線 (Public Wireless)** ■ **私人有線 (Private Wired)** ■ **介面 (Interface)** - 連結操控會繫結至實體介面，主要將用於路由目的。 **備註** 此選項只能在 Edge 覆寫層級使用。 ■ **WAN 連結 (WAN Link)** - 允許根據特定的私人連結定義原則規則。在此選項中，介面組態是獨立的，且不同於 WAN 連結組態。您將能夠選取手動設定或自動探索到的 WAN 連結。 **備註** 此選項只能在 Edge 覆寫層級使用。 如需與連結操控模式和 DSCP、底層和覆疊流量的 DSCP 標記相關的詳細資訊，請參閱設定連結操控模式。
NAT	停用或啟用 NAT。如需詳細資訊，請參閱設定以原則為基礎的 NAT。
服務類別 (Service Class)	選取下列其中一個服務類別選項： ■ **即時 (Real-time)** ■ **交易式 (Transactional)** ■ **大量 (Bulk)** **備註** 此選項僅適用於自訂應用程式。 VMware 應用程式/類別屬於其中一個類別。

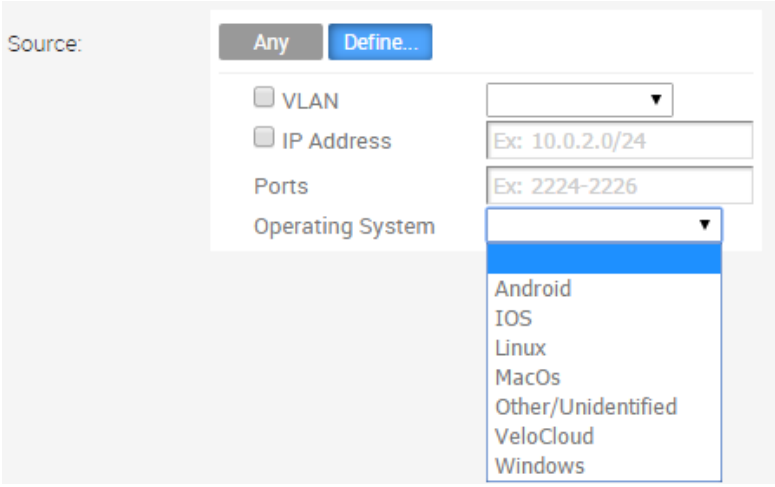
6 按一下**確定 (OK)**。系統會為選取的設定檔建立商務原則規則，並將其顯示在**設定檔商務原則 (Profile Business Policy)** 頁面的**商務原則 (Business Policy)** 區域下方。

相關資訊：覆疊 QoS CoS 對應

設定比對來源

本節將詳細說明**比對來源 (Match Source)**、**目的地 (Destination)** 和**應用程式 (Application)** 等選項。對於每個比對選項，都可使用**任何 (Any)** 指定來自來源、目的地或應用程式的任何流量。

如果選擇**比對來源定義 (Match Source Define)** 選項，則來源流量的範圍可縮小至特定 VLAN、IP 位址、連接埠、作業系統，或這些選項的任意組合。



設定比對目的地

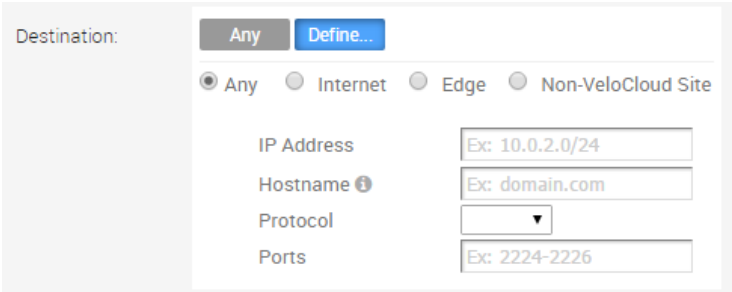
如果選擇**比對目的地定義 (Match Destination Define)** 選項，請指定用來識別流量目的地的其他參數。

目的地可以先縮小為某個類型 (**任何 (Any)**、**網際網路 (Internet)**、**Edge** 或 Non VMware SD-WAN Site)。如需上述流量目的地的說明，請參閱下表。

選項	說明
任何 (Any)	所有流量，無論目的地或路由為何。
網際網路 (Internet)	不符合 SD-WAN 路由的流量。
Edge	為網路中的其他站台指定的流量。此類站台會使用 SD-WAN Edge。
非 VeloCloud 站台 (Non-VeloCloud Site)	不使用 SD-WAN Edge，但具有網路內部路由的站台。Non VMware SD-WAN Site 可在**設定 (Configure)** > **網路服務 (Network Services)** 中設定。

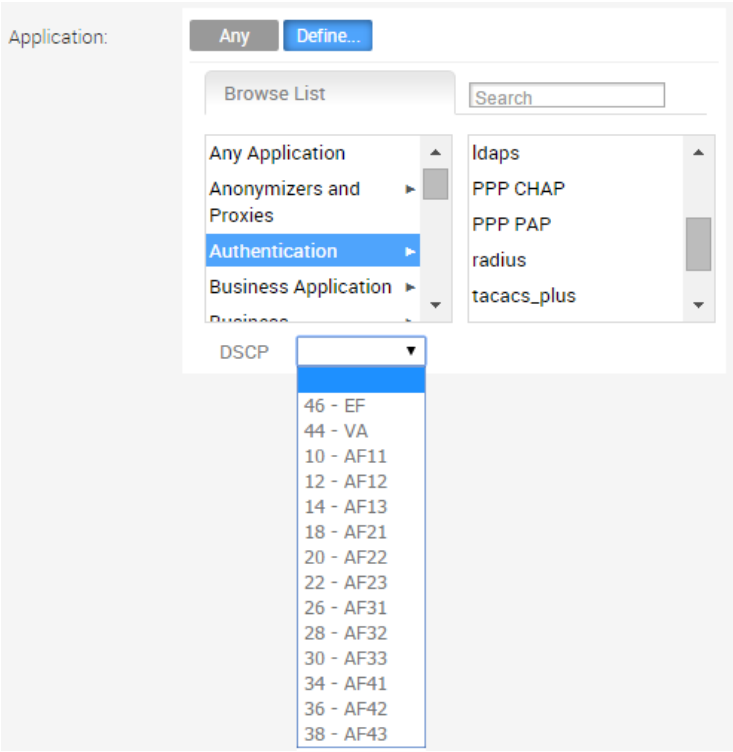
然後，藉由指定 **IP 位址 (IP Address)**、**主機名稱 (Hostname)**、**通訊協定 (Protocol)** (GRE、ICMP、TCP 或 UDP) 和連接埠，即可進一步定義目的地。

如果需要根據採用的路由為相同的流量比對模式指派不同的 QoS 值，則**比對目的地 (Match Destination)** 選項將特別實用。例如相較於一般的雲端式網際網路流量，您可能會想要為以 VMware SD-WAN Site 為目的地的流量指派較高的優先順序。使用目的地組態值即可輕鬆達到此目的。



設定比對應用程式

如果選取**比對應用程式定義 (Match Application Define)** 選項，則會先依類別，然後依特定應用程式來選擇應用程式。此外也可以指定 DSCP 值，以比對具有預設 DSCP/TOS 標籤的傳入流量。

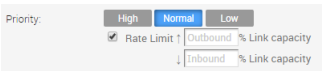


以下幾節將詳細說明**動作 (Action)**、**優先順序 (Priority)**、**網路服務 (Network Service)**、**連結操控 (Link Steering)**、NAT 和**服務類別 (Service class)** 等選項。

備註 根據您的**比對 (Match)** 選項，某些動作可能無法使用。例如，如果選擇**所有應用程式 (All Applications)**，則**網路服務 (Network Service)** 和**連結動作 (Link Actions)** 會顯示為灰色，而無法供您選取。同樣地，如果為 VPN 設定檔選取**網際網路 (Internet)** 類型的**目的地 (Destination)**或**可路由的應用程式 (Routable Apps)** 類型的**應用程式 (Application)**，則**網際網路回傳 (Internet Backhaul)** 會成為額外的**網路服務 (Network Service)** 可用選項。

設定動作優先順序

動作**優先順序 (Priority)** 參數可讓流量分類為**高 (High)**、**一般 (Normal)** 或**低 (Low)**。**速率限制 (Rate Limit)** 百分比也可套用在**輸出 (Outbound)** 和**輸入 (Inbound)** 方向中。



設定動作網路服務

建立或更新商務原則規則和動作時，您可以將**網路服務 (Network Service)** 設定為**直接 (Direct)**、**多重路徑 (Multi-Path)** 和**網際網路回傳 (Internet Backhaul)**。

直接

繞過 SD-WAN Gateway，直接將 WAN 線路的輸出流量傳送至目的地。如果在**裝置 (Device)** 索引標籤下方的**介面設定 (Interface Settings)** 上啟用 **NAT 直接流量 (NAT Direct Traffic)** 核取方塊，則會將 NAT 套用至流量。當您設定 NAT Direct 時，請考慮下列限制。

- NAT 必須在包含下一個躍點的 Edge 路由表中叫用流量作為雲端 VPN 或雲端閘道。
- 即使商務原則允許將私人 IP 位址設定為目的地，NAT 僅適用於公用 IP 位址的流量。

多重路徑

將流量從一個 SD-WAN Edge 傳送至另一個 SD-WAN Edge。

網際網路回傳

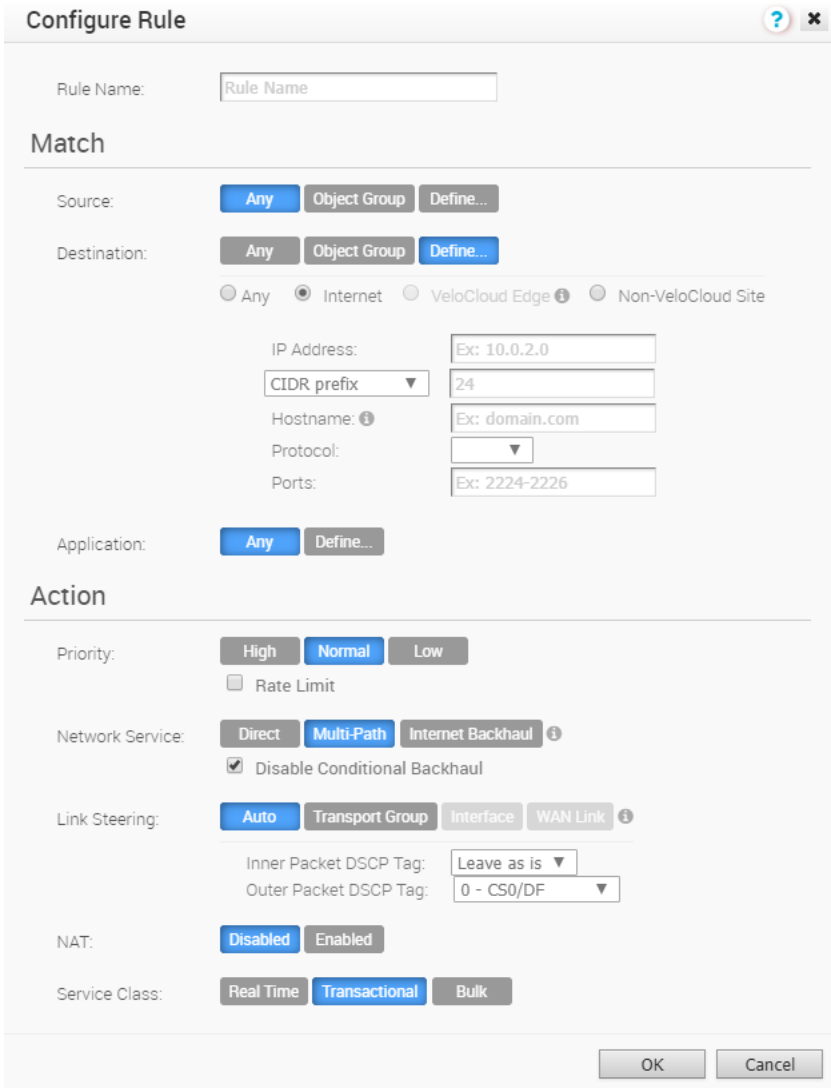
設定商務原則規則符合準則時，如果您將**目的地 (Destination)** 定義為**網際網路 (Internet)**，則會啟用**網際網路回傳 (Internet Backhaul)** 網路服務。

備註 **網際網路回傳 (Internet Backhaul)** 網路服務只會套用至網際網路流量 (以不符合已知本機路由或 VPN 路由而已網路首碼為目的地的 WAN 流量)。

選取**網際網路回傳 (Internet Backhaul)** 時，您必須選取下列其中一項：

- **回傳中樞 (Backhaul Hubs)**
- **非 VeloCloud 站台 (Non-VeloCloud Site)**
- **雲端安全性服務 (Cloud Security Service)**

您應該可以為回傳設定多個 VMware SD-WAN Sites，以支援原本在 Non VMware SD-WAN Site 連線中內建的備援性，但保持服務無法使用而導致流量捨棄的一致行為。



如果在設定檔層級啟用了條件式回傳，則依預設會將其套用至針對該設定檔而設定的所有商務原則。您可以停用所選原則的條件式回傳，將選取的流量 (直接和多重路徑) 排除於此行為外，方法是在所取商務原則的**設定規則 (Configure Rule)** 畫面中，選取**動作 (Action)** 區域中的**停用條件式回傳 (Disable Conditional Backhaul)** 核取方塊。如需詳細資訊，請參閱條件式回傳。

設定連結操控模式

在商務原則中，有四個連結操控模式：**自動 (Auto)**、**傳輸群組 (Transport Group)**、**WAN 連結 (WAN Link)** 和**介面 (Interface)**。

連結選取：自動

依預設會為所有應用程式指定自動連結操控模式。這表示 DMPO 會根據應用程式類型自動選取最佳的連結，並在必要時自動啟用隨選修復。網際網路應用程式的連結操控和隨選修復有四種可能的組合。如前所述，企業內的流量 (VPN) 一律會流經 DMPO 通道，因此一律可受益於隨選修復。

案例	預期的 DMPO 行為
至少一個連結符合應用程式的 SLA。	選擇最適用的連結。
單一連結，且封包遺失率超過應用程式的 SLA。	為此連結上傳送的即時應用程式啟用 FEC。
兩個連結，只有一個連結發生遺失。	在兩個連結上啟用 FEC。
多個連結，且有多個連結發生遺失。	在兩個最佳連結上啟用 FEC。
兩個連結，但有一個連結可能不穩定，例如遺失三個連續的活動訊號。	將連結標記為無法使用，並將流程導向至下一個最佳的連結。
兩個連結都發生抖動和遺失。	在兩個連結上啟用 FEC，並在接收端啟用抖動緩衝區。當語音的抖動大於 7 毫秒，且視訊抖動超過 5 毫秒時，就會啟用抖動緩衝區。 傳送 DMPO 端點會通知接收 DMPO 端點啟用抖動緩衝區。接收 DMPO 端點最多將緩衝處理 10 個封包或 200 毫秒的流量 (以先發生者為準)。接收 DMPO 端點會使用內嵌於 DMPO 標頭中的原始時間戳記，來計算要在消除抖動緩衝區中使用的流動率。如果流量未以固定速率傳送，則會停用抖動緩衝處理。

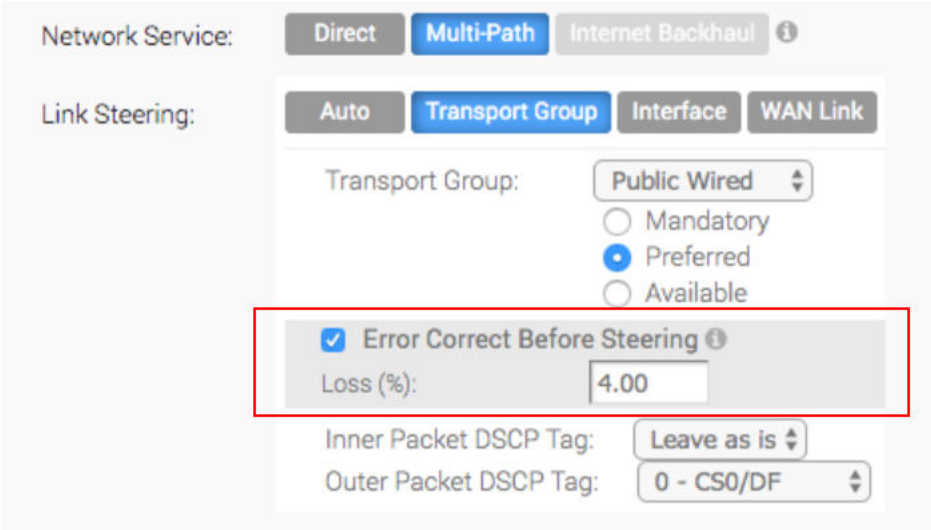
依傳輸群組的連結操控

傳輸群組代表根據類似的特性和功能結合在一起的 WAN 連結。定義傳輸群組可允許商務抽象概念，使類似的原則能夠套用於不同的硬體類型。

不同的位置可能有不同的 WAN 傳輸 (例如 WAN 電信業者名稱、WAN 介面名稱)；DMPO 會使用傳輸群組的概念，從商務原則組態中擷取基礎 WAN 電信業者和介面。商務原則組態可以在操控原則中指定傳輸群組 (**公用有線 (Public Wired)**、**公用無線 (Public Wireless)** 或**私人有線 (Private Wired)**)，以便可以在不同的裝置類型或位置之間套用相同的商務原則組態，這可能會有完全不同的 WAN 載體和 WAN 介面。DMPO 在執行 WAN 連結探索時，它也會將傳輸群組指派給 WAN 連結。這是在商務原則中指定連結時最理想的選項，因為 IT 管理員不需要知道實體連線類型或 WAN 電信業者。

如果您選擇**慣用 (Preferred)** 選項，則會顯示**在操控前修正錯誤 (Error Correct Before Steering)** 核取方塊。

如果選取**在操控前修正錯誤 (Error Correct Before Steering)** 核取方塊，則會顯示遺失 % 變數文字方塊。當您定義遺失率百分比 (例如 4%) 時，Edge 將繼續使用選取的連結或傳輸群組並套用錯誤修正，直到遺失率達到 4%，屆時即會將流量導向至其他路徑。當**在操控前修正錯誤 (Error Correct Before Steering)** 核取方塊取消選取時，如果連結的遺失率超過應用程式 SLA (例如依預設即時應用程式 SLA 為 0.3%)，Edge 就會開始將流量導向至他處。如果停用此核取方塊，應用程式將會在錯誤修正發生前進行操控。



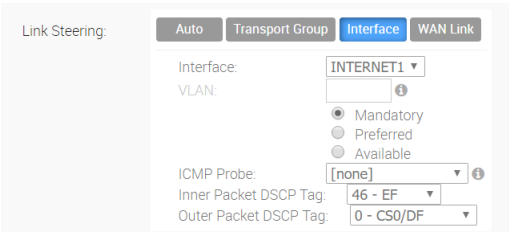
備註 Edge 覆寫層級和設定檔層級皆允許此選項。

依介面的連結操控

使用此選項時，連結操控會繫結至實體介面。依介面的連結操控主要用於路由用途。但是，即便此選項在邏輯上只能用來直接從 VMware SD-WAN Site 路由流量，如果指定的規則具有需要網際網路多重路徑優點的網路服務，它仍會選取連線至介面的單一 WAN 連結。

如果您選擇**慣用 (Preferred)** 選項，則會顯示**在操控前修正錯誤 (Error Correct Before Steering)** 核取方塊。如果勾選此核取方塊，則將有額外的遺失 % 變數可供使用。此選項停用時，如果連結的遺失率超過應用程式 SLA (依預設即時應用程式 SLA 為 0.3%)，Edge 就會開始將流量導向至他處。如果套用 [在操控前修正錯誤 (Error Correct Before Steering)]，且已定義遺失率百分比 (在此範例中假設為 4%)，Edge 將繼續使用選取的連結或傳輸群組並套用錯誤修正，直到遺失率達到 4%，屆時即會將流量導向至其他路徑。如果停用此核取方塊，應用程式將會在錯誤修正發生前進行操控。

備註 此選項只能在 Edge 覆寫層級使用。這可確保提供的連結選項一律符合 SD-WAN Edge 硬體型號。



WAN 連結

在此選項中，介面組態是獨立的，且不同於 WAN 連結組態。您將能夠選取手動設定或自動探索到的 WAN 連結。

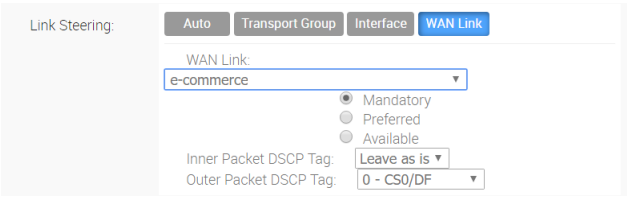
WAN 連結下拉式功能表

您可以根據特定的私人連結來定義原則規則。如果您已建立私人網路名稱，並將其指派給個別的私人 WAN 覆疊，則這些私人連結名稱將會顯示在 **WAN 連結 (WAN Link)** 下拉式功能表中。

如需如何定義多個私人網路名稱並將其指派給個別私人 WAN 覆疊的相關資訊，請參閱私人網路名稱和選取私人名稱連結。

如果您選擇**慣用 (Preferred)** 選項，則會顯示**在操控前修正錯誤 (Error Correct Before Steering)** 核取方塊。如果停用此核取方塊，應用程式將會在錯誤修正發生前進行操控。

備註 此選項只能在 Edge 覆寫層級使用。

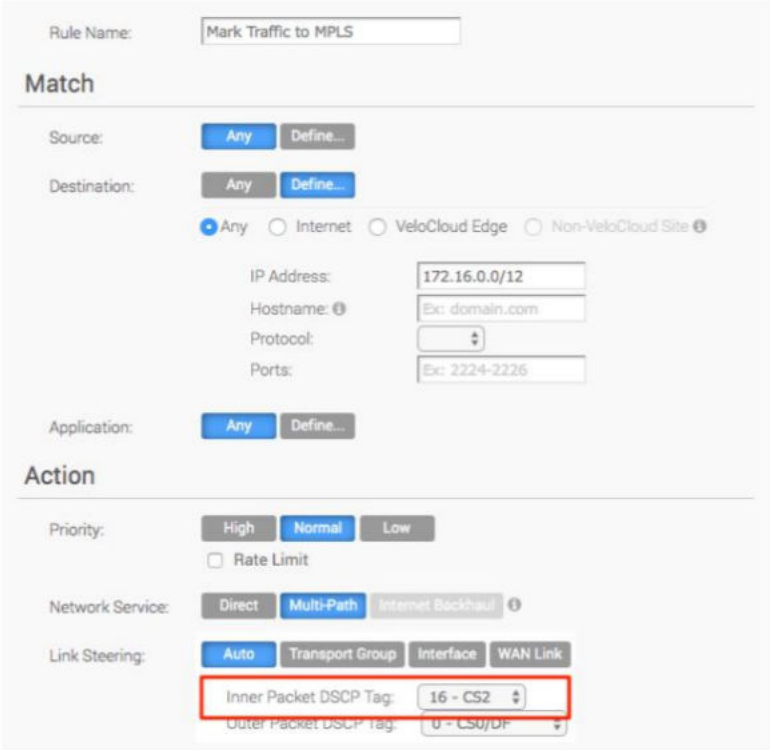


使用**介面 (Interface)** 和 **WAN 連結 (WAN Link)** 選項時，您必須選取下列其中一個選項：

選項	說明
必要 (Mandatory)	表示將透過指定的 WAN 連結或連結服務群組傳送流量。如果指定的連結 (或所選服務群組內的所有連結) 處於非作用中狀態，**或**如果多重路徑閘道路由無法使用，則系統將會捨棄對應的封包。
慣用 (Preferred)	表示最好應透過指定的 WAN 連結或連結服務群組來傳送流量。如果指定的連結 (或所選服務群組內的所有連結) 處於非作用中狀態，或如果選擇的多重路徑閘道路由不穩定，或是不符合連結服務層級目標 (SLO)，則系統會將對應的封包導向至下一個最佳的連結。如果慣用的連結再次成為可用狀態，則流量將導向回慣用的連結。
可用 (Available)	表示最好應透過指定的 WAN 連結或連結服務群組 (只要處於可用狀態) 傳送流量 (而不考量連結 SLO)。如果指定的連結 (或所選服務群組內的所有連結) 無法使用，或選取的多重路徑閘道路由無法使用，則會將對應的封包導向至下一個最適用的連結。如果慣用連結恢復為可用狀態，則流量將導向回到可用連結。

連結操控：底層和覆疊流量的 DSCP 標記概觀

VMware 支援由 Edge 轉送至底層之封包的 DSCP 重新標記。只要在介面上啟用**底層計量 (Underlay Accounting)**，SD-WAN Edge 便可以重新標記在 WAN 連結上轉送的底層流量。DSCP 重新標記可在 [連結操控 (Link Steering)] 區域的商務原則組態中啟用。請參閱建立商務原則規則。在下方所示的範例圖中 (假設 Edge 已連線至 MPLS，且底層和覆疊流量皆轉送至 MPLS)，如果流量符合網路首碼 172.16.0.0/12，則 Edge 將會為底層封包重新標記 DSCP 值 16 或 CS2，並忽略**外部封包 DSCP 標籤 (Outer Packet DSCP Tag)** 欄位。若要讓傳送至 MPLS 的覆疊流量符合相同的商務原則，外部標頭的 DSCP 值會設為**外部封包 DSCP 標籤 (Outer Packet DSCP Tag)**。

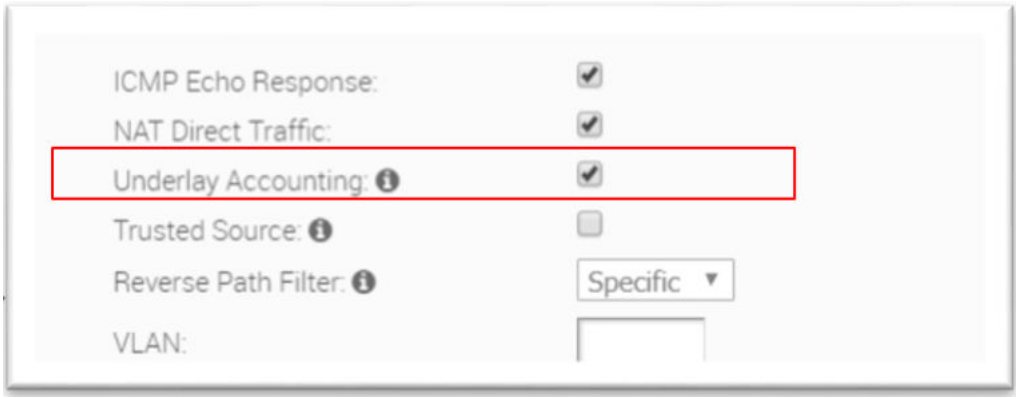


連結操控：底層流量的 DSCP 標記使用案例

連線至 MPLS 的 Edge 通常會先在封包上標記 DSCP，然後將其傳送至 PE，讓 SP 根據 SLA 處理封包。必須在 WAN 介面上啟用**底層計量 (Underlay Accounting)**，透過商務原則在底層流量上進行 DSCP 標記才會生效。

連結操控：底層 DSCP 組態

1 在 SD-WAN Orchestrator 中確認已依預設為 WAN 覆疊啟用**底層計量 (Underlay Accounting)** (**設定 (Configure)** > **Edge 裝置 (Edge Devices)** > **裝置設定 (Device Settings)** 區域)。



2 從 SD-WAN Orchestrator 移至**設定 (Configure)** > **Edge** > **商務原則 (Business Policy)**。

3 在**商務原則 (Business Policy)** 畫面中按一下現有的規則，或按一下**新增規則 (New Rule)** 按鈕以建立新規則。

4 在**動作 (Action)** 區段中，移至**連結操控 (Link Steering)** 區域。

5 視情況按一下以下其中一項：自動、傳輸群組、介面或 WAN 連結。

6 為底層流量和**內部封包 DSCP 標籤 (Inner Packet DSCP Tag)** 組態設定**比對 (Match)** 準則。

連結操控：覆疊 DSCP 組態

1 在 SD-WAN Orchestrator 中確認已依預設為 WAN 覆疊啟用**底層計量 (Underlay Accounting)** (**設定 (Configure)** > **Edge 裝置 (Edge Devices)** > **裝置設定 (Device Settings)** 區域)。

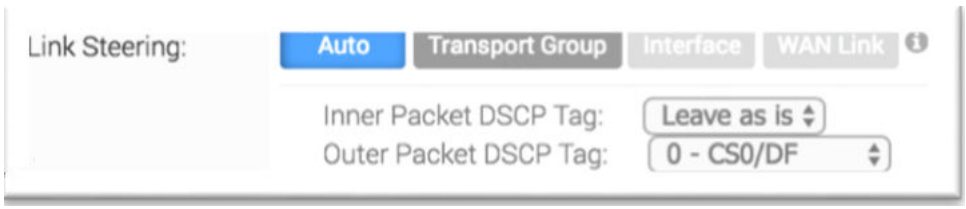
2 從 SD-WAN Orchestrator 移至**設定 (Configure)** > **Edge** > **商務原則 (Business Policy)**。

3 在**商務原則 (Business Policy)** 畫面中按一下現有的規則，或按一下**新增規則 (New Rule)** 按鈕以建立新規則。

4 在**動作 (Action)** 區段中，移至**連結操控 (Link Steering)** 區域。

5 視情況按一下以下其中一項：**自動 (Auto)**、**傳輸群組 (Transport Group)**、**介面 (Interface)**或 **WAN 連結 (WAN Link)**。

6 為底層流量以及**內部封包 DSCP 標籤 (Inner Packet DSCP Tag)** 和**外部封包 DSCP 標籤 (Outer Packet DSCP Tag)** 組態設定**比對 (Match)** 準則。



設定以原則為基礎的 NAT

您可以為來源和目的地設定以原則為基礎的 NAT。NAT 可套用至 Non VMware SD-WAN Site 流量或使用多重路徑的合作夥伴閘道遞交流量。設定 NAT 時，您必須定義要進行 NAT 處理的流量，以及您要執行的動作。NAT 組態有兩種類型：多對一和一對一。

存取 NAT

您可以從 **設定 (Configure)** > **設定檔 (Profiles)** > **商務原則索引標籤 (Business Policy Tab)** 中存取 NAT 功能，然後按一下**新增規則 (New Rule)** 按鈕。NAT 功能位於**動作 (Action)** 區域下。

多對一 NAT 組態

在此組態中，您可以使用 NAT，針對源自 Edge 後方主機的流量，將其來源或目的地 IP 對應至不同的唯一來源或目的地 IP 位址。例如，即使流量源自 Edge 後方的不同主機，使用者仍可針對以資料中心內主機或伺服器為目標 (其位置在具有唯一 IP 位址的合作夥伴閘道後方) 的流量設定來源 NAT。

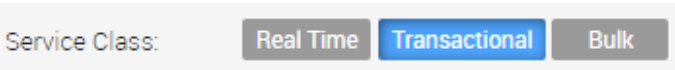
下圖顯示多對一組態的範例。在此範例中，連線至 VLAN **100 - 公司 2** (其位置在以網際網路主機或 DC 後方的主機為目標的 Edge 後方) 的主機所產生的所有流量，都將以 IP 位址 72.4.3.1 作為來源 NAT。

一對一 NAT 組態

在此組態中，分支 Edge 會使用 NAT 將主機或伺服器的單一本機 IP 位址對應至另一個全域 IP 位址。如果 Non VMware SD-WAN Site 或資料中心的主機將流量傳送至全域 IP 位址 (在一對一 NAT 組態中設定為來源 NAT IP 位址)，則 SD-WAN Gateway 會將該流量轉送至分支中主機或伺服器的本機 IP 位址。

設定動作服務類別

服務類別參數可設為**即時 (Real Time)** (具時間性的流量)、**交易式 (Transactional)** 或**大量 (Bulk)**。此選項僅適用於自訂應用程式。VMware 應用程式/類別屬於其中一個類別。

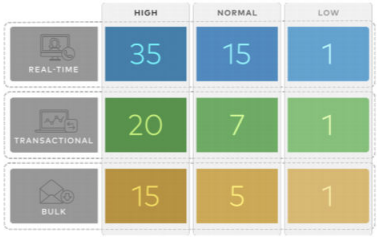


覆疊 QoS CoS 對應

流量類別會使用優先順序 (高、一般或低) 和服務類別 (即時、交易式或大量) 來組合定義，結果會產生具有九個流量類別的 3x3 矩陣。您可以將應用程式/類別和排程器權重對應到這些流量類別上。流量類別中的所有應用程式將會與彙總 QoS 處理 (包括排程和監控) 一起套用。

指定流量類別中的所有應用程式在擁塞期間會根據排程器權重 (或頻寬百分比) 獲得保證的最小彙總頻寬。沒有擁塞時，系統會允許應用程式使用最大彙總頻寬。您可以套用監控器，以對指定流量類別中的所有應用程式進行頻寬限制。請參閱下圖，以瞭解應用程式/類別和流量類別對應的預設值。

商務原則包含立即可用的智慧型預設功能，可將超過 2,500 應用程式對應至流量類別。您可以使用應用程式感知 QoS，而無須定義原則。在排程器中會為每個流量類別指派一個預設權重，且這些參數可在商務原則中變更。以下是具有九個流量類別的 3x3 矩陣的預設值。請參閱下圖，以瞭解權重和流量類別對應的預設值。



範例：

在此範例中，客戶在 Edge 上具有 90 Mbps 網際網路連結和 10 Mbps 的 MPLS，且彙總頻寬為 100 Mbps。根據以上的預設權重和流量類別對應，所有對應至企業協作的應用程式都將有保證頻寬 35 Mbps，而所有對應至電子郵件的應用程式都將有保證頻寬 15 Mbps。請注意，您可以為整體類別定義商務原則，例如企業協作、應用程式 (例如商務用 Skype)，以及更精細的子應用程式 (例如 Skype 檔案傳輸、Skype 語音和 Skype 視訊)。

設定覆疊 QoS CoS 對應

備註 只有在操作員已啟用 SD-WAN 流量類別和權重的對應功能時，才可編輯此功能。若要取得此功能的存取權，請洽詢您的操作員以取得詳細資訊。

若要啟用覆疊 QoS CoS 對應：

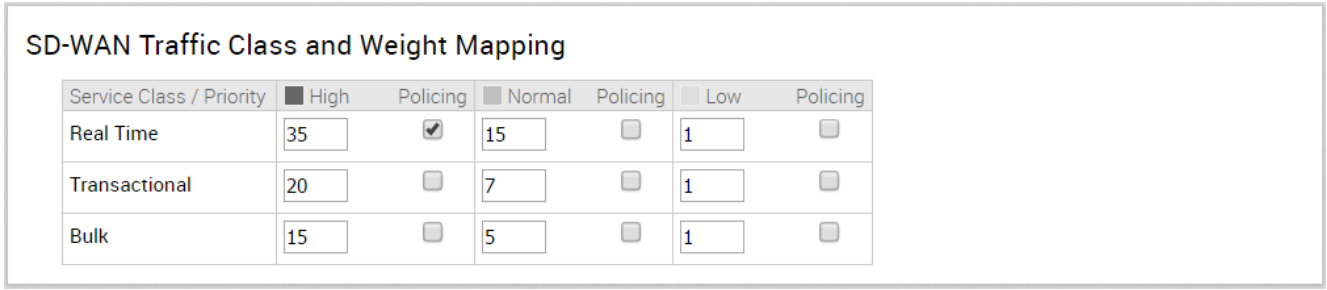
1 移至**設定 (Configure)** > **設定檔 (Profiles)**。

2 按一下適當組態設定檔的連結。

3 按一下**商務原則 (Business Policy)** 索引標籤。

4 在 **SD-WAN 流量類別和權重的對應 (SD-WAN Traffic Class and Weight Mapping)** 區域中，視需要輸入**即時 (Real Time)**、**交易式 (Transactional)** 和/或**大量 (Bulk)** 的數值。

5 如有必要，請勾選服務類別的**監控 (Policing)** 核取方塊。

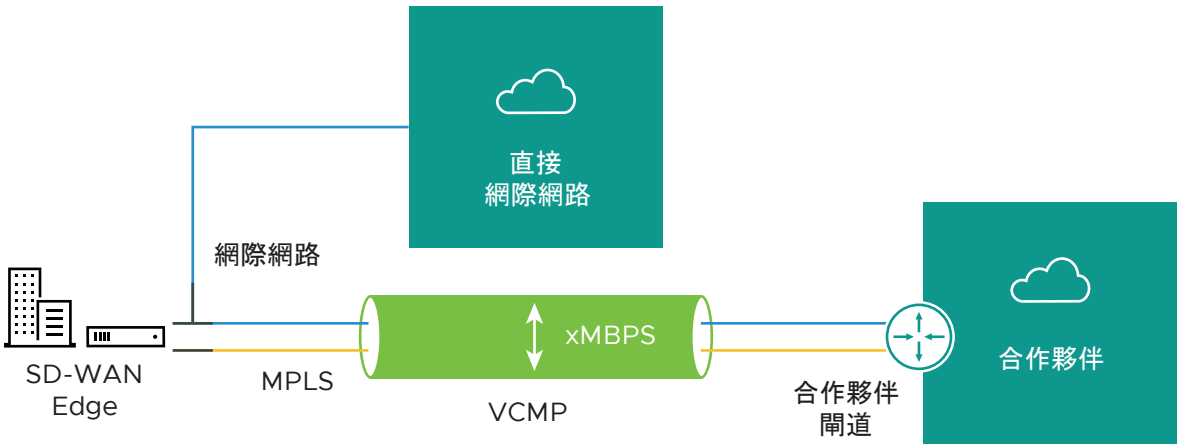


服務提供者可用於合作夥伴閘道的通道塑形器

本節說明服務提供者可用於合作夥伴閘道的通道塑形器。

相較於本機分支上 WAN 連結的彙總容量，服務提供者所提供的 SD-WAN 服務可能容量較低。例如，客戶可能已向其他廠商和提供 SD-WAN 服務的 SP 購買了寬頻連結，但主控的 VMware 合作夥伴閘道無法控制底層寬頻連結。在這種情況下，為了確保 SD-WAN 服務容量的有效性，並且避免對合作夥伴閘道造成擁塞，服務提供者可在通道與合作夥伴閘道之間啟用 DMPO 通道塑形器。

通道塑形器範例



考慮具有兩個 WAN 連結、20 Mbps 網際網路和 20 Mbps MPLS 的 SD-WAN Edge，並使用從服務提供者 (SP) 提供的 35 Mbps SD-WAN 服務。在此情況中，SD-WAN 服務 (35 Mbps) 的頻寬低於 WAN 連結的彙總頻寬 (40 Mbps)。若要確保通往合作夥伴閘道的流量不超過 35 Mbps (在上圖中顯示為「X」)，服務提供者可在 DMPO 通道上設置通道塑形器。

設定速率限制通道流量

備註 只有在操作員已啟用速率限制通道流量功能時，才可編輯該功能。若要取得此功能的存取權，請洽詢您的操作員以取得詳細資訊。

若要啟用速率限制通道流量：(To enable Rate-Limit Tunnel Traffic:)

1 移至導覽面板中的**設定 (Configure)** > **設定檔 (Profiles)**。

2 按一下適當組態設定檔的連結。

3 按一下**商務原則 (Business Policy)** 索引標籤。

4 在 **SD-WAN 覆疊速率限制 (SD-WAN Overlay Rate Limit)** 區域中，勾選**速率限制通道流量 (Rate-Limit Tunnel Traffic)** 核取方塊。(請參閱下圖)。

5 選取**百分比 (Percent)** 或**速率 (Mbps) (Rate (Mbps))** 選項按鈕。

6 在**限制 (Limit)** 文字方塊中，輸入通道流量的數值限制。

7 按一下**儲存變更 (Save Changes)**。


SD-WAN Overlay Rate Limit
Rate-Limit Tunnel Traffic:
Percent (%):
Rate (Mbps):
Limit:
20

設定防火牆

12

防火牆是一種網路安全性裝置，可監控傳入和傳出的網路流量，並根據已定義的一組安全性規則來決定是否允許或封鎖特定流量。SD-WAN Orchestrator 支援為設定檔和 Edge 設定無狀態和可設定狀態的防火牆。

可設定狀態的防火牆會監控並追蹤透過防火牆所傳入每個網路連線的作業狀態和特性，並使用這項資訊決定要允許哪些網路封包通過防火牆。可設定狀態的防火牆會建置狀態資料表，並使用此資料表，而僅允許從目前在狀態資料表中列出的連線傳回流量。從狀態資料表中移除某個連線後，即不允許外部裝置透過該連線傳入的流量。

可設定狀態的防火牆功能有下列優點：

- 防止攻擊，例如拒絕服務 (DoS) 和詐騙
- 更可靠的記錄
- 更高的網路安全性

備註 依預設會為企業啟用**可設定狀態的防火牆 (Stateful Firewall)** 功能。SD-WAN Orchestrator 可讓企業使用者使用各自的**防火牆 (Firewall)** 頁面，在設定檔和 Edge 層級上啟用或停用可設定狀態的防火牆功能。若要為企業停用可設定狀態的防火牆功能，請連絡具有超級使用者權限的操作員。

備註 Edge 中若已啟用可設定狀態的防火牆，即不支援非對稱路由。

備註 依預設會為企業停用 **Syslog 轉送 (Syslog Forwarding)** 功能。若要將源自企業 SD-WAN Edges 的防火牆記錄收集到一或多個集中式遠端 Syslog 收集器 (伺服器)，企業使用者必須在企業層級啟用此功能。如需如何在 SD-WAN Orchestrator 中為每個區段設定 Syslog 收集器詳細資料的步驟，請參閱在設定檔層級設定 Syslog 設定。

若要在設定檔和 Edge 層級設定防火牆設定，請參閱：

- 設定設定檔的防火牆
- 設定 Edge 的防火牆

本章節討論下列主題：

- 設定設定檔的防火牆
- 設定 Edge 的防火牆
- 設定防火牆規則

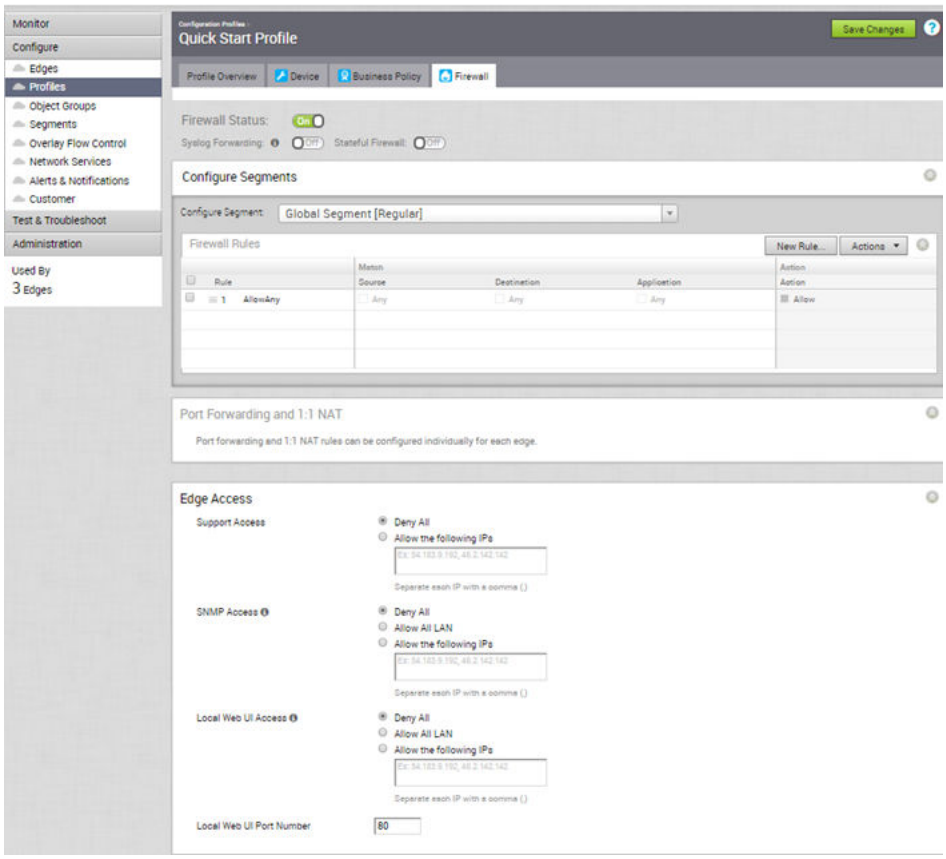
- 設定 Edge 存取
- 對防火牆進行疑難排解

設定設定檔的防火牆

身為企業管理員，您可以使用**設定檔組態 (Profile Configuration)** 對話方塊中的**防火牆 (Firewall)** 索引標籤來設定防火牆規則、Edge 存取資訊，以及啟用或停用防火牆狀態和記錄。

防火牆設定檔可辨識區段。所有可用於設定的區段，都會列在**設定區段 (Configure Segment)** 下拉式功能表中。當您從**設定區段 (Configure Segment)** 下拉式功能表中選取要設定的區段時，與該區段相關聯的設定和選項將會顯示在**設定區段 (Configure Segments)** 區域中。**全域區段 [一般] (Global Segment [Regular])** 是預設區段。

如需分割的詳細資訊，請參閱第 7 章 設定區段。



設定檔層級的防火牆組態包括：

- 啟用 [Syslog 轉送 (Syslog Forwarding)]。依預設會為企業停用 [Syslog 轉送 (Syslog Forwarding)] 功能。若要將源自企業 SD-WAN Edges 的 SD-WAN Orchestrator 繫結事件和防火牆記錄收集到一或多個集中式遠端 Syslog 收集器 (伺服器)，企業使用者必須在企業層級啟用此功能。如需如何在 SD-WAN Orchestrator 中為每個區段設定 Syslog 收集器詳細資料的步驟，請參閱在設定檔層級設定 Syslog 設定。

- 在設定檔和 Edge 層級啟用可設定狀態的防火牆。依預設會為企業啟用 [可設定狀態的防火牆 (Stateful Firewall)] 功能。若要為企業停用可設定狀態的防火牆功能，請連絡具有超級使用者權限的操作員。
- 設定防火牆規則。
- 設定 Edge 存取

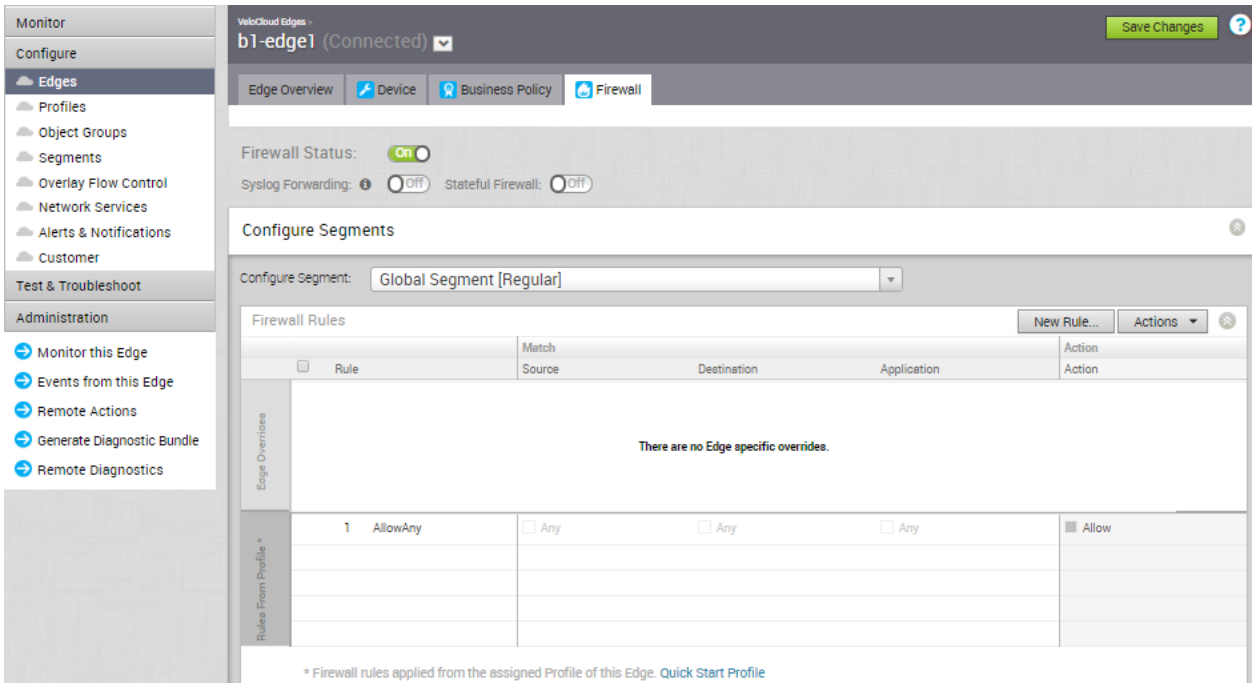
備註 您可以將**防火牆狀態 [Firewall Status]** 設為關閉，以停用設定檔的防火牆功能。

相關連結

- 設定 Edge 的防火牆
- 對防火牆進行疑難排解

設定 Edge 的防火牆

所有 Edge 都會從相關聯的設定檔繼承防火牆規則和 Edge 存取組態。在 **Edge 組態 (Edge Configuration)** 對話方塊的**防火牆 (Firewall)** 索引標籤下，您可以在**設定檔中的規則 (Rule From Profile)** 區域中檢視所有繼承的防火牆規則。或者，在 Edge 層級上，您也可以覆寫設定檔防火牆規則和 Edge 存取組態。



身為企業管理員，您可以依照此頁面上的指示，為每個 Edge 個別設定連接埠轉送和 1:1 NAT 防火牆規則。

連接埠轉送和 1:1 NAT 防火牆規則

備註 您只能在 Edge 層級個別設定連接埠轉送和 1:1 NAT 規則。

連接埠轉送和 1:1 NAT 防火牆規則可讓網際網路用戶端存取連線至 Edge LAN 介面的伺服器。存取權可透過連接埠轉送規則或 1:1 NAT (網路位址轉譯) 規則來提供。

連接埠轉送規則

連接埠轉送規則可讓您設定規則，將流量從特定 WAN 連接埠重新導向至本機子網路內的裝置 (LAN IP/LAN 連接埠)。或者，您也可以依據 IP 或子網路來限制輸入流量。可以使用位於 WAN IP 相同子網路上的外部 IP，來設定連接埠轉送規則。如果 ISP 將子網路的流量路由至 SD-WAN Edge，此對應也可轉譯與 WAN 介面位址位於不同子網路中的外部 IP 位址。

若要設定連接埠轉送規則，請提供下列詳細資料。

1 在**名稱 (Name)** 文字方塊中，輸入規則的名稱 (選用)。

2 在**通訊協定 (Protocol)** 下拉式功能表中，選取 TCP 或 UDP 作為連接埠轉送的通訊協定。

3 在**介面 (Interface)** 下拉式功能表中，選取輸入流量的介面。

4 在**外部 IP (Outside IP)** 文字方塊中，輸入可用以從外部網路存取主機 (應用程式) 的 IP 位址。

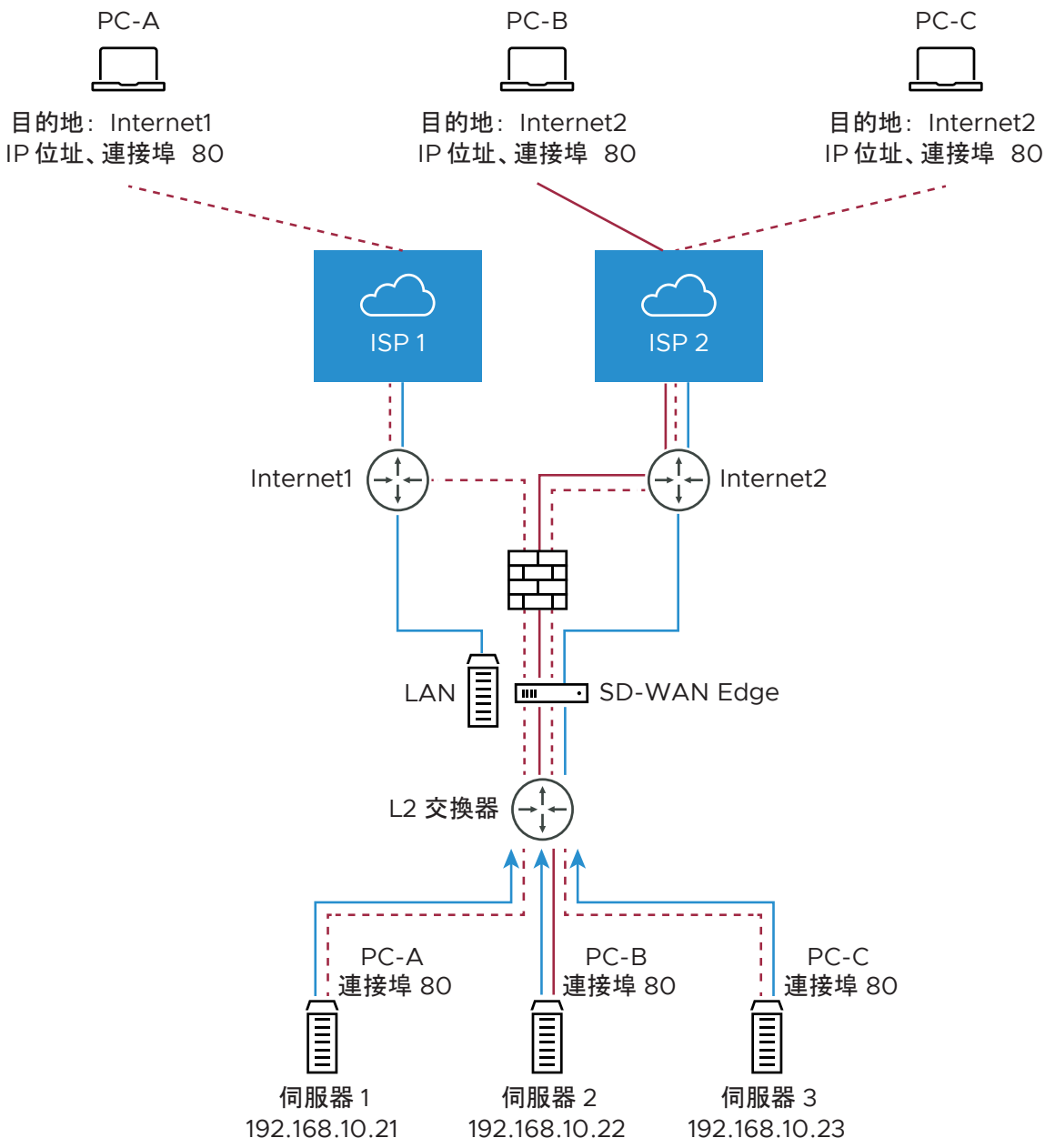
5 在 [WAN 連接埠 (WAN Ports)] 文字方塊中，輸入一個 WAN 連接埠，或以破折號 (-) 分隔的連接埠範圍，例如 20-25。

6 在 **LAN IP** 和 **LAN 連接埠 (LAN Port)** 文字方塊中，輸入將轉送要求之 LAN 的 IP 位址和連接埠號碼。

7 在**區段 (Segment)** 下拉式功能表中，選取 LAN IP 所屬的區段。

8 在**遠端 IP/子網路 (Remote IP/subnet)** 文字方塊中，指定要轉送至內部伺服器之輸入流量的 IP 位址。若未指定任何 IP 位址，則會允許任何流量。

下圖顯示連接埠轉送組態。


PC-A
PC-B
PC-C
目的地：Internet1
IP 位址、連接埠 80
目的地：Internet2
IP 位址、連接埠 80
目的地：Internet2
IP 位址、連接埠 80
ISP 1
ISP 2
Internet1
Internet2
LAN
SD-WAN Edge
L2 交換器
PC-A
連接埠 80
PC-B
連接埠 80
PC-C
連接埠 80
伺服器 1
192.168.10.21
伺服器 2
192.168.10.22
伺服器 3
192.168.10.23

1:1 NAT 設定

這些設定可用來將 SD-WAN Edge 所支援外部 IP 位址對應至連線至 Edge LAN 介面的伺服器 (例如 Web 伺服器或郵件伺服器)。如果 ISP 將子網路的流量路由至 SD-WAN Edge，此對應也可轉譯與 WAN 介面位址位於不同子網路中的外部 IP 位址。每個對應的兩端分別是特定 WAN 介面的防火牆外的一個 IP 位址，和防火牆內的一個 LAN IP 位址。在每個對應內，您可以指定將轉送至內部 IP 位址的連接埠。您可以使用右側的「+」圖示來新增其他 1:1 NAT 設定。

若要設定 1:1 NAT 規則，請提供下列詳細資料。

1 在**名稱 (Name)** 文字方塊中，輸入規則的名稱。

2 在**外部 IP (Outside IP)** 文字方塊中，輸入可藉以從外部網路存取主機的 IP 位址。

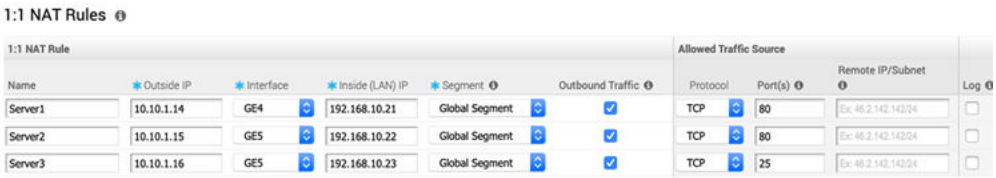
3 在**介面 (Interface)** 下拉式功能表中，選取將繫結外部 IP 位址的 WAN 介面。

4 在**內部 (LAN) IP (Inside (LAN) IP)** 文字方塊中，輸入主機的實際 IP (LAN) 位址。

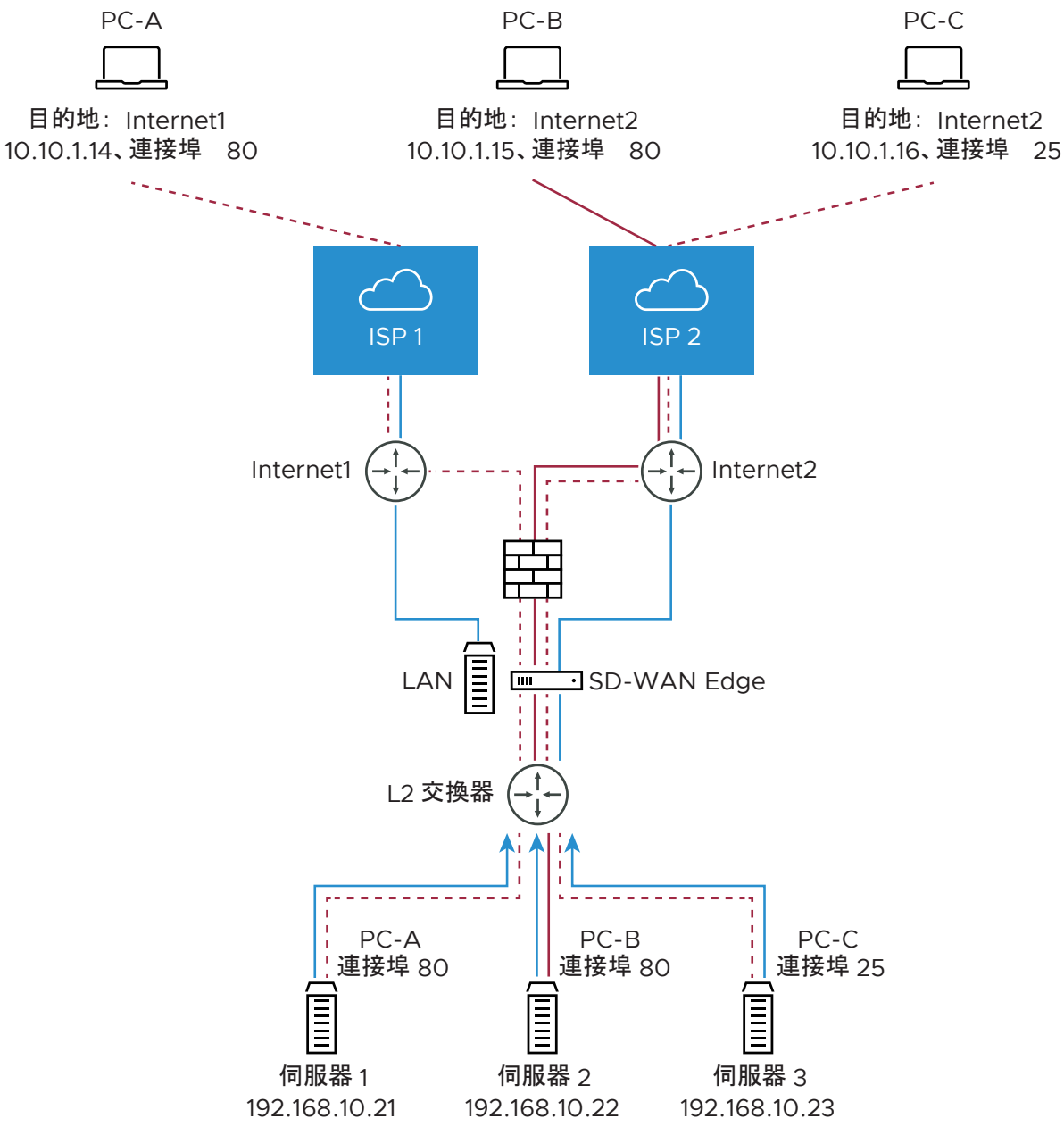
5 在**區段 (Segment)** 下拉式功能表中，選取 LAN IP 所屬的區段。

6 如果您想要允許從網際網路到 LAN 用戶端的輸出流量經由防火牆連線進入 Edge，請選取**輸出流量 (Outbound Traffic)** 核取方塊。

7 在各自的欄位中，輸入對應的 [允許的流量來源 (Allowed Traffic Source)] (通訊協定、連接埠、遠端 IP/子網路) 詳細資料。



下圖顯示 1:1 NAT 組態。


PC-A
PC-B
PC-C
目的地：Internet1
10.10.1.14、連接埠 80
目的地：Internet2
10.10.1.15、連接埠 80
目的地：Internet2
10.10.1.16、連接埠 25
ISP 1
ISP 2
Internet1
Internet2
LAN
SD-WAN Edge
L2 交換器
PC-A
連接埠 80
PC-B
連接埠 80
PC-C
連接埠 25
伺服器 1
192.168.10.21
伺服器 2
192.168.10.22
伺服器 3
192.168.10.23

設定 Edge 覆寫

在 Edge 層級上，您可以選擇覆寫繼承的設定檔防火牆規則。若要覆寫 Edge 層級上的防火牆規則，請按一下**防火牆規則 (Firewall Rules)** 下的**新增規則 (New Rule)**，然後依照設定防火牆規則中的步驟操作。覆寫規則會出現在 **Edge 覆寫 (Edge Overrides)** 區域中。Edge 覆寫規則的優先權會高於 Edge 繼承的設定檔規則。與任何設定檔防火牆規則相同的任何防火牆覆寫相符值，都將覆寫該設定檔規則。

設定 Edge 存取覆寫

或者，在 Edge 層級上，您也可以覆寫 Edge 存取組態。若要覆寫 Edge 存取，請在 **Edge 防火牆 (Edge Firewall)** 頁面的 **Edge 存取 (Edge Access)** 區域中選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。如需詳細資訊，請參閱設定 Edge 存取。

相關連結

- 設定設定檔的防火牆
- 在 Edge 層級設定 Syslog 設定
- 對防火牆進行疑難排解

設定防火牆規則

SD-WAN Orchestrator 可讓您在設定檔和 Edge 層級設定防火牆規則，以允許、捨棄、拒絕或略過輸入和輸出流量。防火牆會使用來源 IP 位址/連接埠、目的地 IP 位址/連接埠、應用程式、應用程式類別和 DSCP 標籤等參數來建立防火牆規則。

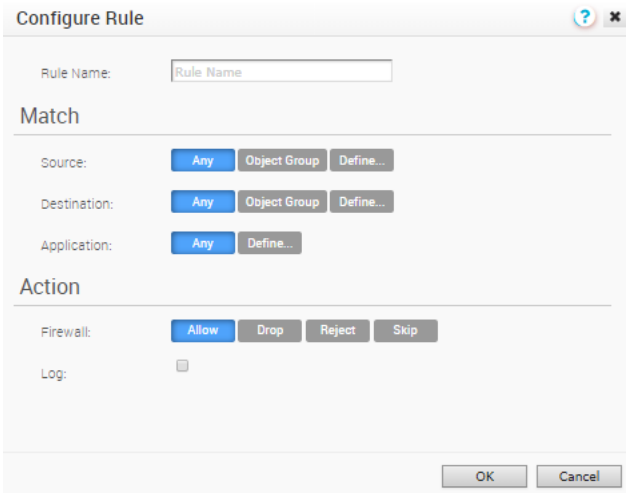
若要使用在設定檔層級啟用「可設定狀態的防火牆」的防火牆規則，請執行此程序的步驟。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)** > **防火牆 (Firewall)**。

2 為選取的設定檔啟用**可設定狀態的防火牆 (Stateful Firewall)**。

3 在**防火牆規則 (Firewall Rules)** 區域中，按一下**新增規則 (New Rule)**。**設定規則 (Configure Rule)** 對話方塊隨即出現。



4 在**規則名稱 (Rule Name)** 方塊中，輸入規則的唯一名稱。

5 在**比對 (Match)** 區域下，設定規則的比對條件：

設定	說明

來源 (Source)	允許指定封包的來源。請選取下列任一選項：
	■ **任何 (Any)** - 依預設會允許所有來源位址。
	■ **物件群組 (Object Group)** - 可讓您選取位址群組和連接埠群組的組合。
	■ **定義 (Define)** - 可讓您定義特定 VLAN、IP 位址、MAC 位址或連接埠的來源流量。對於 IP 位址，請選擇下列三個選項之一：
	  ■ **CIDR 首碼 (CIDR prefix)** - 如果您想要將網路定義為 CIDR 值 (例如：`172.10.0.0 /16`)，請選擇此選項。
	  ■ **子網路遮罩 (Subnet mask)** - 如果您想要根據子網路遮罩定義網路 (例如 `172.10.0.0 255.255.0.0`)，請選擇此選項。
	  ■ **萬用字元遮罩 (Wildcard mask)** - 如果您想要能夠將強制執行原則的範圍縮小到共用相符主機 IP 位址值之不同 IP 子網路間的一組裝置，請選擇此選項。萬用字元遮罩會根據反向的子網路遮罩比對 IP 或一組 IP 位址。遮罩的二進位值中若包含「0」，表示值是固定的，遮罩的二進位值中若包含「1」，則表示值是萬用字元 (可以是 1 或 0)。以 IP 位址為 172.0.0 的萬用字元遮罩 0.0.0.255 (二進位對等項目 = 00000000.00000000.00000000.11111111) 為例，前三個八位元數字是固定值，最後一個八位元數字是變數值。

目的地	允許指定封包的目的地。請選取下列任一選項： ■ **任何 (Any)** - 依預設會允許所有目的地位址。 ■ **物件群組 (Object Group)** - 可讓您選取位址群組和連接埠群組的組合。如需物件群組的詳細資訊，請參閱第 16 章 物件群組。 ■ **定義 (Define)** - 可讓您定義特定 VLAN、IP 位址、MAC 位址或連接埠的目的地流量。對於 IP 位址，請選擇下列三個選項之一：**CIDR 首碼 (CIDR prefix)**、**子網路遮罩 (Subnet mask)** 或**萬用字元遮罩 (Wildcard mask)**。
應用程式	允許指定要套用防火牆規則的應用程式。請選取下列任一選項： ■ **任何 (Any)** - 依預設會將防火牆規則套用至任何應用程式。 ■ **定義 (Define)** - 可讓您選取特定的應用程式。

6 在**動作 (Action)** 區域下，設定規則的動作：

設定	說明
防火牆	選取符合規則的條件時，防火牆應對封包執行的下列任一動作： ■ **允許 (Allow)** - 依預設會允許資料封包。 ■ **捨棄 (Drop)** - 無訊息地捨棄資料封包，且不傳送任何通知給來源。 ■ **拒絕 (Reject)** - 捨棄封包，並傳送明確的重設訊息以通知來源。 ■ **略過 (Skip)** - 在查閱期間略過規則，並處理下一個規則。但是，此規則會在部署 SD-WAN 時使用。
記錄	如果您想要在觸發此規則時建立記錄項目，請選取此核取方塊。

7 按一下**確定 (OK)**。

結果

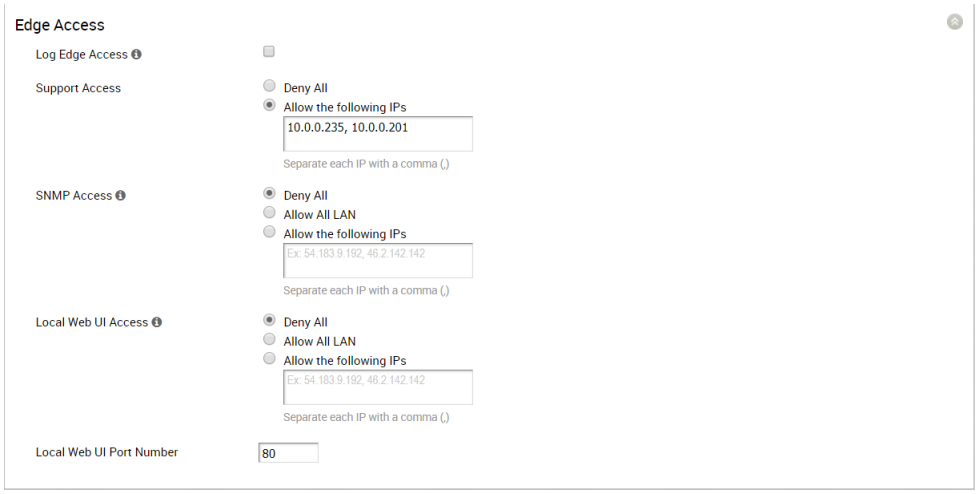
系統會為選取的設定檔建立防火牆規則，並將其顯示在**設定檔防火牆 (Profile Firewall)** 頁面的**防火牆規則 (Firewall Rules)** 區域下方。

設定 Edge 存取

設定 Edge 存取的設定檔時，您必須在防火牆設定下方選取適用於支援存取、SNMP 存取和本機 Web UI 存取的選項。基於安全考量，依預設會停用支援存取、SNMP 存取和本機 Web UI 存取。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **設定檔 (Profiles)** > **防火牆 (Firewall)**。



2 在 **Edge 存取 (Edge Access)** 區域下，選取**記錄 Edge 存取 (Log Edge Access)** 核取方塊，以記錄所有的 Edge 存取。

3 針對**支援存取 (Support Access)**，請選取**允許下列 IP (Allow the following IPs)** 選項，並明確指定可作為來源讓您使用 SSH 連線至此 Edge 的 IP 位址。

4 針對來自路由介面/WAN 的 **SNMP 存取 (SNMP Access)**，如果 SNMP 伺服器位於 LAN 中，請選擇**允許所有 LAN (Allow All LAN)** 或**允許下列 IP (Allow the following IPs)** 選項。

5 針對來自路由介面/WAN 的**本機 Web UI 存取 (Local Web UI Access)**，請選擇**允許所有 LAN (Allow All LAN)** 或**允許下列 IP (Allow the following IPs)**。

6 在**本機 Web UI 連接埠號碼 (Local Web UI Port Number)** 文字方塊中，輸入本機 Web UI 的連接埠號碼。

7 按一下**儲存變更 (Save Changes)**。

結果

後續步驟

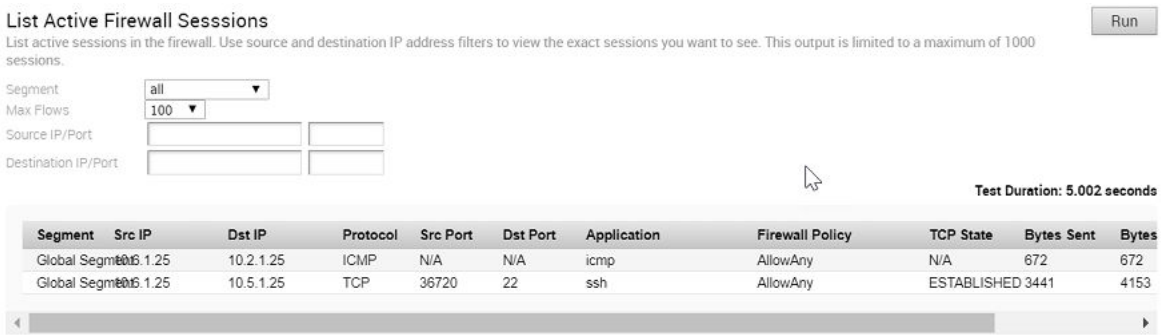
如果您想要覆寫特定 Edge 的 Edge 存取設定，請使用 **Edge 防火牆 (Edge Firewall)** 頁面上的**啟用 Edge 覆寫 (Enable Edge Override)** 選項。如需相關資訊，請參閱設定 Edge 的防火牆

對防火牆進行疑難排解

您可以在 Edge 上執行遠端診斷測試，以收集防火牆診斷記錄。

下列遠端診斷測試可用來取得防火牆診斷資訊：

- **列出作用中防火牆工作階段 (List Active Firewall Sessions)** - 列出防火牆中的作用中工作階段，如下列螢幕擷取畫面所示。



- **排清防火牆工作階段 (Flush Firewall Sessions)** - 重設防火牆中已建立的工作階段。

如需如何在 Edge 上執行遠端診斷的詳細資訊，請參閱遠端診斷。

佈建 Edge

13

本節說明如何佈建 Edge。

本章節討論下列主題：

- 佈建新的 Edge
- 啟用 Edge
- SD-WAN Edges

佈建新的 Edge

企業管理員可以佈建單一 Edge 或多個 Edge，例如將設定檔組態指派給 Edge，或變更其他 Edge 特定參數。您必須為將要部署到特定站台的每個 Edge 建立組態。

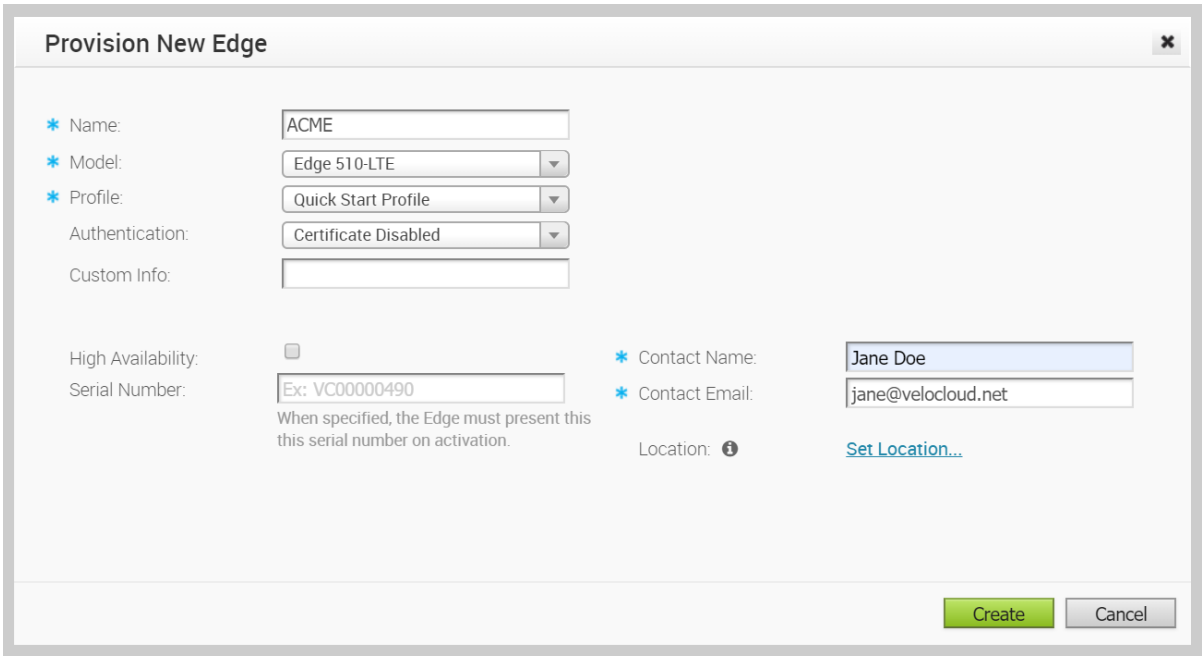
您可以執行下列步驟，從 **Edge** 畫面佈建新的 Edge：

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **Edge**。

2 在 Edge 畫面中，按一下畫面右上角的**新增 Edge (New Edge)**。

此時會顯示**佈建新的 Edge (Provision New Edge)** 對話方塊。



3 在**名稱 (Name)** 文字方塊中，輸入 Edge 的唯一名稱。

4 從**型號 (Model)** 下拉式功能表中，選取 Edge 型號。

備註 從 3.4 版開始，已可支援和佈建 Edge 510-LTE。

5 在**設定檔 (Profile)** 下拉式功能表中，選取要指派給 Edge 的設定檔。

- 如果因為推送啟用而將 Edge 預備設定檔顯示為選項，則使用此設定檔的，將會是新指派、但尚未設定生產設定檔的 Edge。
- 如果客戶具有以網路為基礎的操作員設定檔，則客戶只能佈建以網路為基礎的 Edge。此外，如果客戶具有以區段為基礎的操作員設定檔，則客戶只能佈建以區段為基礎的 Edge。(如需設定檔移轉的詳細資訊，請參閱網路到區段的移轉。如需如何建立新設定檔的詳細資訊，請參閱第 9 章 設定設定檔一節，其標題為建立設定檔)。

6 在**驗證 (Authentication)** 下拉式功能表中，選取下列其中一個選項：**已停用憑證 (Certificate Disabled)**、**選擇性憑證 (Certificate Optional)** 和**需要憑證 (Certificate Required)**，以進行以憑證為基礎的憑證。

7 在**自訂資訊 (Custom Info)** 文字方塊中，輸入與 Edge 相關聯的自訂資訊

。客戶資訊不可超過 255 個字元。

備註 企業/MSP/操作員角色 (具有 UPDATE_EDGE 權限) 的超級使用者和標準管理員使用者，可以新增或更新 Edge 的自訂資訊。

8 若要套用高可用性 (HA)，請選取**高可用性 (High Availability)** 核取方塊。(Edge 可安裝為單一獨立裝置，或與另一個 Edge 配對，以提供高可用性 (HA) 支援。如需 HA 的詳細資訊，請參閱高可用性選項一節)。

9 在**序號 (Serial Number)** 文字方塊中，輸入 Edge 的序號。如果指定，序號必須與將啟用的 Edge 序號相符。

10 在**連絡人名稱 (Contact Name)** 和**連絡人電子郵件 (Contact Email)** 文字方塊中，輸入 Edge 站台連絡人的名稱和電子郵件地址。

11 按一下**設定位置 (Set Location)** 連結，以設定 Edge 的位置。

12 按一下**建立 (Create)**。

結果

Edge 會使用啟用金鑰進行佈建。

備註 如果 Edge 裝置未使用啟用金鑰進行啟動，金鑰將在一個月後到期。如需如何啟動 Edge 的相關資訊，請參閱《Edge 啟用快速入門指南》中的設定 Edge 啟用一節。

後續步驟

按一下**建立 (Create)** 後，**Edge 概觀 (Edge Overview)** 畫面隨即出現，並且在畫面頂端顯示 Edge 啟用金鑰。若要檢視剛建立之 Edge 的概觀，或對其進行任何變更，請參閱第 14 章 Edge 概觀索引標籤一節。

佈建 Edge 之後，您可以使用**動作 (Actions)** 下拉式功能表執行下列動作：

- **新增 Edge (New Edge)** - 建立新的 Edge。
- **本機認證 (Local Credentials)** - 指派所選 Edge 的本機組態認證。
- **刪除 Edge (Delete Edge)** - 刪除選取的 Edge。
- **指派設定檔 (Assign Profile)** - 變更所選 Edge 的設定檔。
- **指派操作員設定檔 (Assign Operator Profile)** - 變更操作員設定檔。

  備註 此選項僅適用於操作員使用者。

- **更新預先通知 (Update Pre-notifications)** - 啟用或停用操作員的 Edge 警示通知。
- **Edge 授權 (Edge Licensing)** - 將授權類型指派給選取的 Edge。

  備註 超級使用者管理員和標準管理員可將授權類型指派給 Edge。

- **更新客戶警示 (Update Customer Alerts)** - 啟用或停用客戶的 Edge 警示通知。
- **重新平衡閘道 (Rebalance Gateways)** - 在企業 Edge 中重新平衡 SD-WAN 主控閘道。

  備註 此選項僅適用於操作員使用者。

如需詳細資訊，請參閱 SD-WAN Edges。

Edge 疑難排解

在 3.4 版中，如果您設定 Edge 510 LTE 裝置，您可以執行「LTE 數據機資訊」診斷測試。**LTE 數據機資訊**診斷測試將會擷取診斷資訊，例如訊號強度、連線資訊等。如需如何執行診斷測試的相關資訊，請參閱標題為**遠端診斷**一節

啟用 Edge

VMware 解決方案支援兩種 SD-WAN Edge 部署和啟用方法：零接觸佈建和電子郵件。

活動	電子郵件 (辦公室管理員啟用)	零接觸佈建 (中央 NOC 啟用)
不需要 IT 造訪	✓	✓
不需要預先準備	✓	✓
裝置遺失時不會有安全性風險	✓	✓
不需要站對站連結設定檔	✓	✓
不需要裝置追蹤	✓	
需要傳送電子郵件給辦公室管理員	✓	
需具備裝置到站台的知識	✓	✓

使用零接觸佈建來啟用 Edge (技術預覽)

在這種方法中，會啟用 SD-WAN Edge，而不需要辦公室管理員按一下啟用連結。

在下列這些案例中，您需要使用「零接觸佈建」方法來啟用 SD-WAN Edge：

- 服務提供者將站台上裝置的實體安裝委外處理時 (在多數情況下，只要接上纜線和電源即可)。裝置的安裝人員可能既不是客戶的員工，也不是服務提供者。
- 當遠端站台的人員無法將筆記型電腦/平板電腦/手機連線至 SD-WAN Edge，因而無法使用電子郵件，或無法點按啟用代碼/URL 時。

備註 若要讓零接觸佈建推送啟用正常運作，請使用 Orchestrator 軟體 4.3.0 版或更新版本。

如需有關如何使用「零接觸佈建」方法來啟用 Edge 的詳細資料，請連絡 VMware 客戶支援。

使用電子郵件來啟用 Edge

使用此方法時，SD-WAN Edge 在交付至客戶站台時會隨附原廠預設的組態。在啟用之前，SD-WAN Edge 不會包含任何用來連線至企業網路的組態或認證。

完成以下工作，以使用電子郵件來啟用 SD-WAN Edge：

1 傳送啟用電子郵件。

管理員會將啟用程序電子郵件傳送給即將安裝 Edge 的人員 (通常是站台連絡人)，以用於起始啟用程序。

2 啟用 Edge 裝置。

依照啟用程序電子郵件中的指示操作的人員，將會啟用 Edge 裝置。

完成下列有關 Edge 啟用程序的指示。

傳送啟用電子郵件

啟動 Edge 的程序從起始啟用程序電子郵件開始，此郵件會由 IT 管理員傳送給站台連絡人。

若要傳送啟用程序電子郵件：

1 移至 Orchestrator 中的**設定 (Configure) > Edge**。

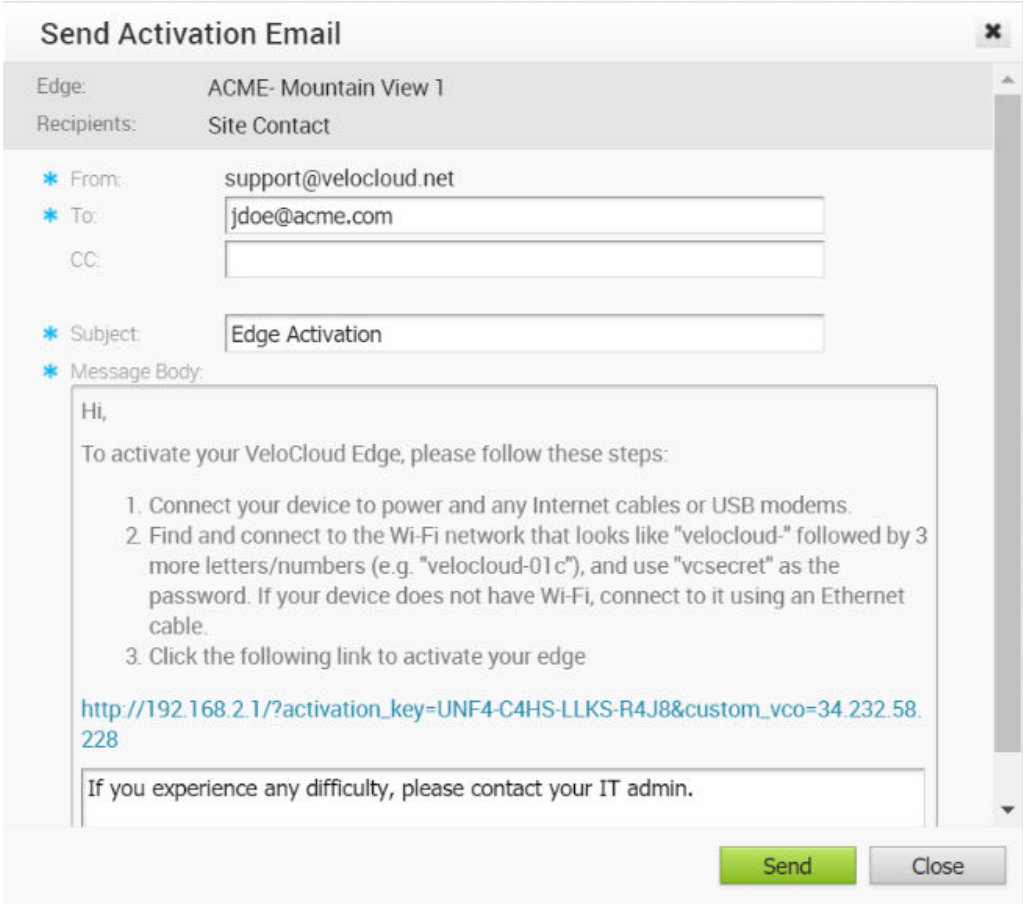
2 選取您要啟動的 Edge。**Edge 概觀索引標籤 (Edge Overview Tab)** 視窗隨即出現。

3 您也可以選擇性地在**內容 (Properties)** 區域中，輸入將在**序號 (Serial Number)** 文字欄位中啟動的 Edge 序號。序號區分大小寫，因此請確定「VC」為大寫。

備註 此為選用步驟。但若已指定，則序號必須與啟動的 Edge 相符。

4 按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕，將啟用電子郵件傳送至站台連絡人。

5 **傳送啟用電子郵件 (Send Activation Email)** 快顯視窗隨即出現。其中說明站台連絡人為了啟動 Edge 裝置所需完成的步驟。



備註 在 3.4 版中，如果已設定 Edge 510 LTE 裝置，則啟用電子郵件將會包含手機設定 (例如，SIM 卡 PIN 碼、網路、APN、使用者名稱)。

6 按一下**傳送 (Send)** 按鈕，將啟用程序電子郵件傳送至站台連絡人。

備註 如果您設定 Edge 510 LTE 裝置，則可以執行「LTE 數據機資訊」診斷測試以進行疑難排解。**LTE 數據機資訊**診斷測試將會擷取診斷資訊，例如訊號強度、連線資訊等。如需如何執行診斷測試的相關資訊，請參閱標題為遠端診斷一節。

啟動 Edge 裝置

站台連絡人會執行 Edge 啟用程序電子郵件中概述的步驟。

一般而言，站台連絡人會完成下列步驟：

1 將 Edge 裝置連線至電源，並插入任何網際網路纜線或 USB 數據機。

2 找出並連線至看起來像 `velocloud-` 再加上三個字母/數字 (例如 `velocloud-01c`) 的 Wi-Fi 網路，並使用密碼 `vcsecret` 進行連線。

3 按一下電子郵件中的超連結以啟用 Edge。

備註 參考 Edge 裝置中的 Wi-Fi SSID。預設的 Wi-Fi 為 `vc-wifi`。Edge 啟用電子郵件提供了使用一或多個 Wi-Fi 連線的指示。

Edge 啟用電子郵件可能會提供用來連線 WAN 纜線和 USB 數據機、將裝置連線至 LAN 連線，以及將其他網路裝置連線至 Edge 的特定指示。如需詳細程序，請參考下列各節：

使用 iOS 裝置和乙太網路纜線啟用 Edge

使用 Android 裝置和乙太網路纜線啟用 Edge

在 Edge 啟用期間會顯示啟用狀態畫面。

Edge 會從 SD-WAN Orchestrator 下載組態和軟體。Edge 成功啟動，且可供服務使用。Edge 已啟用後，將「可用來」路由網路流量。此外也啟用多項進階功能，例如監控、測試和疑難排解。

使用 iOS 裝置和乙太網路纜線啟用 Edge

有多種方式可啟用 VMware SD-WAN Edge。建議盡可能使用零接觸佈建推送啟用。或者，您也可以使用電子郵件啟用 (提取啟用) 方法，透過 iOS 裝置和乙太網路纜線來啟用。

必要條件

此程序所需的元件包括：

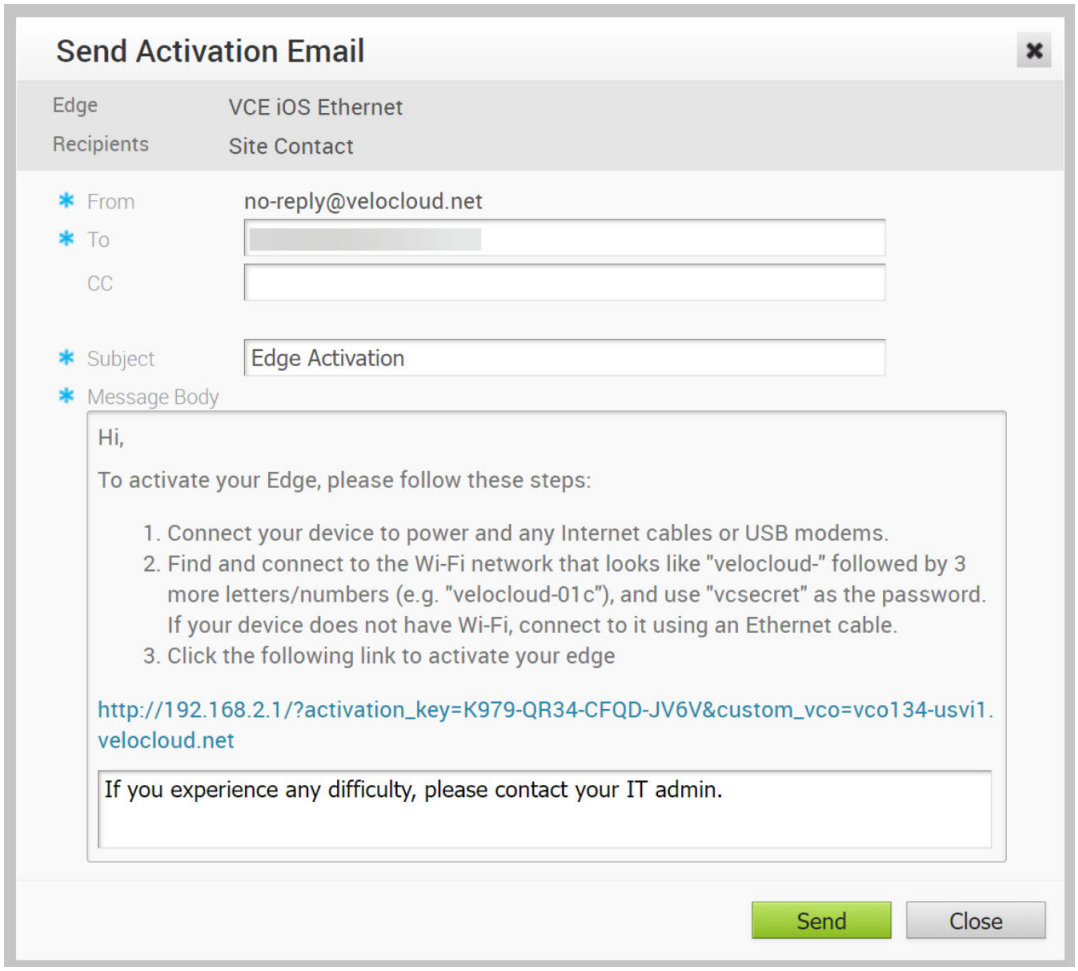
- 具有電子郵件存取權的 iPhone/iPad
- 適用於手機或平板電腦的乙太網路介面卡

備註 此處使用的範例是 Edge 540 和 iPhone 12 Pro Max。您也可以使用其他 Edge 和 iPhone/iPad 型號。

程序

1 在 Orchestrator 軟體上完成 Edge 組態。如需詳細資料，請參閱第 15 章 設定 Edge 裝置。

2 導覽至 **設定 (Configure)** > **Edge** > **Edge 概觀 (Edge Overview)** 索引標籤，然後按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕。



3 輸入人員用來啟用 Edge 的電子郵件地址，然後按一下**傳送 (Send)**。

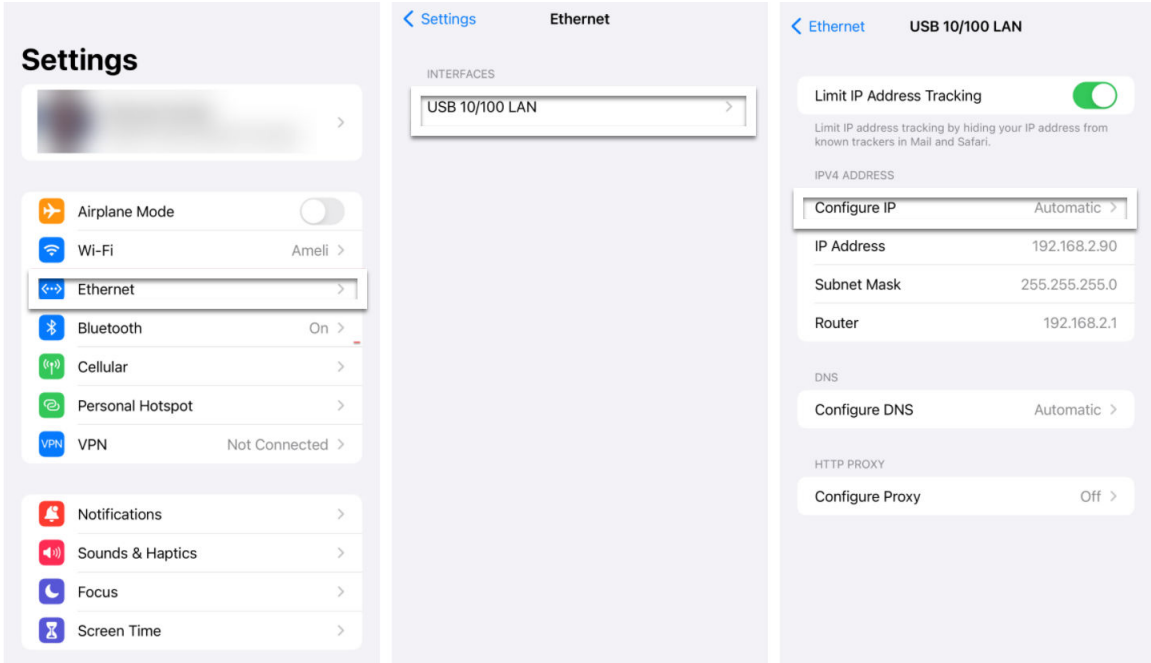
4 開啟 Edge 電源，然後使用乙太網路纜線將其連線至可用的網際網路連線。

備註 請參閱《Edge 啟用指南》，查看要安裝的型號的詳細資料以確定正確的連接埠。

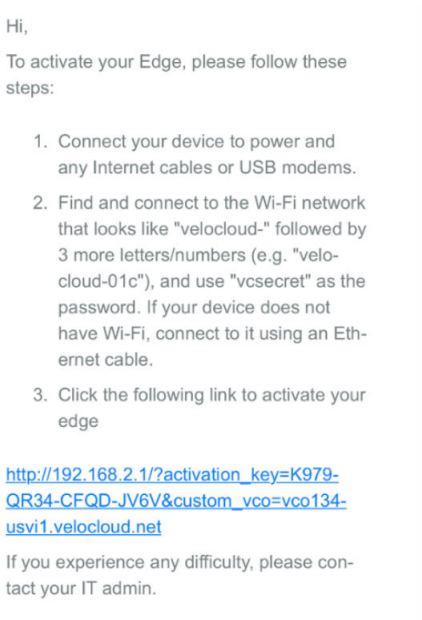
5 將乙太網路介面卡連線至手機，然後將 Edge 的 LAN 連接埠連線至乙太網路介面卡。

備註 依預設，Edge 會設定為從 WAN (上行) 上的 ISP 取得 DHCP IP 位址。Edge 還會為連線至 LAN 連接埠的手機指派 DHCP 位址。當 WAN 連線完整運作時，位於 Edge 前方的雲端 LED 燈會變成綠色。

6 在 iOS 裝置中，移至**設定 (Settings) > 乙太網路 (Ethernet)**。選取適當的介面。在 [IPv4 位址 (IPv4 Address)] 下，將**設定 IP (Configure IP)** 選取為**自動 (Automatic)**。



7 從手機中開啟啟用電子郵件，然後按一下螢幕底部顯示的啟用連結以啟用 Edge。下列螢幕擷取畫面為範例。



8 您可以在手機螢幕上查看啟用進度。完成後，將顯示**啟用成功 (Activation successful)** 訊息。

結果

您的 Edge 裝置現在已啟用。

使用 Android 裝置和乙太網路纜線啟用 Edge

下列程序說明使用 Android 裝置和乙太網路纜線的 Edge 電子郵件啟用 (提取啟用)。

必要條件

此程序所需的元件包括：

- 具有電子郵件存取權的 Android 手機
- 適用於手機的乙太網路介面卡

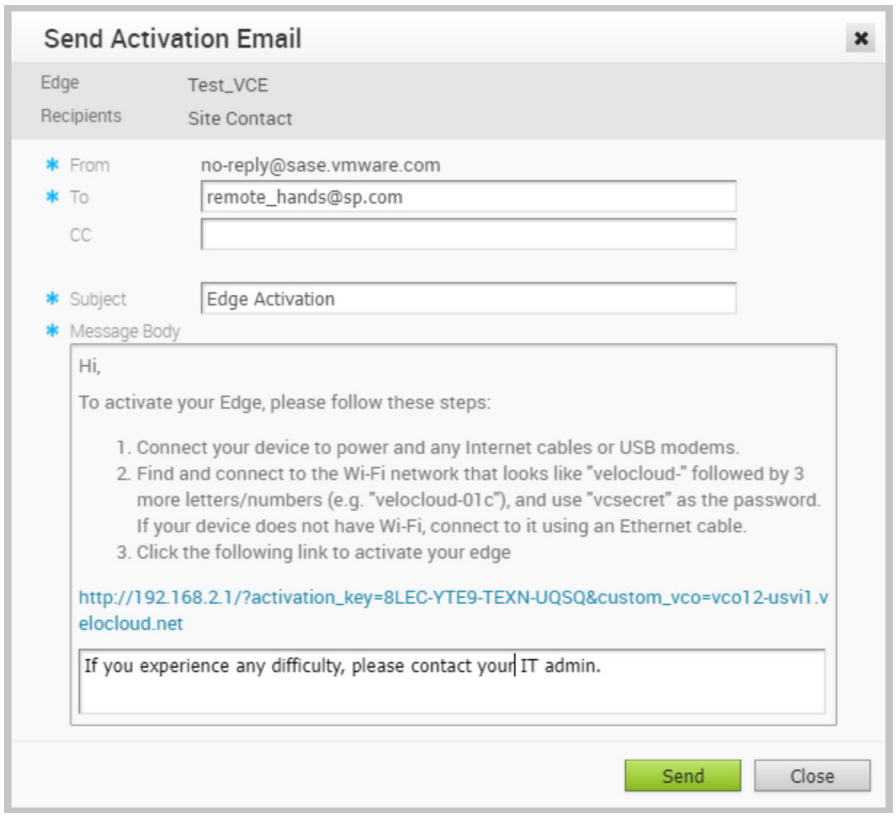
備註 此處使用的範例是 Edge 610 和 Samsung Galaxy S10+ 智慧型手機。您也可以使用其他 Edge 和 Android 手機型號。

程序

1 在 Orchestrator 軟體上完成 Edge 組態。如需詳細資料，請參閱第 15 章 設定 Edge 裝置。

2 導覽至 **設定 (Configure) > Edge > Edge 概觀 (Edge Overview)** 索引標籤，然後按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕。

3 輸入人員用來啟用 Edge 的電子郵件地址，然後按一下**傳送 (Send)**。



4 開啟 Edge 電源，然後使用乙太網路纜線將其連線至可用的網際網路連線。

備註 請參閱《Edge 啟用指南》，查看要安裝的型號的詳細資料以確定正確的連接埠。

5 將乙太網路介面卡連線至手機，然後將 Edge 的 LAN 連接埠連線至乙太網路介面卡。

備註 依預設，Edge 會設定為從 WAN (上行) 上的 ISP 取得 DHCP IP 位址。Edge 還會為連線至 LAN 連接埠的手機指派 DHCP 位址。當 WAN 連線完整運作時，位於 Edge 前方的雲端 LED 燈會變成綠色。

6 從手機中開啟啟用電子郵件，然後按一下螢幕底部顯示的啟用連結以啟用 Edge。下列螢幕擷取畫面為範例。

Hi,
To activate your Edge, please follow these steps:
1. Connect your device to power and any Internet cables or USB modems.
2. Find and connect to the Wi-Fi network that looks like "velocloud-" followed by 3 more letters/numbers (e.g. "velocloud-01c"), and use "vcsecret" as the password. If your device does not have Wi-Fi, connect to it using an Ethernet cable.
3. Click the following link to activate your edge

http://192.168.2.1/?activation_key=9CLJ-GVS4-X3NE-8CMR&custom_vco=vco12-usvi1.velocloud.net

If you experience any difficulty, please contact your IT admin.

7 您可以在手機螢幕上查看啟用進度。完成後，將顯示**啟用成功 (Activation successful)** 訊息。

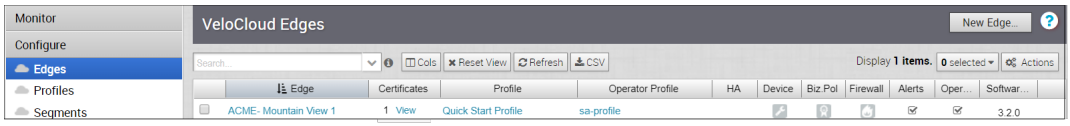
結果

您的 Edge 裝置現在已啟用。

SD-WAN Edges

SD-WAN Edges 的 [組態 (Configuration)] 畫面會列出企業網路中所有已佈建的 Edge，也讓您可按一下畫面右上角的**新增 Edge (New Edge)** 按鈕來佈建新的 Edge。您也可以在此處選取 Edge 並執行各種動作，例如變更本機認證、刪除 Edge、指派設定檔、指派操作員設定檔、啟用預先通知等 (使用**動作 (Actions)** 下拉式功能表)。

下方的企業 Edge 識別 (Enterprise Edges Identification) 資料表詳細列出此畫面上顯示的每個欄位和按鈕。



備註 如果您使用具有客戶支援權限的使用者識別碼登入，您將只能檢視 SD-WAN Orchestrator 物件。您將無法建立新的物件，也無法設定/更新現有物件。

企業 Edge 畫面識別碼資料表

大部分的資料行標頭都有排序功能，可依字母順序、數字順序或類型列出資料行中的項目。([裝置 (Device)]、[Biz 原則 (Biz Policy)]、[防火牆 (Firewall)]、[警示 (Alerts)] 和 [操作員警示 (Operator Alerts)] 資料行沒有此功能)。按一下具有此功能的資料列標頭，即可對清單進行排序。

選項	說明
Edge	顯示 Edge 的名稱。按一下 **Edge** 資料行標頭，可依字母順序對 Edge 清單進行排序。Edge 名稱也是一個連結；按一下連結即會開啟第 14 章 Edge 概觀索引標籤畫面。選取 Edge 名稱旁邊的核取方塊，以選取 Edge。
憑證 (Certificates)	顯示 Edge 目前和已到期的憑證。按一下憑證數目旁邊的**檢視連結 (View link)**，可取得詳細資訊。
設定檔 (Profile)	列出指派給 Edge 的設定檔。設定檔名稱也是一個連結；按一下連結會開啟 設定檔概觀畫面 索引標籤畫面。附註：如果由於〈推送啟用〉而顯示了 Edge 預備設定檔，則此設定檔將由新指派、但尚未設定生產設定檔的 Edge 來使用。企業管理員必須手動將設定檔指派給這些 Edge。如需如何手動將設定檔指派給 Edge 的指示，請參閱標題為〈指派設定檔 (變更設定檔)〉一節。
操作員設定檔 (Operator Profile)	此資料行只有操作員可看見。操作員設定檔是操作員在建立客戶時指派給客戶的範本。其中包括 Edge 的軟體映像、應用程式對應、閘道選取和管理設定。操作員層級的管理員可以變更特定 Edge 的操作員設定檔。企業管理員具有唯讀存取權。操作員設定檔名稱也是一個連結；按一下連結會開啟操作員設定檔 (Operator Profiles) 畫面。
HA	選取 **HA** 核取方塊可啟用主動備用 HA 選項。
裝置 (Device)	如果已設定 Edge 特定組態，則會顯示藍色的 圖示。顯示灰色 圖示，以指出所有設定 (若有的話) 都已繼承自設定檔。若要導覽至**裝置 (Device)** 設定畫面，請按一下**裝置 (Device)** 資料行中的圖示，然後按一下**裝置 (Device)** 索引標籤。
Biz 原則 (Biz Policy)	如果已設定商務原則規則，則會顯示藍色的 圖示。顯示灰色 圖示，以指出所有規則 (若有的話) 都已繼承自設定檔。若要導覽至**商務原則 (Business Policy)** 畫面，請按一下 **Biz 原則 (Biz Policy)** 資料行中的圖示，然後按一下**商務原則 (Business Policy)** 索引標籤。
防火牆 (Firewall)	如果已設定防火牆規則，則會顯示藍色的 圖示。顯示灰色 圖示，以指出所有規則 (若有的話) 都已繼承自設定檔。 如果防火牆已停用，則會在 圖示上顯示紅色斜線。防火牆停用時，表示它已在 Edge 的設定檔組態中關閉。若要開啟防火牆，請移至設定檔組態 (**設定 (Configure)** > **設定檔 (Profiles)** > **防火牆 (Firewall)** 索引標籤)。 若要導覽至**防火牆 (Firewall)** 畫面，請按一下**防火牆 (Firewall)** 資料行中的圖示，然後按一下**防火牆 (Firewall)** 索引標籤。
警示 (Alerts)	如果已啟用 Edge 的客戶警示，則會在此資料行中勾選**警示 (Alerts)** 核取方塊。在 **Edge** 資料行中按一下 Edge 的名稱，可開啟第 14 章 Edge 概觀索引標籤以啟用或停用客戶警示。
操作員警示 (Operator Alerts)	如果已啟用 Edge 的操作員警示，則會在此資料行中勾選**操作員警示 (Operator Alerts)** 核取方塊。在 **Edge** 資料行中按一下 Edge 的名稱，可開啟第 14 章 Edge 概觀索引標籤以啟用或停用操作員警示。
軟體版本 (Software Version)	Edge 的軟體版本將會顯示在此資料行中。
原廠軟體版本 (Factory Software Version)	Edge 從原廠運送時，會隨附預設軟體版本。
組建編號 (Build Number)	顯示已啟動 Edge 的組建編號。
型號 (Model)	顯示 Edge 的型號類型。
序號 (Serial Number)	顯示 Edge 的序號。將序號指派給 Edge 是選擇性的。如果未將序號指派給 Edge，此欄位將會呈現為空白。
已建立 (Created)	顯示佈建 Edge 的日期和時間。
已啟動 (Activated)	顯示啟動 Edge 的日期和時間。

選項	說明
上次連絡 (Last Contact)	Edge 上次與 SD-WAN Orchestrator 通訊的日期和時間。
資料行 (Cols) (Column (Cols))	按一下 **Cols** 按鈕，以選取您想要在企業 Edge 清單中顯示的選項 (請參閱上圖)。
重設視圖 (Reset View)	將企業 Edge 清單重設為預設視圖。(這將會移除篩選器，並將從 **Cols** 按鈕下拉式功能表中選取的任何選項重設為預設視圖)。
重新整理 (Refresh)	使用伺服器中目前的資料重新整理企業 Edge 清單。
CSV	若要匯出企業 Edge 清單中顯示的內容，請按一下 **CSV** 按鈕。
已選取 (Selected)	指出從 **Edge** 資料行中選取的 Edge 數目。按一下**已選取 (Selected)** 按鈕，可選取 **Edge** 資料行中列出的所有 Edge，或全部取消選取。
動作 (Actions)	列出下列您可以對所選 Edge 執行的動作： ■ **新增 Edge (New Edge)** ■ **本機認證 (Local Credentials)** ■ **刪除 Edge (Delete Edge)** ■ **指派設定檔 (Assign Profile)** ■ **指派操作員設定檔 (Assign Operator Profile)** ■ **更新預先通知 (Update Pre-notifications)** ■ **Edge 授權 (Edge Licensing)** ■ **更新客戶警示 (Update Customer Alerts)** ■ **重新平衡閘道 (Rebalance Gateways)** **備註** 指派操作員設定檔和重新平衡閘道是僅適用於操作員層級的功能。 如需詳細資訊，請參閱佈建新的 Edge。
新增 Edge (New Edge)	開啟**佈建新的 Edge (Provision New Edge)** 對話方塊，以佈建新的 Edge。 如需詳細資訊，請參閱佈建新的 Edge。
說明 (Help)	按一下**問號 (Question Mark)** 圖示可存取此功能的線上說明。

將 Edge 重設為原廠設定

基於若干原因，SD-WAN Edges 必須重設為原廠設定，其中的部分原因如下：

- 為另一個站台重新規劃 Edge 時，您必須清除現有的組態，使 Edge 能夠在新站台啟動。
- 您的站台發生問題，因此 VMware SD-WAN 支援建議您執行硬重設以將 Edge 還原為原廠設定，並在站台重新啟動 Edge 以嘗試解決問題。
- Edge 無法存取或沒有回應，且在多次重新開機後仍無法解決問題。建議您執行硬重設以將 Edge 還原為原廠設定以嘗試解決問題。

您可以使用下列其中一種方法將 Edge 重設為原廠設定：

- 軟重設或停用 — Edge 會停用，並且會完全移除 Edge 使用的所有現有組態。Edge 此時會使用原始的原廠組態。不過，Edge 軟體不受影響，且會保留在軟重設之前具備的軟體版本。軟重設的 Edge 可在其他站台或相同的站台上重新啟動。

- 硬重設 — Edge 會完全重設為原廠設定，即 Edge 不僅會停用並使用原廠組態，也會將 Edge 軟體變更為原廠軟體版本。Edge 的狀態實際上與剛出廠時一樣。

如果您重設站台正在使用的 Edge，您將完全失去站台上的用戶端裝置連線，直到您在站台上重新啟動相同的 Edge，或在站台上啟動其他 Edge 為止。

如需如何將 Edge 重設為原廠設定的指示，請參閱如何將 VMware SD-WAN Edge 重設為原廠預設值。

Edge 概觀索引標籤

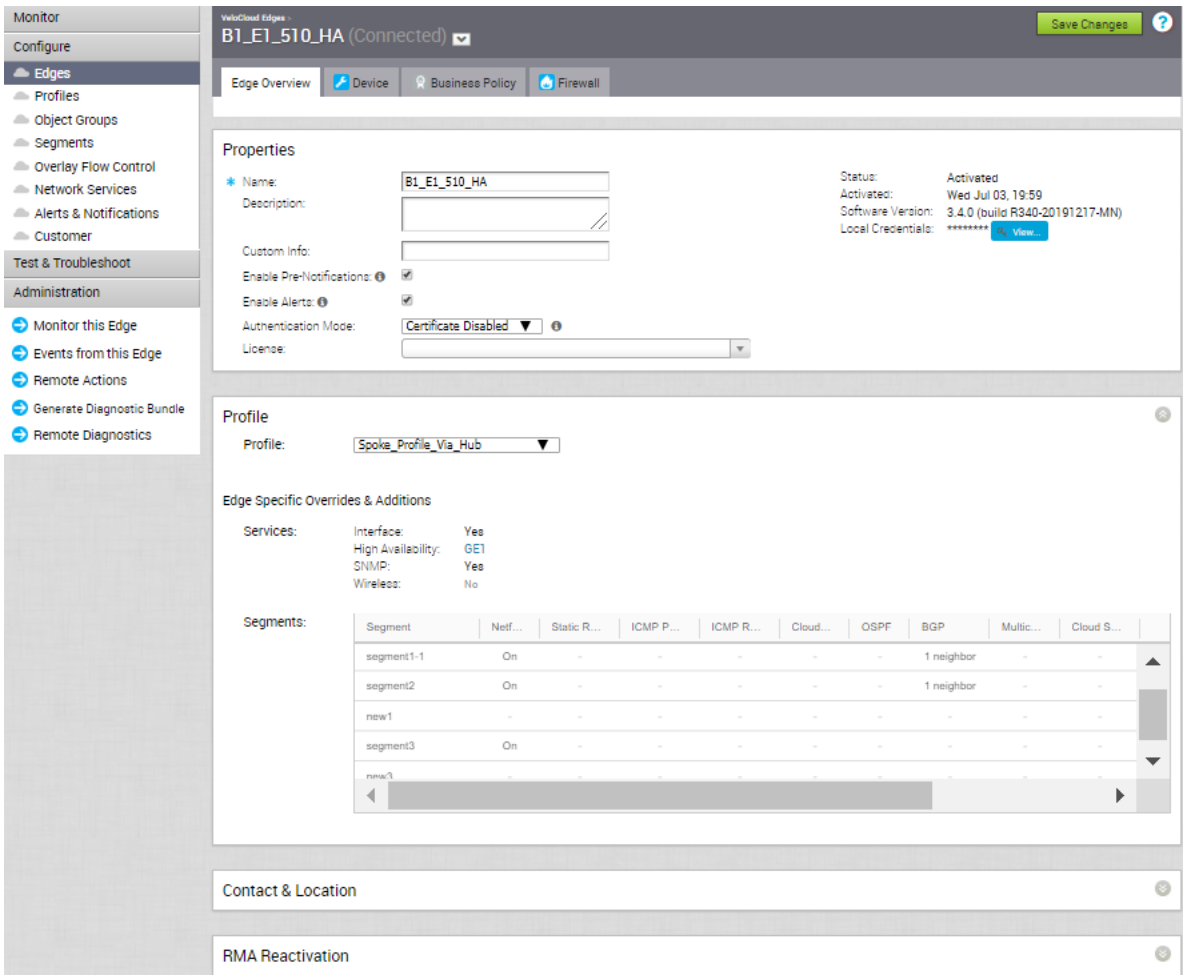
14

Edge 概觀 (Edge Overview) 索引標籤會提供 Edge 特定的內容資訊，例如名稱、說明、自訂資訊、與 Edge 相關聯的設定檔、Edge 站台連絡人的名稱和電子郵件地址。在 **Edge 概觀 (Edge Overview)** 索引標籤中，您可以傳送 Edge 啟用電子郵件、啟用特定 Edge 的警示、對特定內容進行變更、將不同的設定檔指派給選取的 Edge、設定 Edge 位置、更新 Edge 連絡人和位置資訊，以及要求 RMA 重新啟用。

若要存取 **Edge 概觀 (Edge Overview) 索引標籤**：

1 在 SD-WAN Orchestrator 的導覽面板上，移至**設定 (Configure) > Edge**。

2 在**企業 Edge (Enterprise Edge)** 畫面中，按一下 Edge 以開啟 **Edge 概觀索引標籤 (Edge Overview Tab)**。



在 **Edge 概觀索引標籤 (Edge Overview Tab)** 上：

- 若要啟用特定 Edge 的警示，或傳送 Edge 啟用電子郵件，請參閱〈Edge 概觀內容〉和〈起始 Edge 啟用〉小節。
- 若要檢視特定設定檔的 Edge 覆寫概觀，或者需要變更為不同的設定檔，請參閱〈Edge 設定檔〉一節。
- 若要變更 Edge 的連絡人、位置或運送地址，請參閱〈Edge 連絡人和位置〉一節。
- 若要要求 RMA 重新啟用，請參閱〈RMA 重新啟用〉一節。

以下幾節將詳細說明 **Edge 概觀 (Edge Overview)** 索引標籤的每個區域。

Edge 概觀內容

在**內容 (Properties)** 區域中，您可以藉由傳送 Edge 啟用電子郵件來起始 Edge 啟用程序，也可以檢視和變更所選 Edge 的特定內容。Edge 狀態、啟用日期和軟體版本也會顯示在此區域中。

下表說明**內容 (Properties)** 區域中的欄位。

欄位/核取方塊	說明
名稱	顯示 Edge 在客戶層級上的唯一名稱。如果變更 Edge 的名稱，請記得按一下**儲存變更 (Save Changes)** 按鈕。
說明	可讓您提供 Edge 的相關資訊。如果您對 Edge 說明進行更新，請記得按一下**儲存變更 (Save Changes)** 按鈕。 **備註** 這是唯一會顯示 Edge 說明的位置。
自訂資訊	顯示與 Edge 相關聯的自訂資訊。
啟用預先通知 (Enable Pre-Notifications) 核取方塊	依預設會在 Edge 佈建後啟用此核取方塊。 若要讓操作員接收警示，則必須勾選**啟用預先通知 (Enable Pre-Notifications)** 核取方塊，且必須透過**設定 (Configure) > 警示和通知 (Alerts & Notifications)** 上的電子郵件、SMS 或 SNMP 設陷選取並啟用警示。 除了接收電子郵件、SMS 或 SNMP 設陷以外，也可以在**監控 (Monitor) > 警示 (Alerts)** 的**警示 (Alerts)** 畫面上檢視警示。取消勾選此核取方塊，可為所選 Edge 的操作員停用警示通知。
啟用警示 (Enable Alerts) 核取方塊	依預設會在 Edge 佈建後啟用此核取方塊。 若要讓客戶接收 Edge 裝置警示，則必須勾選**啟用警示 (Enable Alerts)** 核取方塊，且必須透過**設定 (Configure) > 警示和通知 (Alerts & Notifications)** 上的電子郵件、SMS 或 SNMP 設陷選取並啟用警示。 除了接收電子郵件、SMS 或 SNMP 設陷以外，也可以在**監控 (Monitor) > 警示 (Alerts)** 的**警示 (Alerts)** 畫面上檢視警示。取消勾選此核取方塊，可停用所選 Edge 的警示。
驗證模式 (Authentication Mode)	驗證模式有三個選項 (已停用憑證、選擇性憑證、需要憑證)。 ■ **已停用憑證 (預設值)：(Certificate Disabled (default):)**如果選取 [已停用憑證 (Certificate Disabled)] 選項，則 Edge 將使用驗證的預先共用金鑰模式。 ■ **選擇性憑證：(Certificate Optional:)**如果選取 [選擇性憑證 (Certificate Optional)] 選項，則 Edge 將使用 PKI 憑證或預先共用金鑰 (視另一個 Edge 或閘道所使用的憑證而定)。 **備註** 操作員必須在 [設定 (Configure)] > [客戶 (Customers)] 上啟用 PKI。 ■ **需要憑證：(Certificate Required:)**Edge 取得有效憑證後，[需要憑證 (Certificate Required)] 就會成為下拉式功能表中的可用選項。如果選取 [需要憑證 (Certificate Required)] 選項，則 Edge 將使用 PKI 憑證作為驗證模式。 **備註** 操作員必須在**設定 (Configure) > 客戶 (Customers)** 上啟用 PKI。
授權 (License)	**授權 (License)** 下拉式功能表會顯示可指派給 Edge 的可用授權類型。 **備註** 標準管理員超級使用者和標準管理員可以指派及監控已指派給他們的 Edge 授權類型。
檢視憑證 (View Certificate)	如果 Edge 具備有效憑證，則會顯示**檢視 (View)** 連結。按一下**檢視 (View)** 連結可檢視、匯出或撤銷憑證。
狀態 (Status)	顯示下列狀態選項：[擱置中 (Pending)]、[已啟動 (Activated)]、[重新啟用擱置中 (Reactivation Pending)]。 ■ **擱置中：(Pending:)**Edge 尚未啟動。 ■ **已啟動：(Activated:)**Edge 已啟動。 ■ **重新啟用擱置中：(Reactivation Pending:)**如果按一下**要求重新啟用 (Request Reactivation)** 按鈕，狀態將會變更為 [重新啟用擱置中 (Reactivation Pending)]。此狀態更新並不會變更 Edge 的功能，而只會指出有新的或取代的 Edge 可使用現有的組態來啟動。
已啟動 (Activated)	顯示啟動 Edge 的日期和時間。
軟體版本 (Software Version)	顯示 Edge 的軟體版本和組建編號。

欄位/核取方塊	說明
本機認證 (Local Credentials)	顯示本機 UI 的認證。預設認證為使用者名稱 admin 和密碼 admin123 (區分大小寫)。按一下**檢視 (View)** 按鈕可變更認證。
序號 (Serial Number)	如果 Edge 處於閒置中狀態，則會顯示**序號 (Serial Number)** 文字欄位。輸入序號是選擇性的，但如果指定，序號必須與將啟用的 Edge 序號相符。
啟用金鑰 (Activation Key)	如果 Edge 處於閒置中狀態，則會顯示 Edge 啟用金鑰。啟用金鑰的有效期只有一個月。一個月後金鑰即到期，屆時會有警告訊息顯示在啟用金鑰下方。您可以按一下位於警告訊息下方的**產生新的啟用金鑰 (Generate New Activation Key)** 按鈕，以產生新的金鑰。 如需詳細資訊，請參閱〈到期的 RMA 啟用金鑰〉一節。
傳送啟用電子郵件	當您按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕時，將會有包含啟用指示的電子郵件傳送給站台連絡人。

起始 Edge 啟用

儲存 Edge 組態後，即會指派啟用金鑰。在**內容 (Properties)** 區域中，按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕，以起始 Edge 啟用程序。按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕並不會啟動 Edge，僅會傳送電子郵件給站台連絡人以指示啟動 Edge 裝置的方法，進而起始啟用程序。

按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕後，快顯視窗會顯示將傳送給站台連絡人的電子郵件。電子郵件中提供協助站台連絡人連線並啟動 Edge 硬體的指示。如需如何啟動 Edge 的詳細資訊，請參閱線上說明中的《Edge 啟用快速入門指南》。如需提取啟用和推送啟用的相關資訊，請參閱〈零接觸佈建〉。

Edge 設定檔

設定檔 (Profile) 下拉式功能表會顯示可指派給特定 Edge 的設定檔清單。切換至 Edge 上的其他設定檔時，除了 Edge 覆寫組態以外，所有相關組態都將變更。覆寫的組態會顯示在**設定檔 (Profile)** 區域中。

備註 切換至不同的設定檔時，將不會變更 Edge 已覆寫的組態。

備註 如果由於推送啟用而將 Edge 預備設定檔顯示為選項，那將會是新指派且尚未由生產設定檔設定的 Edge。企業管理員必須從**設定檔 (Profile)** 下拉式功能表中選擇新的設定檔，以手動將設定檔指派給那些 Edge。

操作員設定檔選取

下表提供客戶所指派操作員設定檔與 Edge 所指派企業設定檔的相容性對照表。切換設定檔時，請參閱此對照表。

操作員設定檔選取對照表 (Operator Profile Selection Matrix)

客戶操作員設定檔類型	目前的 Edge 企業設定檔 (Current Edge Enterprise Profile)	選取的 Edge 企業設定檔 (Selected Edge Enterprise Profile)	結果
以區段為基礎	以區段為基礎	以區段為基礎	無變更
以網路為基礎	以網路為基礎	以網路為基礎	無變更
以區段為基礎	以網路為基礎	以區段為基礎	Edge 組態將轉換為以區段為基礎的組態。不過，在 Edge 軟體映像更新至 ≧ 3.0 版之前，組態將不會傳遞到 Edge。
以網路為基礎	以網路為基礎	以區段為基礎	Edge 組態將轉換為以區段為基礎的組態。不過，在 Edge 軟體映像更新至 ≧ 3.0 版之前，組態將不會傳遞到 Edge。
以區段為基礎	以網路為基礎	以網路為基礎	Edge 將不會接收映像更新。
以網路為基礎	以區段為基礎	以區段為基礎	Edge 將不會接收映像更新。

Edge 覆寫表示對 Edge 層級上繼承的設定檔組態進行變更。Edge 新增是不會包含在設定檔中的組態，但會新增至選取的 Edge。所有 Edge 覆寫和新增的摘要會顯示在 [設定檔 (Profile)] 區域中

Edge 連絡人和位置

連絡人和位置 (Contact & Location) 區域會顯示 Edge 連絡資訊和位置，此外也可讓您變更 Edge 位置和運送地址。

若要變更 Edge 位址：

1 按一下**更新位置 (Update Location)** 連結。

2 在**設定 Edge 位置 (Set Edge Location)** 快顯視窗中，使用**搜尋位址 (Search Address)** 功能 (依預設選取) 更新位置，或藉由手動輸入位址來更新。

3 如果您選擇手動輸入位址，請按一下**手動位址輸入 (Manual Address Entry)** 按鈕，然後輸入位址或輸入緯度和經度。

4 如果您選擇輸入位址，請按一下**從位址更新經緯度 (Update Lat,Lng From Address)** 按鈕。

5 如果您選擇輸入緯度和經度，請按一下**從經緯度更新位址 (Update Address From Lat,Lng)** 按鈕。

6 完成後，按一下**確定 (OK)**。

如果運送地址與 Edge 位置不同，請取消選取運送地址的**同上 (Same as above)** 核取方塊，然後在適當的文字欄位中輸入運送連絡人。

若要變更 Edge 送貨位置：

1 按一下**設定位置 (Set Location)** 連結。

2 在 **Edge 運送位置 (Edge Shipping Location)** 快顯視窗中，使用**搜尋位址 (Search Address)** 功能 (依預設選取) 更新位置，或藉由手動輸入位址來更新。

3 如果您選擇手動輸入位址，請按一下**手動位址輸入 (Manual Address Entry)** 按鈕，並輸入位址，然後按一下**更新地圖上的位置 (Update Location on Map)** 按鈕。

4 按一下**確定 (OK)**。

RMA 重新啟用

在下列情況下，您可以從 **Edge 概觀索引標籤 (Edge Overview Tab)** 起始 Edge RMA 重新啟用要求：

- 因發生故障而取代 Edge
- 升級 Edge 硬體型號

若要完成 RMA 重新啟用程序：

1 在 Orchestrator 中，移至**設定 (Configure) > Edge**。

2 選取要重新啟用的 Edge。

3 在 **Edge 概觀索引標籤 (Edge Overview Tab)** 中，向下捲動至畫面底部的 **RMA 重新啟用 (RMA Reactivation)** 區域。按一下右上方的灰色箭頭以展開區域。

4 按一下**要求重新啟用 (Request Reactivation)** 按鈕。此步驟會產生新的啟用金鑰，並將 Edge 狀態置於 [重新啟用擱置中 (Reactivation Pending)] 模式。

備註 重新啟用金鑰的有效期間只有重新啟用要求提出後的一個月。

5 若基於任何原因需要取消啟用要求，請按一下**取消重新啟用要求 (Cancel Reactivation Request)** 按鈕。Edge 狀態會從**重新啟用擱置中 (Reactivation Pending)** 變更為**已啟動 (Activated)**。

6 如果啟用金鑰已到期 (此金鑰有效期間為一個月)，您將需要產生新的啟用金鑰。如需詳細資訊，請參閱〈到期的 RMA 啟用金鑰〉一節。

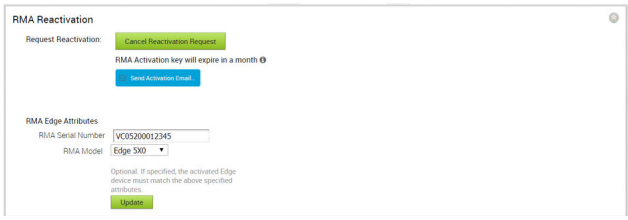
7 (選擇性步驟) 您可以輸入將在 [RMA 序號 (RMA Serial Number)] 文字欄位中啟動的 Edge 序號。

備註 序號區分大小寫。如果序號不符合將啟動的 Edge，則啟動將會失敗。

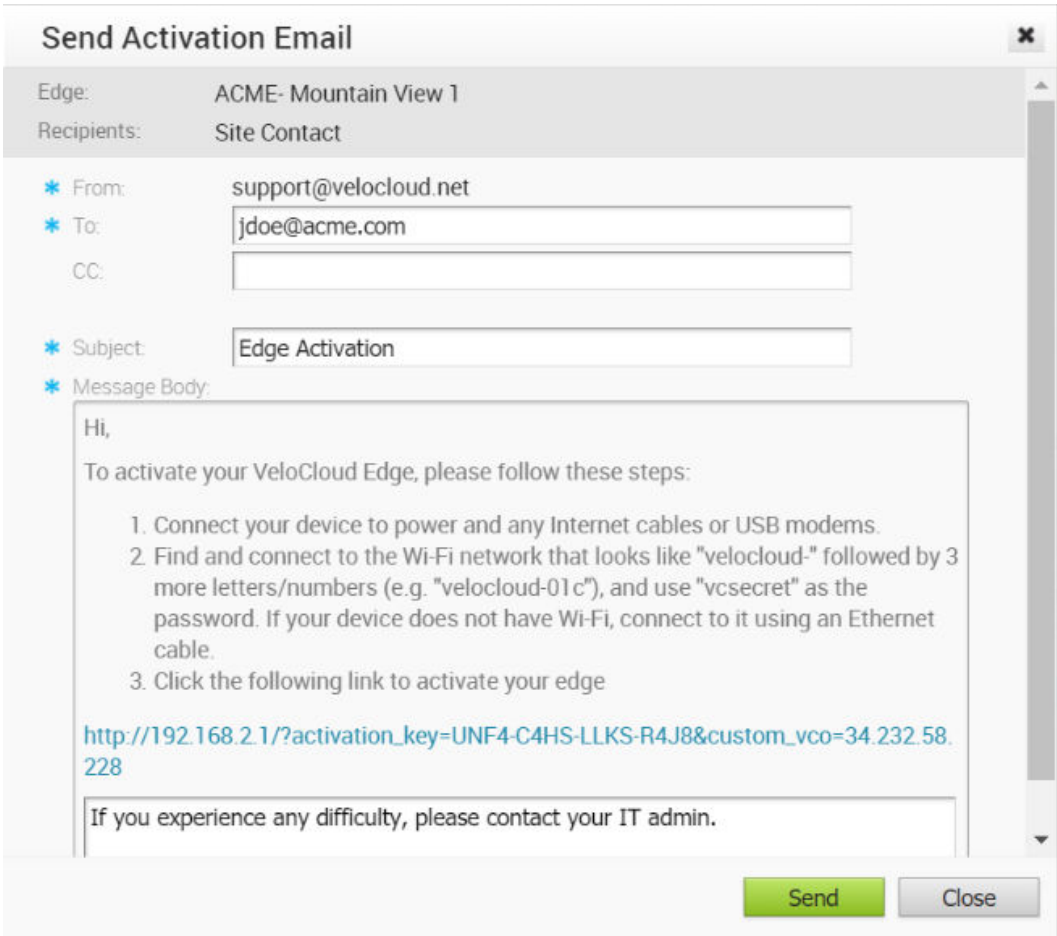
8 **RMA 型號 (RMA Model)** 下拉式功能表依預設會顯示選取的 Edge。如果要重新啟動不同的 Edge 型號，請從 **RMA 型號 (RMA Model)** 下拉式功能表中選取將啟動的 Edge 型號。

備註 如果選取的 **RMA 型號 (RMA model)** 與目前的 Edge 型號不同，會顯示警告訊息。在重新啟用時，將移除 Edge 特定的組態設定和設定檔覆寫，但仍會保留統計資料。建議記下 Edge 特定的組態設定，然後在重新啟用後，將這些組態設定重新新增至全新更換的 Edge。

9 如果您輸入序號，或從 [RMA 型號 (RMA Model)] 下拉式功能表中選取型號，請按一下**更新 (Update)** 按鈕。



10 按一下**傳送啟用電子郵件 (Send Activation Email)** 按鈕。**傳送啟用電子郵件 (Send Activation Email)** 快顯視窗隨即出現。



11 按一下**傳送 (Send)** 按鈕，將啟用程序電子郵件傳送至站台連絡人。此電子郵件將包含**傳送啟用電子郵件 (Send Activation Email)** 快顯視窗中所顯示的相同資訊。

剩餘指示會提供啟動替代 Edge 裝置的步驟。

12 中斷舊的 Edge 與電源和網路連線。

13 將新的 Edge 連線至電源和網路。確定 Edge 已連線至網際網路。

14 依照您在電子郵件中收到的啟用程序操作。

備註 請務必按一下電子郵件中的啟用連結以啟動 Edge。

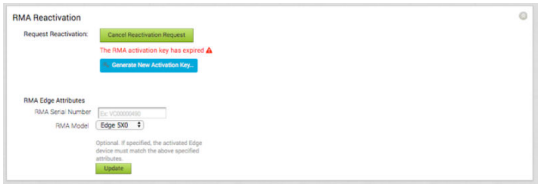
Edge 會從 SD-WAN Orchestrator 下載組態和軟體。新的 Edge 將成功啟動，且將可供服務使用。

到期的 RMA 啟用金鑰

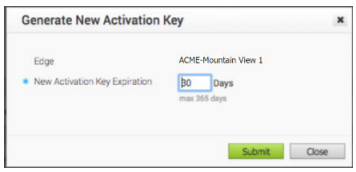
RMA 啟用金鑰的有效期只有重新啟用要求提出後的一個月。如果 RMA 啟用金鑰已到期，則會在 SD-WAN Orchestrator 的 [RMA 重新啟用 (RMA Reactivation)] 區域中顯示警告訊息。您可以取消重新啟用要求 (按一下**取消重新啟用要求 (Cancel Reactivation Request)** 按鈕)，或產生新的金鑰。在一個月的到期日之後，請依照下列指示產生新的金鑰。

若要產生新的 RMA 啟用金鑰：

1 按一下**產生新的啟用金鑰 (Generate New Activation Key)** 按鈕。



2 在**產生新的啟用金鑰 (Generate New Activation Key)** 對話方塊中，指定要讓金鑰處於作用中狀態的天數。



3 按一下**提交 (Submit)**。

4 依照〈RMA 重新啟用步驟〉完成 RMA 重新啟用程序。

設定 Edge 裝置

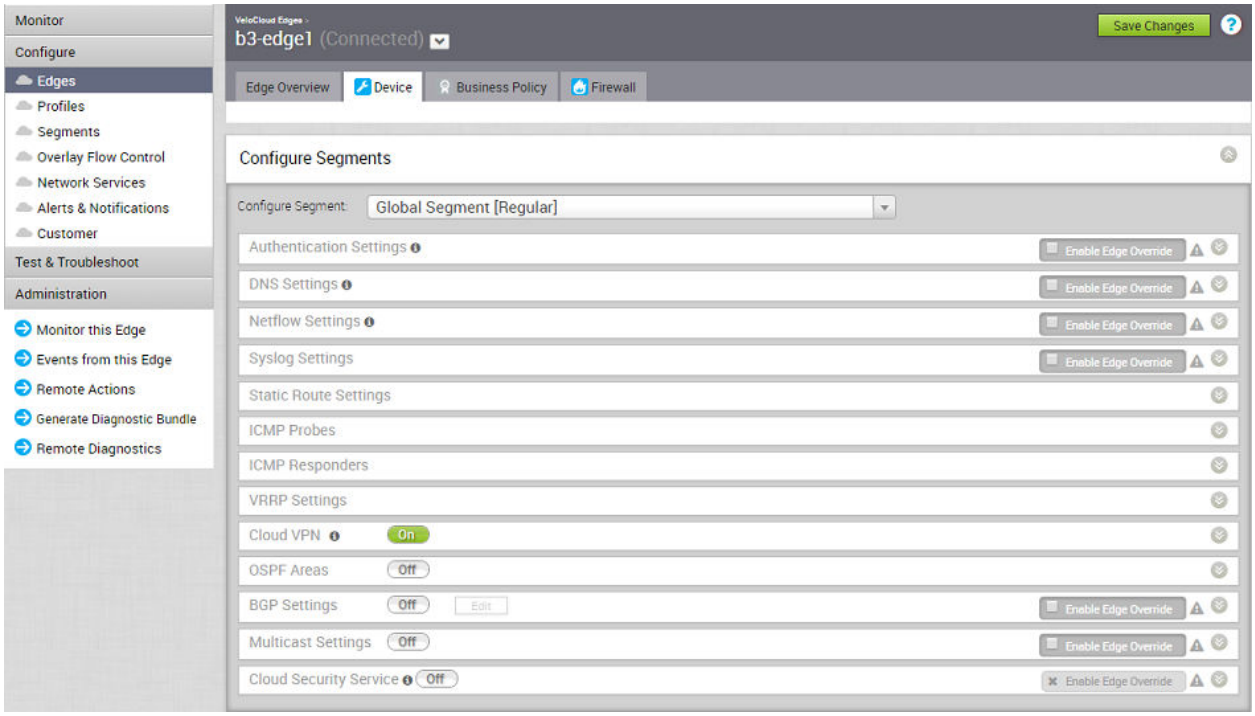
15

您可以對已指派給 Edge 的某些設定進行組態覆寫。在多數情況下，必須先啟用覆寫，才能進行變更。

您可以對介面、DNS 和驗證進行覆寫。此外，也可以將覆寫規則新增至現有的商務原則和防火牆規則。覆寫規則的優先於所有為商務原則或防火牆定義的其他規則。

備註 Edge 覆寫可用來對顯示的設定進行 Edge 特定編輯，以及停止來自組態設定檔的後續自動更新。您可以隨時停用覆寫並回復為自動更新。

以下幾節說明**設定 (Configure) > Edge > 裝置 (Device)** 索引標籤畫面中的區域。



部分區域可辨識區段。

區段感知組態：

- 驗證設定
- DNS 設定

- Netflow 設定
- Syslog 設定
- 靜態路由設定
- ICMP 探查
- ICMP 回應程式
- VRRP 設定
- 雲端 VPN
- OSPF 區域
- BGP 設定
- 多點傳播設定
- 雲端安全性服務

一般組態：

- 高可用性
- VLAN
- 裝置設定
- WAN 設定
- 多重來源 QoS
- SNMP 設定
- NTP 伺服器
- 可見度模式

備註 如需 OSPF 和 BGP 的相關資訊，請參閱第 18 章 使用 OSPF 或 BGP 設定動態路由一節。

本章節討論下列主題：

- 設定 DSL 設定
- 在 Edge 層級設定 Netflow 設定
- 在 Edge 層級設定 Syslog 設定
- 設定靜態路由設定
- 設定 ICMP 探查/回應程式
- 設定 VRRP 設定
- Edge 雲端 VPN
- 設定 Edge 的 VLAN

- 設定裝置設定
- 設定 Edge 的 SNMP 設定
- 設定 Wi-Fi 無線電覆寫
- 安全性 VNF
- 設定 Edge 商務原則
- 設定 Edge 啟用
- Edge 層級上的 LAN 端 NAT 規則

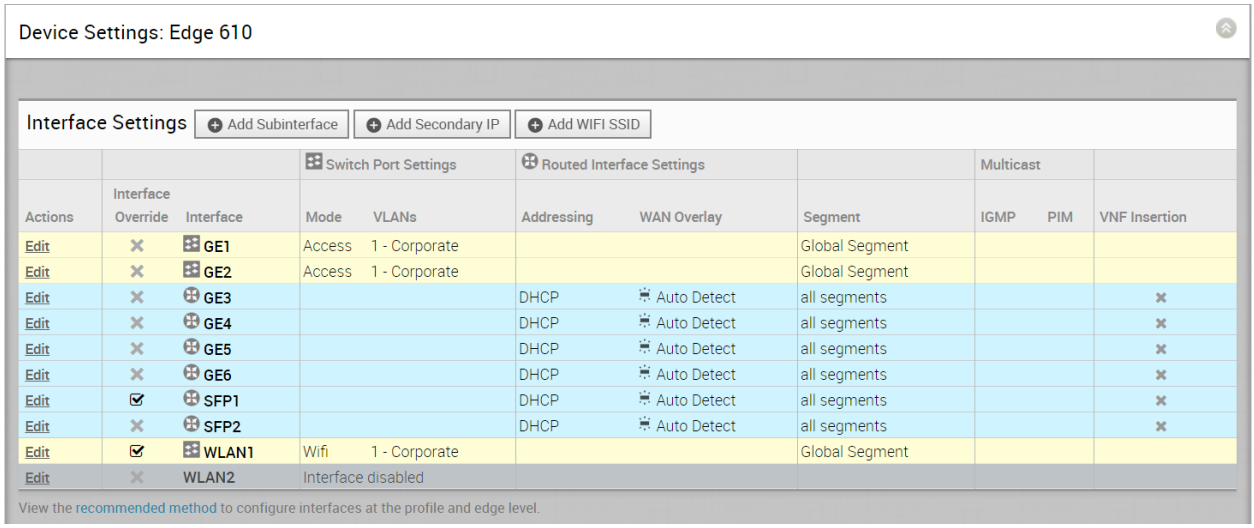
設定 DSL 設定

可支援 Metanoia xDSL SFP 模組 (MT 5311)。這是高度整合的 SFP 橋接數據機，能夠提供與插入式 SFP 相容的介面，以將現有的 DSL IAD 或主閘道裝置升級至更高的頻寬服務。

Metanoia xDSL SFP 模組 (MT 5311) 可插入至 Edge 610 裝置 SFP 插槽中，以及在 ADSL2+/VDSL2 模式中使用。此模組必須由使用者取得。DSL 的設定僅適用於 610 Edge 裝置。

設定 SFP

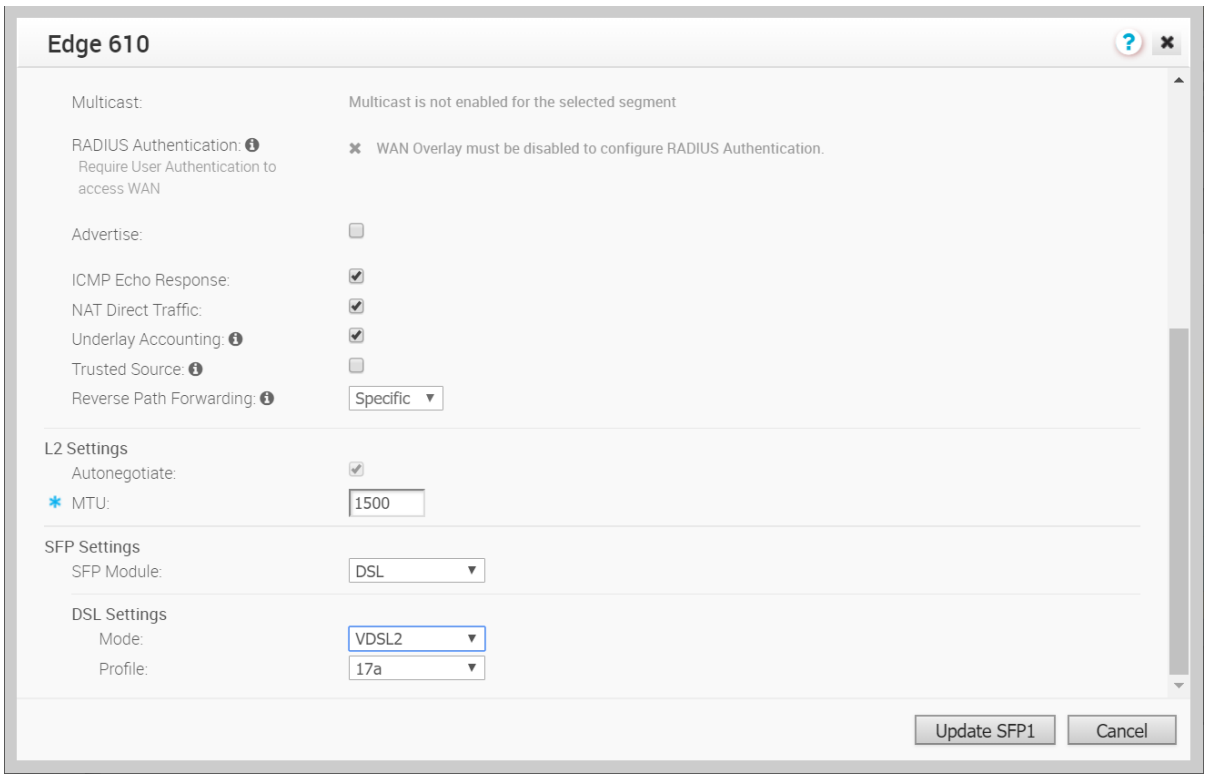
按一下已插入特定 DSL 模組的 SFP 介面。插入 SFP 後，插槽名稱會顯示為 SFP1 和 SFP2。



若要設定 SFP：

1 按一下**動作 (Actions)** 資料行中的**編輯 (Edit)** 連結，如上圖所示。

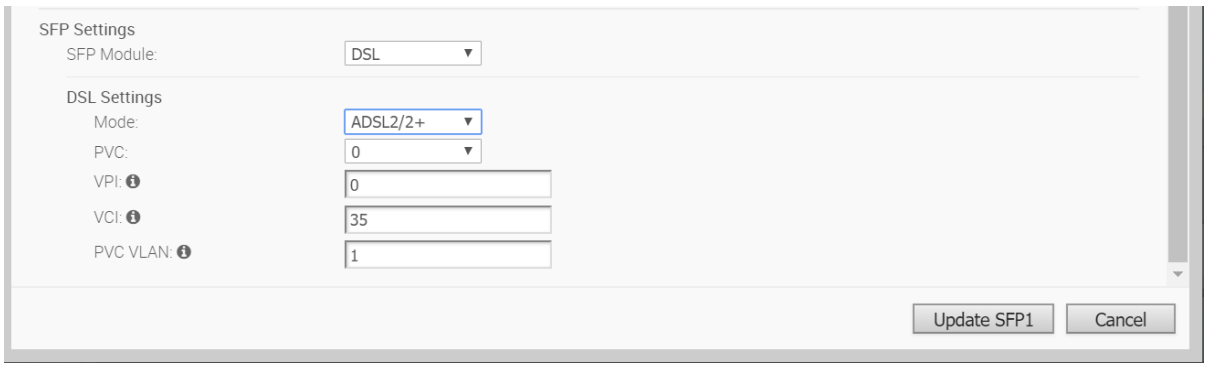
Edge 裝置 (在此範例中為 Edge 610) 的**介面 SFP1 (Interface SFP1)** 對話方塊隨即出現，如下圖所示。



2 必須勾選**覆寫介面 (Override Interface)** 核取方塊，才能設定 DSL 設定。

3 勾選**已啟用介面 (Interface Enabled)** 核取方塊。

4 在 **SFP 設定 (SFP Settings)** 區域中，可從下拉式功能表中選取兩個選項：[標準 (Standard)] 和 DSL。**請選擇 DSL** 作為 SFP 模組，如下圖所示。



5 在 **DSL 設定 (DSL Settings)** 區域中，依照下列說明選擇型號和設定檔設定 (如需可用選項的說明，請參閱「DSL 設定」表格)：

a 在**模式 (Mode)** 下拉式功能表中，選擇以下兩個選項之一：**VDSL 2** 或 **ADSL2/2+**。如果您在 [模式 (Mode)] 選項中選擇 **ADSL2/2+**，請在下方設定下列項目。

1 從 **PVC** 下拉式功能表中選擇 PVC 號碼 (0-7)。

2 輸入 VPI 號碼，或使用向上/向下箭頭在 **VPI** 文字方塊中選取號碼。

3 輸入 VCI 號碼，或使用向上/向下箭頭在 **VCI** 文字方塊中選取號碼。

4 輸入 PVC VLAN 號碼，或使用向上/向下箭頭在 **PVC VLAN** 文字方塊中選擇號碼。

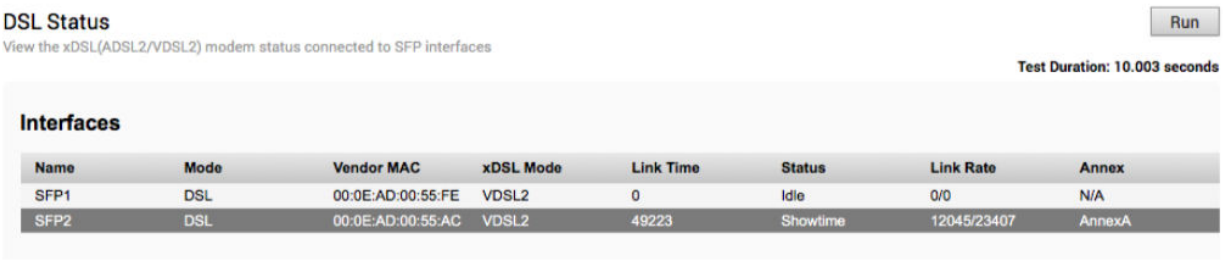
b 在**設定檔 (Profile)** 下拉式功能表中，從**設定檔 (Profile)** 下拉式功能表中選擇 30a 或 17a。

6 DHCP 伺服器類型。

7 按一下**更新 SFP1 (Update SFP1)** 按鈕。

對 DSL 設定進行疑難排解

DSL 診斷測試：DSL 診斷測試僅適用於 610 裝置。執行此測試後將會顯示 DSL 狀態，其中包括模式 (標準或 DSL)、設定檔、xDSL 模式等資訊。如下圖所示。



在 Edge 層級設定 Netflow 設定

身為企業管理員，在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 Netflow 設定。

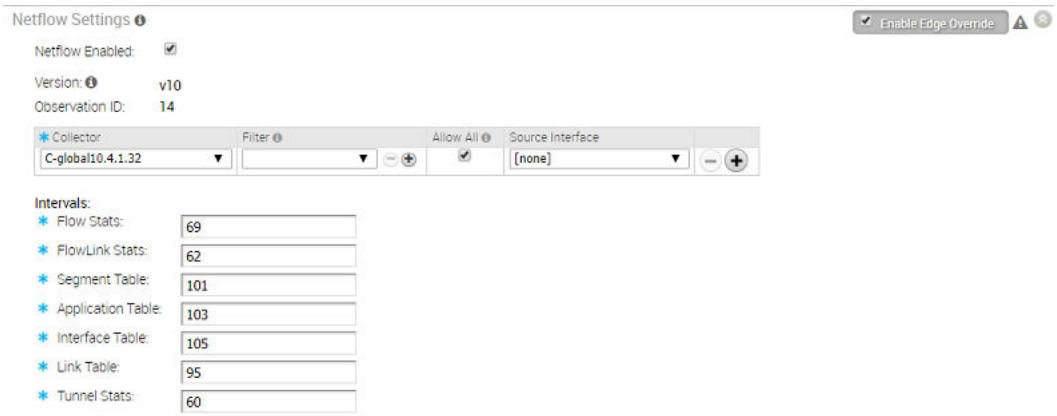
程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **Edge**。

隨即顯示 **VeloCloud Edges** 頁面。

2 選取要覆寫 Netflow 設定的 Edge，然後按一下**裝置 (Device)** 資料行下的圖示。

所選 Edge 的 [裝置設定 (Device Settings)] 頁面隨即出現。



3 在**設定區段 (Configure Segment)** 下拉式功能表中，選取設定檔區段以設定 Netflow 設定。

4 移至 **Netflow 設定 (Netflow Settings)** 區域，然後選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。

在 Edge 層級，**觀察識別碼 (Observation ID)** 欄位會自動填入 8 位元的區段識別碼和 24 位元的 Edge 識別碼，且您無法加以編輯。觀察識別碼對於每個企業每個區段的匯出程序都是唯一的。

5 參閱在設定檔層級設定 Netflow 設定中的步驟 4，以覆寫設定檔中指定的收集器、篩選器和 Netflow 匯出間隔資訊。

6 在**來源介面 (Source Interface)** 下拉式功能表中，選取在區段中設定的 Edge 介面作為來源介面，以選擇 NetFlow 封包的來源 IP。

備註 請確保手動選取已啟用「通告」旗標的 Edge LAN 介面 (VLAN/路由/子介面) 做為來源介面。如果選取**無 (none)**，則 Edge 會自動選取從對應區段啟用「開啟」和「通告」的 LAN 介面 (VLAN/路由/子介面) 做為該收集器的來源介面。如果 Edge 沒有已啟用「開啟」和「通告」的介面，則不會選取來源介面，並且不會產生 Netflow 封包。

7 按一下**儲存變更 (Save Changes)**。

在 Edge 層級設定 Syslog 設定

在企業網路中，SD-WAN Orchestrator 可用來將源自企業 SD-WAN Edges 的 SD-WAN Orchestrator 繫結事件和防火牆記錄，以原生 Syslog 格式收集到一或多個集中式遠端 Syslog 收集器 (伺服器)。在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 Syslog 設定。

若要覆寫 Edge 層級的 Syslog 設定，請執行下列步驟。

必要條件

- 確定已為 SD-WAN Edge (此為產生 SD-WAN Orchestrator 繫結事件之處) 設定雲端 VPN (分支到分支 VPN 設定)，以建立 SD-WAN Edge 與 Syslog 收集器之間的路徑。如需詳細資訊，請參閱設定雲端 VPN。

程序

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **Edge**。

SD-WAN Edges 頁面隨即出現。

2 選取要覆寫 Syslog 設定的 Edge，然後按一下**裝置 (Device)** 資料行下的圖示。

所選 Edge 的 [裝置設定 (Device Settings)] 頁面隨即出現。

3 在**設定區段 (Configure Segment)** 下拉式功能表中，選取設定檔區段以設定 Syslog 設定。依預設會選取**全域區段 [一般] (Global Segment [Regular])**。

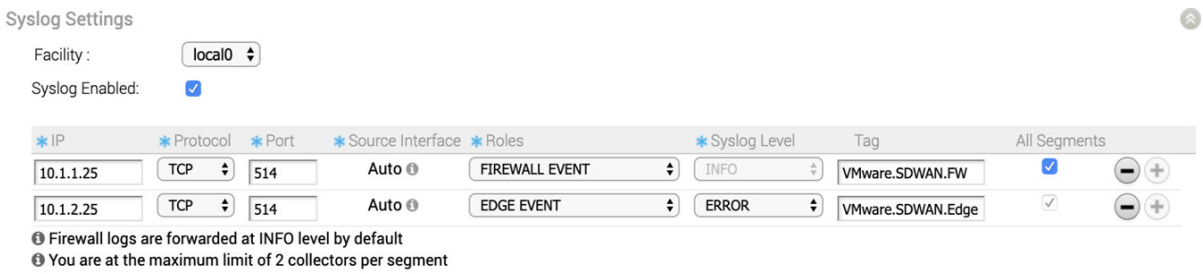
4 移至 **Syslog 設定 (Syslog Settings)** 區域，然後選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。

5 在**來源介面 (Source Interface)** 下拉式功能表中，選取在區段中設定的其中一個 Edge 介面作為來源介面。

6 依照 在設定檔層級設定 Syslog 設定 中的步驟 4，覆寫與 Edge 相關聯的設定檔中指定的其他 Syslog 設定。

7 按一下 + 按鈕以新增另一個 Syslog 收集器，或按一下**儲存變更 (Save Changes)**。Edge 的 Syslog 設定將被覆寫。

備註 每個區段最多可設定兩個 Syslog 收集器，每個 Edge 可設定 10 個 Syslog 收集器。當已設定的收集器數目達到允許的限制上限時，就會停用 + 按鈕。



備註 根據選取的角色，Edge 會將指定嚴重性層級的對應記錄匯出至遠端 Syslog 收集器。如果您想要在 Syslog 收集器上接收 SD-WAN Orchestrator 自動產生的本機事件，則必須使用 `log.syslog.backend` 和 `log.syslog.upload` 系統內容在 SD-WAN Orchestrator 層級上設定 Syslog。

若要瞭解防火牆記錄的 Syslog 訊息格式，請參閱防火牆記錄的 Syslog 訊息格式。

後續步驟

在 Edge 組態的**防火牆 (Firewall)** 頁面上，如果您想要將源自企業 SD-WAN Edges 的防火牆記錄轉送至已設定的 Syslog 收集器，請啟用 **Syslog 轉送 (Syslog Forwarding)** 按鈕。

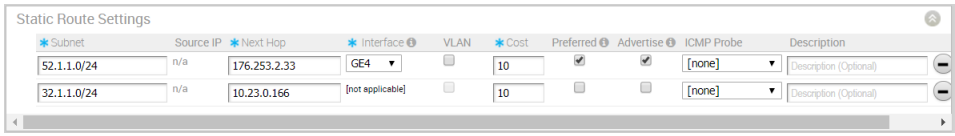
備註 依預設，**Syslog 轉送 (Syslog Forwarding)** 按鈕會在設定檔或 Edge 組態的**防火牆 (Firewall)** 頁面上顯示並停用。

如需 Edge 層級上防火牆設定的詳細資訊，請參閱設定 Edge 的防火牆。

設定靜態路由設定

靜態路由設定 (Static Route Settings) 對於現有的網路連結裝置 (例如印表機) 需使用靜態路由的特殊情況非常實用。您可以新增其他靜態路由設定 (加號「+」圖示)，或刪除位於對話方塊右側的靜態路由設定 (減號 - 圖示)。

如需對話方塊中設項設定的詳細資料，請參閱後續的資料表。



若要指定靜態路由設定：

1 輸入路由的子網路。

2 輸入路由的 IP 位址。

3 選取將繫結靜態路由的 WAN 介面。

4 選取**廣播 (Broadcast)** 核取方塊以對 VPN 通告此路由，並允許網路中的其他 Edge 擁有此資源的存取權。

5 您也可以選擇性地新增路由的說明。

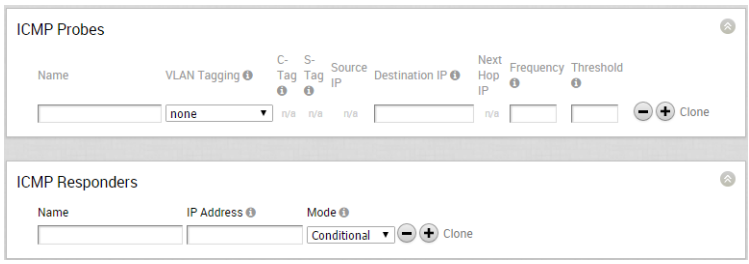
設定 ICMP 探查/回應程式

若外部路由器執行動態路由功能，且需透過 VMware 取得路由連線能力的相關狀態資訊，則可能必須要有 ICMP 處理常式，才能與外部路由器進行整合。**裝置設定 (Device Settings)** 區域提供指定 ICMP 探查和回應程式的區段。

對 ICMP 探查可以指定下列設定：名稱、VLAN 標記 (無、802.1q、802.1ad、QinQ (0x8100) 或 QinQ (0x9100))、C 標籤、S 標籤、來源/目的地/下一個躍點 IP、傳送 Ping 要求的頻率，以及將導致路由標示為無法連線之遺失 Ping 數目的臨界值。

對 ICMP 回應程式可以指定下列設定：**名稱 (Name)**、**IP 位址 (IP Address)** 和**模式 (Mode)** (**條件式 (Conditional)** 或**一律 (Always)**)。

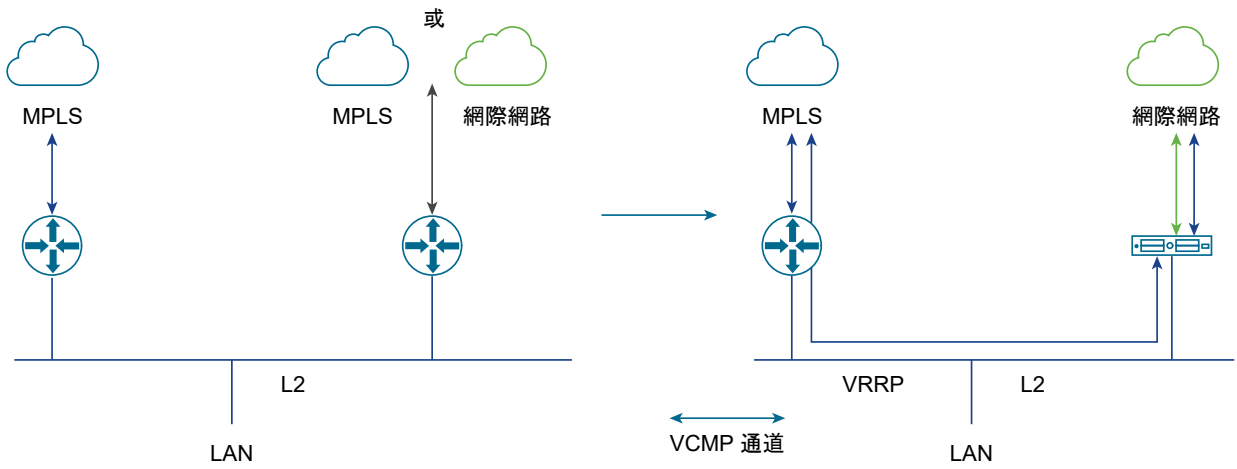
- **一律：(Always:)** Edge 一律會回應 ICMP 探查。
- **條件式：(Conditional:)** Edge 僅在 SD-WAN 覆疊啟動時回應 ICMP 探查。



設定 VRRP 設定

您可以在 Edge 上設定虛擬路由器備援通訊協定 (VRRP)，以在 SD-WAN Orchestrator 網路中與第三方 CE 路由器對等來啟用下一個躍點備援。您可以將 Edge 設定為主要 VRRP 裝置，並將該裝置與第三方路由器配對。

下圖顯示使用 VRRP 設定的網路：



必要條件

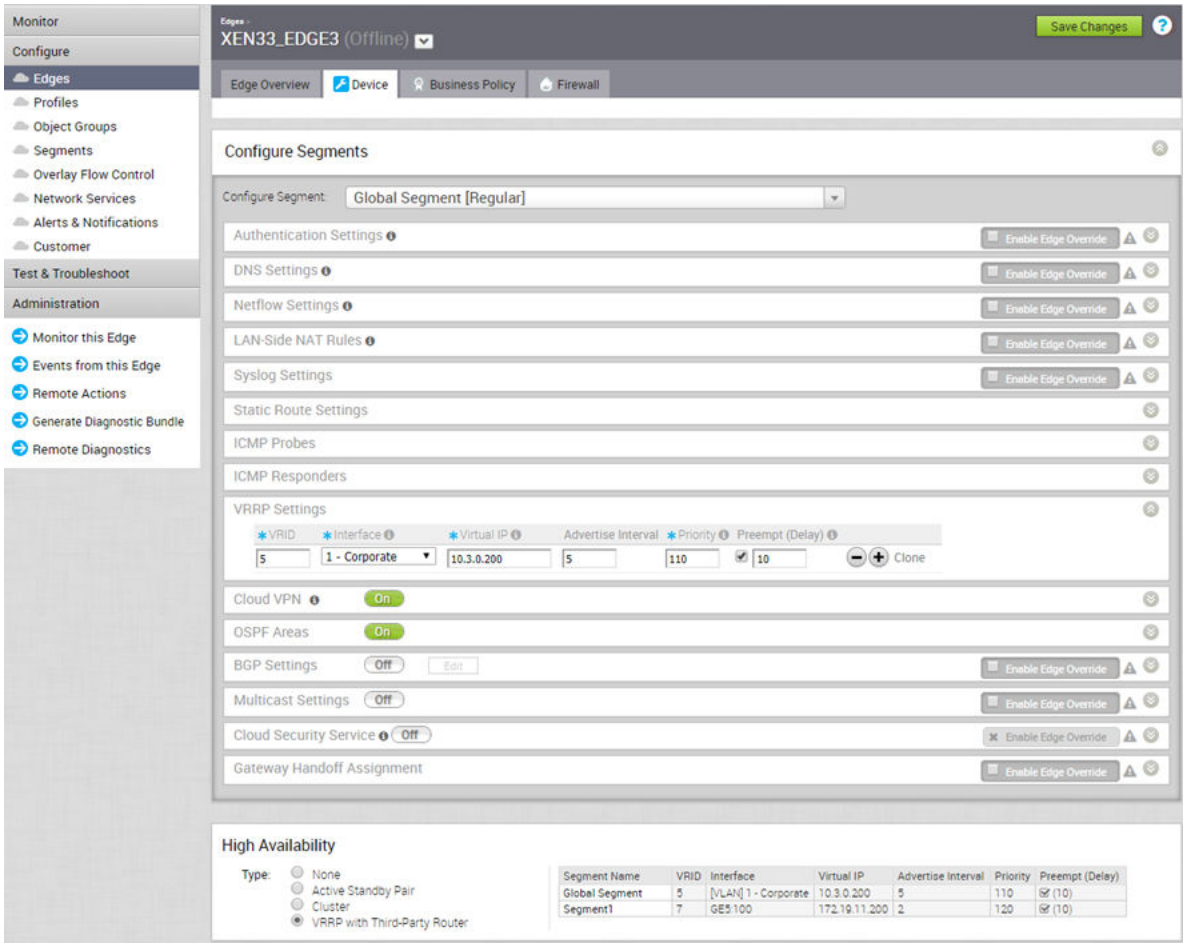
設定 VRRP 之前，請考慮下列準則：

- 您只能在 SD-WAN Edge 與透過 L2 交換器連線至相同子網路的第三方路由器之間啟用 VRRP。
- 您只能將一個 SD-WAN Edge 新增至分支中的 VRRP HA 群組。
- 您無法同時啟用作用中/待命 HA 和 VRRP HA。
- 主要路由連接埠、子介面和 VLAN 介面支援 VRRP。
- 必須透過設定較高優先順序，將 SD-WAN Edge 設定為主要 VRRP 裝置，以便透過 SD-WAN 來操控流量。
- 如果 SD-WAN Edge 設定為 DHCP 伺服器，則會將虛擬 IP 位址設定為用戶端的預設閘道位址。當您針對 LAN 使用個別的 DHCP 伺服器轉送時，管理員必須將 VRRP 虛擬 IP 位址設定為預設閘道位址。
- 在 SD-WAN Edge 和第三方路由器中同時啟用 DHCP 伺服器時，請分割 Edge 與第三方路由器之間的 DHCP 集區，以避免 IP 位址重疊。
- 在使用 WAN 覆疊 (位於 WAN 連結上) 啟用的介面上不支援 VRRP。如果您想要對 LAN 使用相同的連結，請建立子介面，並在子介面上設定 VRRP。
- 您只能在 VLAN 的廣播網域中設定一個 VRRP 群組。您無法為次要 IP 位址新增其他 VRRP 群組。
- 請勿將 WI-FI 連結新增至已啟用 VRRP 的 VLAN。由於連結失敗永遠不會發生，因此 SD-WAN Edge 一律會維持為主要裝置。

程序

1. 在企業入口網站中，按一下**設定 (Configure) > Edge**。
2. 按一下對應至 Edge 的**裝置 (Device)** 圖示，或按一下 Edge，然後按一下**裝置 (Device)** 索引標籤。
3. 在**裝置 (Device)** 索引標籤中，選取**高可用性 (High Availability)** 下方的 **使用第三方路由器的 VRRP (VRRP with Third-Party Router)** 核取方塊。

4 在 **VRRP 設定 (VRRP Settings)** 中，設定下列項目：



a **VRID** – 輸入 VRRP 群組識別碼。範圍從 1 到 255。

b **介面 (Interface)** – 從清單中選取實體或 VLAN 介面。系統會在所選介面中設定 VRRP。

c **虛擬 IP (Virtual IP)** – 輸入用於識別 VRRP 配對的虛擬 IP 位址。確保虛擬 IP 位址與 Edge 介面或第三方路由器的 IP 位址不同。

d **通告間隔 (Advertise Interval)** - 輸入主要 VRRP 裝置用來將 VRRP 通告封包傳送至 VRRP 群組中其他成員的時間間隔。

e **優先順序 (Priority)** - 若要將 Edge 設定為主要 VRRP 裝置，請輸入超過第三方路由器優先順序值的值。預設值為 100。

f **先佔延遲 (Preempt Delay)** - 選取此核取方塊，以便 SD-WAN Edge 可以在指定的先佔延遲後，先佔目前為主要裝置的第三方路由器。

5 按一下**儲存變更 (Save Changes)**。

結果

在分支網路 VLAN 中，如果 Edge 關閉，則 VLAN 後方的用戶端會透過備份路由器重新導向。

作為主要 VRRP 裝置的 SD-WAN Edge 會成為子網路的預設閘道。

如果 SD-WAN Edge 中斷了與所有 SD-WAN Edge/控制器的連線，則 VRRP 優先順序會降低至 10，而 SD-WAN Edge 會將從 SD-WAN Edge 和遠端 Edge 中學習的路由退出。這會導致第三方路由器成為主要裝置並接管流量。

SD-WAN Edge 會自動追蹤 SD-WAN Edge 的覆疊失敗。當 SD-WAN Edge 的所有覆疊路徑遺失時，SD-WAN Edge 的 VRRP 優先順序會減少到 10。

當 Edge 進入 VRRP 備份模式時，Edge 會捨棄經過虛擬 MAC 的所有封包。當路徑啟動時，Edge 會再次成為主要 VRRP 裝置，前提是已啟用先佔模式。

在路由介面上設定 VRRP 時，介面會用於本機 LAN 存取，且可以容錯移轉至備份路由器。

使用 WAN 覆疊啟用的路由介面不支援 VRRP。在此類情況下，必須設定共用相同實體介面的子介面，本機 LAN 存取才能支援 VRRP。

當 LAN 介面關閉時，VRRP 執行個體會移至 INIT 狀態，然後 SD-WAN Edge 會將路由撤銷要求傳送至 SD-WAN Edge/控制器，而所有遠端 SD-WAN Edge 則會移除這些路由。此行為適用於新增至已啟用 VRRP 介面的靜態路由。

如果已存在具有 SD-WAN Edge 對等中樞的私人覆疊，則不會從中樞移除該路由，且可能會導致非對稱路由。例如，當 SD-WAN 支點 Edge 中斷與公用閘道的連線時，第三方路由器會將封包從 LAN 轉送至 SD-WAN HubEdge。中樞會將傳回封包傳送至 SD-WAN 支點 Edge，而非第三方路由器。因應措施是啟用 **可連線的 SD-WAN (SD-WAN Reachable)** 功能，以便 SD-WAN Edge 可在私人覆疊上連線，並維持為主要 VRRP 裝置。由於網際網路流量也是透過 SD-WAN Edge 與覆疊上的私人連結進行操控，因此可能會對效能或總流量有某些限制。

條件式回傳選項用於操控透過中樞的網際網路流量。但是，在已啟用 VRRP 的 SD-WAN Edge 中，當公用覆疊關閉時，Edge 即成為備份 (Backup)。因此，無法在已啟用 VRRP 的 Edge 上使用條件式回傳功能。

監控 VRRP 事件

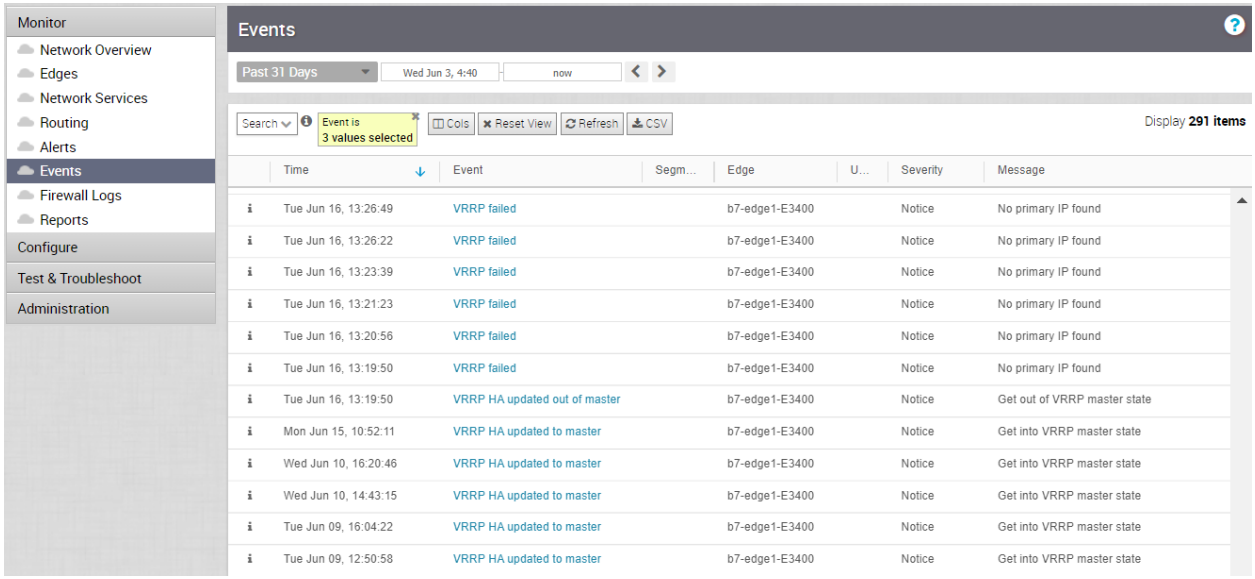
您可以監控與 VRRP 組態中變更相關的事件。

在企業入口網站中，按一下**監控 (Monitor) > 事件 (Events)**。

若要檢視與 VRRP 相關的事件，您可以使用篩選選項。按一下搜尋 (Search) 選項旁的下拉式箭頭，然後選擇依事件 (Event) 資料行進行篩選。以下是適用於 VRRP 的事件：

- VRRP HA 已更新為主節點
- VRRP HA 已更新為非主節點
- VRRP 失敗

下圖顯示部分 VRRP 事件。

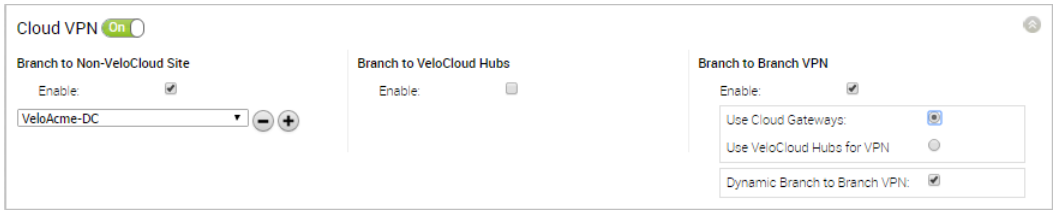


您也可以在新的 Orchestrator UI 中檢視事件。

按一下**開啟新的 Orchestrator UI (Open New Orchestrator UI)**，然後在快顯視窗中按一下**啟動新的 Orchestrator UI (Launch New Orchestrator UI)**。UI 會在新的索引標籤中開啟，並顯示監控選項。按一下**事件 (Events)**。按一下搜尋 (Search) 選項中的篩選器圖示以篩選 VRRP 事件。

Edge 雲端 VPN

Edge 雲端 VPN 設定會繼承自為 Edge 選取的設定檔，並且可在 Edge **裝置 (Device)** 索引標籤中檢閱。雲端 VPN 設定只能在相關聯的設定檔中進行變更。



設定 Edge 的 VLAN

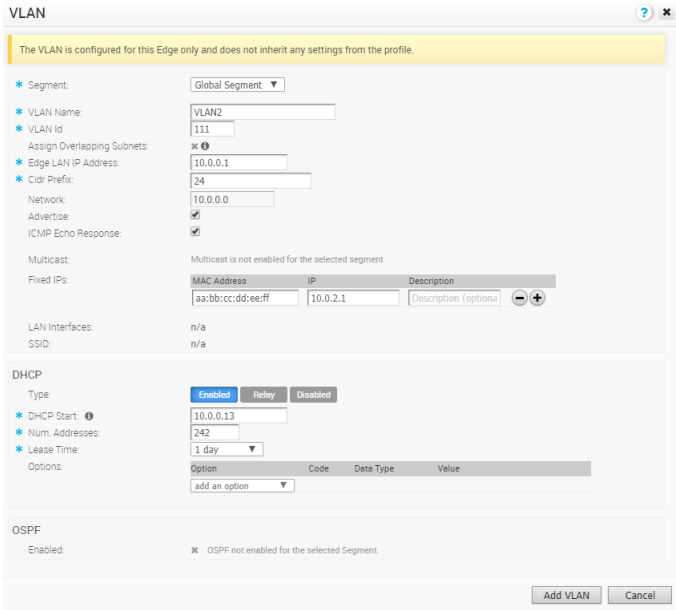
在 Edge 層級上，您可以新增 VLAN 或更新從相關聯設定檔繼承的現有 VLAN 設定。在 Edge 層級設定新的 VLAN 時，SD-WAN Orchestrator 可讓您設定其他 Edge 特定的 VLAN 設定，例如固定 IP 位址、LAN 介面，以及 Wi-Fi 介面的服務設定識別碼 (SSID)。

若要設定 Edge 層級的 VLAN 設定，請執行下列步驟：

1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **Edge**。SD-WAN Edges 頁面隨即出現。

2 選取要設定 VLAN 的 Edge，然後按一下**裝置 (Device)** 資料行下的圖示。所選設定檔的 [裝置設定 (Device Setting)] 頁面隨即出現。

3 若要新增 VLAN，請移至**設定 VLAN (Configure VLAN)** 區域，然後按一下**新增 VLAN (Add VLAN)**。



4 在 **VLAN** 對話方塊中，設定下列詳細資料：

a 在**區段 (Segment)** 下拉式功能表中，選取設定檔區段以設定 VLAN。

b 在 **VLAN 名稱 (VLAN Name)** 文字方塊中，輸入 VLAN 的唯一名稱。

c 在 **VLAN 識別碼 (VLAN ID)** 文字方塊中，輸入 VLAN 的唯一識別碼。

d 允許 LAN IP 定址的**指派重疊的子網路 (Assign Overlapping Subnets)** 欄位是從此 Edge 的指派設定檔進行管理。勾選**指派重疊的子網路 (Assign Overlapping Subnets)** 時，**Edge LAN IP 位址 (Edge LAN IP Address)**、**CIDR 首碼 (CIDR Prefix)**，以及 **DHCP** 的值會繼承自相關聯的設定檔並成為唯讀。將根據子網路遮罩和 CIDR 值自動設定**網路 (Network)** 位址。

e 選取**通告 (Advertise)** 核取方塊，將 VLAN 通告至網路中的其他分支。

f 選取 **ICMP 回顯回應 (ICMP Echo Response)** 核取方塊，以啟用 VLAN 來回應 ICMP 回顯訊息。

g 選取 **VNF 插入 (VNF Insertion)** 核取方塊，以啟用 Edge 虛擬網路功能 (VNF) 插入。

備註 VNF 插入需要選取的區段具有服務 VLAN。如需 VNF 的詳細資訊，請參閱安全性 VNF。

h 在**固定 IP (Fixed IPs)** 欄位中，輸入繫結至 VLAN 特定 MAC 位址的固定 IP 位址。

i 設定 VLAN 的 LAN 介面和 Wi-Fi SSID。

j 如果為所選區段啟用了多點傳播功能，則可以透過啟用 **IGMP** 和 **PIM** 核取方塊來設定**多點傳播 (Multicast)** 設定。

k 在 **DHCP** 區域下，選擇下列其中一項做為 DHCP 類型：

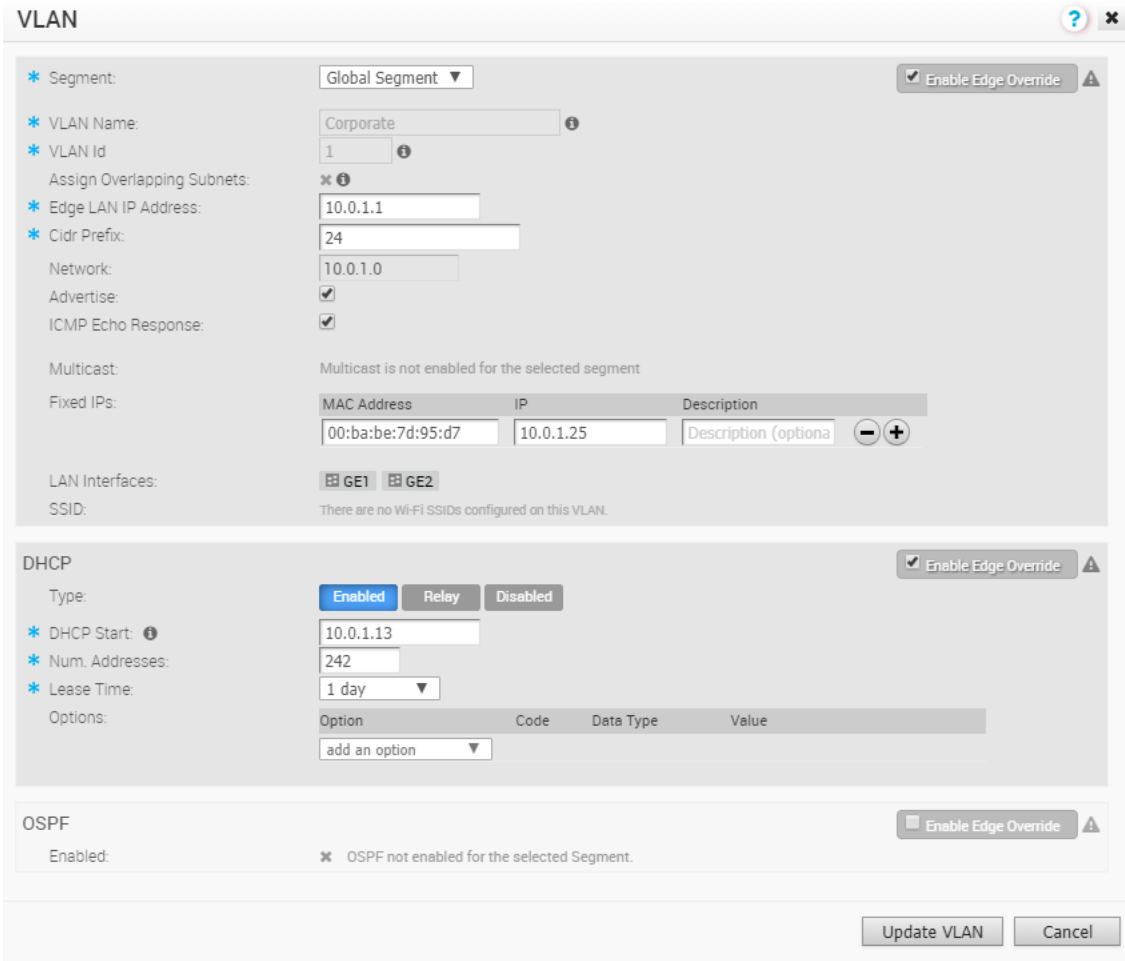
- **已啟用 (Enabled)** - 使用 Edge 啟用 DHCP 做為 DHCP 伺服器。選擇此選項時，您必須提供下列詳細資料：
  - **DHCP 啟動 (DHCP Start)** - 輸入子網路內可用的有效 IP 位址做為 DHCP 啟動 IP。
  - **位址數目 (Num Addresses)** - 輸入 DHCP 伺服器子網路上可用的 IP 位址數目。
  - **租用時間 (Lease Time)** - 從下拉式功能表中，選取允許 VLAN 使用由 DHCP 伺服器動態指派之 IP 位址的時段。

  此外，您可以新增一或多個 DHCP 選項，用以指定預先定義的選項或新增自訂選項。
- **轉送 (Relay)** - 使用在遠端位置安裝的 DHCP 轉送代理程式來啟用 DHCP。如果您選擇此選項，則可以指定一或多個轉送代理程式的 IP 位址。
- **已停用 (Disabled)** - 停用 DHCP。

l 如果已針對選取的區段啟用 OSPF 功能，請設定 **OSPF** 設定。

m 按一下**新增 VLAN (Add VLAN)**。

5 若要更新繼承自設定檔的 VLAN 設定，請在**動作 (Actions)** 資料行下，按一下對應 VLAN 的**編輯 (Edit)** 連結。**VLAN** 對話方塊隨即顯示。



6 按一下**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫繼承自設定檔的 VLAN 設定。

備註 您將無法覆寫設定檔的 VLAN 名稱和識別碼。

若要在設定檔層級設定 VLAN，請參閱 設定設定檔的 VLAN。

設定裝置設定

Edge **裝置設定 (Device Settings)** 畫面提供執行下列工作的功能：

- 設定 VLAN 設定
- 覆寫 Syslog 設定
- 覆寫設定檔介面設定
- 新增使用者定義的 WAN 覆疊
- 為重疊的網路設定 NAT

在路由介面上設定 DHCP 伺服器

您可以在 Edge 中的路由介面上，設定 DHCP 伺服器。

若要設定 DHCP 伺服器設定：

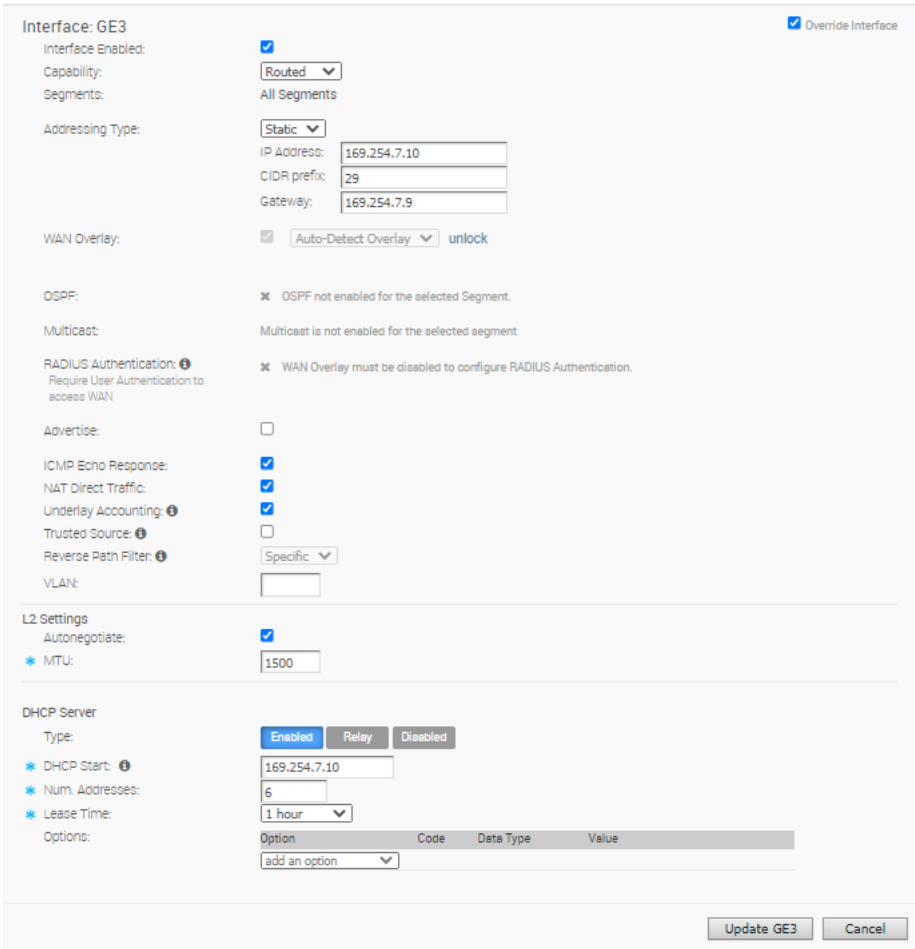
1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 按一下 Edge 旁的裝置圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 向下捲動至**裝置設定 (Device Settings)** 區段，然後按一下向下箭頭，以檢視 Edge 的**介面設定 (Interface Settings)**。

4 **介面設定 (Interface Settings)** 區段會顯示 Edge 中可用的現有介面。

5 按一下您要設定 DHCP 設定之路由介面的**編輯 (Edit)** 選項。



6 在**介面 (Interface)** 視窗中，將**定址類型 (Addressing Type)** 選取為**靜態 (Static)**，並輸入 Edge 介面和閘道的 IP 位址。

7 在 **DHCP 伺服器 (DHCP Server)** 區段中，選擇下列其中一個 DHCP 設定：

- **已啟用 (Enabled)** - 使用 Edge 啟用 DHCP 做為 DHCP 伺服器。設定下列詳細資料：
  - **DHCP 開始 (DHCP Start)** - 輸入子網路內可用的有效 IP 位址。
  - **位址數目 (Num. Addresses)** - 輸入 DHCP 伺服器子網路上可用的 IP 位址數目。
  - **租用時間 (Lease Time)** - 從下拉式清單選取時間。這是允許 VLAN 使用 DHCP 伺服器動態指派的 IP 位址的持續時間。

- **選項 (Options)** - 從下拉式清單中新增預先定義或自訂的 DHCP 選項。DHCP 選項是從 DHCP 伺服器傳遞至用戶端的網路服務。若為自訂選項，請輸入代碼、資料類型和值。
- **轉送 (Relay)** - 使用在遠端位置安裝的 DHCP 轉送代理程式來啟用 DHCP。如果您選擇此選項，請設定下列項目：
  - **轉送代理程式 IP (Relay Agent IP(s))** - 指定轉送代理程式的 IP 位址。按一下加號 (+) 圖示以新增更多 IP 位址。
- **已停用 (Disabled)** - 停用 DHCP。

如需**介面設定 (Interface Settings)** 視窗中其他選項的詳細資訊，請參閱設定介面設定。

備註 如需詳細資訊，請參閱通道額外負荷和 MTU。

高可用性 (HA)

在此處可為 Edge 啟用高可用性 (HA)。

如需與 HA 之設定和組態有關的詳細資訊，請參閱《HA 組態》。

在路由介面上啟用 RADIUS

在任何可設定為路由介面的介面上都可啟用 RADIUS。如需逐步指示，請參閱以下一節。

需求

- 必須設定 RADIUS 伺服器並將其新增至 Edge。此作業可在 VMware SD-WAN Orchestrator 的**設定 (Configure) > 網路服務 (Network Services)** 畫面中的執行。
- 在任何可設定為路由介面的介面上都可啟用 RADIUS。其中包括任何 Edge 型號的介面，但 Edge 型號 500/520/540 上的 LAN 1-8 連接埠除外。

備註 已啟用 RADIUS 的介面不會使用 DPDK。

在路由介面上啟用 RADIUS

1 移至 VMware SD-WAN Orchestrator 上的**設定 (Configure) -> 裝置 (Device)**，針對要啟用 RADIUS 驗證的介面，按一下**編輯 (Edit)**。

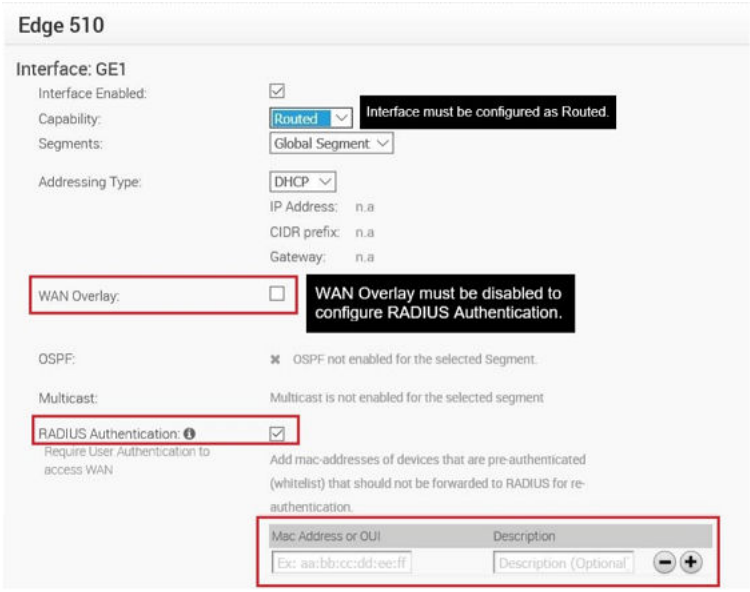
2 將功能參數設定為**路由 (Routed)**。

3 取消勾選方塊以停用 **WAN 覆蓋 (WAN Overlay)**。

4 若要啟用 **RADIUS 驗證 (RADIUS Authentication)**，請勾選該方塊。

5 針對已預先驗證且不應轉送至 RADIUS 進行重新驗證的裝置設定允許清單。您可以依個別的 MAC 位址 (例如 8c:ae:4c:fd:67:d5) 以及依 OUI (組織唯一識別碼 [例如 8c:ae:4c:00:00:00]) 來新增裝置。

備註 介面將使用已指派給 Edge 的伺服器 (例如兩個介面無法使用兩個不同的 RADIUS 伺服器)。



設定 Edge LAN 覆寫

選取**覆寫介面 (Override Interface)** 核取方塊，可覆寫設定檔中指定的 LAN 設定。

請參閱第 10 章 設定設定檔裝置，以瞭解 LAN 介面組態參數。

設定 Edge WAN 覆寫

選取**覆寫介面 (Override Interface)** 核取方塊，可覆寫設定檔中指定的 WAN 設定。

請參閱第 10 章 設定設定檔裝置，以瞭解 LAN 介面組態參數。

設定 Edge WAN 覆疊設定

WAN 設定可讓您新增或修改使用者定義的 WAN 覆疊。

使用者定義的覆疊需要連結至已提前設定 WAN 覆疊的介面。您可以設定下列其中一個覆疊：

- **私人覆疊 (Private Overlay)**：當您想要讓 Edge 在指派給私人網路上每個 Edge 的私人 IP 位址之間建置直接覆疊 VCMP 通道時，需要在私人網路上進行此設定。
- **公用覆疊 (Public Overlay)**：當您想要為 VCMP 通道設定自訂 VLAN 或來源 IP 位址以及閘道位址，以透過網際網路連線至由 SD-WAN Orchestrator 所判斷的 VMware SD-WAN Gateways 時，此功能相當實用。

您也可以修改或刪除已在路由介面上偵測到的現有自動偵測 WAN 覆疊。只有在 Edge 已透過使用 WAN 覆疊設定的路由介面成功建立 VCMP 通道時，自動偵測到的覆疊才可供 SD-WAN Orchestrator 所指定的閘道使用。

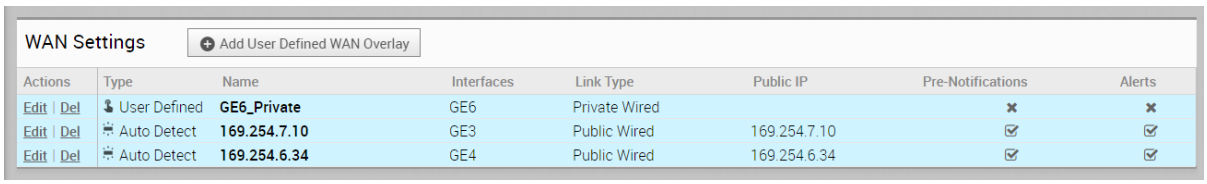
備註 即使介面已關閉或不在使用中，WAN 設定下方列出的 WAN 覆疊仍會保留，且在不再需要時可加以刪除。

程序

1 在 SD-WAN Orchestrator 入口網站中，按一下**設定 (Configure) > Edge**。

2 在 **Edge** 頁面中按一下 Edge 旁的裝置圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 向下捲動至 **WAN Settings (WAN 設定)**。



4 對於自動偵測或使用者定義的現有 WAN 覆疊，按一下**編輯 (Edit)** 以修改設定。

5 若要建立新的公用或私人覆疊，請按一下**新增使用者定義的 WAN 覆疊 (Add User Defined WAN Overlay)**。

6 在**使用者定義的 WAN 覆疊 (User Defined WAN Overlay)** 視窗中，從下列可用選項中選擇**連結類型 (Link Type)**：

- **公用 (Public)** 覆疊用於網際網路，可讓 SD-WAN 雲端閘道在網際網路上與其連線。必須將使用者定義的覆疊連結至介面。公用覆疊會指示 Edge 透過連結的介面指派主要和次要閘道，以協助判斷外部全域 NAT 位址。如果設定為將 VCMP 通道建置到目前選取的 Edge，則系統會向 Orchestrator 報告此外部全域位址，以便所有其他的 Edge 均使用此外部全域位址。

  備註 依預設，所有路由介面將透過網際網路上預先指派的雲端閘道，即建置 VCMP 通道以嘗試**自動偵測 (Auto Detect)**。如果嘗試成功，則會建立自動偵測公用覆疊。只有在您的網際網路服務需要 VLAN 標籤，或者您想要使用的公用 IP 位址與 Edge 在對外公開的介面上透過 DHCP 學習的公用 IP 位址不同時，才需要使用者定義的公用覆疊。

- **私人 (Private)** 覆疊用於私人網路，例如 MPLS 網路或點對點連結。私人覆疊會如同任何使用者定義的覆疊連結至介面，並假設其所連結介面上的 IP 位址可供相同私人網路上的所有其他 Edge 進行路由。這表示介面的 WAN 端上沒有 NAT。將私人覆疊連結至介面時，Edge 會向 Orchestrator 建議介面上的 IP 位址應用於設定為建置其通道的任何遠端 Edge。

下表說明覆疊設定：

表 15-1. 對公用和私人覆疊通用的設定 (Settings common for Public and Private Overlay)

選項	說明
名稱 (Name)	輸入公用或私人連結的描述性名稱。您在商務原則中選擇 WAN 連結時，可以參考此名稱。請參閱設定連結操控模式。
預先通知警示 (Pre-Notification Alerts)	將與覆疊網路相關的警示傳送給操作員。請確定您已在**設定 (Configure) > 警示和通知 (Alerts & Notifications)** 頁面中啟用連結警示，以接收警示。
警示 (Alerts)	將與覆疊網路相關的警示傳送給客戶。請確定您已在**設定 (Configure) > 警示和通知 (Alerts & Notifications)** 頁面中啟用連結警示，以接收警示。
介面 (Interfaces)	從**更新選取項目 (update selection)** 下拉式清單中選取一或多個路由介面，並將目前使用者定義的覆疊連結至選取的介面。此清單包含已啟用 WAN 覆疊且設定為**使用者定義的覆疊 (User Defined Overlay)** 的路由介面。

表 15-2. 公用覆疊設定 (Public Overlay Settings)

選項	說明
公用 IP 位址 (Public IP Address)	顯示已探索到公用覆疊的公用 IP 位址。一旦使用閘道方法探索到外部全域 NAT 位址後，就會填入此欄位。

下圖顯示公用覆疊設定的範例：

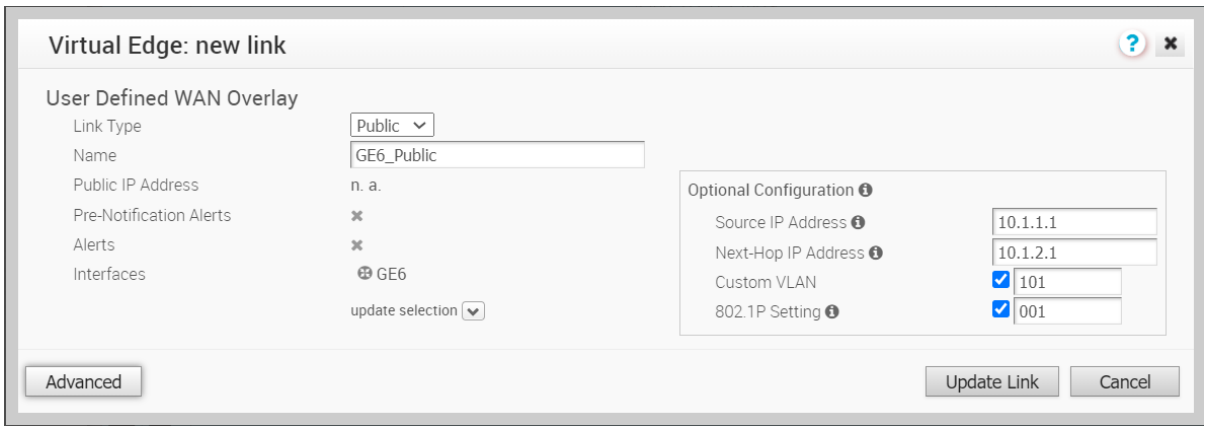


表 15-3. 私人覆疊設定 (Private Overlay Settings)

選項	說明
可連線的 SD-WAN 服務 (SD-WAN Service Reachable)	建立私人覆疊並將其連結至私人 WAN (例如 MPLS 網路) 時，您可能也可以透過相同的 WAN (通常是透過資料中心中的防火牆) 連線至網際網路。在此情況下，建議啟用可連線的 SD-WAN 服務 (SD-WAN Service Reachable)，因為它提供下列項目： ■ 用於存取網際網路所主控 SD-WAN Gateways 的網際網路次要路徑。此 Edge 對網際網路的所有直接連結皆失敗時，則會使用此路徑。 ■ 此 Edge 對網際網路的所有直接連結皆失敗時的 Orchestrator 次要路徑。Edge 用於通訊的管理 IP 位址必須可在 MPLS 內路由，否則必須在私人介面上檢查 NAT Direct，Orchestrator 流量才能正確傳回。 **備註** 相較於透過私人網路 (長路徑) 使用遠端防火牆建立對網際網路的 VCMP 通道，此 SD-WAN Edge 一律偏好透過本機網際網路連結 (短路徑) 建立的 VCMP 通道。 **備註** 系統不會在短路徑和長路徑之間執行每個封包或循環組態資源負載平衡。 在無法直接存取公用網際網路的站台中，[可連線的 SD-WAN 服務 (SD-WAN Service Reachable)] 選項允許將私人 WAN 用於私人的站台間 VCMP 通道，作為與網際網路所主控 VMware 服務通訊的路徑。
公用 SD-WAN 位址 (Public SD-WAN Addresses)	當您選取**可連線的 SD-WAN 服務 (SD-WAN Service Reachable)** 核取方塊時，將會顯示 SD-WAN Gateways 和 SD-WAN Orchestrator 的公用 IP 位址清單，如果預設路由尚未從防火牆通告至相同的私人網路，則可能需要在私人網路之間通告這些位址。 清單中的某些 IP 位址 (例如閘道) 可能會隨著時間變更。

下圖顯示私人覆疊設定的範例：

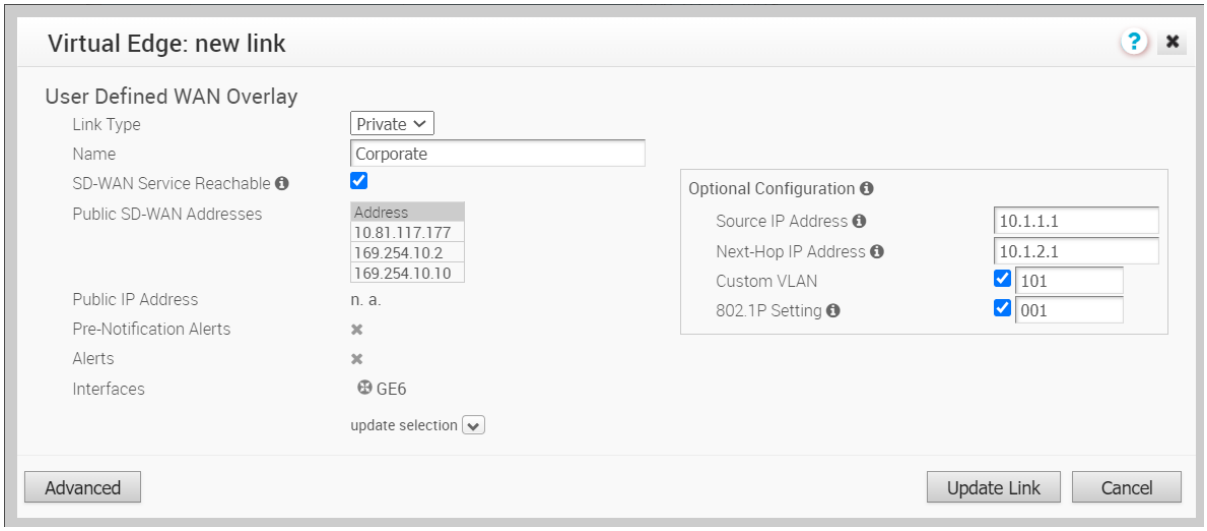


表 15-4. 選用組態 (Optional Configuration)

選項	說明
來源 IP 位址 (Source IP Address)	這是原始通訊端來源 IP 位址，用於源自目前覆疊所連結介面的 VCMP 通道封包。 來源 IP 位址無須在任何位置預先設定，但必須可與所選介面往來路由。
下一個躍點 IP 位址 (Next-Hop IP Address)	輸入封包 (來自指定於**來源 IP 位址 (Source IP Address)** 欄位中的原始通訊端來源 IP 位址) 所要路由到的下一個躍點 IP 位址。
自訂 VLAN (Custom VLAN)	請選取此核取方塊以啟用自訂 VLAN，並輸入 VLAN 識別碼。範圍為 2 到 4094。 此選項會將 VLAN 標籤套用至源自 VCMP 通道的來源 IP 位址 (來自目前覆疊所連結介面) 的封包。
802.1P 設定 (802.1P Setting)	設定框架上的 802.1p PCP 位元，使其保留目前覆疊所連結的介面。此設定僅適用於特定的 VLAN。PCP 優先順序值是 3 位數的二進位數字。範圍從 000 到 111，預設值為 000。 僅在系統內容 **session.options.enable8021PConfiguration** 必須設定為 True 時，才能使用此核取方塊。依預設，此值為 False。 如果您無法使用此選項，請連絡作業團隊的 VMware 支援人員以啟用此設定。

按一下**進階 (Advanced)** 以設定下列設定：

表 15-5. 對公用和私人覆疊通用的進階設定 (Advanced Settings common for Public and Private Overlay)

選項	說明
頻寬測量 (Bandwidth Measurement)	從下列選項中選擇測量頻寬的方法： ■ **測量頻寬 (慢速啟動) (Measure Bandwidth (Slow Start))**：測量預設頻寬時若報告不正確的結果，則可能是 ISP 節流所致。若要避免此行為，請選擇此選項，以先維持一段時間的慢速 UDP 流量高載，再轉為較大的高載。 ■ **測量頻寬 (高載模式) (Measure Bandwidth (Burst Mode))**：選擇此選項可對公用連結的 SD-WAN Gateway 或對私人連結的對等執行短暫的 UDP 流量高載，以評估連結的頻寬。 ■ **不測量 (手動定義) (Do Not Measure (define manually))**：選擇此選項可手動設定頻寬。建議將此用於中樞站台，因為： a 中樞站台通常只能測量連結較中樞更慢的遠端分支。 b 如果中樞 Edge 失敗且正在使用動態頻寬測量模式，則可能會在中樞 Edge 重新測量可用頻寬時，在該中樞 Edge 增加延遲。
上游頻寬 (Upstream Bandwidth)	輸入上游頻寬 (以 Mbps 為單位)。只有在選擇 [不測量 (手動定義) (Do Not Measure (define manually))] 時，才可使用此選項。
下游頻寬 (Downstream Bandwidth)	輸入下游頻寬 (以 Mbps 為單位)。只有在選擇 [不測量 (手動定義) (Do Not Measure (define manually))] 時，才可使用此選項。
動態頻寬調整 (Dynamic Bandwidth Adjustment)	動態頻寬調整會嘗試根據封包遺失來動態調整可用的連結頻寬，並適用於在頻寬可能會突然減少的情況下搭配使用無線寬頻服務。 **備註** 此組態不建議用於軟體版本為 3.3.x 或更早版本的 Edge。您可以針對版本為 3.4 或更新版本的 Edge 設定此選項。
僅作為備份 (Use as Backup Only)	此選項會將此 WAN 覆疊所連結的介面置於備份模式。這表示，已針對此介面中斷 VCMP (管理) 通道，並且僅在重新建立管理通道時使用該選項，因為從 Edge 到所有作用中的連結上的主要閘道的路徑都已關閉。 僅能將 Edge 上的一個介面置於備份模式。啟用時，介面會在**監視器 (Monitor) > Edge** 頁面中顯示為**雲端狀態：待命 (Cloud Status: standby)**。 **備註** 使用此選項，可減少 4G 或 LTE 服務上的使用者資料和 SD-WAN 效能測量頻寬耗用量。不過，相較於非備份模式中的連結，以及用來減少頻寬耗用量的商務原則，容錯移轉時間將會較慢。如果 Edge 用作中樞或叢集的一部分，請勿使用此功能。

表 15-5. 對公用和私人覆疊通用的進階設定 (Advanced Settings common for Public and Private Overlay) (續)

選項	說明
MTU	SD-WAN Edge 會執行路徑 MTU 探索，且會在此欄位中更新探索到的 MTU 值。多數有線網路支援 1500 個位元組，而支援 VoLTE 的 4G 網路通常僅允許最多 1358 個位元組。 建議不要將 MTU 設定為低於 1300 個位元組，因為這可能會導致框架處理額外負荷。除非路徑 MTU 探索失敗，否則不需要設定 MTU。 您可以從**遠端診斷 (Remote Diagnostics) > 清單路徑 (List Paths)** 頁面中發現 MTU 是否較大，因為介面的 VCMP 通道 (路徑) 永遠不會變穩定，且會重複連線至封包遺失超過 25% 的「無法使用」狀態。 由於 MTU 在每個路徑上的頻寬測試期間會緩慢增加，如果設定的 MTU 大於網路 MTU，則系統會捨棄大於網路 MTU 的所有封包，導致路徑上的嚴重封包遺失。 如需詳細資訊，請參閱通道額外負荷和 MTU。
額外負荷位元組 (Overhead Bytes)	輸入額外負荷頻寬的值 (以位元組為單位)。此選項可指出 WAN 路徑中存在的 L2 框架處理額外負荷。 當您設定額外負荷位元組時，除了實際封包長度以外，QoS 排程器還會額外考量每個封包的位元組。這可確保不會因為任何上游 L2 框架處理額外負荷而過度訂閱連結頻寬。

表 15-6. 公用覆疊的進階設定 (Advanced Settings for Public Overlay)

選項	說明
UDP 打孔 (UDP Hole Punching)	如果需要分支到分支 SD-WAN 覆疊，且分支 Edge 部署在 NAT 裝置後方，即 NAT 裝置是 Edge 的 WAN 端，則在 NAT 裝置並未設定為允許來自其他 Edge 之 UDP 連接埠 2426 上傳入的 VCMP 通道時，UDP/2426 上的直接 VCMP 通道將不可能出現。 使用**分支到分支 VPN (Branch to Branch VPN)**，以啟用分支到分支的通道。請參閱設定分支到分支 VPN 和 Edge 雲端 VPN。 使用**遠端診斷 (Remote Diagnostics) > 清單路徑 (List Paths)**，以檢查一個 Edge 是否已建置至另一個 Edge 通道。 UDP 打孔會嘗試解決封鎖傳入連線的 NAT 裝置。但是，此技術不適用於所有案例或所有類型的 NAT，因為 NAT 作業特性並非標準化。 在 Edge 覆疊介面上啟用 UDP 打孔時，系統會指示所有遠端 Edge 使用探索到的 NAT 公用 IP 以及透過 SD-WAN Gateway 探索到的 NAT 動態來源連接埠作為目的地 IP 和目的地連接埠，以建立此 Edge 覆疊介面的 VCMP 通道。 **備註** 啟用 UDP 打孔之前，請先將分支 NAT 裝置設定為允許透過連接埠轉送的 UDP/2426 輸入至 Edge 私人 IP 位址，或將 NAT 裝置 (通常是路由器或數據機) 置於橋接器模式。僅使用 UDP 打孔作為最後一個手段，因為它無法搭配使用防火牆、對稱 NAT 裝置、4G/LTE 網路 (由於 CGNAT) 以及最新式的 NAT 裝置。 當遠端站台嘗試將新的 UDP 動態連接埠用於 VCMP 通道時，UDP 打孔功能可能會導致其他連線問題。
類型 (Type)	設定 Edge 的商務原則時，您可以選擇**連結操控 (Link Steering)**，以偏好**傳輸群組 (Transport Group)** 為：公用有線、公用無線或私人有線。請參閱設定連結操控模式。 選擇**有線 (Wired)** 或**無線 (Wireless)**，將覆疊置於公用有線或無線傳輸群組。

下圖顯示公用覆疊的進階設定：

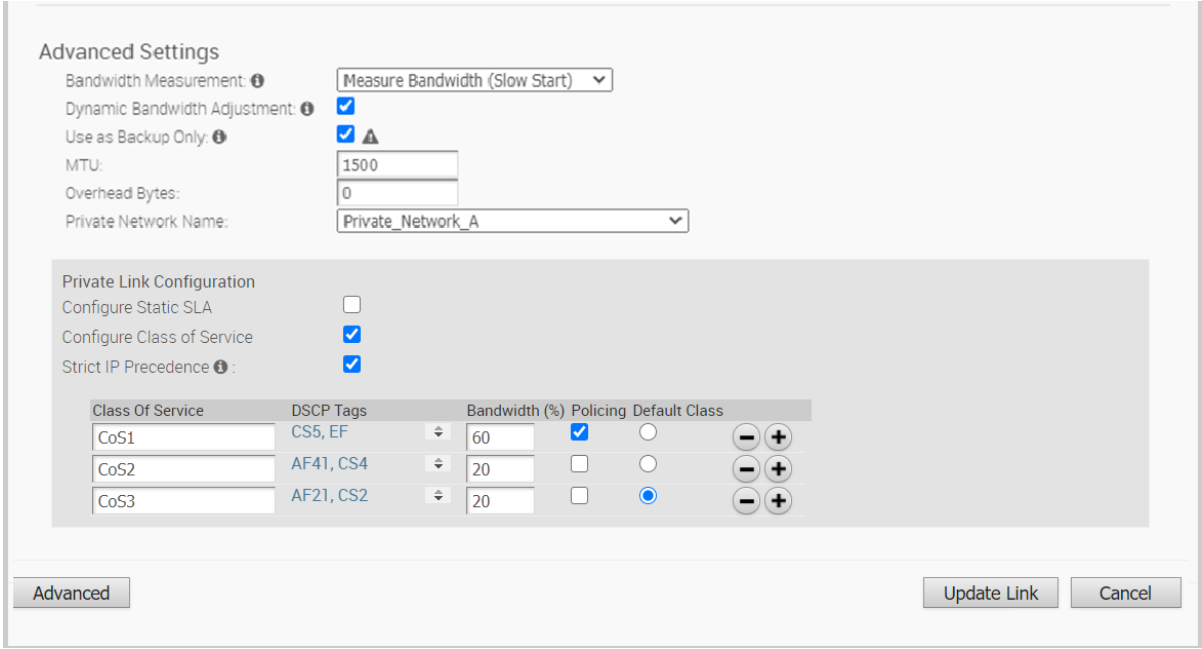
表 15-7. 私人覆疊的進階設定 (Advanced Settings for Private Overlay)

選項	說明
私人網路名稱 (Private Network Name)	如果您有多個私人網路且想要區分這些私人網路，以確保 Edge 僅嘗試通道連線至相同私人網路上的 Edge，請定義私人網路名稱 (Private Network Name)，並將其連結至覆疊。這可防止通道連線至不同私人網路上無法連線的 Edge。此外，請設定此私人網路上其他位置中的 Edge，以使用相同的私人網路名稱。 例如： Edge1 GE1 會連結至私人網路 A。對連結至 GE1 的私人覆疊使用私人網路 A。 Edge1 GE2 會連結至私人網路 B。對連結至 GE2 的私人覆疊使用私人網路 B。 針對 Edge2 重複相同的連結和命名。 當您啟用分支到分支或當 Edge2 為中樞站台時： ■ Edge1 GE1 會嘗試連線至 Edge2 GE1，而非 GE2。 ■ Edge1 GE2 會嘗試連線至 Edge2 GE2，而非 GE1。
設定靜態 SLA (Configure Static SLA)	強制覆疊假設所設定的 SLA 參數是路徑的實際 SLA 值。此覆疊上不會執行封包遺失、延遲或抖動的動態測量。QoE 報告會根據臨界值將這些值著色為綠色/黃色/紅色。 **備註** 自版本 3.4 起不支援靜態 SLA 組態。建議不要使用此選項，因為封包遺失、延遲和抖動的動態測量將提供更佳的結果。

表 15-7. 私人覆疊的進階設定 (Advanced Settings for Private Overlay) (續)

選項	說明
設定服務類別 (Configure Class of Service)	SD-WAN Edges 可以排列流量的優先順序，並同樣提供同時處於網際網路和私人網路的 3x3 QoS 類別矩陣。但是，某些 MPLS 網路包含其自己的服務品質 (QoS) 類別，每個都具有特定特性，例如速率保證、速率限制、封包遺失機率等。 此選項可讓 Edge 瞭解特定介面上私人覆疊可用的私人網路 QoS 頻寬和監控。 **備註** 每個應用程式/規則的商務原則中都必須設定外部 DSCP 標籤，且在此功能中，每個服務類別行都將符合商務原則中所設定的這些 DSCP 標籤。 選取此核取方塊後，請設定下列項目： ■ **服務類別 (Class of Service)**：輸入服務類別的描述性名稱。您在商務原則中選擇 WAN 連結時，可以參考此名稱。請參閱設定連結操控模式。 ■ **DSCP 標籤 (DSCP Tags)**：服務類別將符合此處定義的 DSCP 標籤。使用商務原則指派給每個應用程式的 DSCP 標籤。 ■ **頻寬 (Bandwidth)**：此類別可用的介面傳輸/上傳頻寬百分比，由保證的私人網路 QoS 類別頻寬所決定。 ■ **監控 (Policing)**：此選項會監控服務類別中的流量所使用的頻寬，當流量超過頻寬時，就會對流量進行速率限制。 ■ **預設類別 (Default Class)**：如果流量不屬於任何已定義的類別，該流量將會與預設 CoS 相關聯。 如需服務類別的詳細資訊，請參閱設定 MPLS CoS。
嚴格 IP 優先順序 (Strict IP precedence)	當您選取**設定服務類別 (Configure Class of Service)** 核取方塊時，即可使用此核取方塊。 當您啟用此選項時，會建立與 8 個 IP 優先順序位元對應的 8 個 VCMP 子路徑。當您要將服務類別合併到服務提供者網路中的較少類別數目時，請使用此選項。 依預設，會停用此選項，並針對已設定之服務類別的確切數目建立 VCMP 子路徑。未套用分組。

下圖顯示私人覆疊的進階設定：



7 按一下**更新連結 (Update Link)** 以儲存設定。

設定 MPLS CoS

您可以在私人 WAN 連結中定義服務類別 (CoS)，以管理流量。您可以將類似的流量類型分組為一個類別。CoS 會以服務優先順序的層級處理每個類別。

對於包含私人 WAN 連結的每個 Edge，您可以定義 CoS。

1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 按一下 Edge 旁邊的裝置圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在 **WAN 設定 (WAN Settings)** 區段中，按一下**新增使用者定義的 WAN 覆疊 (Add User Defined WAN Overlay)**，然後選擇**私人 (Private)** 作為連結類型。

4 您也可以按一下**編輯 (Edit)** 以定義現有私人連結的 CoS。

5 在 **WAN 覆疊 (WAN Overlay)** 設定中，按一下**進階 (Advanced)**，然後選取**設定服務類別 (Configure Class of Service)** 核取方塊。當您啟用此選項時，下列設定隨即顯示，請進行適當設定。您可以按一下加號 (+) 圖示以新增多個服務類別。

- **嚴格 IP 優先順序 (Strict IP precedence)**：選取此核取方塊可強制執行嚴格 IP 優先順序。

  當您啟用此選項時，會建立與 8 個 IP 優先順序位元對應的 8 個 VCMP 子路徑。當您要將服務類別合併到服務提供者網路中的較少類別數目時，請使用此選項。

  依預設，會停用此選項，並針對已設定之服務類別的確切數目建立 VCMP 子路徑。未套用分組。

- **服務類別 (Class of Service)**：輸入服務類別的描述性名稱。名稱可以是英數字元和特殊字元的組合。

- **DSCP 標籤 (DSCP Tags)**：按一下**設定 (Set)**，將 DSCP 標籤指派給服務類別。您可以從可用清單中選取多個 DSCP 標籤。

  備註 您應將相同 IP 優先順序的 DSCP 標籤對應至相同的服務類別。CoS 佇列可以是多個類別的彙總，但相同類別的 DSCP 值不可以是多個類別佇列的一部分。

  例如，下列這一組 DSCP 標籤集不可散佈在多個佇列之間：

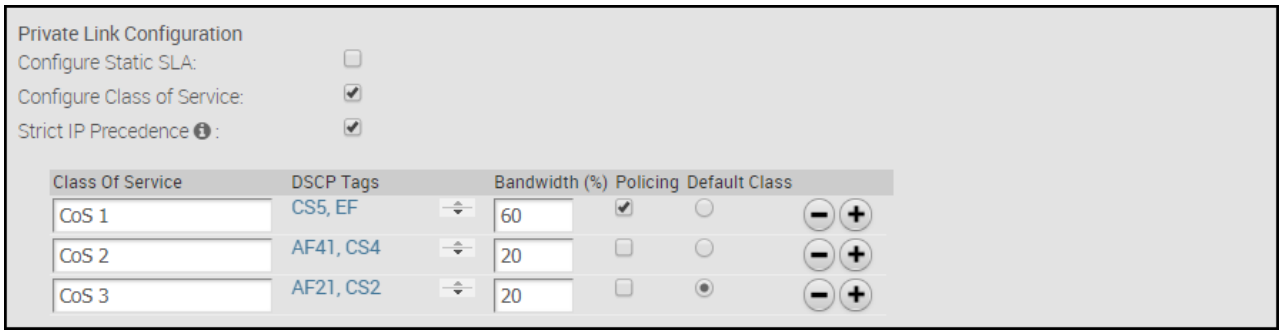
  - CS1 和 AF11 到 AF14
  - CS2 和 AF21 到 AF24
  - CS3 和 AF31 到 AF34
  - CS4 和 AF41 到 AF44

- **頻寬 (Bandwidth)**：為指定至 CoS 的流量輸入百分比值。此值會為類別配置權重。傳入流量會根據相關聯的權重進行處理。如果您有多個類別的服務，則頻寬的總值最多可增加至 100。
- **監控 (Policing)**：選取此核取方塊可啟用以類別為基礎的監控。此選項會監控服務類別中的流量所使用的頻寬，當流量超過頻寬時，就會對流量進行監控。
- **預設類別 (Default Class)**：按一下此選項可將對應的服務類別設定為預設值。如果傳入流量不屬於任何已定義的類別，該流量將會與預設 CoS 相關聯。

6 按一下**更新連結 (Update Link)** 以儲存設定。

下列範例顯示具有不同組 DSCP 標籤的多個服務類別。

服務類別	說明	DSCP 標籤	監控
CoS1	語音	CS5、EF	已啟用
CoS2	視訊	AF41、CS4	已停用
CoS3	檔案傳輸	AF21、CS2	已停用



如需 WAN 覆蓋設定的詳細資訊，請參閱設定 Edge WAN 覆蓋設定。

透過 MPLS 的 SD-WAN 服務可連線性

僅具有私人 MPLS 連結的 Edge，可使用 [可連線的 SD-WAN 服務 (SD-WAN Service Reachable)] 選項連線到位於公有雲中的 Orchestrator 和閘道。

在無法直接存取公用網際網路的站台中，[可連線的 SD-WAN 服務 (SD-WAN Service Reachable)] 選項允許將私人 WAN 用於私人的站台間 VCMP 通道，作為與網際網路所主控 VMware 服務通訊的路徑。

對於僅具有僅限 MPLS 連結或需要容錯移轉至 MPLS 連結的混合環境，您可以啟用 [可連線的 SD-WAN 服務 (SD-WAN Service Reachable)] 選項。

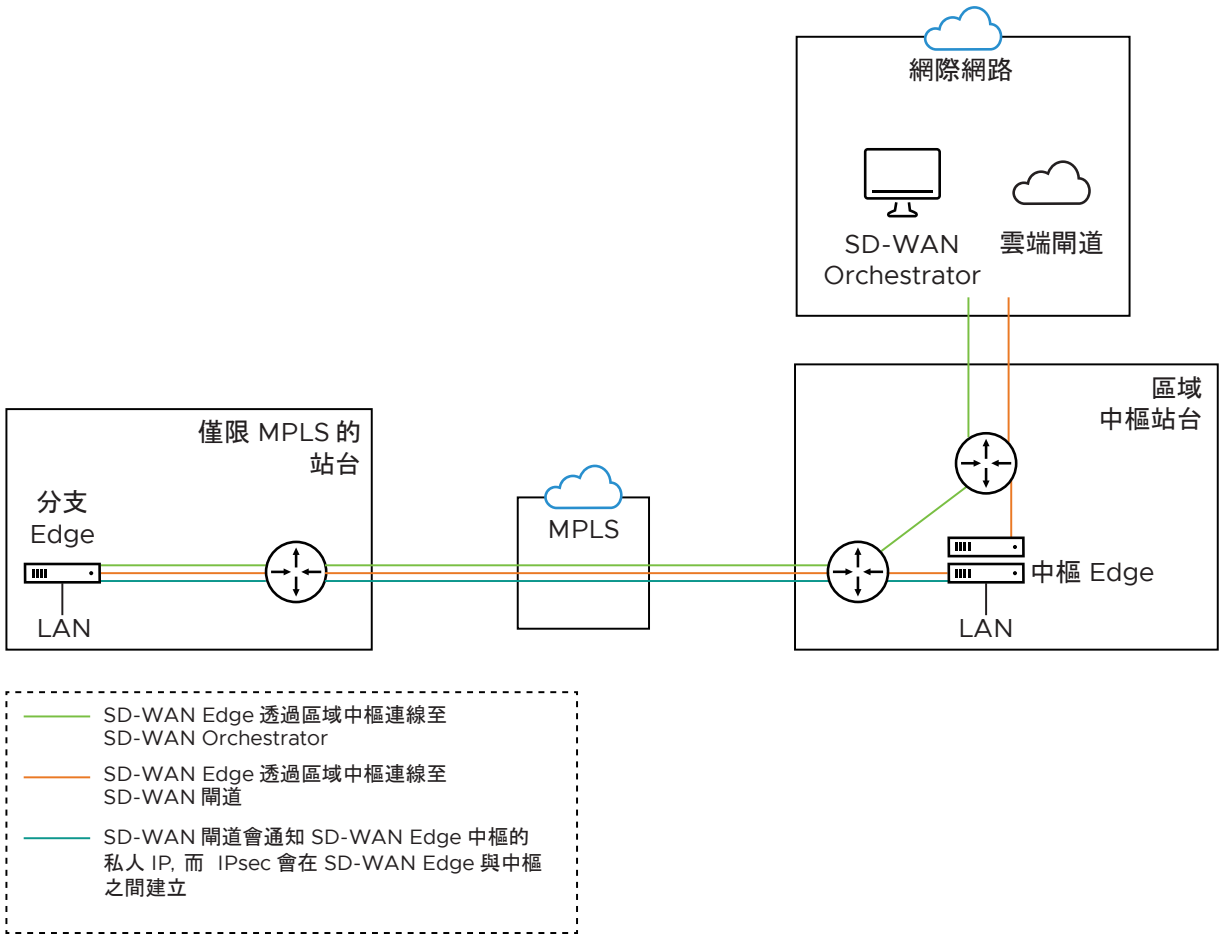
僅限 MPLS 的站台

VMware 支援使用混合環境在僅具有私人 WAN 連結的站台中部署的客戶，以主控的 VMware 服務進行私人 WAN 部署。

在不具公用覆蓋的站台中，私人 WAN 可作為與 VMware 服務進行通訊的主要機制，其中包括：

- 已啟用透過私人連結的 SD-WAN 服務可連線性
- 已啟用使用私人 NTP 伺服器的 NTP 覆寫

下圖顯示具有網際網路連線的區域中樞，以及僅具有 MPLS 連線的 SD-WAN Edge。



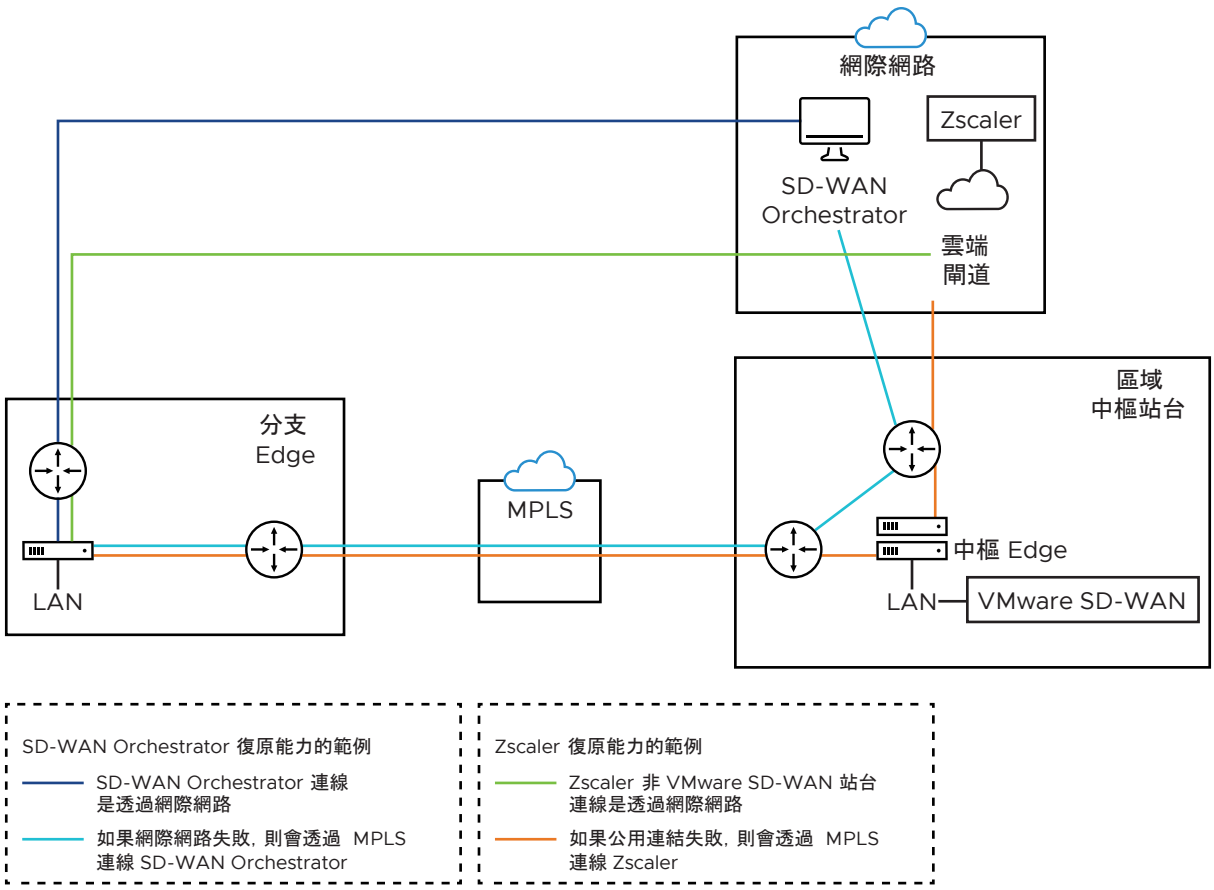
具有僅限 MPLS 連結的 SD-WAN Edge 所傳輸的流量，會透過區域中樞路由至 Orchestrator 和閘道，藉此能夠分流至公有雲。[可連線的 SD-WAN 服務 (SD-WAN Service Reachable)] 選項可讓 Edge 保持線上狀態，且可從 Orchestrator 進行管理，並且允許透過閘道進行公用網際網路連線，無論是否有公用連結連線。

透過 MPLS 的動態容錯移轉

如果所有公用網際網路連結皆失敗，您可以將重要的網際網路流量容錯移轉至私人 WAN 連結。

備註 無論優先順序或服務類別如何，分類為 [直接導向網際網路 (Direct to Internet)] 的流量均不會容錯移轉至私人 WAN 連結。也就是說，即使優先順序為 [高 (High)] 且服務類別為 [即時 (Real Time)]，網路服務為 [直接 (Direct)] 的流量也不會容錯移轉至私人連結。只有分類為 [多路徑 (Multipath)] 的流量才會容錯移轉至私人連結。

下圖說明 SD-WAN Orchestrator 和 Non VMware SD-WAN Site Zscaler 的復原能力。



- **Orchestrator 復原能力 (Orchestrator Resiliency)** – Orchestrator 會連線至網際網路。如果網際網路失敗，Orchestrator 將透過 MPLS 進行連線。Orchestrator 連線是使用透過 MPLS 通告的 IP 位址而建立的。連線會使用區域中樞的公用網際網路連結。

- **Zscaler 復原能力 (Zscaler Resiliency)** – Zscaler 連線會透過網際網路來建立。如果公用連結失敗，則 Zscaler 會透過 MPLS 進行連線。

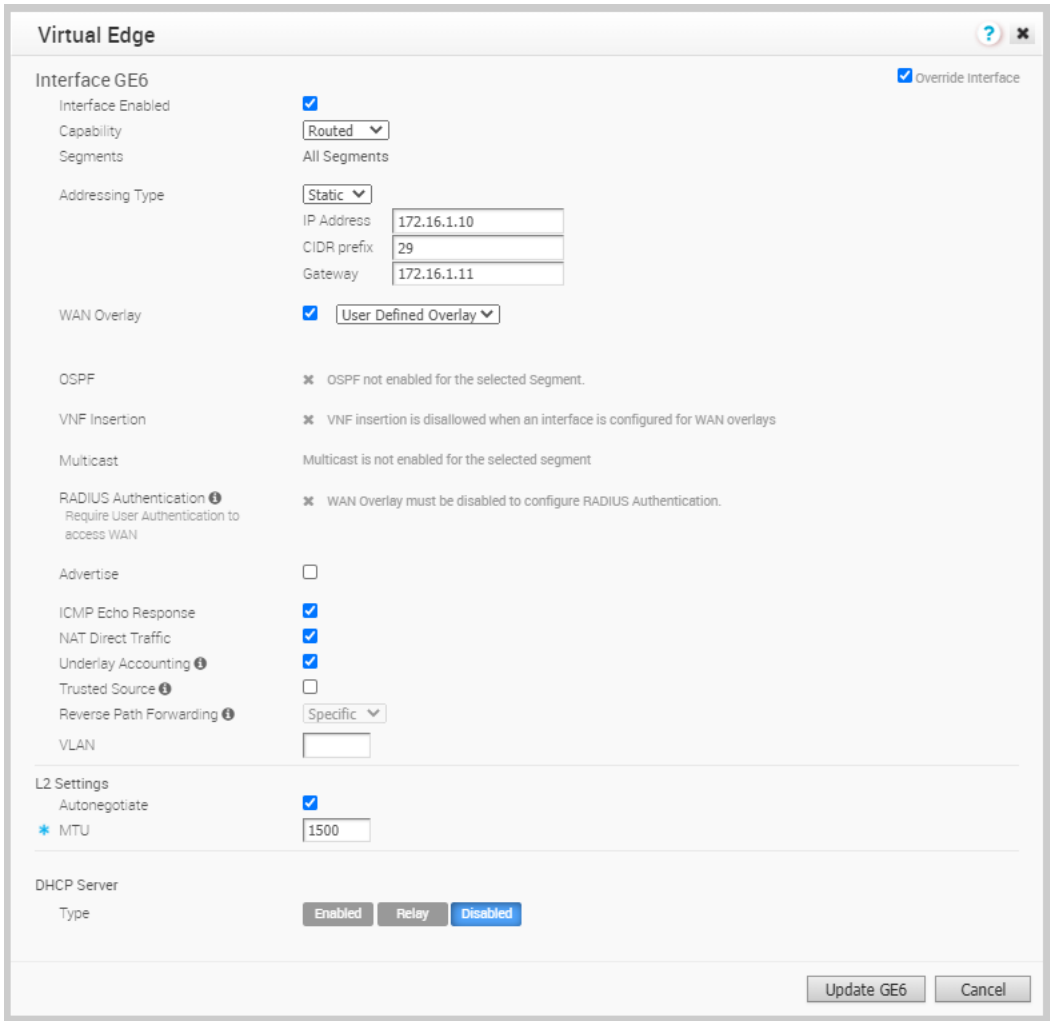
設定可連線的 SD-WAN 服務

1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 在 [Edge] 頁面中按一下 Edge 旁的裝置圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 向下捲動至**介面設定 (Interface Settings)**，並**編輯**連線至 MPLS 連結的介面。

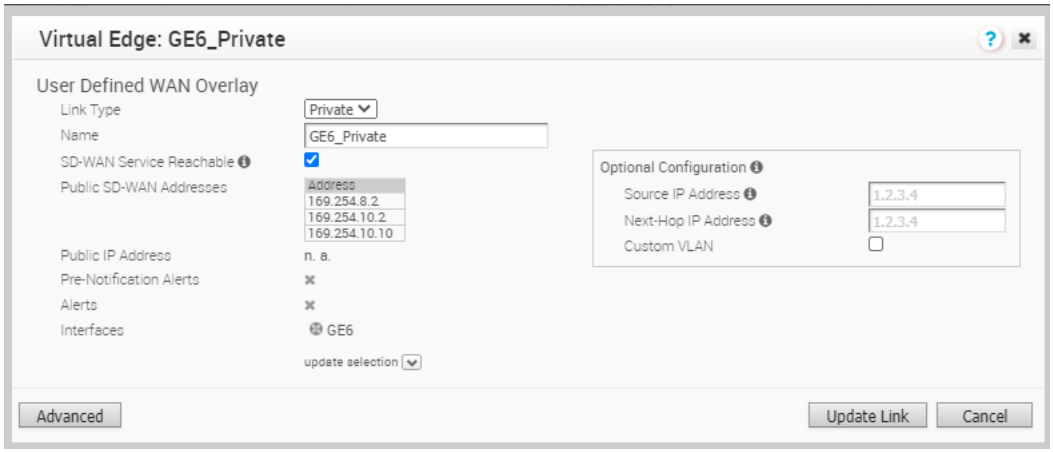
4 在**介面 (Interface)** 視窗中，選取**使用者定義的覆疊 (User Defined Overlay)** 核取方塊。



可連線的 SD-WAN 服務 (SD-WAN Service Reachable) 僅適用於**使用者定義的覆疊 (User Defined Overlay)** 網路。

5 在 **WAN 設定 (WAN Settings)** 區段中，**編輯**已啟用**使用者定義的覆疊 (User Defined Overlay)** 的介面。

6 在**使用者定義的 WAN 覆疊 (User Defined WAN Overlay)** 視窗中，選取**可連線的 SD-WAN 服務 (SD-WAN Service Reachable)** 核取方塊，以部署僅具有私人 WAN 連結的站台，和/或啟用將重要網際網路流量容錯移轉至私人 WAN 連結的功能。



當您選取**可連線的 SD-WAN 服務 (SD-WAN Service Reachable)** 核取方塊時，將會顯示 SD-WAN Gateways 和 SD-WAN Orchestrator 的公用 IP 位址清單，如果預設路由尚未從防火牆通告至相同的私人網路，則可能需要在私人網路之間通告這些位址。

7 視需要設定其他選項，然後按一下**更新連結 (Update Link)** 以儲存設定。

如需 **WAN 覆疊 (WAN Overlay)** 視窗中其他選項的詳細資訊，請參閱設定 Edge WAN 覆疊設定。

設定 Edge 的 SNMP 設定

SNMP 是網路監控常用的通訊協定，而 MIB 是與 SNMP 相關聯以管理實體的資料庫。若要啟用 SNMP，請選取所需的 SNMP 版本，如下列步驟中所述。在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 SNMP 設定。

備註 SD-WAN Edge 不會產生 SNMP 設陷。如果在 Edge 層級發生故障，Edge 會以事件形式向 SD-WAN Orchestrator 報告故障，SD-WAN Orchestrator 進而會根據針對所接收事件設定的警示來產生設陷。

開始之前：

- 若要下載 SD-WAN Edge MIB：請移至**遠端診斷 (Remote Diagnostics)** 畫面 (**測試和疑難排解 (Test & Troubleshooting) > 遠端診斷 (Remote Diagnostics)**)，然後針對 SD-WAN Edge 執行 MIB。將結果複製並貼到本機電腦上。
- 在 SNMP 管理器上安裝 VELOCLOUD-EDGE-MIB 所需的所有 MIB，包括 SNMPv2-SMI、SNMPv2-CONF、SNMPv2-TC、INET-ADDRESS-MIB、IF-MIB、UUID-TC-MIB 和 VELOCLOUD-MIB。上述所有的 MIB 皆可從 [遠端診斷 (Remote Diagnostics)] 頁面取得。

關於此工作：在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 SNMP 設定。[Edge 覆寫 (Edge Override)] 選項可用來對顯示的設定進行 Edge 特定編輯，以及停止來自組態設定檔對此模組的後續自動更新。若要維持持續的一致性並簡化更新，建議您在設定檔中設定組態，而非 Edge 例外狀況層級設定。

支援的 MIB

- SNMP MIB-2 系統
- SNMP MIB-2 介面
- VELOCLOUD-EDGE-MIB
- HOST-RESOURCES-MIB，來自 RFC 1514

在 Edge 層級設定 SNMP 設定的程序：

1 在 SD-WAN Orchestrator 的 [遠端診斷 (Remote Diagnostic)] 畫面上取得 VELOCLOUD-EDGE-MIB。

2 安裝 VELOCLOUD-EDGE-MIB 所需的所有 MIB。

3 從 SD-WAN Orchestrator，移至**設定 (Configure) > Edge**。

4 選取您要為其設定 SNMP 設定的 Edge，然後按一下 [裝置 (Device)] 資料行下的**裝置 (Device)** 圖示。

所選 Edge 的**組態 Edge (Configuration Edges)** 畫面隨即出現。

5 向下捲動至 **SNMP 設定 (SNMP Settings)** 區域，然後勾選**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。您有兩個版本可供選擇：v2c 或 v3。

6 若要設定 SNMP v2c，請依照下列步驟操作：

a 勾選 **v2c** 核取方塊。

b 在**連接埠 (Port)** 文字方塊中輸入連接埠。預設設定為 161。

c 在**社群 (Community)** 文字方塊中輸入文字或數字序列，這將作為讓您存取 SNMP 代理程式的「密碼」。

d 針對允許的 IP：

- 勾選**任何 (Any)** 核取方塊，以允許任何 IP 存取 SNMP 代理程式。
- 若要限制對 SNMP 代理程式的存取，請取消選取**任何 (Any)** 核取方塊，然後輸入將可存取 SNMP 代理程式的 IP 位址。

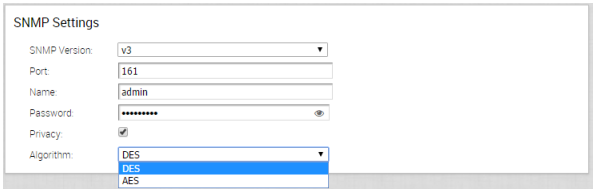
7 針對提供更高安全性支援的 SNMP v3 組態，請依照下列步驟操作：

a 在**連接埠 (Port)** 文字方塊中輸入連接埠。161 是預設設定。

b 在適當的文字方塊中輸入使用者名稱和密碼。

c 如果您要讓封包傳輸加密，請勾選**隱私權 (Privacy)** 核取方塊。

d 如果您已勾選**隱私權 (Privacy)** 核取方塊，請從 **演算法 (Algorithm)** 下拉式功能表中選擇 DES 或 AES。



8 設定防火牆設定。設定 SNMP 設定後，請移至防火牆設定 (**設定 (Configure) > 設定檔 (Profiles) > 防火牆 (Firewall)**)，以設定將啟用 SNMP 設定的防火牆設定。

備註 已啟用 DPDK 的介面支援 3.3.0 及更新版本的 SNMP 介面監控。

設定 Wi-Fi 無線電覆寫

在 Edge 層級，您可以選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊，以覆寫設定檔中指定的 Wi-Fi 無線電設定。根據 Edge 型號和為 Edge 設定的國家/地區，Wi-Fi 無線電設定可讓您選取 Edge 支援的無線電頻帶和通道。

若要覆寫 Edge 層級的 Wi-Fi 無線電設定，請執行下列步驟。

必要條件

- 為 Edge 設定 Wi-Fi 無線電頻帶和通道之前，請務必為 Wi-Fi 無線電設定正確的營運國家/地區，以符合 Wi-Fi 傳輸的當地需求。確定營運此 Edge 的正確國家/地區設定於 **Edge 概觀 (Edge Overview)** 組態頁面的**連絡人和位置 (Contact & Location)** 區段中。位址會在 Edge 啟動後自動填入；但您可以視需要手動覆寫位址。

  備註 國家/地區應使用 2 個字元的 ISO 3166-1-Alpha-2 表示法 (例如 US、DE、IN 等) 指定。

程序

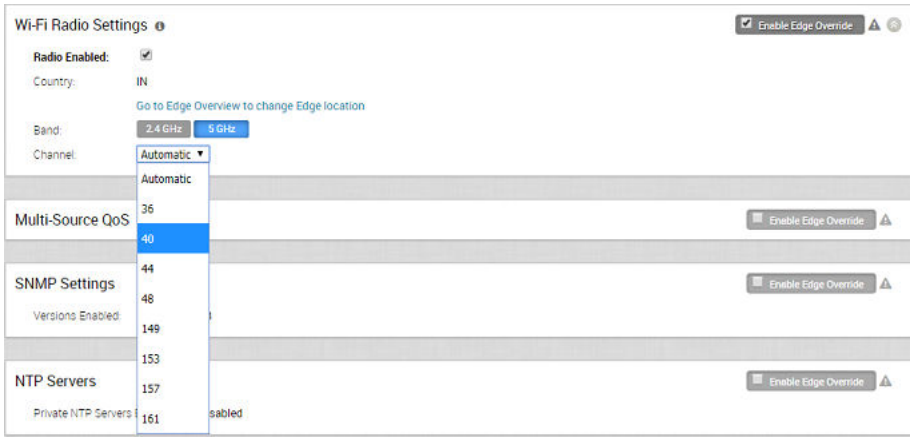
1 從 SD-WAN Orchestrator，移至**設定 (Configure)** > **Edge**。

2 選取要覆寫 Wi-Fi 無線電設定的 Edge，然後按一下**裝置 (Device)** 資料行下的圖示。

所選 Edge 的**裝置設定 (Device Settings)** 頁面隨即出現。

3 在**設定區段 (Configure Segment)** 下拉式功能表中，依預設會選取**全域區段 [一般] (Global Segment [Regular])**。如有需要，您可以從下拉式功能表中選取不同的設定檔區段。

4 移至 **Wi-Fi 無線電設定 (Wi-Fi Radio Settings)** 區域，然後選取**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。



5 從 Edge 支援的無線電頻率的**頻帶 (Band)** 中選取無線電頻帶。

6 在**通道 (Channel)** 下拉式功能表中，選取 Edge 支援的無線電通道。

備註 **頻帶 (Band)** 和**通道 (Channel)** 選取器只會顯示已設定 Edge 位置支援的無線電頻帶和通道。

7 如果您想要變更 Edge 的位置，請按一下**移至 Edge 概觀以變更 Edge 位置 (Go to Edge Overview to change edge location)**。所選 Edge 的 **Edge 概觀 (Edge Overview)** 頁面隨即出現。

a 在**連絡人和位置 (Contact & Location)** 區域中，按一下**更新位置 (Update Location)** 連結以設定 Edge 位置，然後按一下**儲存變更 (Save Changes)**。

8 按一下**儲存變更 (Save Changes)**。此時會覆寫所選 Edge 的 Wi-Fi 無線電設定。

備註 若未設定 Edge 的國家/地區，或者國家/地區無效，則無線電**頻帶 (Band)** 會設定為 **2.4 GHz**，**通道 (Channel)** 會設定為**自動 (Automatic)**。

安全性 VNF

虛擬網路功能 (VNF) 是個別網路服務，例如路由器和防火牆，在一般硬體上作為僅限軟體的虛擬機器 (VM) 執行個體執行。例如，路由 VNF 會實作路由器的所有功能，但在一般硬體上會以僅限軟體形式獨立執行或連同其他 VNF 一起執行。VNF 會在 NFV 架構內進行管理和協調。

NFV 和 VNF 的虛擬化表示以通用方式 (獨立於基礎硬體) 實作網路功能。VNF 可以在分公司、雲端或資料中心的任何虛擬機器環境中執行。此架構可讓您：

- 在最佳位置插入網路服務，以提供適當的安全性。例如，在連線網際網路的分公司中插入 VNF 防火牆，而非透過相距遙遠的防火牆內資料中心使流量繞道，從而造成 MPLS 連結的效率降低。
- 最佳化應用程式效能。使用 VNF 的安全性或流量優先順序，流量可以遵循使用者與雲端應用程式之間的最直接路由。在虛擬機器環境中，多個 VNF 可能會同時執行、彼此隔離，並且可以獨立變更或升級。

下表列出 VMware 支援的第三方防火牆，以及支援對照表：

表 15-8. Palo Alto Networks 防火牆 – 支援對照表

VMware SD-WAN Edge 平台	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
建議的虛擬機器系列防火牆模型	VM-50 Lite	VM-100	VM-50 Lite	VM-100	VM-100
可供虛擬機器系列防火牆使用的 vCPU 數目	2	2	2	2	2
可供 VNF 使用的記憶體	4.5 GB	6.5 GB	4.5 GB	6.5 GB	6.5 GB
Edge 上可供 VNF 使用的儲存空間	64 GB	120 GB	64 GB	120 GB	120 GB
VMware 軟體版本	3.2.0 版或更新版本	3.2.0 版或更新版本	3.4.3 版或更新版本	3.4.3 版或更新版本	3.4.3 版或更新版本
Panorama 版本	8.0.5 版或更新版本	8.0.5 版或更新版本	8.0.5 版或更新版本	8.0.5 版或更新版本	8.0.5 版或更新版本

表 15-9. Check Point 防火牆 – 支援對照表

VMware SD-WAN Edge 平台	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
可供 VNF 使用的記憶體	2 GB	4 GB	2 GB	4 GB	4 GB
可供 VNF 使用的 vCPU 數目	2	2	2	2	2
Edge 上可供 VNF 使用的儲存區	64 GB	100 GB	120 GB	120 GB	120 GB
SD-WAN 和 CheckPoint VNF 的最大總流量	100 Mbps	550 Mbps	100 Mbps	350 Mbps	500 Mbps
VMware 軟體版本	3.3.2 版或更新版本	3.3.2 版或更新版本	3.4.3 版或更新版本	3.4.3 版或更新版本	3.4.3 版或更新版本
Checkpoint VNF 作業系統版本	R77.20 版或更新版本	R77.20 版或更新版本	R77.20 版或更新版本	R77.20 版或更新版本	R77.20 版或更新版本
Checkpoint 管理程式軟體版本	80.30 版或更新版本	80.30 版或更新版本	80.30 版或更新版本	80.30 版或更新版本	80.30 版或更新版本

表 15-10. Fortinet 防火牆 – 支援對照表

VMware SD-WAN Edge 平台	Edge 520v	Edge 840
建議的虛擬機器系列防火牆模型	VM00、VM01	VM00、VM01、VM02
可供 VNF 使用的記憶體	2 GB	4 GB
可供 VNF 使用的 vCPU 數目	2	2
Edge 上可供 VNF 使用的儲存區	64 GB	100 GB

表 15-10. Fortinet 防火牆 – 支援對照表 (續)

VMware SD-WAN Edge 平台	Edge 520v	Edge 840
SD-WAN 和 FortiGate VNF 的最大總流量	100 Mbps	500 Mbps
VMware 軟體版本	3.3.1 版或更新版本	3.3.1 版或更新版本
FortiOS 版本	6.0 和 6.2.0 版	6.0 和 6.2.0 版

您可以透過 SD-WAN Edge 上的 VNF 部署及轉送流量。

設定 VNF 管理服務

VMware 支援可用作 VNF 以透過 Edge 傳遞流量的第三方防火牆。

選擇第三方防火牆，然後據以進行設定。您可能還需要在第三方防火牆中進行其他設定。請參閱對應第三方防火牆的部署指南，以進行其他組態。

對於 VNF 類型 **Check Point 防火牆 (Check Point Firewall)** 和 **Fortinet 防火牆 (Fortinet Firewall)**，使用系統內容 **edge.vnf.extraImageInfos** 來設定 VNF 映像。您必須是操作員使用者，才能設定系統內容。如果您沒有操作員角色存取權，請連絡您的操作員來設定 VNF 映像。

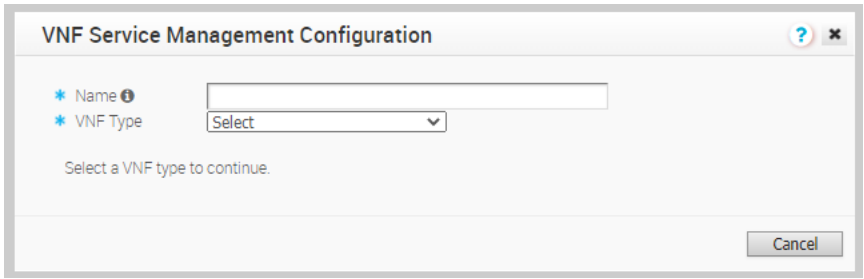
備註 您必須在系統內容中提供正確的總和檢查碼值。Edge 會計算已下載 VNF 映像的總和檢查碼，並將值與系統內容中的可用值進行比較。只有當總和檢查碼值相同時，Edge 才會部署 VNF。

程序

1 在企業入口網站中，按一下**設定 (Configure) > 網路服務 (Network Services)**。

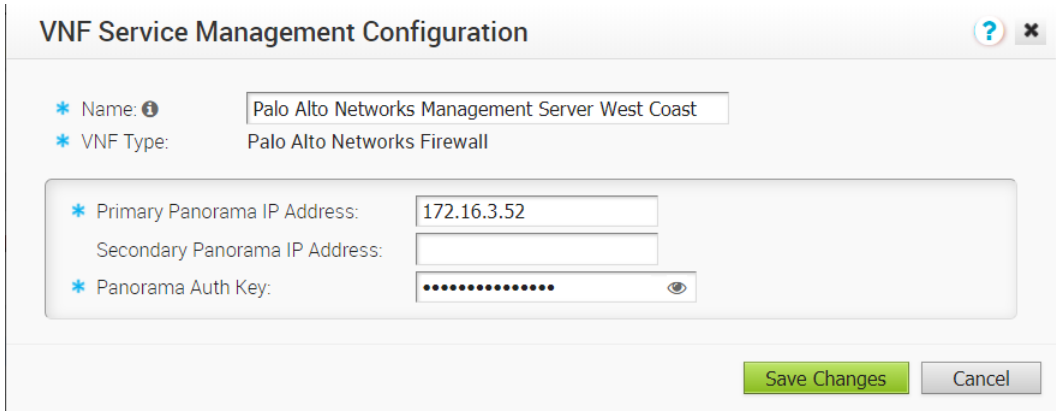
2 在**服務 (Services)** 頁面中，向下捲動至 **VNF** 區段，然後按一下**新增 (New)**。

3 在 **VNF 服務管理組態 (VNF Service Management Configuration)** 視窗中，輸入安全性 VNF 服務的描述性名稱，然後從下拉式清單中選取 VNF 類型。



4 根據選取的 VNF 類型進行設定。

a 對於 VNF 類型 **Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)**，請設定下列項目：



1 **主要 Panorama IP 位址 (Primary Panorama IP Address)** – 輸入 Panorama 伺服器的主要 IP 位址。

2 **次要 Panorama IP 位址 (Secondary Panorama IP Address)** – 輸入 Panorama 伺服器的次要 IP 位址。

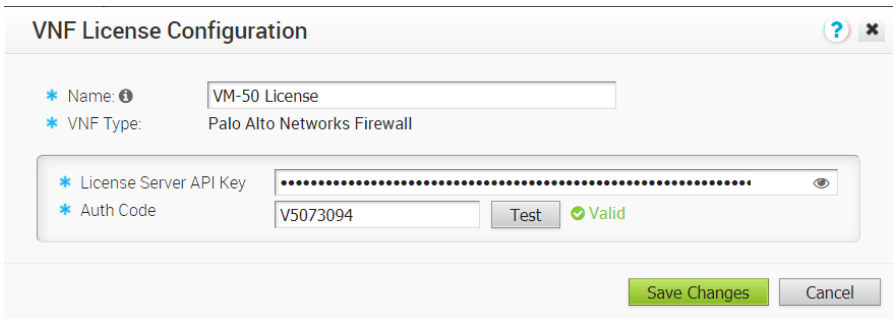
3 **Panorama 驗證金鑰 (Panorama Auth Key)** – 輸入在 Panorama 伺服器上設定的驗證金鑰。VNF 會使用驗證金鑰登入 Panorama 並與其通訊。

4 按一下**儲存變更 (Save Changes)**。

將 Palo Alto 網路設定為 VNF 類型後，請定義 VNF 授權。這些授權將套用到一或多個 VNF 設定的 Edge。

1 在**服務 (Services)** 頁面中，向下捲動至 **VNF 授權 (VNF Licenses)** 區段，然後按一下**新增 (New)**。

2 在 **VNF 授權組態 (VNF License Configuration)** 視窗中，設定下列項目：



- **名稱 (Name)** – 輸入 VNF 授權的描述性名稱。
- **VNF Type (VNF 類型)** – 從下拉式清單中選取 VNF 類型。目前，**Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)** 是唯一可用的選項。

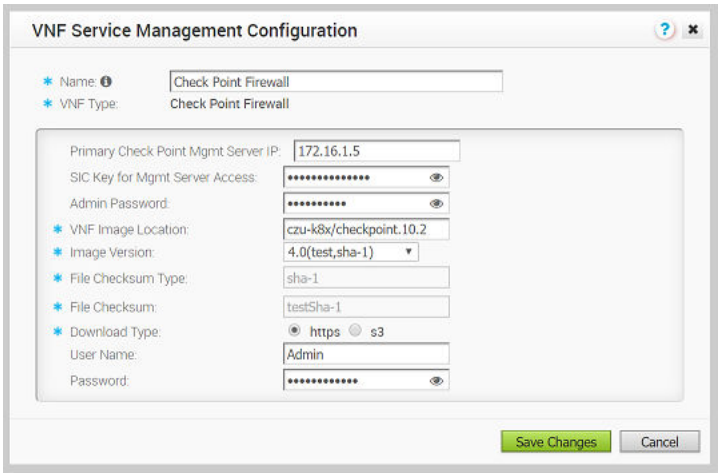
- **授權伺服器 API 金鑰 (License Server API Key)** – 輸入您 Palo Alto Networks 帳戶中的授權金鑰。SD-WAN Orchestrator 可使用此金鑰與 Palo Alto Networks 授權伺服器進行通訊。
- **驗證碼 (Auth Code)** – 輸入從 Palo Alto Networks 購買的授權碼。
- 按一下**測試 (Test)** 以驗證組態。

3 按一下**儲存變更 (Save Changes)**。

將 **Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)** 設定為 Edge 上的 VNF 類型時，您可以套用 VNF 授權。

備註 如果您想要從 VNF 類型移除 **Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)** 組態部署，請確認您先停用 Palo Alto Networks 的 **VNF 授權 (VNF License)**，然後再移除組態。

b 對於 VNF 類型 **Check Point 防火牆 (Check Point Firewall)**，請設定下列項目：



1 **主要 Check Point 管理伺服器 IP (Primary Check Point Mgmt Server IP)** – 輸入將連線至 Check Point 防火牆的 Check Point 智慧型主控台 IP 位址。

2 **管理伺服器存取的 SIC 金鑰 (SIC Key for Mgmt Server Access)** – 輸入用來向 Check Point 智慧型主控台登錄 VNF 的密碼。

3 **管理員密碼 (Admin Password)** – 輸入管理員密碼。

4 **VNF 映像位置 (VNF Image Location)** – 輸入 SD-WAN Orchestrator 將下載 VNF 映像的映像位置。

5 **映像版本 (Image Version)** – 從下拉式清單中選取 Check Point VNF 映像的版本。映像版本衍生自系統內容 **edge.vnf.extraImageInfos**。

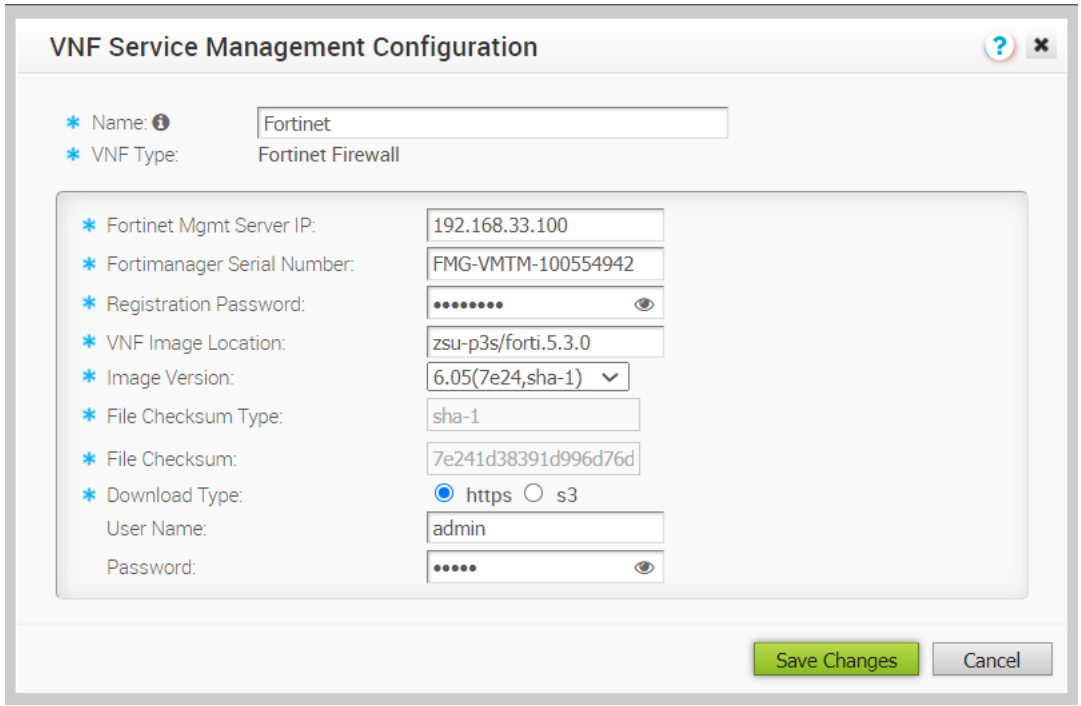
6 **檔案總和檢查碼類型 (File Checksum Type)** – 指定用來驗證 VNF 映像的方法，並在您選取映像版本後自動填入。

7 **檔案總和檢查碼 (File Checksum)** – 指定用來驗證 VNF 映像的總和檢查碼，並在您選取映像版本後自動填入。總和檢查碼值衍生自系統內容 **edge.vnf.extraImageInfos**。

8 **下載類型 (Download Type)** – 選擇映像的類型。對於 **https**，請輸入使用者名稱和密碼。對於 **s3**，請輸入 AccessKeyid 和 SecretAccessKey。

9 按一下**儲存變更 (Save Changes)**。

c 對於 VNF 類型 **Fortinet 防火牆 (Fortinet Firewal)**，請設定下列項目：



1 **Fortinet 管理伺服器 IP (Fortinet Mgmt Server IP)** – 輸入 FortiManager 的 IP 位址，以連線至 FortiGate。

2 **Fortimanager 序號 (Fortimanager Serial Number)** – 輸入 FortiManager 的序號。

3 **登錄密碼 (Registration Password)** – 輸入用來向 FortiManager 登錄 VNF 的密碼。

4 **VNF 映像位置 (VNF Image Location)** – 輸入 SD-WAN Orchestrator 將下載 VNF 映像的映像位置。

5 **映像版本 (Image Version)** – 從下拉式清單中選取 Fortinet VNF 映像的版本。可用選項如下：6.0.5 和 6.20。映像版本衍生自系統內容 **edge.vnf.extraImageInfos**。

6 **檔案總和檢查碼類型 (File Checksum Type)** – 指定用來驗證 VNF 映像的方法，並在您選擇映像版本後自動填入。

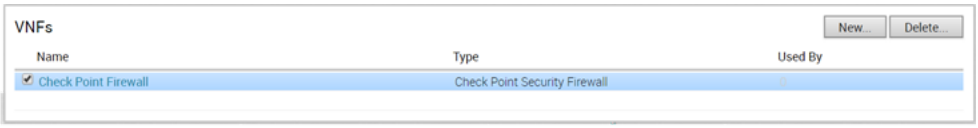
7 **檔案總和檢查碼 (File Checksum)** – 指定用來驗證 VNF 映像的總和檢查碼，並在您選取映像版本後自動填入。總和檢查碼值衍生自系統內容 **edge.vnf.extraImageInfos**。

8 **下載類型 (Download Type)** – 選擇映像的類型。對於 **https**，請輸入使用者名稱和密碼。對於 **s3**，請輸入 AccessKeyid 和 SecretAccessKey。

9 按一下**儲存變更 (Save Changes)**。

結果

VNF 區段會顯示所建立的 VNF 服務。下圖顯示 VNF 類型 (VNF Type) 為 Check Point 防火牆 (Check Point Firewall) 的範例。



後續步驟

您可以為 Edge 設定安全性 VNF，以透過 VNF 管理服務來導向流量。請參閱設定安全性 VNF。

設定安全性 VNF

您可以使用第三方防火牆，透過 SD-WAN Edge 上的 VNF 部署及轉送流量。

只有操作員可以啟用安全性 VNF 組態。如果您無法使用安全性 VNF (Security VNF) 選項，請連絡您的操作員。

必要條件

確保您具有下列項目：

- SD-WAN Orchestrator 及已啟動並執行支援部署特定安全性 VNF 軟體版本的 SD-WAN Edge。如需有關受支援軟體版本和 Edge 平台的詳細資訊，請參閱安全性 VNF 中的支援對照表。
- VNF Manager 附加元件授權。
- 已設定 VNF 管理服務。如需詳細資訊，請參閱設定 VNF 管理服務。

程序

1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 在 **Edge** 頁面中按一下 Edge 旁的**裝置 (Device)** 圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 索引標籤中，向下捲動至**安全性 VNF (Security VNF)** 區段，然後按一下**編輯 (Edit)**。

4 在 **Edge VNF 組態 (Edge VNF Configuration)** 視窗中，勾選**部署 (Deploy)** 核取方塊。

5 在**虛擬機器組態 (VM Configuration)** 中設定下列項目：

   a **VLAN** – 從下拉式清單中選擇要用於 VNF 管理的 VLAN。

   b **VM-1 IP** – 輸入虛擬機器的 IP 位址，並確保 IP 位址位於所選 VLAN 的子網路範圍內。

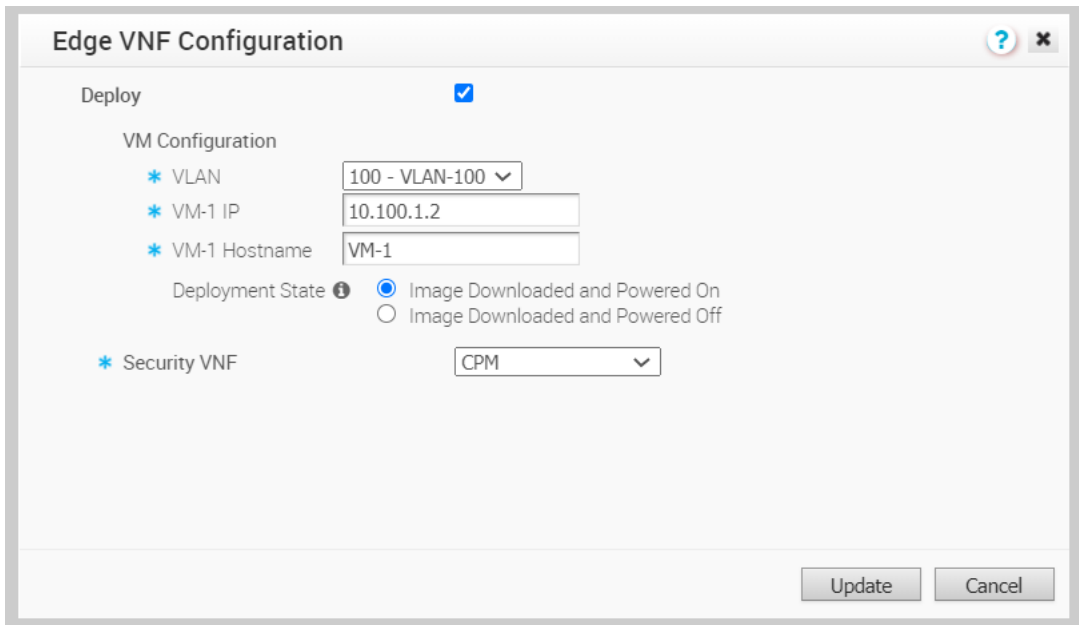
   c **VM-1 主機名稱 (VM-1 Hostname)** – 輸入虛擬機器主機的名稱。

d **部署狀態 (Deployment State)** – 選擇以下其中一個選項：

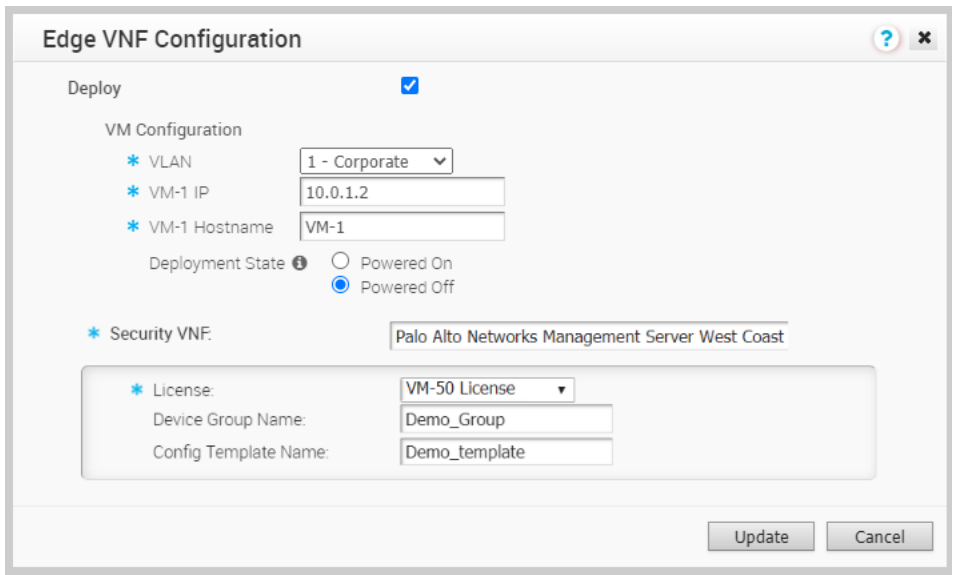
- **映像已下載並開啟電源 (Image Downloaded and Powered On)** – 此選項會在 Edge 上建置防火牆 VNF 後開啟虛擬機器的電源。只有在選擇此選項時，流量才會傳送 VNF，這需要至少為 VNF 插入設定一個 VLAN 或路由介面。
- **映像已下載並關閉電源 (Image Downloaded and Powered Off)** – 此選項會在 Edge 上建置防火牆 VNF 後保持虛擬機器的電源關閉。如果您想要透過 VNF 傳送流量，請勿選取此選項。

e **安全性 VNF (Security VNF)** – 從下拉式清單中選擇預先定義的 VNF 管理服務。您也可以按一下 **新增 VNF 服務 (New VNF Service)**，以建立新的 VNF 管理服務。如需詳細資訊，請參閱設定 VNF 管理服務。

下圖顯示 **Check Point 防火牆 (Check Point Firewall)** 作為安全性 VNF (Security VNF) 類型的範例。



如果您選擇 **Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)** 作為安全性 VNF，請設定下列其他設定：

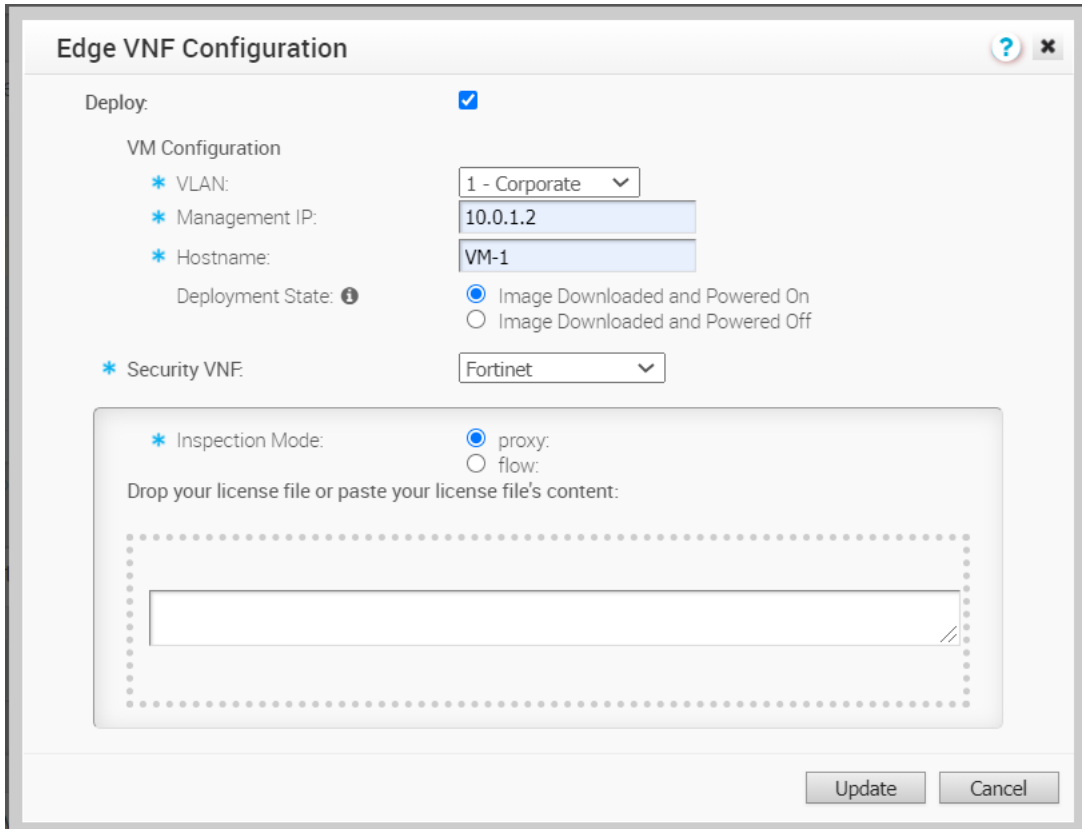


- **授權 (License)** – 從下拉式清單中選取 VNF 授權。
- **裝置群組名稱 (Device Group Name)** – 輸入在 Panorama 伺服器上預先設定的裝置群組名稱。

- **組態範本名稱 (Config Template Name)** – 輸入在 Panorama 伺服器上預先設定的組態範本名稱。

備註 如果您想要從 VNF 類型移除 **Palo Alto Networks 防火牆 (Palo Alto Networks Firewall)** 組態部署，請確認您先停用 Palo Alto Networks 的 **VNF 授權 (VNF License)**，然後再移除組態。

如果您選擇 **Fortinet Firewall (Fortinet 防火牆)**，請設定下列其他設定：



- **檢查模式 (Inspection Mode)** – 選擇以下其中一個選項：
  - **Proxy** – 依預設會選取此選項。以 Proxy 為基礎的檢查涉及緩衝流量，以及檢查整體資料以進行分析。
  - **流量 (Flow)** – 以流量為基礎的檢查會在流量資料透過 FortiGate 單位傳遞而不進行任何緩衝時檢查流量資料。
- **授權 (License)** – 拖放虛擬機器授權。

f 按一下**更新 (Update)**。

結果

組態詳細資料會顯示在**安全性 VNF (Security VNF)** 區段中。

後續步驟

如果您想要將多個流量區段重新導向至 VNF，請定義區段與服務 VLAN 之間的對應。請參閱使用服務 VLAN 定義對應區段

您可以將安全性 VNF 插入 VLAN 以及路由介面，以將流量從 VLAN 或路由介面重新導向至 VNF。請參閱設定含 VNF 插入的 VLAN。

使用服務 VLAN 定義對應區段

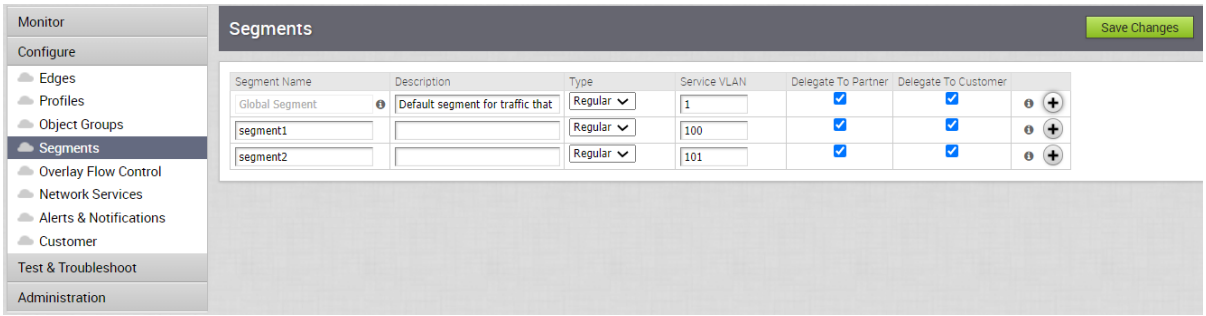
當您想要將多個流量區段重新導向至安全性 VNF 時，請定義區段與服務 VLAN 之間的對應。

將區段與服務 VLAN 對應：

程序

1 在企業入口網站中，按一下**設定 (Configure) > 區段 (Segments)**。

2 在**區段 (Segments)** 頁面中，輸入每個區段的服務 VLAN 識別碼。



3 按一下**儲存變更 (Save Changes)**。

結果

系統會將唯一的 VLAN 識別碼指派給插入 VNF 的區段。VNF 上的防火牆原則可使用這些 VLAN 識別碼來定義。來自這些區段內 VLAN 和介面的流量，皆會使用為指定區段配置的 VLAN 識別碼加以標記。

後續步驟

將安全性 VNF 插入 VLAN 或路由介面，以將流量從 VLAN 或路由介面重新導向至 VNF。請參閱設定含 VNF 插入的 VLAN。

設定含 VNF 插入的 VLAN

您可以將安全性 VNF 插入 VLAN 以及路由介面。

必要條件

確保您已建立安全性 VNF，並已進行設定。請參閱設定安全性 VNF。

將區段與服務 VLAN 對應，以啟用 VNF 插入 VLAN。請參閱使用服務 VLAN 定義對應區段。

程序

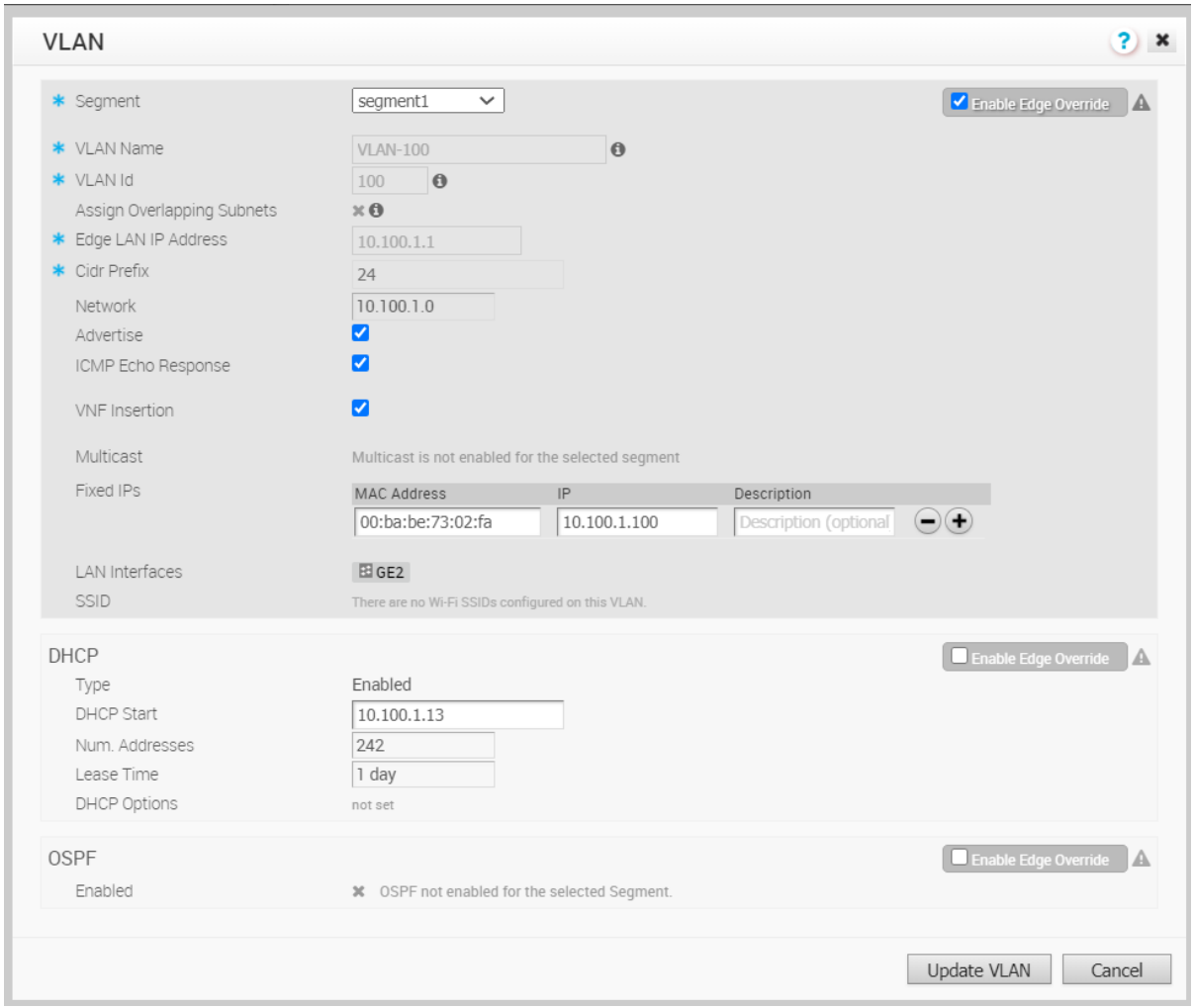
1 在企業入口網站中，按一下**設定 (Configure) > Edge**。

2 在 **Edge** 頁面中按一下 Edge 旁的**裝置 (Device)** 圖示，或按一下 Edge 的連結，然後按一下**裝置 (Device)** 索引標籤。

3 在**裝置 (Device)** 索引標籤中，向下捲動至**設定 VLAN (Configure VLAN)** 區段。

4 按一下您想要向其插入 VNF 的 VLAN 的**編輯 (Edit)** 連結。

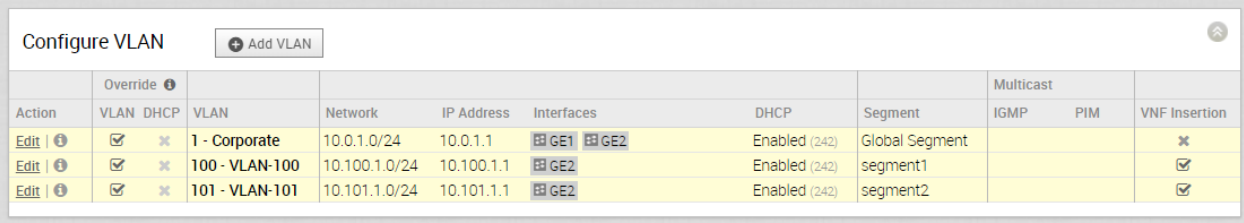
5 在 **VLAN** 視窗中，選取 **VNF 插入 (VNF Insertion)** 核取方塊，將 VNF 插入 VLAN 中。此選項會將特定 VLAN 的流量重新導向至 VNF。



6 按一下**更新 VLAN (Update VLAN)**。

結果

設定 VLAN (Configure VLAN) 區段會顯示 VNF 插入的狀態。



您也可以將 VNF 插入第 3 層介面或子介面中。此插入會將第 3 層介面或子介面的流量重新導向至 VNF。

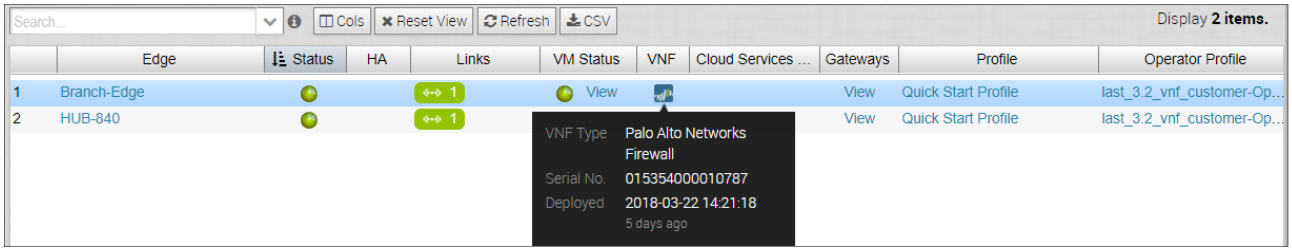
如果您選擇使用路由介面，請確定已在該介面上勾選信任的來源且 WAN 覆疊已停用。

監控 Edge 的 VNF

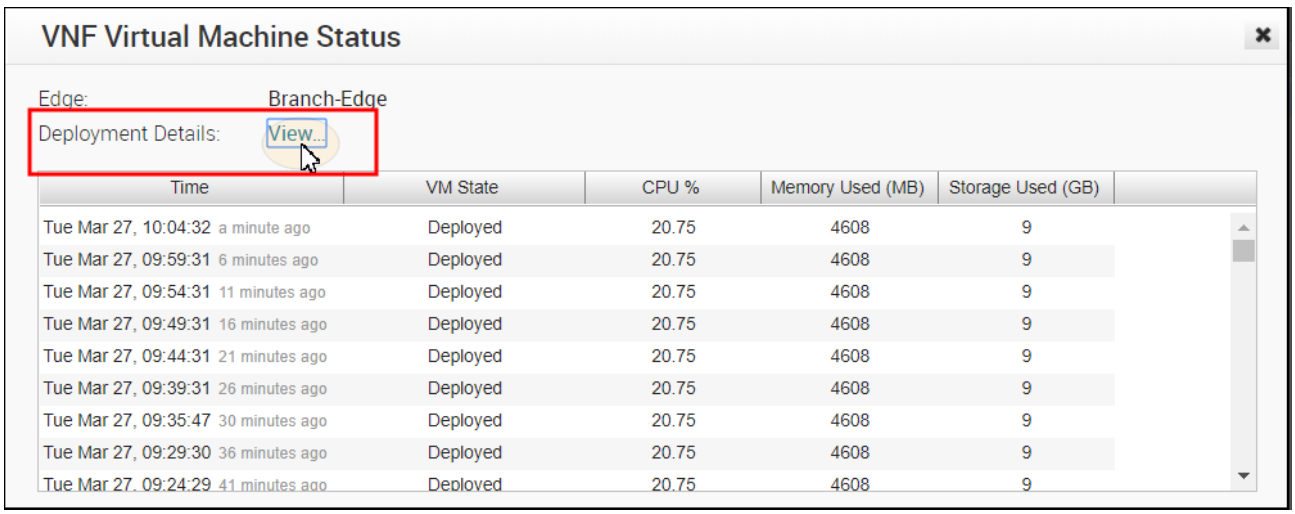
您可以監控 VNF 的狀態和 Edge 的虛擬機器，也可以檢視為企業設定的 VNF 網路服務。

若要監控 Edge 的 VNF 和虛擬機器狀態：

- 在企業入口網站中，按一下**監控 (Monitor) > Edge**。隨即會顯示 Edge 清單以及已設定 VNF 的詳細資料。

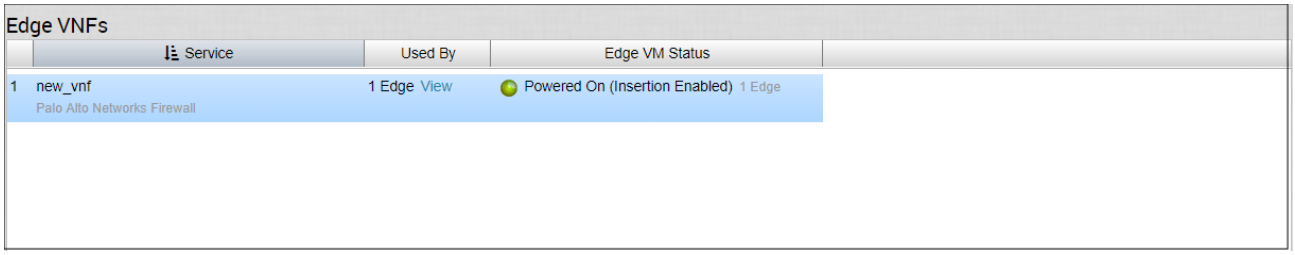


- 使用滑鼠暫留在 **VNF** 資料行中的圖示，以檢視 VNF 類型的其他詳細資料。
- 按一下**虛擬機器狀態 (VM Status)** 資料行中的 **檢視 (View)** 連結會開啟 **VNF 虛擬機器狀態 (VNF Virtual Machine Status)** 視窗，您可以在此處檢視 Edge 的部署狀態。若要檢視部署詳細資料，請按一下**部署詳細資料 (Deployment Details)** 旁的**檢視 (View)** 連結。



若要監控 VNF 和虛擬機器的狀態：

- 在企業入口網站中，按一下**監控 (Monitor) > 網路服務 (Network Services)**。隨即會顯示 Edge 清單以及已設定 VNF 的詳細資料。



VNF 事件

在部署 VNF 虛擬機器時、VNF 虛擬機器組態發生變更時，以及在 VLAN 中啟用 VNF 插入時，您可以檢視事件。

在企業入口網站中，按一下**監控 (Monitor) > 事件 (Events)**。

若要檢視與 VNF 相關的事件，您可以使用篩選選項。按一下**搜尋 (Search)** 選項旁的下拉式箭頭，然後選擇依 [事件 (Event)] 或 [訊息 (Message)] 資料行進行篩選。

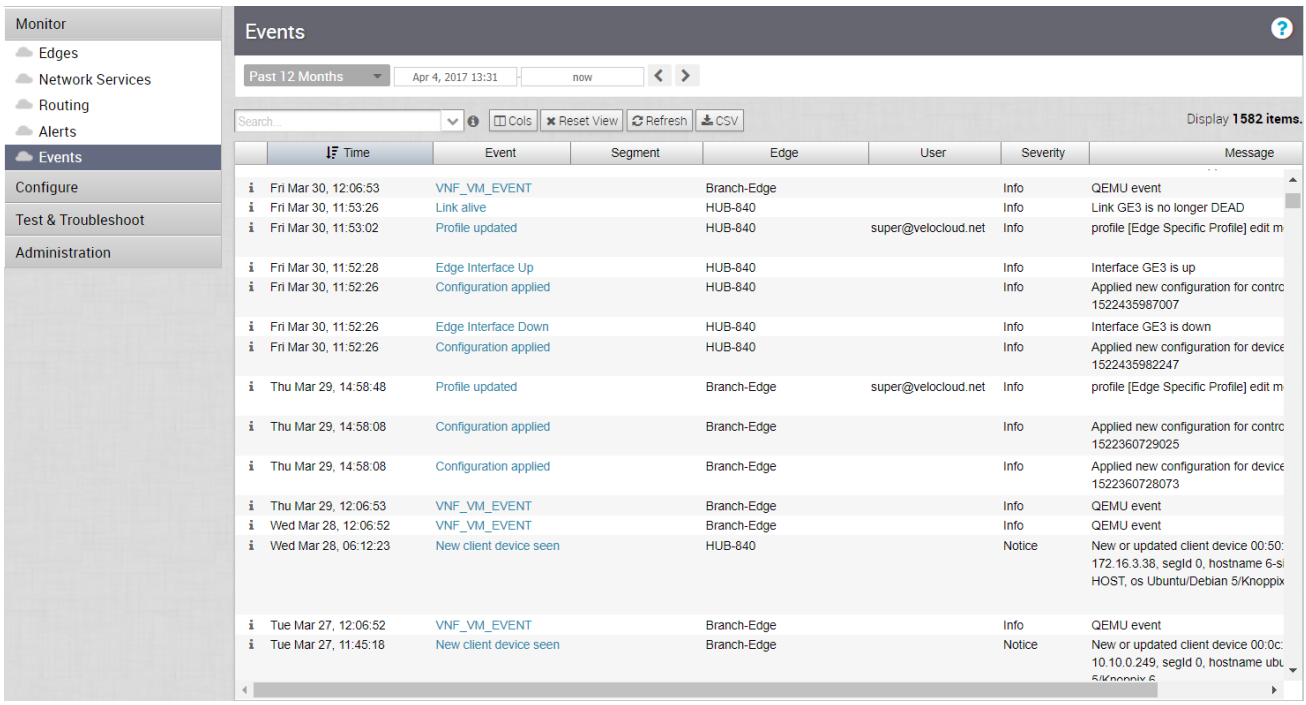
當 VNF 組態發生變更時，會發生下列事件：

- VNF 虛擬機器組態變更
- VNF 虛擬機器刪除
- VNF 虛擬機器部署
- VNF 虛擬機器錯誤
- VNF 映像下載事件

在 VLAN 或路由介面中啟用或停用 VNF 插入時，會發生下列事件。

- VNF 插入停用
- VNF 插入啟用

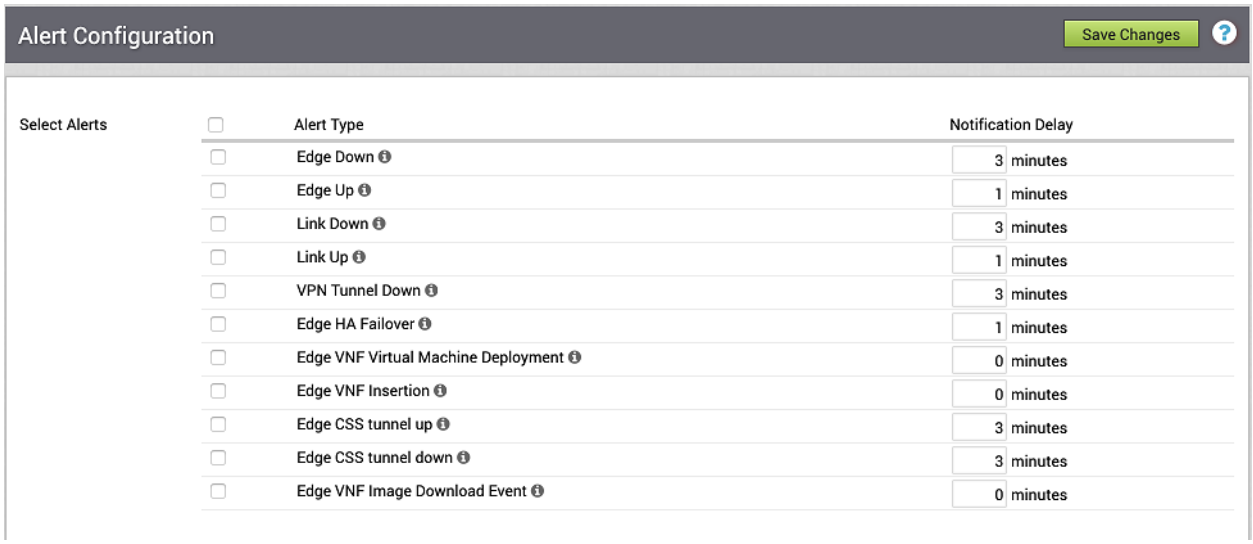
下圖顯示部分 VNF 事件。



設定 VNF 警示

您可以經由設定來接收與 VNF 事件相關的警示和通知。

在企業入口網站中，按一下**設定 (Configure) > 警示和通知 (Alerts & Notifications)**。在**警示組態 (Alert Configuration)** 頁面中，您可以選取警示 (Alert) 類型。



若要接收 VNF 事件的警示，請選取下列警示 (Alert) 類型：

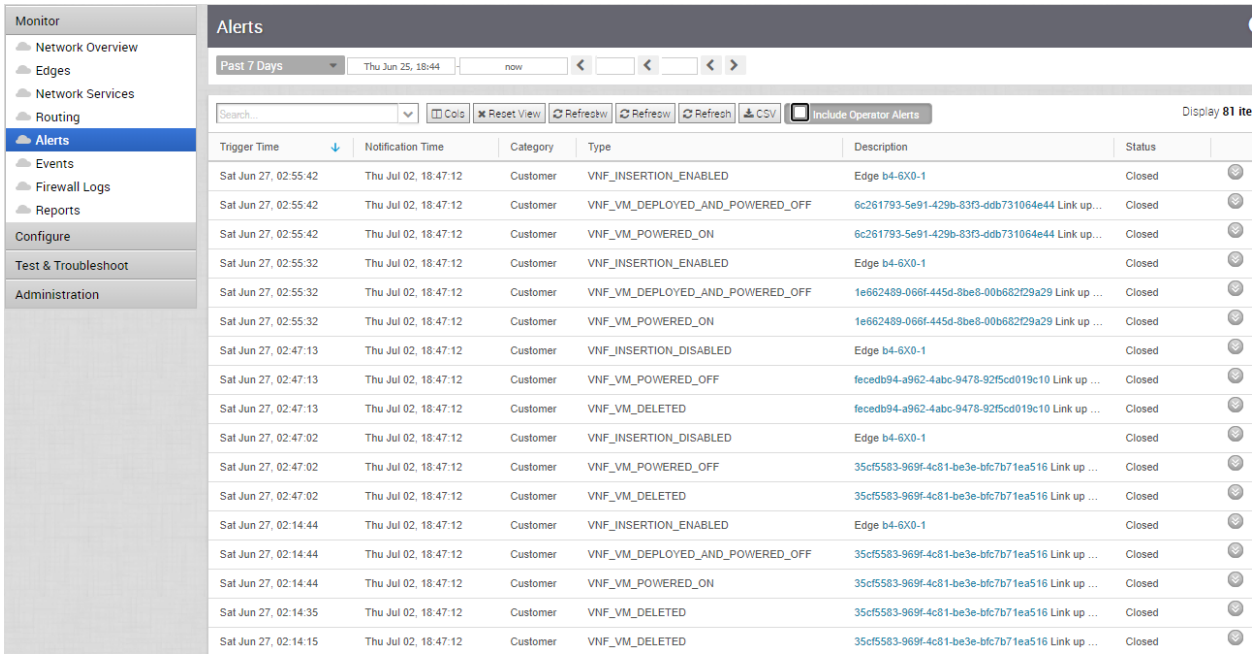
- **Edge VNF 虛擬機器部署 (Edge VNF Virtual Machine Deployment)** – 在 Edge VNF 虛擬機器部署狀態發生變更時，便會收到警示。
- **Edge VNF 插入 (Edge VNF Insertion)** – 在 Edge VNF 部署狀態發生變更時，便會收到警示。

- **Edge VNF 映像下載事件 (Edge VNF Image Download Event)** – 在 Edge VNF 映像下載狀態發生變更時，便會收到警示。

您可以在**監控 (Monitor) > 警示 (Alerts)** 頁面中檢視警示通知。

若要檢視與 VNF 相關的警示，您可以使用篩選選項。按一下**搜尋 (Search)** 選項旁的下拉式箭頭，然後選擇依類型 (Type) 進行篩選。

下圖顯示部分 VNF 警示。



您也可以在新的 Orchestrator UI 中檢視警示。

在快顯視窗中，按一下**啟動新的 Orchestrator UI (Launch New Orchestrator UI)**。UI 會在新的索引標籤中開啟，並顯示監控選項。按一下**警示 (Alerts)**。按一下**搜尋 (Search)** 選項中的篩選器圖示，以篩選 VNF 警示。

設定 Edge 商務原則

本節說明如何設定 Edge 商務原則。

設定 Edge 商務原則

Edge 防火牆主要會使用所指派設定檔中包含的規則。覆寫 Edge 的設定檔商務原則規則是選用步驟。

商務原則覆寫規則

在 Edge 中，可使用以下顯示的 [Edge 商務原則 (Edge Business Policy)] 對話方塊覆寫已指派設定檔中包含的商務原則規則。與任何設定檔商務原則規則相同的任何商務原則覆寫比對值，都會覆寫該設定檔規則。您可以比照建立設定檔規則的相同方式來建立覆寫規則 (請參閱第 11 章 設定設定檔商務原則)。

如下圖所示，商務原則可辨識區段。所有可用於設定的區段皆會在**設定區段 (Configure Segment)** 下拉式功能表中列出。

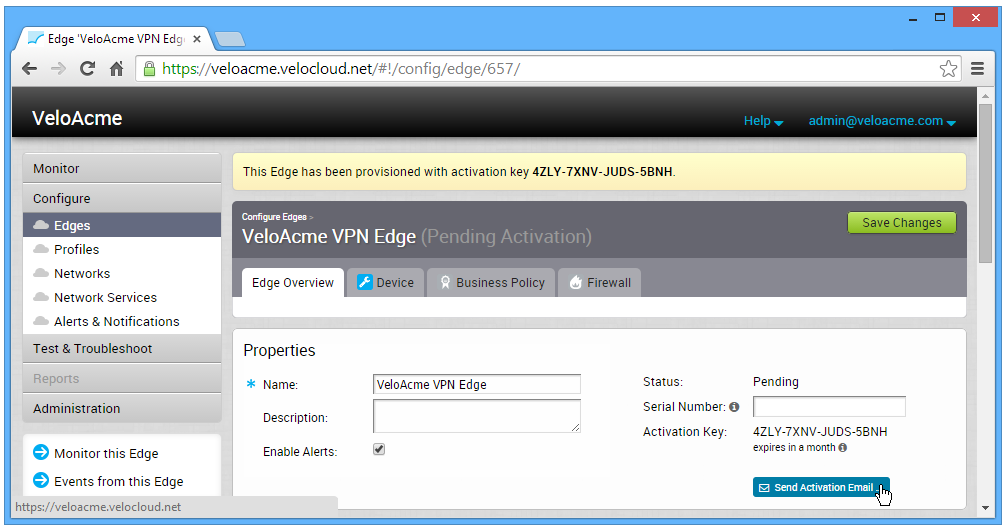
當您從**設定區段 (Configure Segment)** 下拉式清單中選擇要設定的區段時，與該區段相關聯的設定和選項將會顯示在**設定區段 (Configure Segments)** 區域中。**全域區段 [一般] (Global Segment [Regular])** 是預設區段。

如需分割的詳細資訊，請參閱第 7 章 設定區段和設定 Edge 裝置。

設定 Edge 啟用

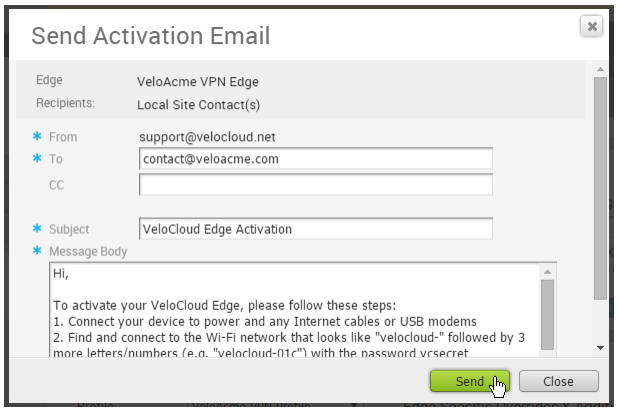
本節說明如何起始 Edge 啟用。

在儲存 Edge 組態之後，系統就會為其指派啟用金鑰。在 **Edge 概觀 (Edge Overview)** 索引標籤上按一下**傳送啟用電子郵件 (Send Activation Email)** 連結，即可開始進行 Edge 啟用。



此時會顯示**傳送啟用電子郵件 (Send Activation Email)** 對話方塊，其中包含要傳送給站台連絡人的建議電子郵件。其中會提供簡單的指示給站台連絡人，以連線和啟動 Edge 硬體。 您可以在電子郵件中指定將特定站台 WAN 和 LAN 網路連線至 Edge 的其他指示。

備註 在 3.4 版中，如果已設定 Edge 510 LTE 裝置，則啟用電子郵件將會包含手機設定 (例如，SIM 卡 PIN 碼、網路、APN、使用者名稱)。



備註 如果您設定 Edge 510 LTE 裝置，則可以執行「LTE 數據機資訊」診斷測試以進行疑難排解。**LTE 數據機資訊**診斷測試將會擷取診斷資訊，例如訊號強度、連線資訊等。如需如何執行診斷測試的相關資訊，請參閱標題為遠端診斷一節。

Edge 層級上的 LAN 端 NAT 規則

LAN 端 NAT 規則可讓您透過 NAT 將未通告子網路中的 IP 位址對應至已通告子網路中的 IP 位址。3.3.2 版在裝置設定組態內導入了 LAN 端 NAT 規則，同時適用於設定檔和 Edge 層級，而 3.4 版則以延伸的形式導入了基於來源和目的地的 LAN 端 NAT，支援相同封包的來源和目的地 NAT。

在 3.3.2 版中，VMware 針對 Edge 上的 NAT VPN 路由導入了新的 LAN 端 NAT 模組。主要使用案例如下所示：

- 分支因 M&A 而出現重疊的 IP
- 基於安全考量而隱藏分支或資料中心的私人 IP

在 3.4 版中，已導入其他的組態欄位以因應其他使用案例。以下將針對不同版本對於 LAN 端 NAT 的支援進行高階解析：

- 支援將來源或目的地 NAT 用於所有相符的子網路，包括 1:1 和多對一 (3.3.2 版)
- 支援基於目的地子網路的來源 NAT，或基於來源子網路的目的地 NAT，包括 1:1 和多對一 (3.4 版)

- 相同封包的來源 NAT 和目的地 1:1 NAT (3.4 版)

備註

- LAN 端 NAT 支援透過 VCMP 通道的流量。它不支援底層流量。
- 支援「多對一」和「1:1」(例如 /24 對 /24) 的來源和目的地 NAT。
- 如果設定了多個規則，則僅會執行第一個相符的規則。
- LAN 端 NAT 會在路由或流量查閱之前執行。若要符合商務設定檔中的流量，使用者必須使用經過 NAT 處理的 IP。
- 依預設不會從 Edge 通告經過 NAT 處理的 IP。因此，請務必為經過 NAT 處理的 IP 新增靜態路由，並通告至覆疊。
- 3.3.2 中的組態將延續使用，而無需在 3.4 升級後重新設定。

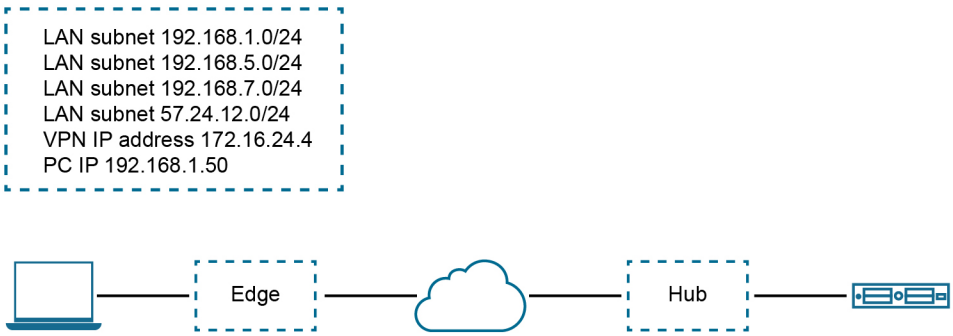
LAN 端 NAT (3.3.2 版)

使用案例一：「多對一來源 NAT」

在此案例中，第三方將多個非重疊的子網路指派給客戶的站台。客戶的資料中心伺服器可藉由在任何指定站台上的單一 IP 位址識別來自此第三方的流量。

在 3.3.2 版中，使用案例一所需的組態為：新規則：LAN 端 NAT 192.168.1.0/24 -> 172.16.24.4/32

如下圖所示，由於 NAT 規則是單一 IP，TCP 和 UDP 流量將會進行 PAT 處理。因此，在此範例中，192.168.1.50 會變成 172.16.24.4，並以暫時性來源連接埠處理 TCP/UDP 流量，ICMP 流量會變成 172.16.24.4，並將自訂 ICMP 識別碼用於反向查閱，且其他所有流量都會被捨棄。

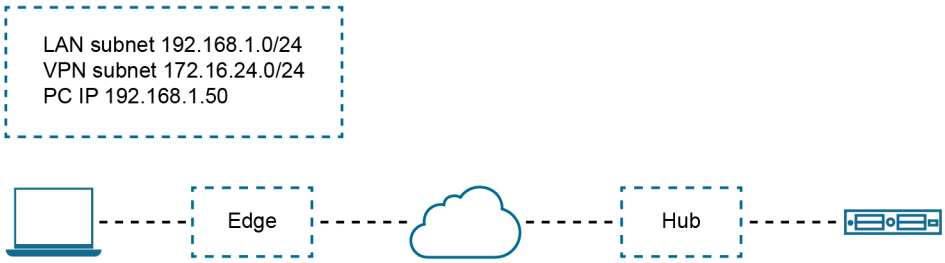


使用案例二：「1:1 來源 NAT」

在此案例中，LAN 子網路為 192.168.1.0/24。但是，這是與其他站台重疊的子網路。已有大小相同的唯一子網路 172.16.24.0/24 被指派用於此站台上的 VPN 通訊。來自電腦的流量必須在路由查閱之前在 Edge 上進行 NAT 處理，否則來源路由將會與尚未從此 Edge 通告的 192.168.1.0/24 相符，而導致流量遭到捨棄。

使用案例二所需的組態為：新規則：LAN 端 NAT 192.168.1.0/24 -> 172.16.24.0/24

由於子網路的大小相同，所有與子網路遮罩相符的位元都將進行 NAT 處理。因此，在下圖的範例中，192.168.1.50 會變成 172.16.24.50。

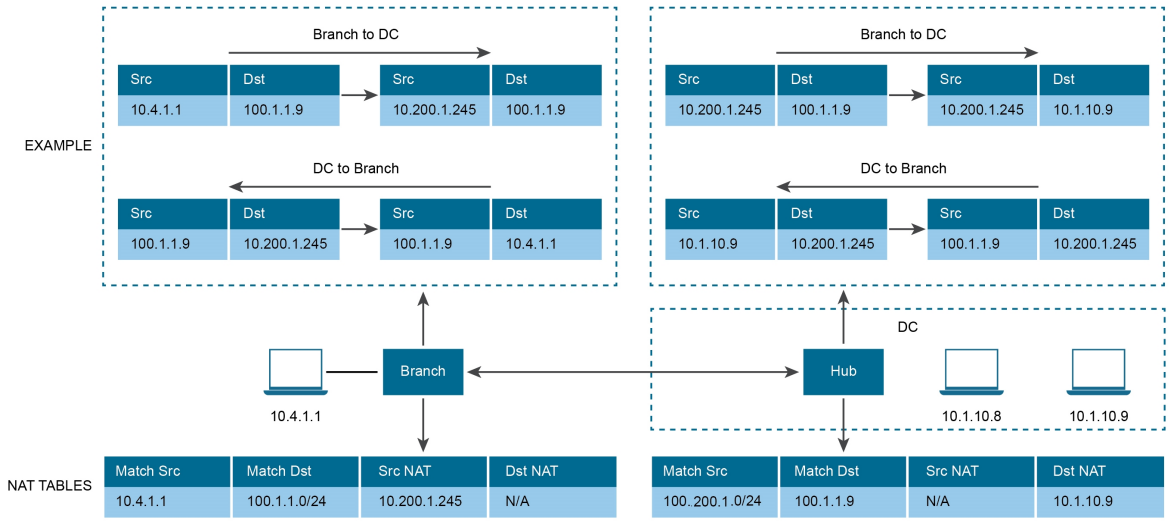


基於來源或目的地的 LAN 端 NAT (3.4 版)

3.4 版導入了基於來源/目的地支援的 LAN 端 NAT，並將其納入單一規則中。在此規則中，您只能根據來源或目的地子網路對流量的子集啟用 NAT。請參閱下列使用案例以瞭解這項增強功能。

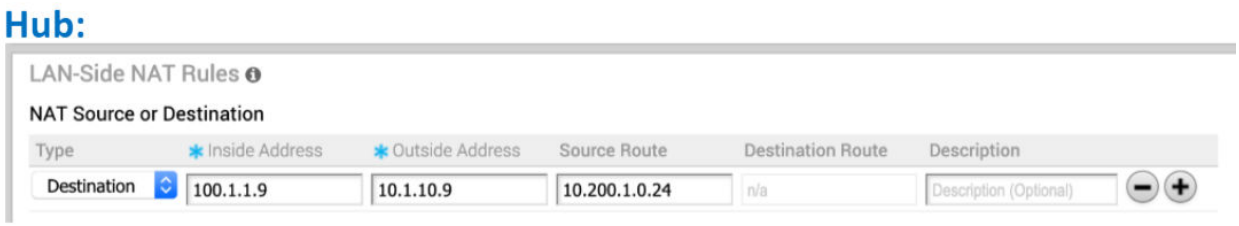
使用案例一：「執行以來源或目的地作為比對準則的 SNAT 或 DNAT」

在下方的圖例中，分支僅應針對以 100.1.1.0/24 為目的地的流量，透過 NAT 將來源 IP 10.4.1.1 對應至 10.200.1.245。同樣地，在 DC 上，只有在從來源 10.200.1.0/24 接收流量時，目的地 IP 100.1.1.9 才應進行 NAT 處理而對應至 10.1.10.9。



請參閱下圖 (分支的 [LAN 端 NAT 規則] 區域)。

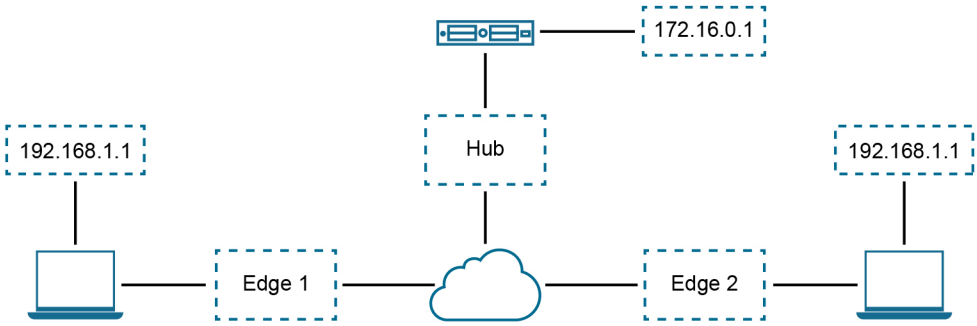
請參閱下圖 (中樞的 [LAN 端 NAT 規則] 區域)。

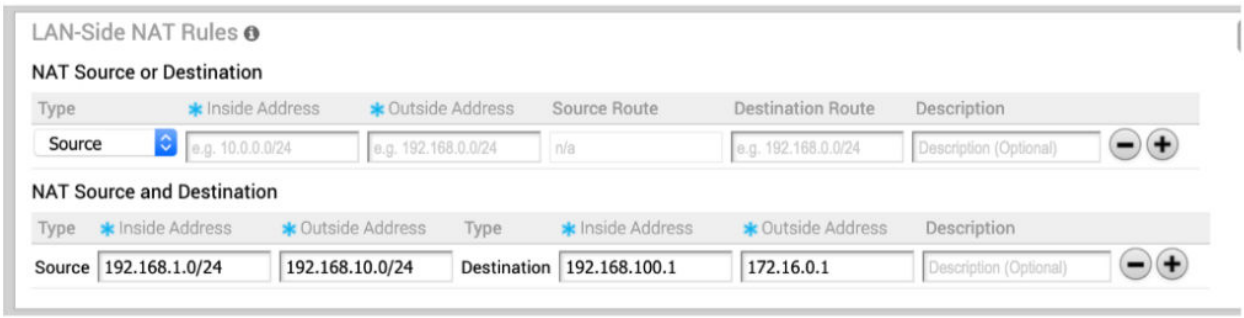


使用案例二：同時對封包的來源和目的地 IP 進行 NAT 處理

請考量下列案例。在此範例中，網路中的每個站台都指派給相同的子網路，使每個站台上的分支 LAN 皆相同。「PC1」和「PC2」具有相同的 IP 位址，且兩者都需要與中樞後方的伺服器進行通訊。我們必須對流量進行來源 NAT 處理才能使用重疊的 IP 位址，例如，在 Edge 1 中，電腦 (192.168.1.0/24) 應進行 NAT 處理而對應至 192.168.10.0/24，在 Edge2 中，電腦 (192.168.1.0/24) 應進行 NAT 處理而對應至 192.168.20.0/24。

此外，基於安全考量，位於中樞後方、實際 IP 為「172.16.0.1」的伺服器應向電腦顯示為「192.168.100.1」，且此 IP 不應分配至中樞與 Edge 之間的 SD-WAN，必須在相同的 Edge 上使用「來源 + 目的地」的組合規則。





備註 LAN 端 NAT 規則可設定於設定檔層級或 Edge 層級。若要在 Edge 層級進行設定，請確實勾選**啟用 Edge 覆寫 (Enable Edge Override)** 核取方塊。

設定程序

附註：使用者若想要設定預設規則「任何」，則必須指定全部皆須為零的 IP 位址，且首碼也必須為零：0.0.0.0/0。

若要套用 LAN 端 NAT 規則：

1 在導覽面板中，移至**設定 (Configure) > Edge**。

2 在**裝置設定 (Device Settings)** 索引標籤畫面中，向下捲動至 **LAN 端 NAT 規則 (LAN-Side NAT Rules)** 區域。

3 在 **LAN 端 NAT 規則 (LAN-Side NAT Rules)** 區域中，完成下列對 NAT 來源或目的地區段的操作：(請參閱下表，以取得下列步驟中各欄位的說明)。

   a 在**內部位址 (Inside Address)** 文字方塊中，輸入位址。

   b 在**外部位址 (Outside Address)** 文字方塊中，輸入位址。

   c 在適當的文字方塊中輸入來源路由。

   d 在適當的文字方塊中輸入目的地路由。

   e 在**說明 (Description)** 文字方塊中輸入規則的說明 (選用)。

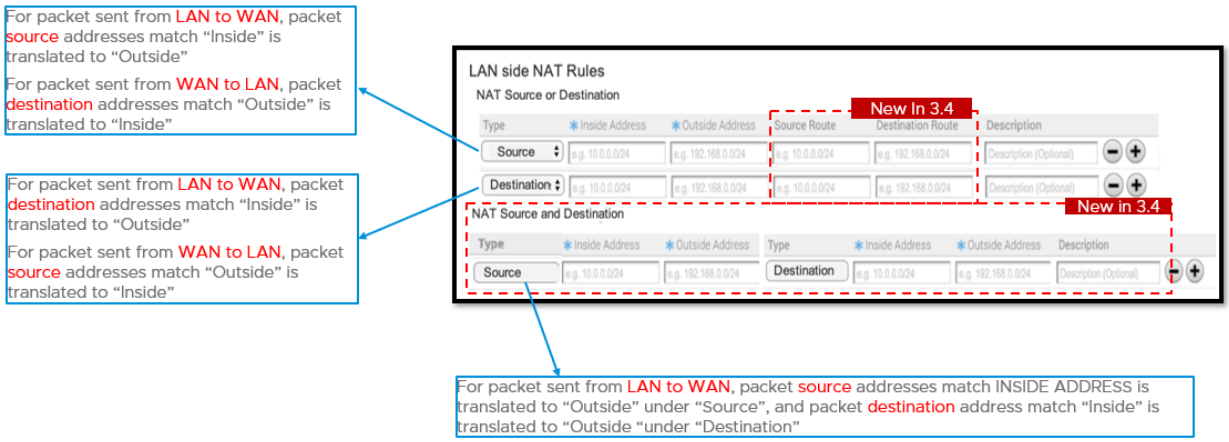
4 在 **LAN 端 NAT 規則 (LAN-Side NAT Rules)** 區域中，完成下列對 NAT 來源和目的地的操作：(請參閱下表，以取得下列步驟中各欄位的說明)。

a 針對**來源 (Sources)** 類型，在適當的文字方塊中輸入**內部位址 (Inside Address)** 和**外部位址 (Outside Address)**。

b 針對**目的地 (Destination)** 類型，在適當的文字方塊中輸入**內部位址 (Inside Address)** 和**外部位址 (Outside Address)**。

c 在**說明 (Description)** 文字方塊中輸入規則的說明 (選用)。

LAN 端 NAT 規則	類型	說明
[類型 (Type)] 下拉式功能表	選取來源 (Source) 或目的地 (Destination)	決定此 NAT 規則應套用於使用者流量的來源還是目的地 IP 位址上。
[內部位址 (Inside Address)] 文字方塊	IPv4 位址/首碼，首碼必須是 1-32	「內部」或「NAT 處理前」的 IP 位址 (如果首碼為 32) 或子網路 (如果首碼小於 32)。
[外部位址 (Outside Address)] 文字方塊	IPv4 位址/首碼，首碼必須是 1-32	「外部」或「NAT 處理後」的 IP 位址 (如果首碼為 32) 或子網路 (如果首碼小於 32)。
[來源路由 (Source Route)] 文字方塊	- 選用 - IPv4 位址/首碼 - 首碼必須是 1-32 - 預設值：任何	針對目的地 NAT，將來源 IP/子網路指定為比對準則。只有在類型為 [目的地 (Destination)] 時才有效。
[目的地路由 (Destination Route)] 文字方塊	- 選用 - IPv4 位址/首碼 - 首碼必須是 1-32 - 預設值：任何	針對來源 NAT，將目的地 IP/子網路指定為比對準則。只有在類型為「來源」時才有效。
[說明 (Description)] 文字方塊	文字	用來說明 NAT 規則的自訂文字方塊。



備註 **重要：**如果內部首碼小於外部首碼，則支援 LAN 到 WAN 方向的多對一 NAT，以及 WAN 到 LAN 方向的 1:1 NAT。例如，如果內部位址 = 10.0.5.0/24，而外部位址 = 192.168.1.25/32，且類型 = 來源，則對於從 LAN 到 WAN，且來源 IP 符合「內部位址」的工作階段而言，10.0.5.1 將會轉譯為 192.168.1.25。對於從 WAN 到 LAN，且目的地 IP 符合「外部位址」的工作階段而言，192.168.1.25 將會轉譯為 10.0.5.25。同樣地，如果內部首碼大於外部首碼，則支援 WAN 到 LAN 方向的多對一 NAT，以及 LAN 到 WAN 方向的 1:1 NAT。經過 NAT 處理的 IP 不會自動通告，您應為經過 NAT 處理的 IP 設定靜態路由，且下一個躍點應為來源子網路的 LAN 下一個躍點 IP。

LAN 端 NAT「速查表」

使用案例 1：

- **流量方向：(Traffic direction:)**LAN -> WAN
- **需轉譯的項目：(What needs to be translated:)** 封包來源位址
- **組態對應：(Config mapping:)**
  - NAT 類型 =「來源」
  - 來源 IP =「內部位址」
  - NAT IP =「外部位址」

NAT 類型	內部	外部	類型 (Type)	LAN -> WAN 行為
來源 (Source)	A.0/24	B.0/24	1:1	A.1 轉譯為 B.1、A.2 轉譯為 B.2，依此類推。
來源 (Source)	A.0/24	B.1/32	多對一	A.1 和 A.2 轉譯為 B.1
來源 (Source)	A.1/32	B.0/24	1:1	A.1 轉譯為 B.1，不使用其他 B.X

使用案例 2：

- **流量方向：(Traffic direction:)** WAN -> LAN
- **需轉譯的項目：(What needs to be translated:)** 封包目的地位址

- **組態對應：(Config mapping:)**
  - NAT 類型 =「來源」
  - 來源 IP =「外部位址」
  - NAT IP =「內部位址」

NAT 類型	內部	外部	類型	WAN -> LAN 行為
來源	A.0/24	B.0/24	1:1	B.1 轉譯為 A.1、B.2 轉譯為 A.2，依此類推
來源	A.0/24	B.1/32	多對一	B.1 轉譯為 A.1
來源	A.1/32	B.0/24	一對多	B.1 和 B.2 轉譯為 A.1

使用案例 3：

- **流量方向：(Traffic direction:)** LAN -> WAN
- **需轉譯的項目：(What needs to be translated:)** 封包目的地位址
- **組態對應：(Config mapping:)**
  - NAT 類型 =「目的地」
  - 來源 IP =「內部位址」
  - NAT IP =「外部位址」

NAT 類型	內部	外部	類型 (Type)	LAN -> WAN 行為
目的地 (Destination)	A.0/24	B.0/24	1:1	A.1 轉譯為 B.1、A.1 轉譯為 B.2，依此類推
目的地 (Destination)	A.0/24	B.1/32	多對一	A.1 和 A.2 轉譯為 B.1
目的地 (Destination)	A.1/32	B.0/24	一對多	A.1 轉譯為 B.1

使用案例 4：

- **流量方向：(Traffic direction:)** WAN -> LAN
- **需轉譯的項目：(What needs to be translated:)** 封包來源位址
- **組態對應：(Config mapping:)**
  - NAT 類型 =「目的地」
  - 來源 IP =「外部位址」

- NAT IP =「內部位址」

NAT 類型	內部	外部	類型	WAN -> LAN 行為
目的地	A.0/24	B.0/24	1:1	B.1 轉譯為 A.1、B.2 轉譯為 A.2，依此類推
目的地 (Destination)	A.0/24	B.1/32	多對一	B.1 轉譯為 A.1
目的地	A.1/32	B.0/24	一對多	B.1 和 B.2 轉譯為 A.1

物件群組

16

物件群組由一個範圍的 IP 位址或連接埠號碼所組成。建立商務原則和防火牆規則時，您可以藉由在規則定義中包含物件群組，來定義 IP 位址範圍或 TCP/UDP 連接埠範圍的規則。

您可以建立位址群組以儲存有效 IP 位址的範圍，並建立連接埠群組以儲存連接埠號碼的範圍。您可以建立特定類型的物件群組，並在原則和規則中重複使用這些群組，從而簡化原則管理。

使用物件群組可讓您：

- 輕鬆管理原則
- 將原則元件模組化並重複使用
- 輕鬆更新所有參考的商務和防火牆原則
- 減少原則數目
- 提高原則偵錯效能和可讀性

備註 如果您擁有 NETWORK_SERVICE 物件的建立、更新和刪除權限，則可以建立、更新或刪除物件群組。如果您擁有 NETWORK_SERVICE 和 ENTERPRISE_PROFILE 物件的讀取權限，則只能檢視物件群組。

本章節討論下列主題：

設定位址群組

位址群組可透過不同選項儲存 IP 位址範圍。

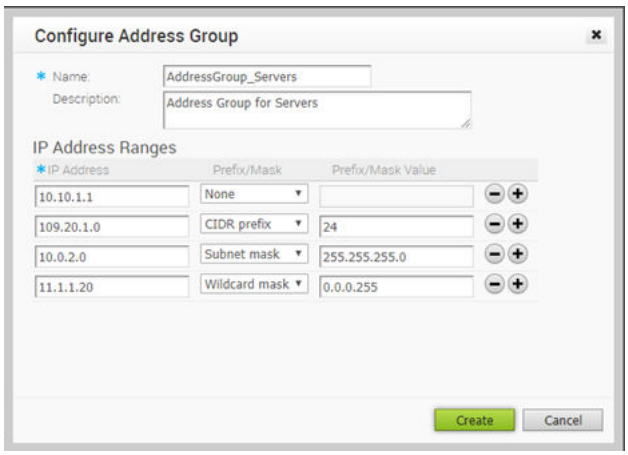
程序

1 在企業入口網站中，按一下**設定 (Configure) > 物件群組 (Object Groups)**。

2 在**位址群組 (Address Groups)** 索引標籤上，按一下**動作 (Actions) > 新增 (New)**。

3 在**設定位址群組 (Configure Address Group)** 視窗中，輸入位址群組的名稱和說明。

4 視需要輸入 IP 位址範圍。



5 按一下**建立 (Create)**。

後續步驟

您可以使用位址群組來定義商務原則或防火牆規則，以在位址群組中包含 IP 位址範圍。

若要新增或修改位址群組中的 IP 位址，您可以在 [位址群組 (Address Groups)] 索引標籤中按一下**動作 (Actions) > 更新 (Update)**。

如果您想要刪除位址群組，請確保將該位址群組排除於商務原則或防火牆規則之外。

設定連接埠群組

連接埠群組可儲存一個範圍的 TCP 和 UDP 連接埠號碼。

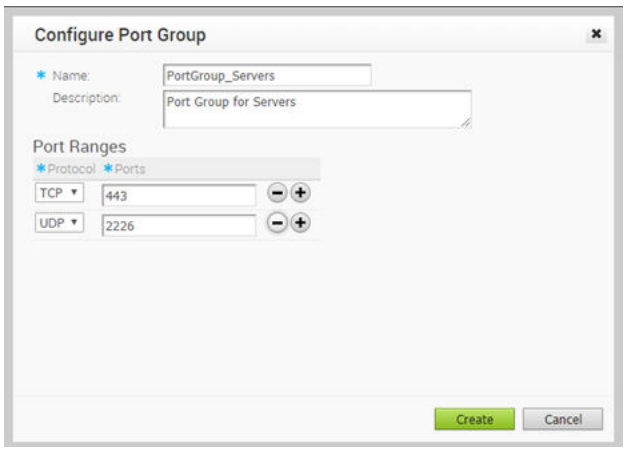
程序

1 在企業入口網站中，按一下**設定 (Configure) > 物件群組 (Object Groups)**。

2 在**連接埠群組 (Port Groups)** 索引標籤上，按一下**動作 (Actions) > 新增 (New)**。

3 在**設定連接埠群組 (Configure Port Group)** 視窗中，輸入連接埠群組的名稱和說明。

4 選取 TCP 或 UDP 通訊協定，然後視需要輸入對應的連接埠號碼。



5 按一下**建立 (Create)**。

後續步驟

您可以使用連接埠群組定義商務原則或防火牆規則，以包含連接埠號碼的範圍。

您可以在 [連接埠群組 (Port Groups)] 索引標籤中按一下**動作 (Actions) > 更新 (Update)**，以新增或修改連接埠群組中的連接埠號碼。

如果您想要刪除連接埠群組，請確保將該連接埠群組排除於商務原則或防火牆規則之外。

使用物件群組設定商務原則

設定商務原則時，您可以選取現有的物件群組以比對來源或目的地。這包括商務原則定義的物件群組中可用的 IP 位址範圍或連接埠號碼。

如需商務原則的詳細資訊，請參閱設定設定檔商務原則。

程序

1 在企業入口網站中，按一下**設定 (Configure) > 設定檔 (Profiles)**。

2 從清單中選取設定檔，然後按一下**商務原則 (Business Policy)** 索引標籤。

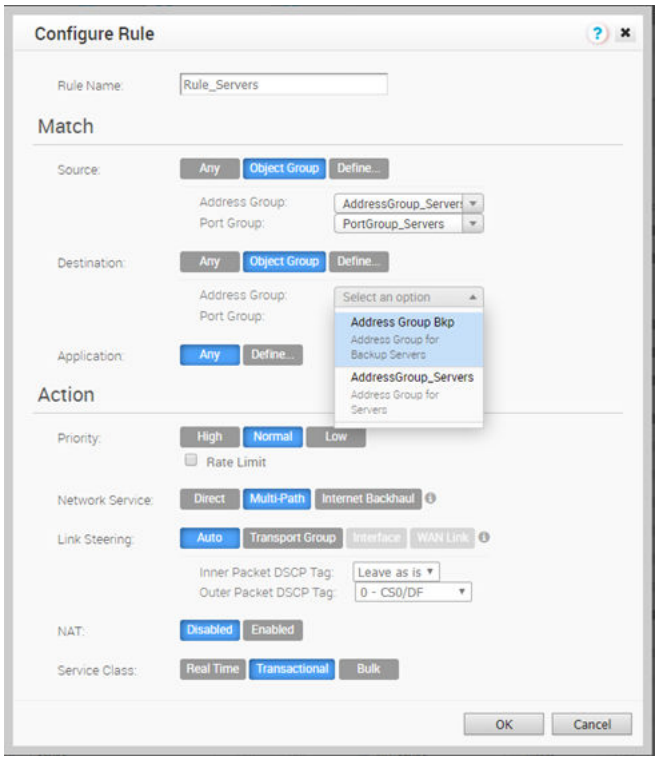
3 按一下**新增規則 (New Rule)** 或**動作 (Actions) > 新增規則 (New Rule)**。

4 輸入商務規則的名稱。

5 在**比對 (Match)** 區域中，針對來源按一下**物件群組 (Object Group)**。

6 從下拉式清單中選取相關的位址群組和連接埠群組。

7 如有需要，您也可以針對目的地選取位址群組和連接埠群組。



8 選擇所需的其他動作，然後按一下**確定 (OK)**。

結果

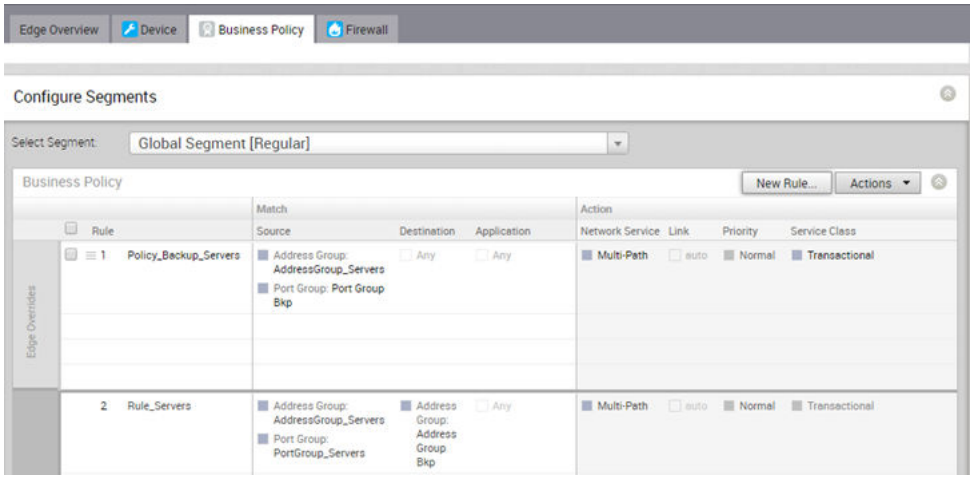
您為設定檔建立的商務原則，會自動套用至與設定檔相關聯的所有 Edge。如有需要，您可以建立專屬於 Edge 的其他商務原則。

1 導覽至**設定 (Configure) > Edge**、選取 Edge，然後按一下**商務原則 (Business Policy)** 索引標籤。

2 按一下**新增規則 (New Rule)** 或**動作 (Actions) > 新增規則 (New Rule)**。

3 使用相關物件群組和其他動作定義規則。

Edge 的 [商務原則 (Business Policy)] 索引標籤會顯示相關聯設定檔中的原則，以及專屬於 Edge 的原則。



備註 依預設會將商務原則指派給全域區段。如有需要，您可以從**選取區段 (Select Segment)** 下拉式清單中選擇區段，並建立專屬於所選區段的商務原則。

後續步驟

您可以使用其他 IP 位址和連接埠號碼來修改物件群組。這些變更會自動包含在使用物件群組的商務原則中。

使用物件群組設定防火牆規則

設定防火牆規則時，您可以選取現有的物件群組以比對來源或目的地。這包括規則的物件群組中可用的 IP 位址範圍或連接埠號碼。

如需防火牆規則的詳細資訊，請參閱《設定防火牆規則》。

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **設定檔 (Profiles)**。

2 從清單中選取設定檔，然後按一下**防火牆 (Firewall)** 索引標籤。

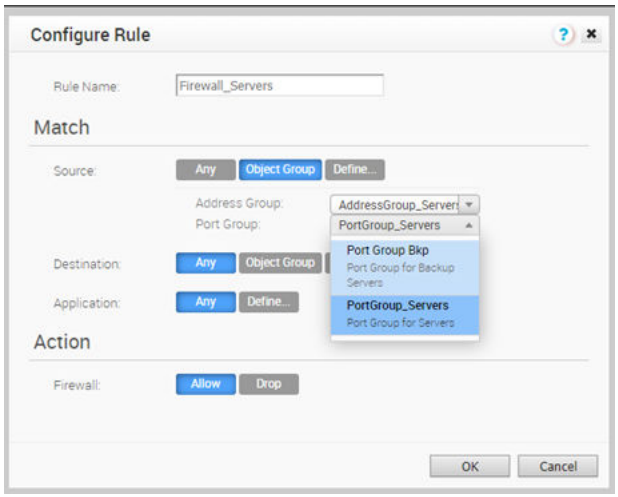
3 按一下**新增規則 (New Rule)** 或**動作 (Actions)** > **新增規則 (New Rule)**。

4 輸入防火牆規則的名稱。

5 在**比對 (Match)** 區域中，針對來源按一下**物件群組 (Object Group)**。

6 從下拉式清單中選取相關的位址群組和連接埠群組。

7 如有需要，您也可以針對目的地選取位址群組和連接埠群組。



8 選擇所需的動作，然後按一下**確定 (OK)**。

結果

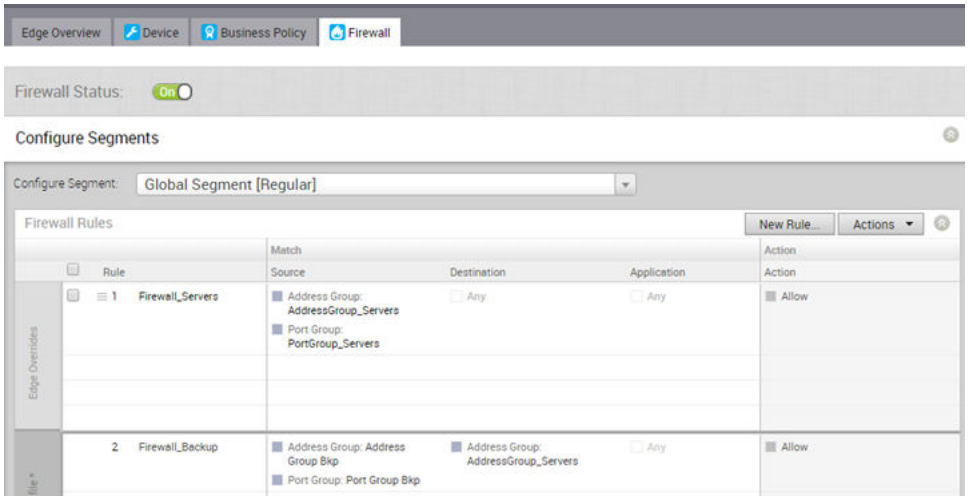
您為設定檔建立的防火牆規則，會自動套用至與設定檔相關聯的所有 Edge。如有需要，您可以建立專屬於 Edge 的其他規則。

1 導覽至**設定 (Configure) > Edge**、選取 Edge，然後按一下**防火牆 (Firewall)** 索引標籤。

2 按一下**新增規則 (New Rule)** 或**動作 (Actions) > 新增規則 (New Rule)**。

3 使用相關物件群組和其他動作定義規則。

Edge 的 [防火牆 (Firewall)] 索引標籤會顯示相關設定檔中的防火牆規則，以及專屬於 Edge 的規則。



備註 依預設會將防火牆規則指派給全域區段。如有需要，您可以從**選取區段 (Select Segment)** 下拉式清單中選擇區段，並建立專屬於所選區段的防火牆規則。

後續步驟

您可以使用其他 IP 位址和連接埠號碼來修改物件群組。這些變更會自動包含在使用物件群組的防火牆規則中。

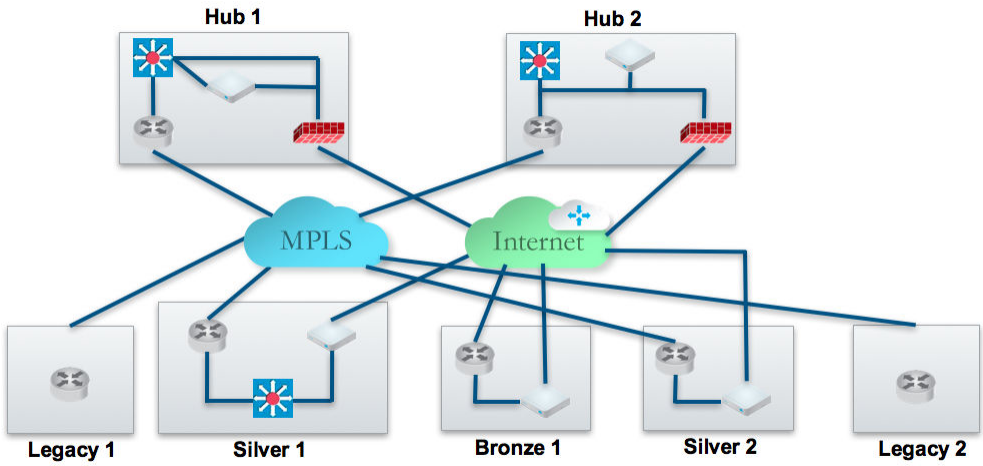
站台組態

17

針對包含 SD-WAN Hub 和 VMware 分支組態 (金級、銀級和銅級) 的資料中心，需要同時使用 MPLS 和網際網路連線來設定其拓撲。舊版分支組態 (不含 SD-WAN Edge 的組態) 會納入其中，且若有舊版分支存在，則會修改中樞和分支組態。

下圖顯示一個範例拓撲，其中包含兩個資料中心中樞，以及金級、銀級和銅級衍生的分支拓撲，並使用 MPLS 與網際網路互連。此範例將用來說明資料中心和分支組態所需的個別工作。我們假設您熟悉本說明文件先前幾節提到的概念和組態詳細資料。本節主要將探討如何設定每個拓撲所需的網路、設定檔裝置設定和 Edge 組態。

此外也會說明流量重新導向、控制路由 (例如用於回傳流量和 VPN) 和 Edge 容錯移轉的其他設定步驟。



本節主要著重於包含不同資料中心和分支位置的拓撲所需的設定，並說明完成這些設定所需的網路、設定檔/Edge 裝置設定，以及設定檔/Edge 商務原則。完整設定 (例如網路服務、裝置 Wi-Fi 無線電、驗證、SNMP 和 Netflow 設定) 可能需要的某些輔助設定步驟不在說明範圍內。

本章節討論下列主題：

- 資料中心組態
- 設定分支和中樞

資料中心組態

資料中心內的 SD-WAN Edge 可以作為中樞，在分支之間導向流量。SD-WAN Edge 可用來管理 MPLS 和網際網路流量。資料中心內的中樞可設定於單臂或雙臂組態中。此外，資料中心也可當作備份。

以下說明可透過不同的選項在拓撲中插入 SD-WAN Edge 的各種選項。

選項	說明
中樞 1 (Hub 1)	在雙臂拓撲中部署了 SD-WAN Edge 的資料中心或區域中樞站台。
中樞 2 (Hub 2)	在單臂拓撲中部署了 SD-WAN Edge 的資料中心或區域中樞站台 (相同的介面具有多個 WAN 連結)。
舊版 1 和 2 (Legacy 1 and 2)	傳統 MPLS 站台。
銀級 1 (Silver 2)	SD-WAN Edge 部署於路徑外。SD-WAN Edge 會在 MPLS 和網際網路路徑之間建立覆疊。流量會先轉向至 SD-WAN Edge。
銀級 2 (Silver 2)	SD-WAN Edge 預設以閘道的形式部署在路徑中。它一律為預設閘道。此拓撲較為簡單，但會使 SD-WAN Edge 成為單一故障點，且可能需要 HA。
銅級 1 (Bronze 1)	雙網際網路站台 (其中一個連結位於 NAT 路由器後方)。

設定分支和中樞

本節提供在雙臂組態中設定 SD-WAN Edge 的概觀。

概觀

若要在雙臂組態中設定 SD-WAN Edge：

1 設定並啟動中樞 1

2 設定並啟動銀級 1 站台

3 啟用分支到中樞的通道 (銀級 1 到中樞 1)

4 設定並啟動銅級 1 站台

5 設定並啟動中樞 2

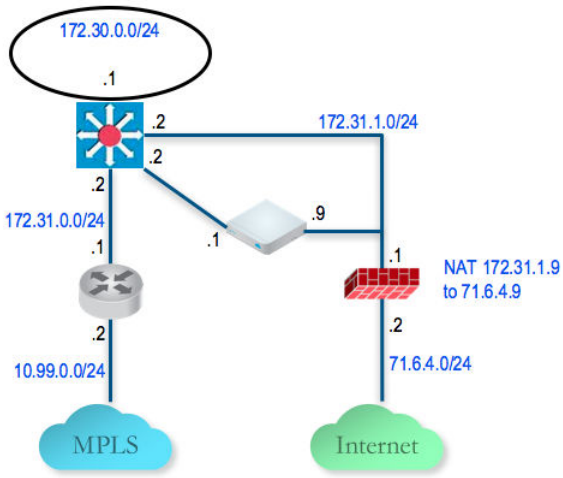
6 設定並啟動銀級 2 站台

以下幾節將詳細說明相關步驟。

設定並啟動中樞 1

此步驟可協助您瞭解如何在中樞位置啟動 SD-WAN Edge 的一般工作流程。SD-WAN Edge 可使用兩個介面進行部署 (每個 WAN 連結使用一個介面)。

您將使用虛擬 Edge 作為中樞。以下是線路和 IP 位址資訊的範例。

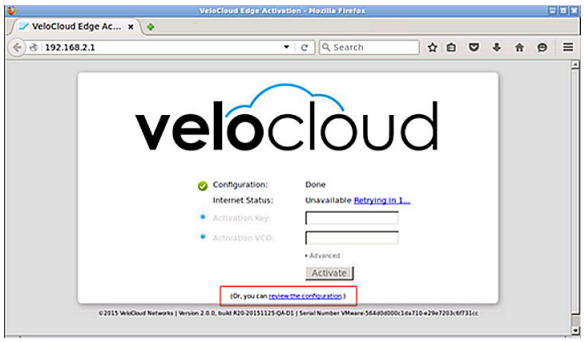


設定並啟動中樞 1 SD-WAN Edge 以連線至網際網路

由於這是資料中心/中樞站台，因此 SD-WAN Edge 無法使用 DHCP 取得其 WAN IP。因此，您必須先啟用 SD-WAN Edge 以透過資料中心防火牆連線至網際網路，之後才能啟用 SD-WAN Edge。

1 為電腦設定靜態 IP **192.168.2.100/24** 和閘道 **192.168.2.1**，這是存取 SD-WAN Edge 的預設 LAN 設定。將電腦連線至 SD-WAN Edge LAN 介面。

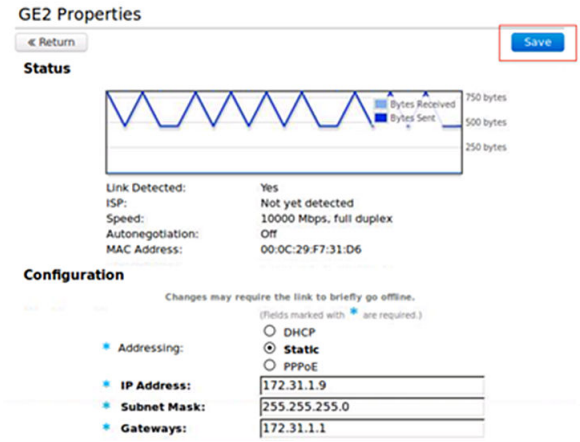
2 從電腦瀏覽至 http://192.168.2.1 (SD-WAN Edge 的本機 Web 介面)。按一下連結**檢閱組態 (review the configuration)**。



3 設定 SD-WAN Edge 的 GE2 靜態 WAN IP 和預設閘道，使其能夠連線至網際網路。

按一下**儲存 (Save)**，並提供**管理員/管理員 (admin/admin)** 的登入/密碼。

一般而言，在資料中心/中樞站台上，系統會將靜態 IP 位址指派給您，而企業 IT 管理員會設定防火牆以將 SD-WAN Edge WAN IP 轉譯為公用 IP，同時篩選適當的流量 (輸出：TCP/443、輸入：UDP/2426、UDP/500、UDP/4500)。



4 此時，網際網路狀態應會顯示為「已連線」。

在 SD-WAN Edge 靜態 WAN IP 位址和相關聯的防火牆組態設定完成後，SD-WAN Edge 網際網路狀態會顯示為「已連線」。

在預設設定檔中啟用虛擬 SD-WAN Edge

1 登入 SD-WAN Orchestrator。

2 預設 VPN 設定檔可讓您啟動 SD-WAN Edge 500。

啟動中樞 1 SD-WAN Edge

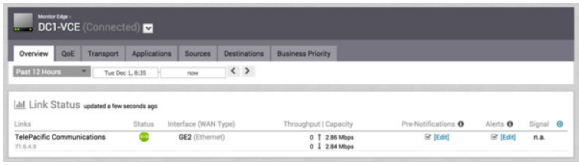
1 移至**設定 (Configure) > Edge**，然後新增 SD-WAN Edge。指定正確的型號和設定檔 (我們使用快速入門 VPN 設定檔)。

2 移至中樞 SD-WAN Edge (DC1-VCE)，然後依照一般啟用程序操作。如果您已設定電子郵件功能，則會將啟用電子郵件傳送至該電子郵件地址。若未設定，您可以移至裝置設定頁面取得啟用 URL。

3 複製啟用 URL 並將其貼到連線至 SD-WAN Edge 之電腦上的瀏覽器，或直接從電腦瀏覽器中按一下啟用 URL。

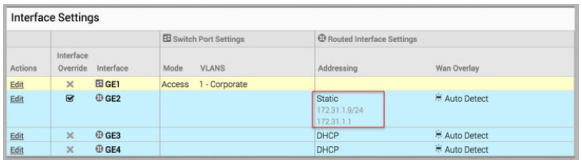
4 按一下**啟動 (Activate)** 按鈕。

5 現在，**DC1-VCE** 資料中心中樞應會啟動。移至**監控 (Monitor) > Edge**。按一下 **Edge 概觀 (Edge Overview)** 索引標籤。系統會偵測公用 WAN 連結容量，以及正確的公用 IP **71.6.4.9** 和 ISP。



6 移至**設定 (Configure) > Edge**，然後選取 **DC1-VCE**。移至**裝置 (Device)** 索引標籤，然後向下捲動至**介面設定 (Interface Settings)**。

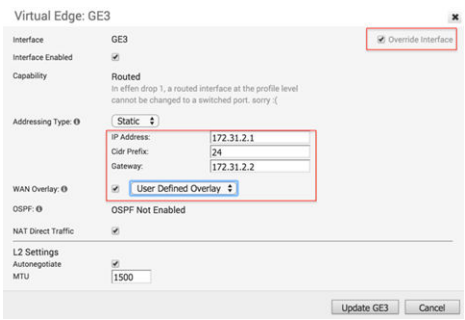
您將會看到登錄程式通知 SD-WAN Orchestrator 已透過本機 UI 設定靜態 WAN IP 位址和閘道。VMware 的組態會據以更新。



7 向下捲動至 **WAN 設定 (WAN Settings)** 區段。連結類型應自動識別為**公用有線 (Public Wired)**。

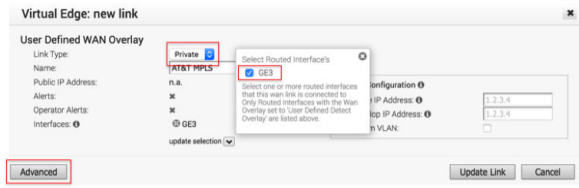
在中樞 1 SD-WAN Edge 上設定私人 WAN 連結

1 直接從 SD-WAN Orchestrator 設定私人 MPLS Edge WAN 介面。移至**設定 (Configure) > Edge**，然後選擇 **DC1-VCE**。移至**裝置 (Device)** 索引標籤，然後向下捲動至 [介面設定 (Interface Settings)] 區段。在 GE3 上將靜態 IP 設定為 **172.31.2.1/24**，並設定預設閘道 **172.31.2.2**。在 **WAN 覆疊 (WAN Overlay)** 下，選取**使用者定義的覆疊 (User Defined Overlay)**。這可以讓我們在下一個步驟中手動定義 WAN 連結。



2 在 **WAN 設定 (WAN Settings)** 下，按一下**新增使用者定義的 WAN 覆疊 (Add User Defined WAN Overlay)** 按鈕 (請參閱下列螢幕擷取畫面)。

3 為 MPLS 路徑定義 WAN 覆疊。選取**私人 (Private)** 的**連結類型 (Link Type)**，然後在 [IP 位址 (IP Address)] 欄位中指定 WAN 連結的下一個躍點 IP (172.31.2.2)。選擇 GE3 作為介面。按一下**進階 (Advanced)** 按鈕。



提示：中樞站台通常會比分支具有更多頻寬。如果選擇自動探索頻寬，中樞站台將會對第一個對等執行頻寬測試 (例如，第一個啟動的分支)，且將停止探索不正確的 WAN 頻寬。對於中樞站台，您應一律以手動方式定義 WAN 頻寬 (在進階設定中執行)。

4 在進階設定中指定私人 WAN 頻寬。下方的螢幕擷取畫面顯示中樞上對稱 MPLS 連結 5 Mbps 的上游和下游頻寬範例。

5 驗證已設定 WAN 連結，並儲存變更。

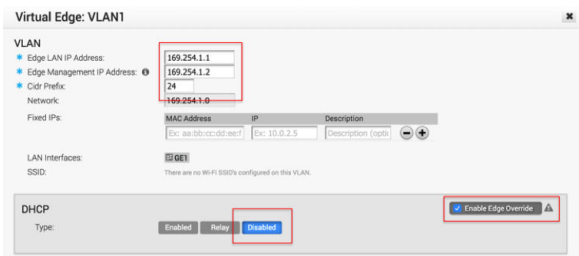
您已完成在中樞上設定 SD-WAN Edge 的作業。在啟用分支 SD-WAN Edge 前，您將不會看到剛才新增的使用者定義 MPLS 覆疊。

(選用) 為 LAN 介面設定管理 IP

1 移至**設定 (Configure) > Edge**，然後選取 **DC1-VCE**。

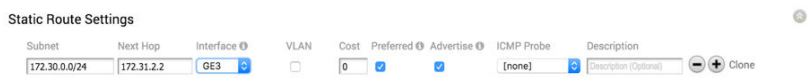
2 **導覽至裝置 (Device)** 索引標籤，然後向下捲動至 [VLAN 設定 (VLAN Settings)] 區段。

3 按一下**編輯 (Edit)**，然後設定介面的 IP 位址。



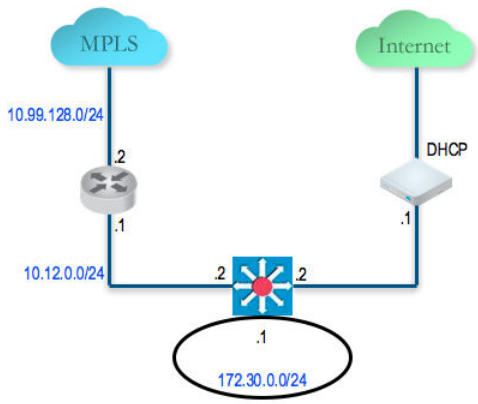
在 L3 交換器後方設定 LAN 網路的靜態路由

透過 L3 交換器將靜態路由新增至 **172.30.0.0/24** 子網路。您必須指定要用來路由至下一個躍點的介面 GE3。請務必啟用 [通告 (Advertise)] 核取方塊，使其他 SD-WAN Edges 能在 L3 交換器後方學習此子網路 (請參閱下列螢幕擷取畫面)。



設定並啟動銀級 1 站台

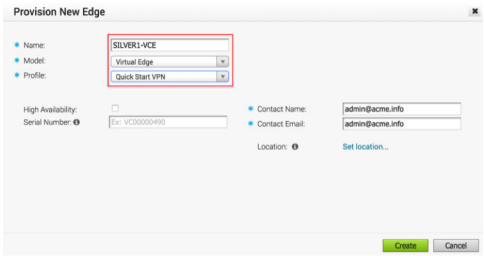
此步驟可協助您瞭解如何在銀級站台插入 SD-WAN Edge 的一般工作流程。SD-WAN Edge 會在路徑外插入，並依賴 L3 交換器來重新導向流量。以下是線路和 IP 位址資訊的範例。



啟動銀級 1 站台分支 SD-WAN Edge

在此範例中，我們假設 SD-WAN Edge 使用 DHCP 取得其公用 IP 位址，因此不需要進行任何設定。SD-WAN Edge 隨附可在所有路由介面上使用 DHCP 的預設組態。

1 建立新的 Edge **SILVER1-DCE**，然後選取適當的型號和設定檔 (請參閱下圖)。



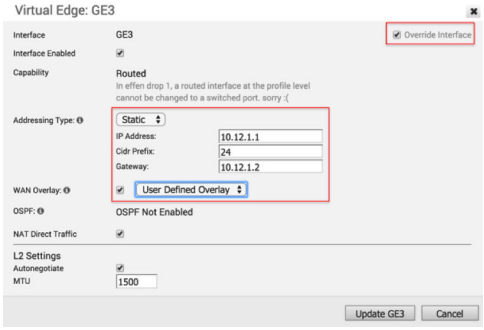
2 將電腦連線至其 LAN 或 Wi-Fi 以啟動此 SD-WAN Edge。

3 SD-WAN Edge 此時應會在 SD-WAN Orchestrator 中處於作用中狀態，且具有一個公用連結。我們現在可以設定私人 WAN 連結。

在銀級 1 站台 SD-WAN Edge 上設定私人 WAN 連結

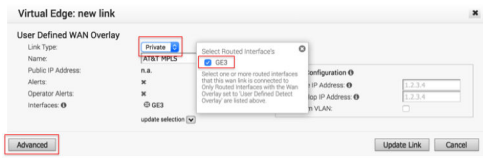
此時，我們必須建置從 SD-WAN Edge 到 L3 交換器的 IP 連線。

1 移至**設定 (Configure) > Edge**，選取 **SILVER1-VCE** 並移至 [裝置 (Device)] 索引標籤，然後向下捲動至 [介面設定 (Interface Settings)] 區段。在 GE3 上將靜態 IP 設定為 **10.12.1.1/24**，並設定預設閘道 **10.12.1.2**。在 **WAN 覆疊 (WAN Overlay)** 下，選取**使用者定義的覆疊 (User Defined Overlay)**。這可以讓我們在下一個步驟中手動定義 WAN 連結。



2 在 **WAN 設定 (WAN Settings)** 區段下，按一下**新增使用者定義的 WAN 覆疊 (Add User Defined WAN Overlay)**。

3 為 MPLS 路徑定義 WAN 覆疊。選取**私人 (Private)** 的**連結類型 (Link Type)**。在 [IP 位址 (IP Address)] 欄位中指定 WAN 連結的下一個躍點 IP (10.12.1.2)。選擇 GE3 作為介面。按一下**進階 (Advanced)** 按鈕。



提示：由於中樞已設定，因此可以自動探索頻寬。此分支將對中樞執行頻寬測試，以探索其連結頻寬。

4 將頻寬測量設定為**測量頻寬 (Measure Bandwidth)**。這將導致分支 SD-WAN Edge 對中樞 SD-WAN Edge 執行頻寬測試，如同連線至 SD-WAN Gateway 時所發生的情況。

5 驗證已設定 WAN 連結，並儲存變更 (請參閱下列螢幕擷取畫面)。

(選用) 為 LAN 介面設定管理 IP

1 移至**設定 (Configure) > Edge**，選取 **SILVER1-VCE**。導覽至**裝置 (Device)** 索引標籤，然後向下捲動至 [VLAN 設定 (VLAN Settings)] 區段。按一下**編輯 (Edit)**。設定 LAN 和管理介面的 IP 位址。

在 L3 交換器後方設定 LAN 網路的靜態路由

透過 L3 交換器將靜態路由新增至 **192.168.128.0/24**。您必須指定介面 GE3。請務必啟用 [通告 (Advertise)] 核取方塊，使其他 SD-WAN Edges 能在 L3 交換器後方學習此子網路 (請參閱下列螢幕擷取畫面)。

啟用分支到中樞的通道 (銀級 1 到中樞 1)

此步驟可協助您建置從分支到中樞的覆疊通道。請注意，此時您可能會看到連結已啟動，但這是透過網際網路路徑連至 SD-WAN Gateway 的通道，而非連至中樞的通道。我們必須啟用雲端 VPN，才能建立從分支到中樞的通道。

現在您已準備就緒，可以建置從分支到中樞的通道。

啟用雲端 VPN 和 Edge 到 SD-WAN Hub 的通道

1 步驟 1：移至**設定 (Configure)** > **設定檔 (Profiles)**，選取**快速入門 VPN 設定檔 (Quick Start VPN Profile)**，然後移至**裝置 (Device)** 索引標籤。啟用雲端 VPN，然後執行下列動作。

- 在**分支到中樞 (Branch to Hubs)** 下，勾選**啟用 (Enable)** 核取方塊。
- 在**分支到分支 VPN (Branch to Branch VPN)** 下，勾選**啟用 (Enable)** 核取方塊。
- 在**分支到分支 VPN (Branch to Branch VPN)** 下，取消勾選 [使用雲端閘道 (Use Cloud Gateways)] 核取方塊。執行此動作將會透過 SD-WAN Gateway 停用分支到分支 VPN 的資料平面。在建立分支到分支的直接通道時，分支到分支的流量會先通過其中一個中樞 (位於您後續將指定的排序清單中)。

按一下**選取中樞 (Select Hubs)** 按鈕。接著，將 **DC1-VCE** 移至右側。這會將 **DC1-VCE** 指定為 SD-WAN Hub。按一下中樞中的 **DC1-VCE**，然後按一下**啟用回傳中樞 (Enable Backhaul Hubs)** 和**啟用 B2B VPN 中樞 (Enable B2B VPN Hubs)** 按鈕。我們會將相同的 **DC1-VCE** 用於分支到分支的流量和中樞的回傳網際網路流量。在 [雲端 VPN (Cloud VPN)] 區段下，**DC1-VCE** 現在會顯示為兩個 SD-WAN Hubs，並且用於分支到分支 VPN 中樞。

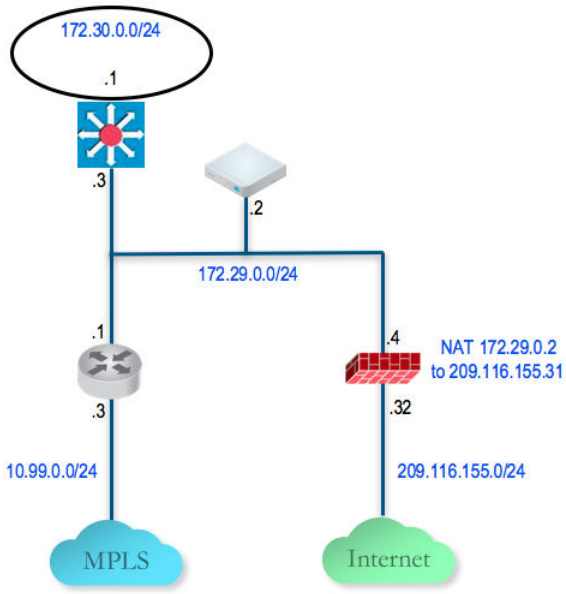
2 此時，應會啟動分支與中樞 SD-WAN Edges 之間的直接通道。偵錯命令此時也會顯示分支與中樞之間的直接通道。以下是來自 **SILVER1-VCE** 的範例。請注意 **71.6.4.9** 和 **172.31.2.1** 以外的通道。這些是連至中樞 SD-WAN Edge 的直接通道 (透過公用網際網路的 GE2，以及透過私人連結的 GE3)。

設定並啟動銅級 1 站台

此步驟可協助您建立銅級站台 - 具有一個 DIA 和一個寬頻的雙網際網路站台。以下是線路和 IP 位址資訊的範例。**BRONZE1-VCE** SD-WAN Edge LAN，並啟動 SD-WAN Edge。WAN 上不需要進行任何設定，因為它會對兩個 WAN 介面使用 DHCP。

設定並啟動中樞 2

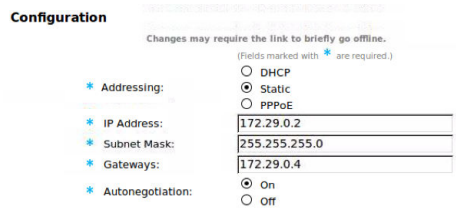
此步驟可協助您設定通常用於單臂中樞部署中的「依 IP 位址操控」。以下是線路和 IP 位址資訊的範例。在單臂部署中，可以使用相同的通道來源 IP 在不同的路徑上建立覆疊。



設定中樞 2 SD-WAN Edge 以連線至網際網路

1 將電腦連線至 SD-WAN Edge，並使用瀏覽器指向 http://192.168.2.1。

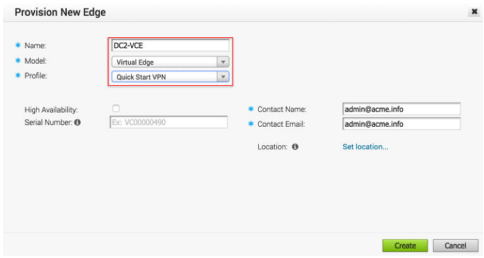
2 藉由設定第一個 WAN 介面 GE2 來設定中樞 SD-WAN Edge，以連線至網際網路。



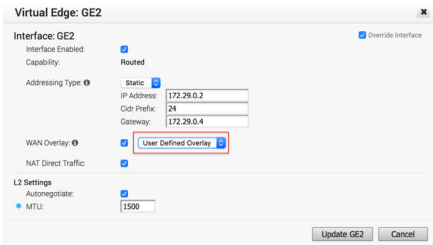
將中樞 2 SD-WAN Edge 新增至 SD-WAN Orchestrator 並啟動

在此步驟中，您將建立名為 **DC2.VCE** 的第二個中樞 SD-WAN Edge。

1 在 SD-WAN Orchestrator 上，移至**設定 (Configure)** > **Edge**，選取**新增 Edge (New Edge)** 以新增 SD-WAN Edge。



2 移至**設定 (Configure)** > **Edge**，選取您剛剛建立的 SD-WAN Edge，然後移至**裝置 (Device)** 索引標籤，以設定您在上一個步驟中設定的相同介面和 IP。

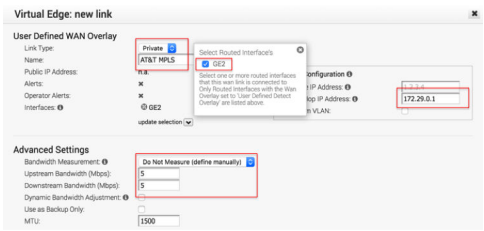


重要 由於我們將在單臂模式中部署 SD-WAN Edge (相同的實體介面，但此介面中會有多個通道)，因此請務必將 WAN 覆疊指定為 [使用者定義 (User Defined)]。

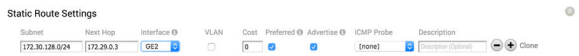
3 此時，您必須建立覆疊。在 **WAN 設定 (WAN Settings)** 下，按一下**新增使用者定義的 WAN 覆疊 (Add User Defined WAN Overlay)**。

4 建立跨公用連結的覆疊。在我們的範例中，我們將使用下一個躍點 IP **172.29.0.4** 以透過防火牆連線至網際網路。防火牆已設定為會將流量 NAT 至 **209.116.155.31**。

5 新增跨私人網路的第二個覆疊。在此範例中，我們會指定下一個躍點路由器 **172.29.0.1**，並指定頻寬，因為這是 MPLS Leg，**DC2-VCE** 是中樞。



透過 GE2 將靜態路由新增至 LAN 端子網路 **172.30.128.0/24** (請參閱下列螢幕擷取畫面)。



6 啟動 SD-WAN Edge。啟用成功後，請回到 Edge 層級組態下的**裝置 (Device)** 索引標籤。請注意，[公用 IP (Public IP)] 欄位現已填入。您現在應該會在**概觀 (Overview)** 索引標籤下的**監控 (Monitor)** > **Edge** 中看到連結。**(選用) 為 LAN 介面設定管理 IP** 移至**設定 (Configure)** > **Edge**，選取 **DC2-VCE**。導覽至**裝置 (Device)** 索引標籤，然後向下捲動至 [VLAN 設定 (VLAN Settings)] 區段。按一下**編輯 (Edit)**。設定 LAN 和管理介面的 IP 位址。

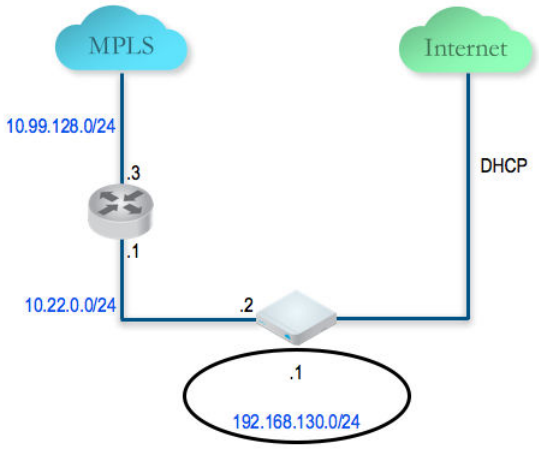
將中樞 2 SD-WAN Edge 新增至快速入門 VPN 設定檔中的中樞清單

1 移至**設定 (Configure) > 設定檔 (Profiles)**，然後選取設定檔**快速入門 VPN**。

2 移至**裝置 (Device)** 索引標籤，然後將這個新的 SD-WAN Edge 新增至中樞清單。

設定並啟動銀級 2 站台

此步驟可協助您建立銀級站台 -- 一個混合式站台 (在 CE 路由器後方有 SD-WAN Edge，且以 SD-WAN Edge 作為 LAN 的預設路由器)。以下是針對每個硬體的線路和 IP 位址資訊範例。



將電腦連線至 SD-WAN Edge LAN 或 Wi-Fi，然後使用瀏覽器指向 http://192.168.2.1。

使用 OSPF 或 BGP 設定動態路由

18

本節說明如何使用 OSPF 或 BGP 設定動態路由。

SD-WAN Edge 會透過 OSPF 和 BGP 學習來自相鄰路由器的路由。它會將學習的路由傳送至閘道/控制器。閘道/控制器的運作方式類似於路由反射程式，會將學習的路由傳送至其他 SD-WAN Edge。覆疊流量控制 (OFC) 可實現企業範圍的路由可見度和控制，以便進行程式設計以及完整和部分覆疊。

VMware 支援對 OSPF 芳鄰、OE1/OE2 路由類型、MD5 驗證的輸入/輸出篩選器。透過 OSPF 學習的路由將自動重新分配至雲端或內部部署中主控的控制器。支援輸入/輸出篩選器，且篩選器可設定為「拒絕」，或者您可以選擇性地新增/變更 BGP 屬性以影響路徑選取，例如 RFC 1998 社群、MED 和本機喜好設定。

備註 如需 OSPF 和 BGP 重新分配的相關資訊，請參閱標題為 OSPF/BGP 重新分配一節。

備註 在 3.2 版中，可以同時在 SD-WAN Edge 中啟用 BGP 和 OSPF。

本章節討論下列主題：

- 啟用 OSPF
- 啟用 BGP
- OSPF/BGP 重新分配
- 覆疊流量控制

啟用 OSPF

「先開啟最短路徑 (OSPF)」只能在作為被動介面的 LAN 介面上啟用。Edge 只會通告與該 LAN 交換器連接埠相關聯的首碼。若要取得完整的 OSPF 功能，您必須在路由介面中使用該功能。

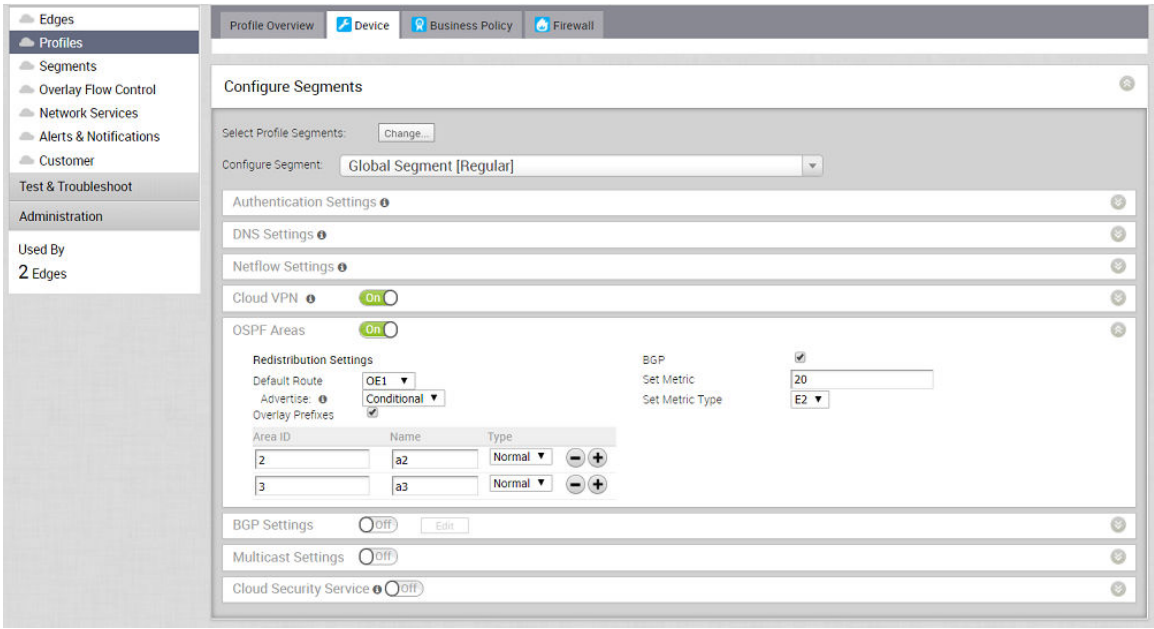
若要啟用 OSPF，請執行此程序的步驟：

1 設定 VPN 設定檔的 OSPF。

   a 移至**設定 (Configure) > 設定檔 (Profile)**。

   b 按一下您要為其設定 OSPF 之 VPN 設定檔對應的**裝置 (Device)** 圖示。

   設定區段 (Configure Segments) 畫面隨即出現。



c 在 **OSPF 區域 (OSPF Areas)** 區段中，**開啟 (ON) OSPF 區域 (OSPF Areas)** 切換按鈕。

d 設定 OSPF 區域的重新分配設定。

1 在**預設路由 (Default Route)** 下拉式功能表中，選擇要用於預設路由的 OSPF 路由類型 (E1 或 E2)。

2 在**通告 (Advertise)** 下拉式功能表中，選擇**一律 (Always)** 或**條件式 (Conditional)**。(選擇 [一律 (Always)] 表示一律會通告預設路由。選擇 [條件式 (Conditional)]，表示只有在 Edge 透過覆疊或底層學習時，才會重新分配預設路由。必須勾選 [覆疊首碼 (Overlay Prefixes)] 選項，才能使用條件式預設路由。

3 如果適用，請勾選**覆疊首碼 (Overlay Prefixes)** 核取方塊。

4 (選用) 若要啟用將 BGP 路由插入至 OSPF 的功能，請選取 **BGP** 核取方塊。BGP 路由可重新分配至 OSPF 中，因此如果適用，請輸入或選擇如下的組態選項：

a 在**設定度量 (Set Metric)** 文字方塊中，輸入度量。(OSPF 會將此度量放入它從重新分配之路由產生的外部 LSA 中)。預設度量為 20。

b 在**設定度量類型 (Set Metric Type)** 下拉式功能表中，選擇度量類型。(可以是類型 E1 或 E2 (OSPF 外部 LSA 類型))；預設類型為 E2)。

5 在**識別碼 (ID)** 文字方塊中，輸入 **OSPF 區域識別碼 (OSPF Area ID)**。

6 在**名稱 (Name)** 文字方塊中，輸入區域的描述性名稱。

7 依預設會選取**一般 (Normal)** 類型。目前僅支援**一般 (Normal)** 類型。

8 如有必要，請按一下 ⊕ 以新增其他區域。

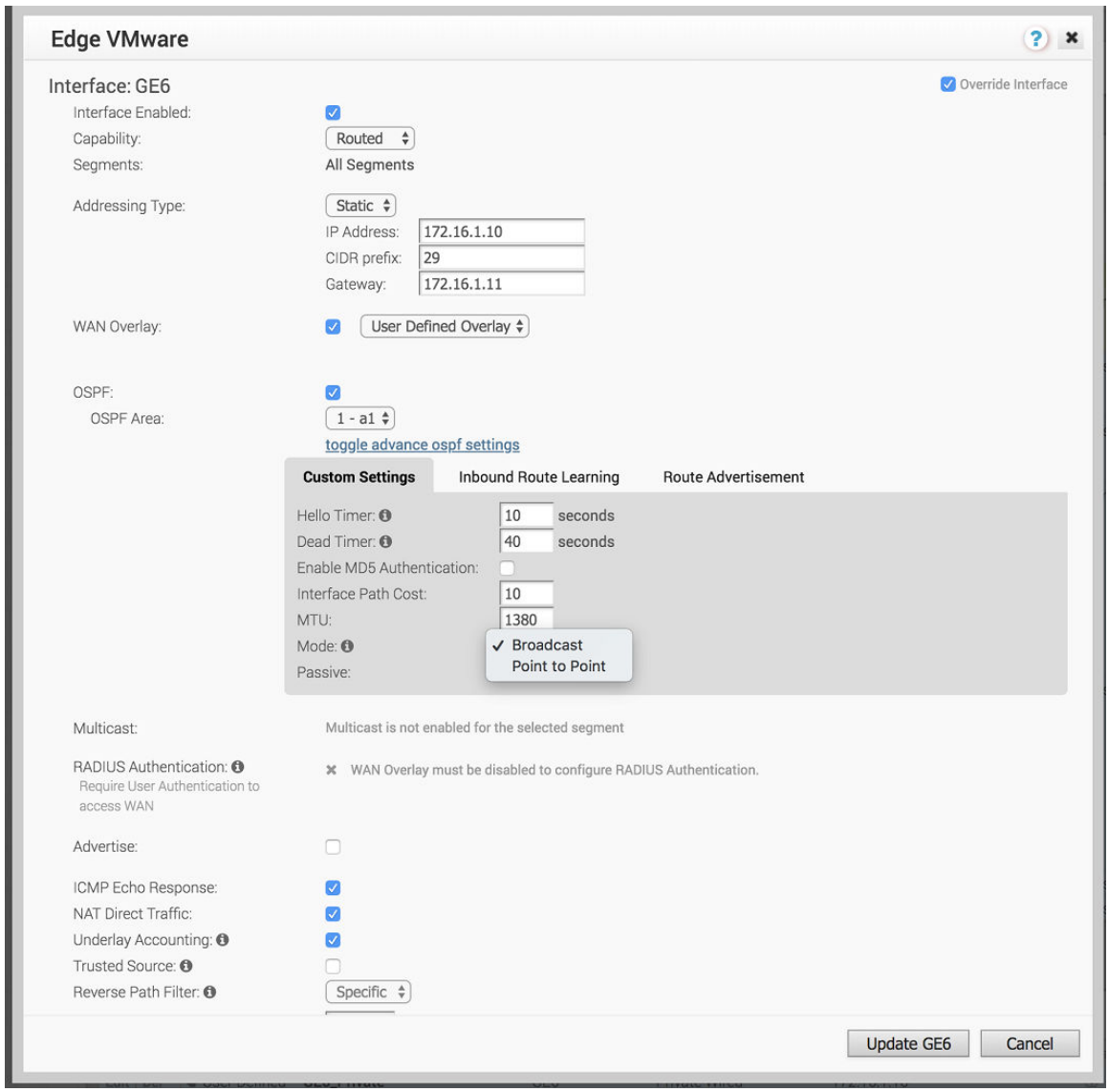
2 為已啟用 OSPF 的 Edge 裝置設定路由介面設定。

備註 SD-WAN Orchestrator 支援在 Edge 和設定檔層級上使用 OSPF **點對點 (Point to Point)** 網路模式。

a 在**設定區段 (Configure Segments)** 畫面中，向下捲動至您要為其設定介面和 OSPF 設定之 Edge 裝置的**裝置設定 (Device Settings)** 區域。

b 按一下對應於 Edge 的展開圖示。

c 在**介面設定 (Interface Settings)** 區域中，按一下介面的**編輯 (Edit)** 連結。Edge 裝置的 [介面設定 (Interface Setting)] 畫面隨即出現。



d 選取 **OSPF** 核取方塊。

e 在 **OSPF 區域 (OSPF Areas)** 下拉式功能表中，選取 OSPF 區域。

f 按一下**切換進階 OSPF 設定 (toggle advance ospf settings)** 連結，以設定進階 OSPF 設定。

1 建立**輸入路由學習 (Inbound Route Learning)** 和**路由通告 (Route Advertisement)** 的篩選器。如需詳細資訊，請參閱路由篩選器。

2 按一下**自訂設定 (Customs Settings)** 索引標籤，然後設定下列 OSPF 設定。

a 在 **Hello Timer** 文字方塊中，輸入 OSPF Hello 時間間隔 (以秒為單位)。允許的範圍為 1 到 255。

b 在 **Dead Timer** 文字方塊中，輸入 OSPF Dead 時間間隔 (以秒為單位)。允許的範圍為 1 到 65535。

c 選取**啟用 MD5 驗證 (Enable MD5 Authentication)** 核取方塊，以啟用 MD5 驗證。

d 在**介面路徑成本 (Interface Path Cost)** 文字方塊中，輸入介面路徑的 OSPF 成本。

e 在 **MTU** 文字方塊中，輸入介面的傳輸單元最大值 (MTU) 值。

f 在**模式 (Mode)** 下拉式功能表中，選取**廣播 (Broadcast)** 或**點對點 (Point to Point)** 作為 OSPF 網路類型模式。預設的 OSPF 模式為**廣播 (Broadcast)**。

g 選取**被動 (Passive)** 核取方塊，以啟用 OSPF 被動模式。

h 按一下**更新 (Update)** 按鈕。

3 按一下**儲存變更 (Save Changes)**。

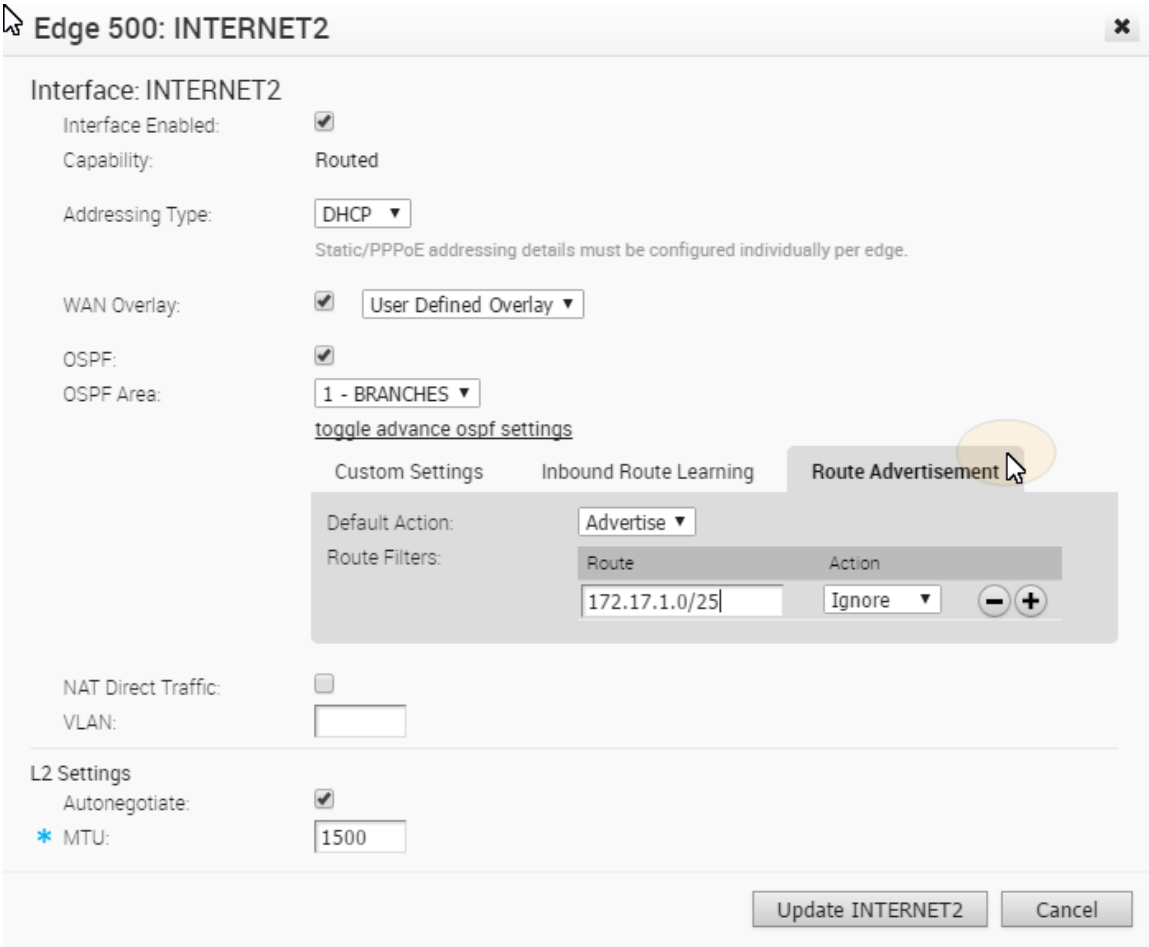
此時會顯示**確認變更 (Confirm Changes)** 對話方塊，要求您確認要啟用的 OSPF 區域。此外也會顯示受影響的 Edge 數目。

備註 如果您擁有在設定檔層級未與 OSPF 組態相關聯的 Edge，則必須從**設定 (Configure) > Edge > 裝置 (Device) > 介面設定 (Interface Settings) 區域**進行 Edge 層級的設定。

路由篩選器

路由分成兩種不同的類型：輸入和輸出。

- 輸入路由包含可從 OSPF 學習或忽略，並安裝在覆疊流量控制中的喜好設定。
- 輸出路由會指出可重新分配到 OSPF 中的首碼。



啟用 BGP

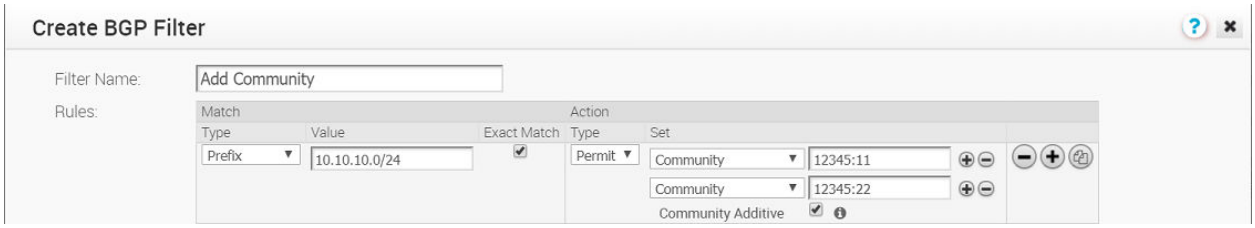
在企業層級上，依預設會啟用路由 BGP 功能。您可以依照此程序的步驟來設定每個區段的 BGP。

備註

- 支援 4-Byte ASN BGP，在路由通告中對等至具有 4-Byte ASN- Accept 4-Byte ASN 的芳鄰。僅支援純文字格式；不支援 asdot/decimal 格式。
- 可為每個區段設定 BGP。您可以在啟用 Edge 覆寫的情況下，在設定檔層級或 Edge 層級進行設定。

社群累加支援 (Community Additive Support)

BGP 輸入和輸出組態支援設定 BGP 社群。社群值可用來識別路由的來源。依預設，如果未勾選「累加」，現有的 BGP 社群將會取代為「設定」值。如果勾選社群累加選項，我們就會將設定的社群值附加至現有的 BGP 社群。如以下範例圖所示，社群 12345:11 和 12345:22 會附加至現有的 BGP 社群。附註：支援的社群字串數目上限為十二個。



1 設定 VPN 設定檔的 BGP：

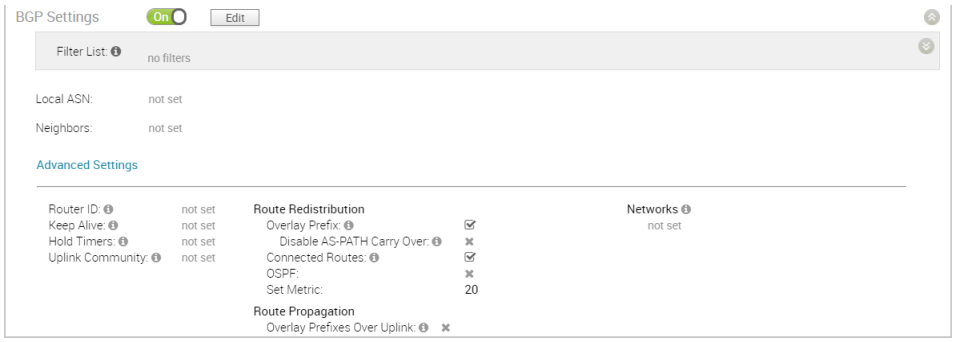
a 移至導覽面板中的**設定 (Configure) > 設定檔 (Profile)**。

組態設定檔 (Configuration Profiles) 畫面隨即出現。

b 選取您要為其啟用 BGP 的設定檔，然後按一下適用設定檔的**裝置 (Device)** 圖示。

所選設定檔的**裝置設定 (Device Settings)** 畫面隨即出現。

2 向下捲動至 **BGP 設定 (BGP Settings)** 區域，然後**開啟 BGP (BGP ON)**，如下圖所示。

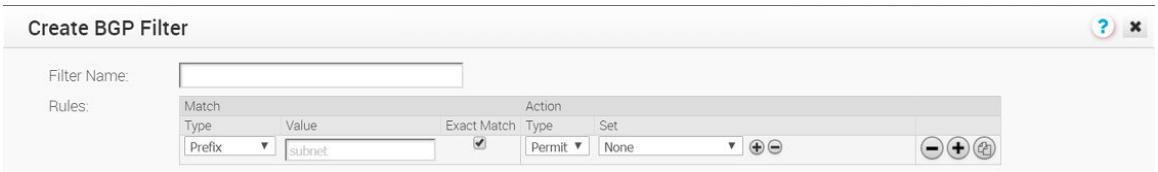


3 按一下**編輯 (Edit)** 按鈕，以定義 BGP 芳鄰。

4 在 **BGP 編輯器 (BGP Editor)** 中：

a 按一下**新增篩選器 (Add Filter)** 按鈕，以建立一或多個篩選器。(這些篩選器將套用至芳鄰，以拒絕或變更路由的屬性。相同的篩選器可用於多個芳鄰)。

建立 BGP 篩選器 (Create BGP Filter) 對話方塊隨即出現 (如下圖所示)。



b 在**建立 BGP 篩選器 (Create BGP Filter)** 對話方塊中：

1 在**篩選器名稱 (Filter Name)** 文字方塊中，輸入篩選器的名稱。

2 設定篩選器的規則。

- 在**類型 (Type)** 下拉式功能表中選擇首碼或社群。
- 在**值 (Value)** 文字方塊中設定首碼或社群的值。

- 如果適用，請勾選**完全相符 (Exact Match)** 核取方塊。
- 在**類型 (Type)** 下拉式功能表中指定動作類型 (允許或拒絕)。
- 在**設定 (Set)** 下拉式功能表中，選擇 [無 (None)]、[本機喜好設定 (Local Preference)]、[度量 (Metric)]、[AS-Path-Prepend] 或 [社群 (Community)]、[社群累加 (Community Additive)] 核取方塊。如需詳細資訊，請參閱上述標題為社群累加支援一節。

請參閱下表以取得這些欄位的說明 (請參閱表格下的影像)。

規則欄位	說明
比對類型：首碼或社群 (Match Type: Prefix or Community)	
值 (Value)	
完全相符 (Exact Match) 核取方塊	
動作類型：允許或拒絕 (Action Type: Permit or Deny)	
設定選項：無 (Set Option: None)	
設定選項：本機喜好設定 (Set Option: Local Preference)	
設定選項 (Set Option:)：社群 (Community) 和社群累加 (Community Additive) 核取方塊	BGP 輸入和輸出組態支援社群組態選項。這會附加傳入的社群屬性與已設定的社群值。社群值可用來識別路由的來源。依預設，如果未勾選「累加」，社群值將會取代為「設定」值。
設定選項：度量 (Set Option: Metric)	
設定選項 (Set Option)：AS-Path-Prepend	

c 設定篩選器的規則後，請按一下**確定 (OK)** 按鈕。

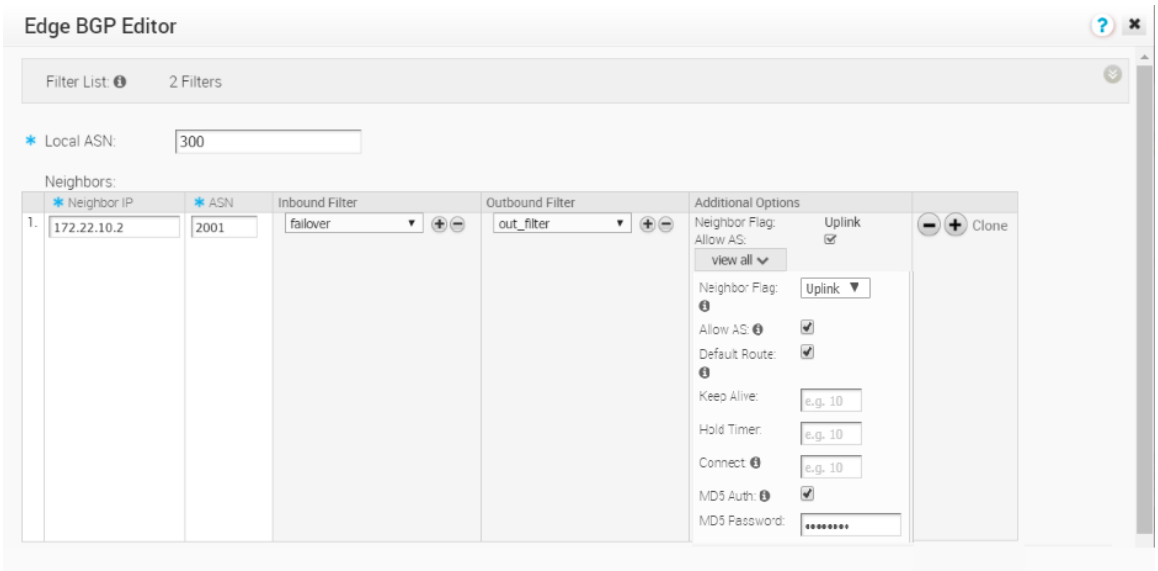
d 在 **BGP 編輯器 (BGP Editor)** 對話方塊中，在**本機 ASN (Local ASN)** 文字方塊中輸入本機 ASN 號碼。

e 在芳鄰的區域中，在適當的文字方塊中輸入**芳鄰 IP (Neighbor IP)** 和 **ASN**，然後從上一步所定義的**篩選器 (Filter)** 清單中指定輸入篩選器或輸出篩選器。

f 按一下**全部檢視 (view all)** 按鈕開啟下拉式功能表，以新增其他選項。視需要套用其他選項。(請參閱下表以取得每個選項的說明，並進一步參考下方的表格)。

其他選項欄位	說明
芳鄰旗標 (Neighbor Flag) 下拉式功能表	用來標示芳鄰類型。從下拉式功能表中選擇兩個選項：[無 (None)] 和 [上行 (Uplink)]。如果將上行用作對 MPLS 的 WAN 覆疊，請選取 [上行 (Uplink)]。它將用作旗標，而藉由將從 SD-WAN 覆疊學習的路由傳播至通往 MPLS 的 WAN 連結，以決定站台是否會成為傳送站台 (例如中樞)。如果需要使其成為傳送站台，請一併在進階選項中勾選 [透過上行覆疊首碼 (Overlay Prefix Over Uplink)]。
允許 AS (Allow AS) 核取方塊	即使 AS 路徑中有相同的 AS，仍會學習 BGP 路由。

其他選項欄位	說明
預設路由 (Default Route) 核取方塊	對芳鄰通告預設路由。如需使用**預設路由 (Default Route)** 核取方塊的詳細資訊，請參閱下方的步驟「i」。
連線 (Connect)	在偵測到 TCP 工作階段並非被動時，嘗試與對等建立新 TCP 連線前的間隔時間 (以秒為單位)。預設值為 120 秒。
MD5 驗證 (MD5 Auth) 核取方塊	啟用 BGP MD5 驗證。[MD5 驗證 (MD5 Auth)] 核取方塊用於舊版網路或聯邦網路中，且通常會以 BGP MD5 作為 BGP 對等的安全防護。
MD5 密碼 (MD5 Password) 文字方塊	啟用 MD5 驗證時需要密碼。



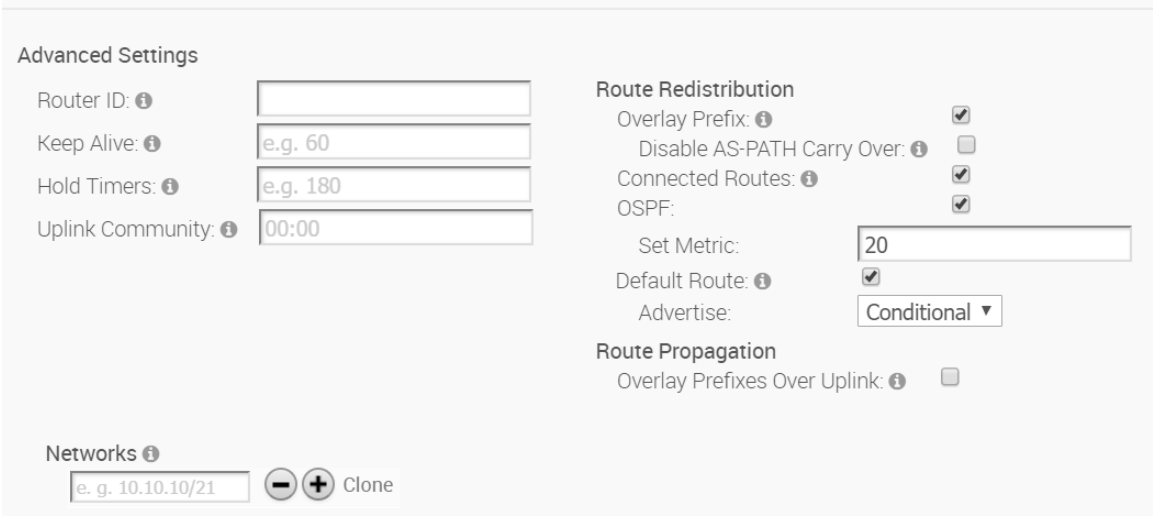
g 按一下**進階設定 (Advanced Settings)** 按鈕。

進階設定 (Advanced Settings) 區域隨即出現。

h 在**其他設定 (Additional Settings)** 區域中，您可以輸入下列其他 BGP 設定，如下表所述。(請進一步參考下方的表格)。

其他設定欄位 (Additional Settings Fields)	說明 (Description)
路由器識別碼 (Router ID)	若未設定識別碼，將會自動指派識別碼。
保持運作 (Keep Alive)	將「保持運作」訊息傳送至其對等的頻率 (以秒為單位)。預設值為 60 秒。範圍為 0-65535。
保存計時器 (Hold Timers)	將對等視為未收到「保持運作」訊息前的間隔時間 (以秒為單位)。預設值為 180 秒。範圍為 0-65535。
上行社群 (Uplink Community)	上行是指連線至提供者 Edge (PE) 的連結。 與此社群相符的輸入路由 (通往 Edge) 將被視為上行路由。(其中不會將中樞/Edge 視為擁有者)。 輸入可採用原始數字格式，或採用新的 AA:NN 格式。
覆疊首碼 (Overlay Prefix)	重新分配從覆疊學習的首碼。

停用 AS-PATH 延續 (Disable AS-PATH Carry Over)	依預設，此選項應保留為不勾選。在某些拓撲中，停用 AS-PATH 延續將會影響到輸出 AS-PATH，而使 L3 路由器優先使用指向 Edge 或中樞的路徑。**警告：如果勾選 [AS-PATH 延續 (AS-PATH Carry Over)]，請調整您的網路以避免發生路由迴圈 (Warning: When the AS-PATH Carry Over is checked, tune your network to avoid routing loops.)。**
連線的路由 (Connected Routes)	重新分配所有已連線的介面子網路。
OSPF 核取方塊	可讓 OSPF 重新分配至 BGP。
預設路由 (Default Route)	只有在 Edge 透過覆疊或底層學習時，才會重新分配預設路由。
設定度量文字方塊 (Set Metric textbox)	您可以選擇啟用 OSPF，以允許將 OSPF 路由插入 BGP 中。已重新分配 OSPF 路由預設的 BGP 度量為 MED 值 20。
透過上行覆疊首碼 (Overlay Prefixes Over Uplink)	上行是指設定為使用**芳鄰 (Neighbor)** 旗標上行的連結/芳鄰 (這類連結通常會連線至提供者 Edge (PE) 路由器)。將從覆疊學習的路由傳播至具有**芳鄰 (Neighbor)** 旗標的上行。
網路 (Networks)	BGP 將以 10.10.10.10/21 格式通告的網路。



i 按一下**確定 (OK)** 以儲存組態。

備註 如果您勾選了位於**其他設定 (Additional Settings)** 區域中的**預設路由 (Default Route)** 核取方塊，請注意下列四種情況：

- 如果啟用了全域**預設路由 (Default Route)** 選項並選取 [條件式 (Conditional)] 選項，且未選取每個 BGP 芳鄰選項**預設路由 (Default Route)**，則在 Edge 透過覆疊或底層學習明確的預設路由時，BGP 只會將預設路由重新分配至其芳鄰。
- 如果啟用了全域**預設路由 (Default Route)** 選項並選取 [條件式 (Conditional)] 選項，且選取了每個 BGP 芳鄰選項**預設路由 (Default Route)**，則每個 BGP 芳鄰組態會覆寫全域組態，因此請「一律對 BGP 對等通告預設路由」。
- 若未啟用全域**預設路由 (Default Route)** 選項，而選取了依據 BGP 芳鄰選項**預設路由 (Default Route)**，請一律對 BGP 對等通告預設路由。
- 若未啟用全域**預設路由 (Default Route)** 選項，且未選取依據 BGP 芳鄰選項**預設路由 (Default Route)**，請勿對 BGP 對等通告/重新分配預設路由。

備註 所有上述選項均可在 Edge 層級使用，並且可以設定為使用針對 BGP 設定啟用的 Edge 覆寫。

OSPF/BGP 重新分配

路由通訊協定 OSPF 和 BGP 可以單獨啟用，且先前僅允許在系統上啟用一個路由通訊協定的型號，已在此版本中移除。此版本也允許重新分配 OSPF 到 BGP 或 BGP 到 OSPF (或兩者同時進行)，且允許其他可能的路由來源，例如透過覆疊、已連線的路由、靜態路由所學習的首碼。

此外，在 3.2 版中， 我們會標準化重新分配行為和較傳統的系列 (與其他路由廠商的類似)。例如，如果有多個路由可用於相同的首碼，則只有該首碼在系統 RIB 中最適用的路由會重新分配到目的地通訊協定，前提是目的地通訊協定中的組態允許為該路由類型進行重新分配。

假設我們要將首碼 192.168.1.0/24 重新分配到 BGP 中。設若首碼 192.168.1.0/24 的路由可在本機取得、可從 OSPF 學習，且能夠以覆疊首碼的形式個別學習。我們進一步假設，在首碼的 OFC 流量順序、路由度量與路由喜好設定之間，OSPF 路由排名高於 (優於) 針對相同首碼而學習的覆疊路由。如此，如果已在 BGP 中開啟 OSPF 重新分配，則會將 OSPF 路由重新分配至 BGP。請注意，由於覆疊學習的首碼並非該首碼在系統 RIB 中的最佳路由，因此，即使已在 BGP 中開啟覆疊首碼的重新分配，也不會將其重新分配至 BGP。

在這類情況下，為了促使將首碼的最佳路由重新分配到指定的目的地通訊協定，使用者可以針對系統中最佳路由的特定路由類型啟用重新分配。

或者，如果使用者針對該首碼傾向於從不同的路由來源重新分配到目的地通訊協定，使用者可以使用管理介面提供的覆疊流量控制設施來控制路由在系統 RIB 中的相對優先順序，或藉由改變路由度量來控制。

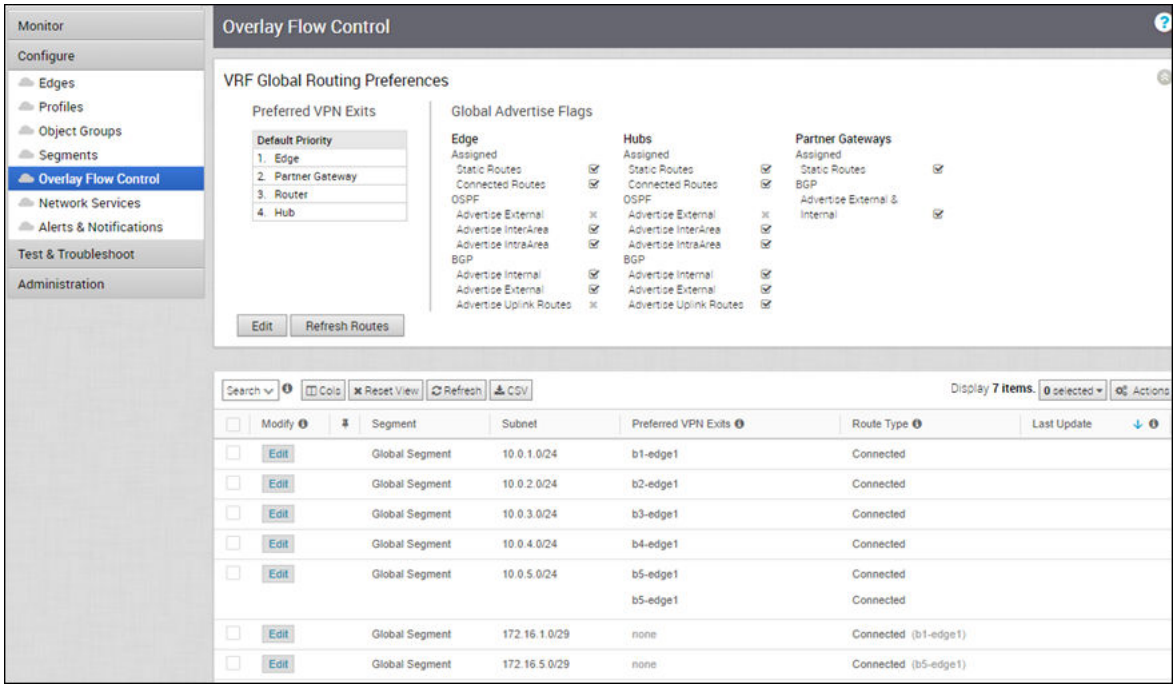
如需詳細資訊，請參閱啟用 OSPF 和啟用 BGP。

覆疊流量控制

覆疊流量控制 (Overlay Flow Control) 頁面會顯示您網路中所有路由的摘要視圖。

您可以檢視和編輯 Edge、中樞以及合作夥伴閘道的全域路由喜好設定和通告動作。

在企業入口網站中，按一下**設定 (Configure)** > **覆疊流量控制 (Overlay Flow Control)**。



覆疊流量控制 (Overlay Flow Control) 頁面會顯示下列詳細資料：

選項	說明
慣用 VPN 結束 (Preferred VPN Exits)	顯示應作為流量路由目的地的優先順序。
全域通告旗標 (Global Advertise Flags)	顯示靜態、已連線、內部、外部和上行路由的通告動作。

- **編輯 (Edit)** – 按一下以更新優先順序和通告動作。請參閱設定全域路由喜好設定。
- **重新整理路由 (Refresh Routes)** – 只有在操作員啟用**分散式成本計算 (Distributed Cost Calculation)** 功能後，才能使用此選項。Orchestrator 依預設會主動參與學習動態路由。Edge 和閘道依賴 Orchestrator 計算初始路由喜好設定，並將資訊傳回給 Edge 和閘道。**分散式成本計算 (Distributed Cost Calculation)** 功能可將路由成本計算散佈至 Edge 和閘道。

  如需**分散式成本計算 (Distributed Cost Calculation)** 的詳細資訊，請參閱《VMware SD-WAN 操作員指南》中的〈**設定分散式成本計算**〉一節，網址為：https://docs.vmware.com/tw/VMware-SD-WAN/index.html。

  備註 若要啟用**分散式成本計算 (Distributed Cost Calculation)** 功能，請洽詢您的支援合作夥伴。如果您可以直接取得 VMware 的支援，請連絡支援團隊。

  按一下**重新整理路由 (Refresh Routes)** 會讓 Edge 和閘道重新計算已知的路由成本，並將其傳送至 Orchestrator。此外，覆疊流量控制中的變更會立即套用至新的和現有的已學習路由。

當您重新整理路由時，客戶企業會對網路產生下列影響：

- 所有本機動態路由將重新整理，並更新這些路由的喜好設定和通告動作。此更新的資訊會向鄰道、Orchestrator 通告，並最終在整個企業中通告。由於這會導致路由資料表中的更新，因此會對所有站台的流量產生短暫影響。
- 使用這些路由的任何現有流量可能會因為路由項目中的變更而受影響。

備註 建議您在維護時段**重新整理路由 (Refresh Routes)**，以盡可能降低對客戶企業的影響。

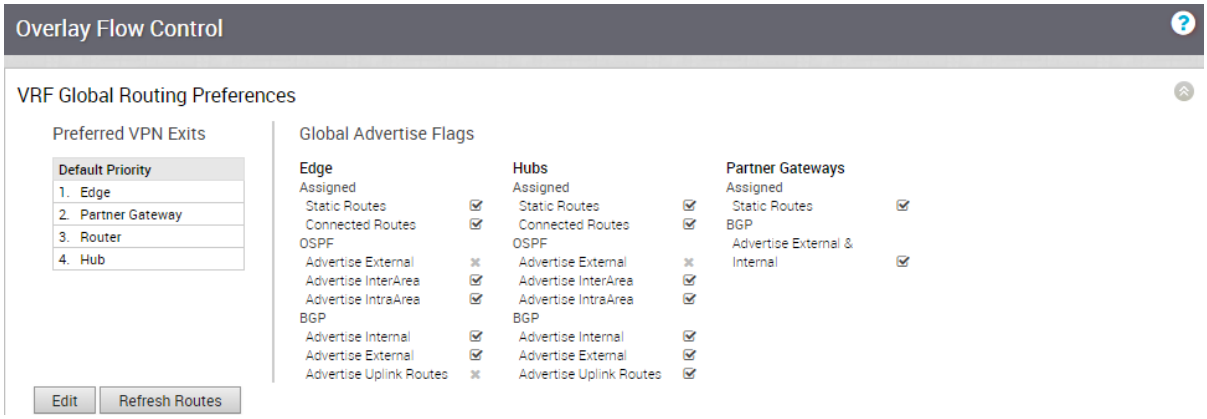
覆疊流量控制 (Overlay Flow Control) 視窗的底部面板會顯示子網路。您可以排列子網路慣用目的地的優先順序，並釘選或取消釘選項已學習路由的喜好設定。如需詳細資訊，請參閱設定子網路。

設定全域路由喜好設定

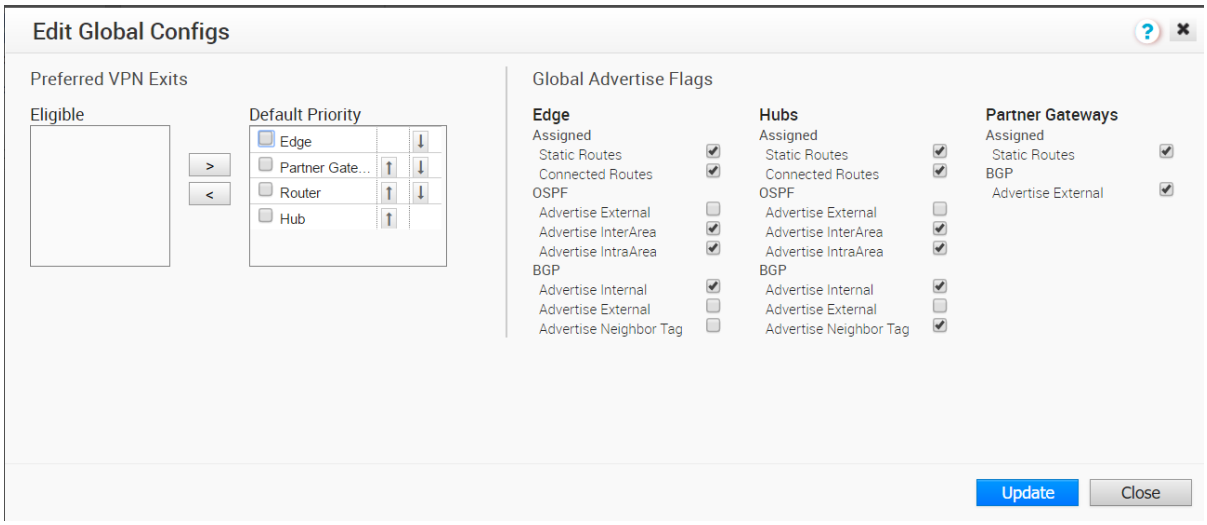
在**覆疊流量控制 (Overlay Flow Control)** 視窗中，您可以編輯全域路由喜好設定、通告動作，以及修改流量應路由之目的地的優先順序。

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **覆疊流量控制 (Overlay Flow Control)**。



2 在**覆疊流量控制 (Overlay Flow Control)** 頁面中，按一下**編輯 (Edit)**，**編輯全域組態 (Edit Global Configs)** 視窗即會顯示。



3 您可以更新下列設定：

a 在**慣用 VPN 結束 (Preferred VPN Exits)** 區域中，按一下**向上鍵 (UP)** 和**向下鍵 (DOWN)** 箭頭以修改優先順序。

b 在**全域通告旗標 (Global Advertise Flags)** 區域中，選取相關核取方塊以修改路由的通告動作。

c 按一下**更新 (Update)** 以儲存變更。

結果

更新的設定會顯示在**覆疊流量控制 (Overlay Flow Control)** 頁面中。

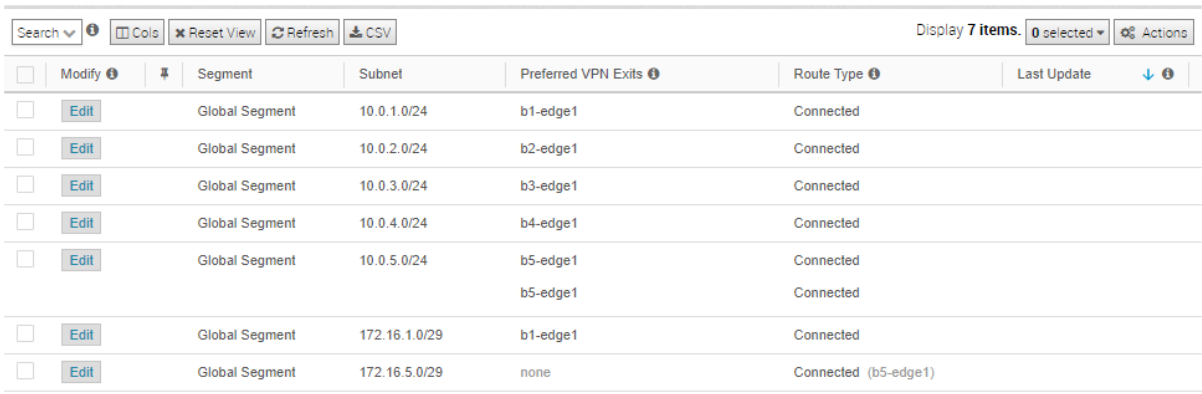
設定子網路

在**覆疊流量控制 (Overlay Flow Control)** 視窗中，您可以更新子網路中所學習路由的目的地優先順序。

程序

1 在企業入口網站中，按一下**設定 (Configure)** > **覆疊流量控制 (Overlay Flow Control)**。

2 **覆疊流量控制 (Overlay Flow Control)** 視窗的底部面板會顯示具有下列詳細資料的子網路：



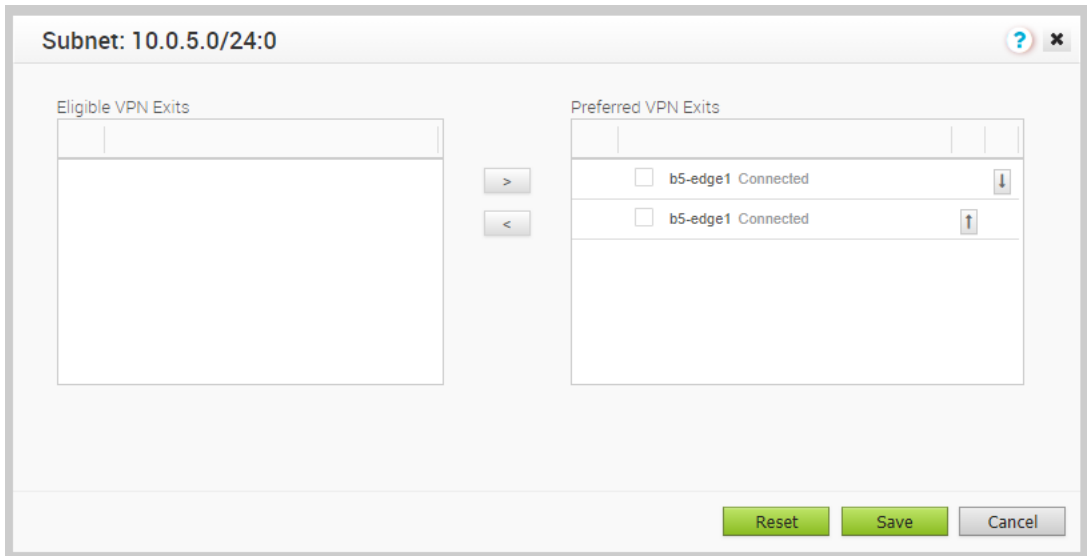
選項	說明
修改 (Modify)	顯示用於編輯子網路的選項。選項會顯示上標數字，表示已學習對應路由的 Edge 和閘道數目。
區段 (Segment)	區段名稱。
子網路 (Subnet)	路由對應的網路，以及學習該路由的 Edge 清單。
慣用 VPN 結束 (Preferred VPN Exits)	其他分支可透過其存取子網路的路由。
路由類型 (Route Type)	顯示路由的類型，可以是下列其中一種類型：[靜態 (Static)]、[已連線 (Connected)] 或 [已學習 (Learned)]。
上次更新時間 (Last Update)	慣用的 VPN 結束的上次更新日期和時間。
建立於 (Created On)	建立此路由的日期和時間。

選取一或多個子網路，然後按一下**動作 (Actions)**，以執行下列活動：

- **編輯子網路 (Edit Subnet)** – 修改慣用的目的地，並排列其優先順序。
- **釘選學習的路由喜好設定 (Pin Learned Route Preference)** – 釘選所選已學習路由的喜好設定。
- **重設學習的路由喜好設定 (Reset Learned Route Preference)** – 將所選已學習路由的喜好設定重設為預設設定。
- **刪除學習的路由 (Delete Learned Routes)** - 刪除學習的路由。該選項不會刪除已連線的路由、靜態路由、[覆疊流量控制 (Overlay Flow Control)] 中的路由以及 Edge 路由表中的路由，而是用來清理失效路由。僅當關閉**設定分散式成本計算 (Configure Distributed Cost Calculation)** 時，才可使用該選項。

3 按一下子網路的**編輯 (Edit)** 選項，以修改慣用目的地的優先順序。

a 在**子網路 (Subnet)** 視窗中，您可以將目的地從**合格的 VPN 結束 (Eligible VPN Exits)** 移至**慣用 VPN 結束 (Preferred VPN Exits)**，反之亦然。



b 在**慣用 VPN 結束 (Preferred VPN Exits)** 面板中，按一下**向上鍵 (UP)** 和**向下鍵 (DOWN)** 箭頭以變更優先順序，然後按一下**儲存 (Save)**。

c 當有固定的路由可供使用時，您可以重設子網路的成本計算。按一下**重設 (Reset)** 讓 Orchestrator 清除固定的路由、根據原則重新計算所選子網路的成本，然後將結果傳送到 Edge 和閘道。

備註 僅在啟用了分散式成本計算時，才能使用**重設 (Reset)** 選項。

如需 [分散式成本計算 (Distributed Cost Calculation)] 的詳細資訊，請參閱《VMware SD-WAN 操作員指南》中的〈**設定分散式成本計算**〉一節，網址為：https://docs.vmware.com/tw/VMware-SD-WAN/index.html。

設定警示

19

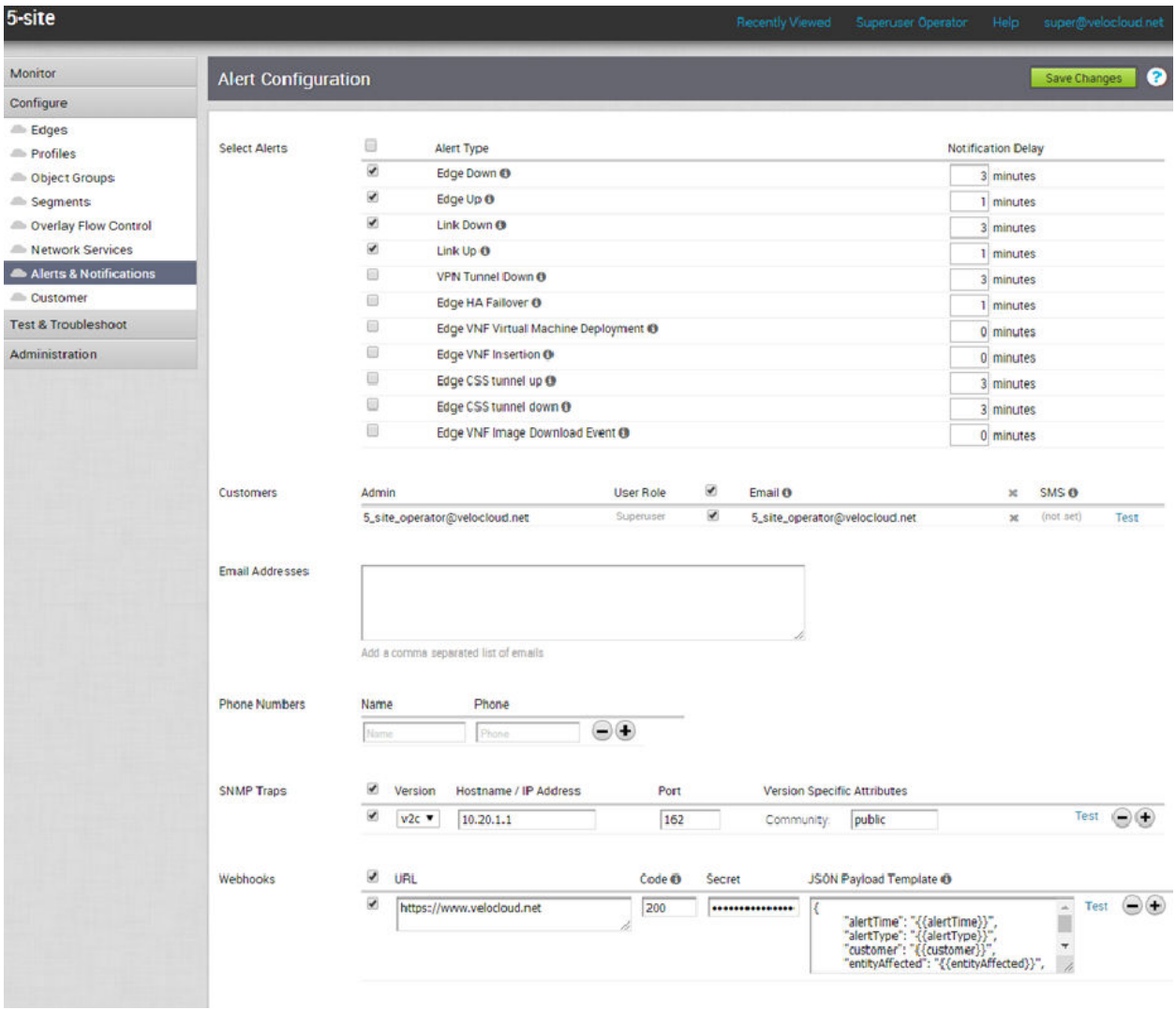
SD-WAN Orchestrator 可讓您設定警示，以在發生事件時通知企業管理員或其他支援使用者。

備註 如果您以具有客戶支援權限的使用者身分登入，您可以檢視警示和其他物件，但無法進行設定。

在企業入口網站中，按一下**設定 (Configure)** > **警示和通知 (Alerts & Notifications)** 以設定警示。

選取需要傳送警示的事件，然後在**選取警示 (Select Alerts)** 下輸入通知延遲時間 (以分鐘為單位)。

您可以使用 `EDIT_ALERT_CONFIGURATION` 事件記錄對企業警示組態所做的變更。



在**客戶 (Customers)** 下方會顯示現有管理員使用者的連絡人詳細資料。您可以選取電子郵件和 SMS 的核取方塊，以將警示傳送給對應的使用者。

SNMP 設陷

簡易網路管理通訊協定 (SNMP) 設陷是傳送至 SNMP 代理程式以指出有事件發生的通知。SD-WAN Orchestrator 會傳送與現有警示 (例如 Edge 關閉和 Edge 啟動) 對應的 SNMP 設陷。您可以選取 SNMP 版本，並在 **SNMP 設陷 (SNMP Traps)** 下方輸入對應的詳細資料。

備註 目前，SNMP v3 設陷僅支援 SHA-1 和 AES-128 演算法。

Webhook

Webhook 會將資料傳送至其他應用程式，由特定警示使用 HTTP POST 觸發。每當發生警示時，來源就會將 HTTP 要求傳送至針對 Webhook 設定的目標應用程式。

SD-WAN Orchestrator 支援在發生事件時透過 HTTP POST 自動將訊息傳送至目標應用程式的 Webhook。您可以在企業入口網站中設定目標 URL，並自動執行動作以回應由 SD-WAN Orchestrator 觸發的警示。Webhook 收件者必須支援 HTTPS，並且必須具有有效的憑證，以確保潛在敏感警示裝載的隱私。如此也可防止裝載遭到篡改。

設定 Webhook

在**警示組態 (Alert Configuration)** 視窗中，您可以在 **Webhook** 下方輸入下列詳細資料。

選項	說明
URL	輸入有效的 HTTPS URL。這會作為 Webhook 的目標應用程式。
代碼 (Code)	為每個 Webhook 收件者輸入預期的 HTTP 回應狀態碼。依預設，SD-WAN Orchestrator 預期 Webhook 收件者應以狀態碼 HTTP 200 回應 HTTP POST 要求。 SD-WAN Orchestrator 從收件者伺服器或 Proxy 伺服器接收到非預期的狀態碼時，它會將警示傳遞視為失敗，並產生一個 `ALERT_DELIVERY_FAILED` 客戶事件。此事件有助於識別 Webhook 收件者伺服器是否無法如預期般運作。

選項	說明
密碼 (Secret)	為每個已設定的 Webhook 收件者指定密碼 Token，用以計算傳送給對應收件者的每個 Webhook 要求的 HMAC。HMAC 會連同用來識別簽章演算法和時間戳記的版本參數內嵌於 `X-Webhook-Signature` HTTP 標頭中。 `X-Webhook-Signature: v=<signature-version>&t=<timestamp>&s=<hmac>` 收件者需要以下列方式解譯元件： ■ `v`：用來產生簽章的演算法版本。唯一支援的值為 **1**。 ■ `t`：毫秒精確度 epoch 時間戳記，對應於發出要求的時間。 ■ `s`：由 SD-WAN Orchestrator 計算的 HMAC。HMAC 的計算方式如下：`HMAC-SHA256(request-body + '.' + timestamp, secret)`。 用來計算 HMAC 的訊息由要求本文、單一期間，以及簽章標頭中顯示的時間戳記參數值串連所組成。用來產生程式碼的特定 HMAC 演算法為 HMAC-SHA256。 收到 Webhook 要求後，接聽伺服器可根據相同演算法來計算要求本身的 HMAC-SHA256 簽章，並將新計算的簽章與 SD-WAN Orchestrator 所產生的簽章進行比較，以驗證要求的真實性。
JSON 裝載範本 (JSON Payload Template)	這是必填欄位。 SD-WAN Orchestrator 可透過包含在傳出 HTTP POST 要求本文中的 JSON 裝載，將警示通知傳送給每個 Webhook 收件者。 SD-WAN Orchestrator 會動態產生裝載內容，因為通知是藉由執行變數插補來傳送的。使用者設定的裝載範本中支援的預留位置變數會取代為警示的特定值。 Webhook 裝載範本支援下列預留位置變數： ■ **alertTime**：觸發警示的時間。 ■ **alertType**：警示的類型，例如 EDGE_DOWN、LINK_UP、VNF_VM_DEPLOYED。 ■ **customer**：傳送通知的目標客戶名稱。 ■ **entityAffected**：套用警示的實體名稱，例如 Edge 或連結或 VNF。 ■ **lastContact**：受影響 Edge 最近與 SD-WAN Orchestrator 通訊的時間。這僅適用於 Edge 警示。 ■ **message**：說明觸發警示之事件的簡短訊息。 ■ **VCO**：從中傳送通知之 SD-WAN Orchestrator 的主機名稱或公用 IP。

下列範例顯示範例 JSON 裝載範本：

```
{
     "alertTime": "{{alertTime}}",
     "alertType": "{{alertType}}",
     "customer": "{{customer}}",
     "entityAffected": "{{entityAffected}}",
     "lastContact": "{{lastContact}}",
```

```
      "message": "{{message}}",
      "vco": "{{vco}}"
}
```

您可以按一下加號 (+) 圖示以新增更多目標 URL 和對應的詳細資料。

按一下**測試 (Test)** 以檢查 Webhook 警示。

每當觸發警示時，警示訊息就會連同相關資訊傳送至目標 URL。

測試和疑難排解

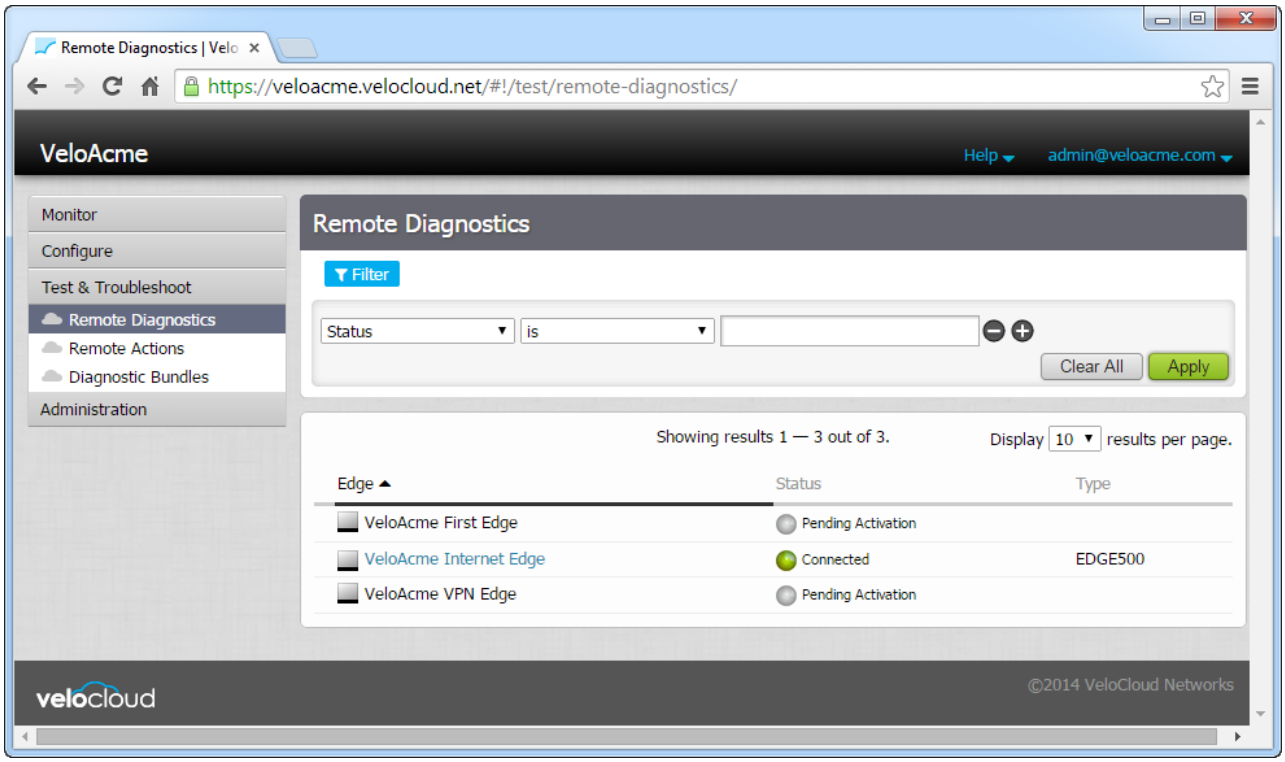
20

SD-WAN Orchestrator 的測試和疑難排解功能有相關工具可測試 VMware 服務的狀態、執行 Edge 動作，以及收集個別 Edge 的封包擷取資訊。

您可以在導覽面板的**測試和疑難排解 (Test & Troubleshoot)** 區段下，依照下列方式存取這些功能：

- 遠端診斷
- 遠端動作
- 診斷服務包

按一下**測試和疑難排解 (Test & Troubleshoot)** 時，會顯示**遠端診斷 (Remote Diagnostics)** 畫面。它會在畫面底部的 **Edge** 資料行中顯示您所定義的所有 Edge。



您可以使用**篩選器 (Filter)**，根據連線狀態、名稱、IP 位址、序號、軟體版本和軟體組建來尋找 Edge。但您必須先從 **Edge** 資料行中選取 Edge，才能執行 [測試和疑難排解 (Test & Troubleshoot)] 選項。請參閱以下幾節，以進一步瞭解導覽面板中的每個 [測試和疑難排解 (Test & Troubleshoot)] 選項 (遠端診斷、遠端動作和診斷服務包)。

本章節討論下列主題：

遠端診斷

您可以在 Edge 上執行測試以取得診斷資訊，方法是按一下**測試和疑難排解 (Test & Troubleshoot)** 下的**遠端診斷 (Remote Diagnostics)**。

若要在單一 Edge 上執行診斷測試：

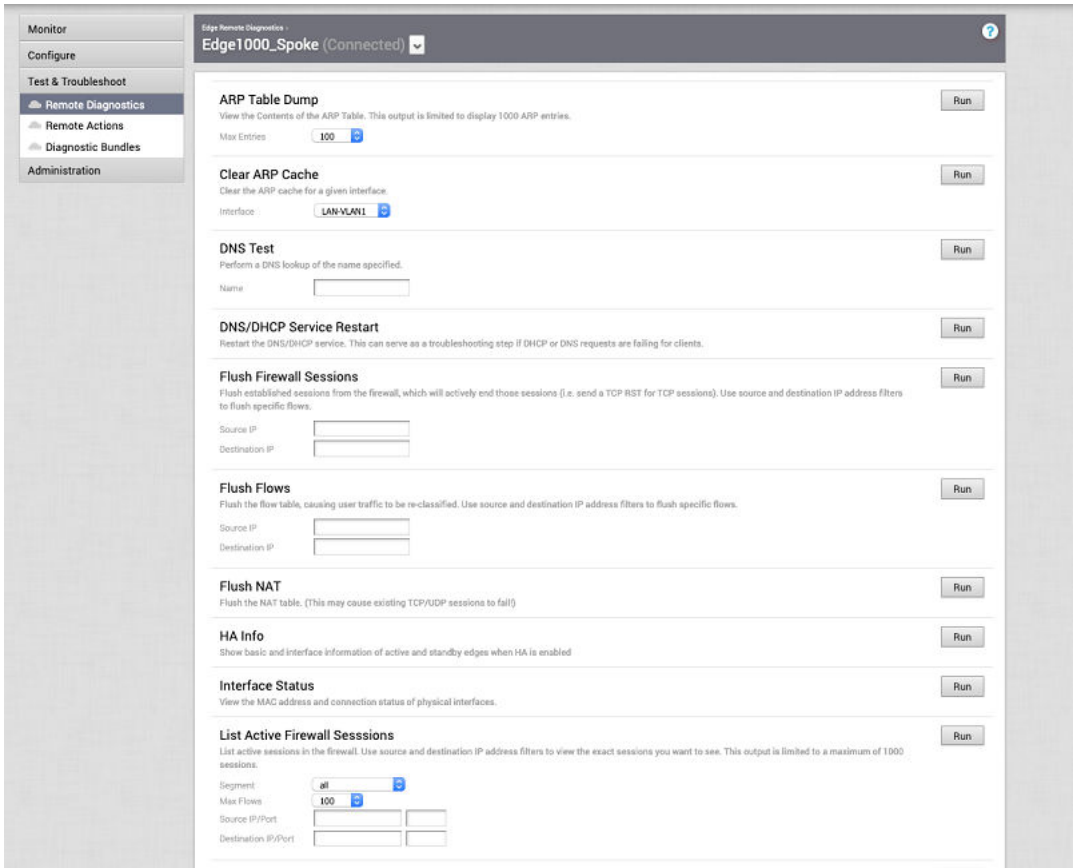
程序

1 在企業入口網站中，按一下**測試和疑難排解 (Test & Troubleshoot)**，然後按一下**遠端診斷 (Remote Diagnostics)**。

2 如有必要，請使用**篩選器 (Filter)** 搜尋 Edge，然後按一下**套用 (Apply)**。

3 選取已連線的 Edge。

此時會顯示**遠端診斷 (Remote Diagnostics)** 畫面，其中顯示所有您可在 Edge 上執行的可能測試。



4 選擇診斷測試並提供必要的詳細資料，然後按一下**執行 (Run)**。

遠端診斷測試

說明您可以在 Edge 上執行以取得診斷資訊的所有可行遠端診斷測試。診斷資訊包含用於分析的 Edge 特定記錄。

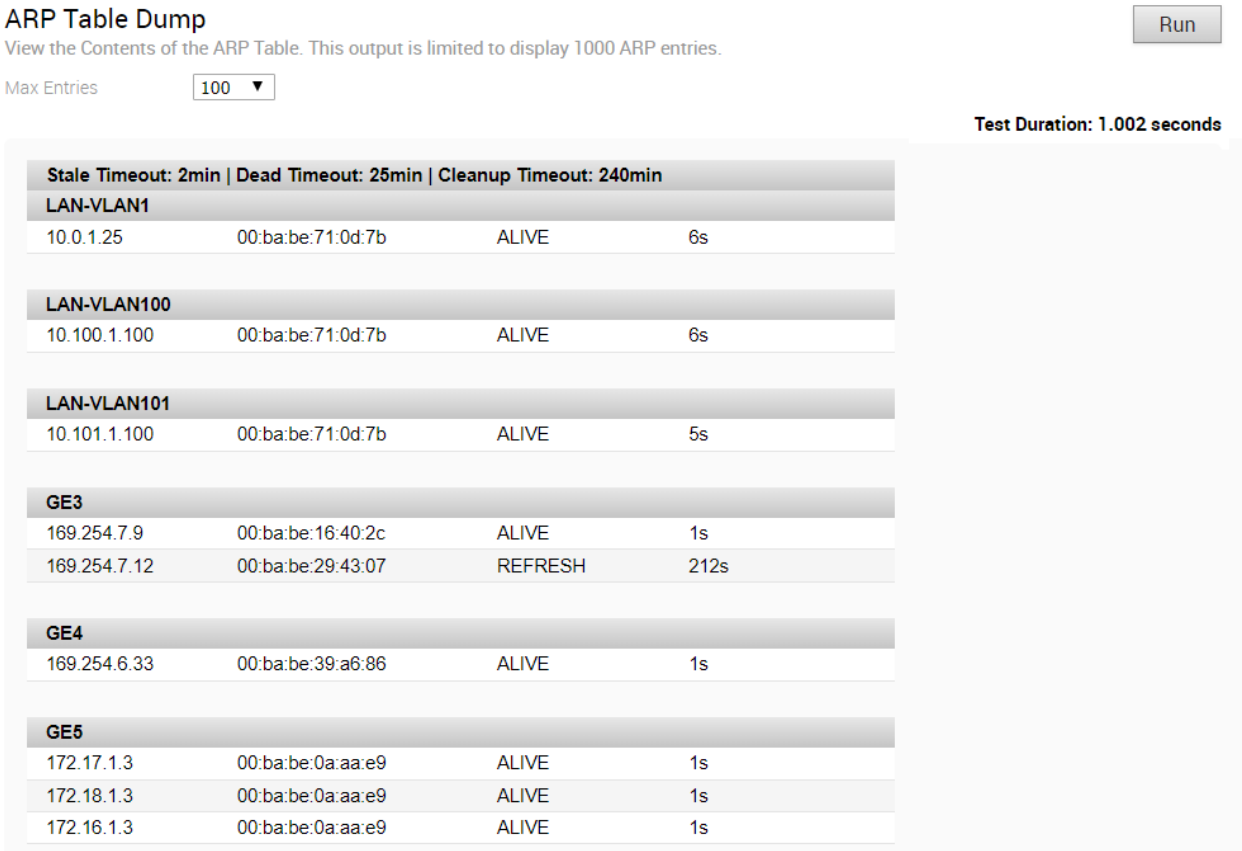
支援的遠端診斷測試如下：

- ARP 資料表傾印
- 清除 ARP 快取
- DNS 測試
- DNS/DHCP 服務重新啟動
- 排清防火牆工作階段
- 排清流量
- 排清 NAT
- 閘道
- 介面狀態
- 列出作用中防火牆工作階段
- 列出作用中流量
- 列出用戶端
- 列出路徑
- Edge 的 MIB
- NAT 資料表傾印
- NTP 傾印
- Ping 測試
- 路由表傾印
- 系統健全狀況
- 路徑追蹤
- 疑難排解 BGP - 列出 BGP 重新分配的路由
- 疑難排解 BGP - 列出 BGP 路由
- 疑難排解 BGP - 列出每個首碼的路由
- 疑難排解 BGP - 顯示 BGP 芳鄰通告的路由
- 疑難排解 BGP - 顯示 BGP 芳鄰學習的路由
- 疑難排解 BGP - 顯示 BGP 芳鄰已接收的路由
- 疑難排解 BGP - 顯示每個首碼的 BGP 路由

- 疑難排解 BGP - 顯示 BGP 摘要
- 疑難排解 BGP - 顯示 BGP 資料表
- 疑難排解 OSPF - 列出 OSPF 重新分配的路由
- 疑難排解 OSPF - 列出 OSPF 路由
- 疑難排解 OSPF - 顯示 OSPF 資料庫
- 疑難排解 OSPF - 顯示 E1 自我產生路由的 OSPF 資料庫
- 疑難排解 OSPF - 顯示 OSPF 芳鄰
- 疑難排解 OSPF - 顯示 OSPF 路由表
- 疑難排解 OSPF - 顯示 OSPF 設定
- VPN 測試
- WAN 連結頻寬測試

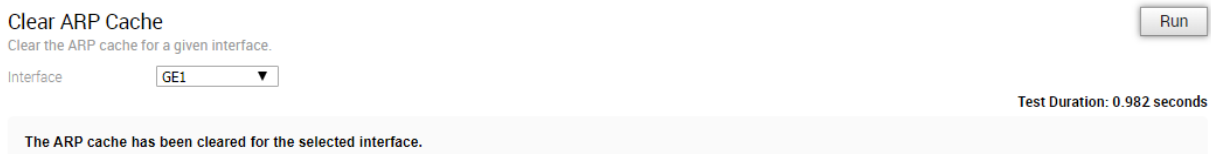
ARP 資料表傾印

執行此測試，以檢視 ARP 資料表的內容。輸出最多可顯示 1000 個 ARP 項目。



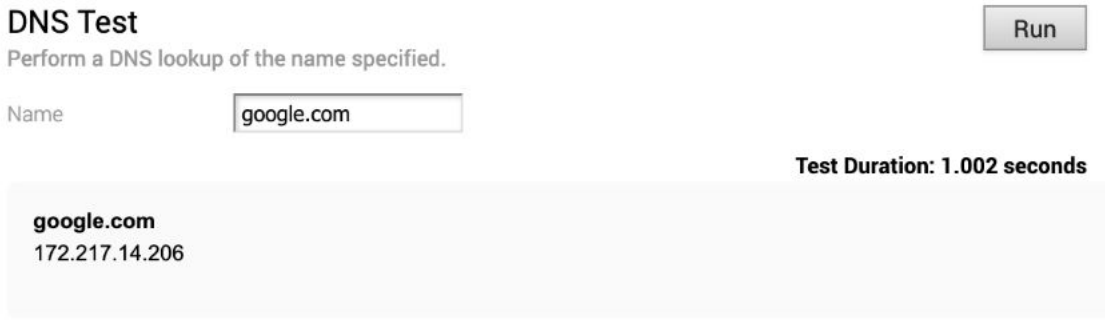
清除 ARP 快取

執行此測試以清除指定介面的 ARP 快取項目。



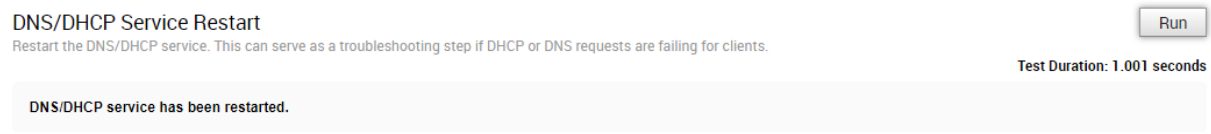
DNS 測試

執行此測試，以執行指定網域名稱的 DNS 查詢。



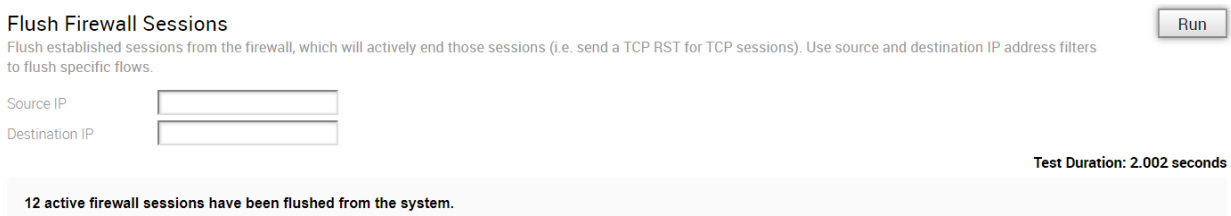
DNS/DHCP 服務重新啟動

執行此測試以重新啟動 DNS/DHCP 服務。如果用戶端的 DHCP 或 DNS 要求失敗，則可將此作業作為疑難排解步驟。



排清防火牆工作階段

執行此測試以重設防火牆中已建立的工作階段。在 Edge 上執行此測試不僅會排清防火牆工作階段，而且會主動為 TCP 型工作階段傳送 TCP RST。

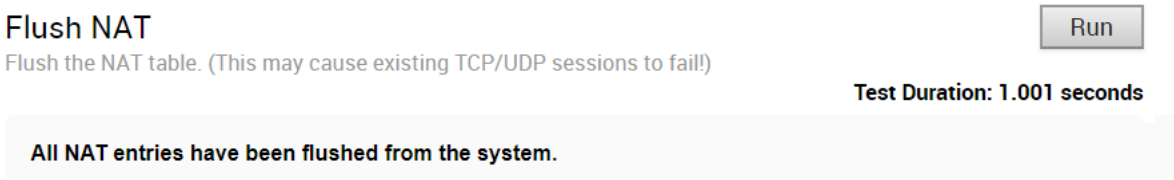


排清流量

執行此測試以排清流量資料表，進而將使用者流量重新分類。請使用來源和目的地 IP 位址篩選器來排清特定流量。

排清 NAT

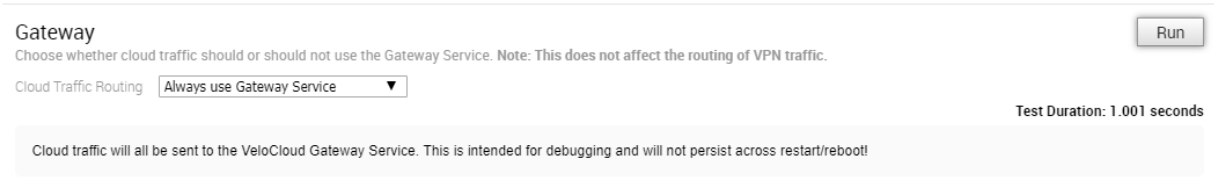
執行此測試以排清 NAT 資料表。



閘道

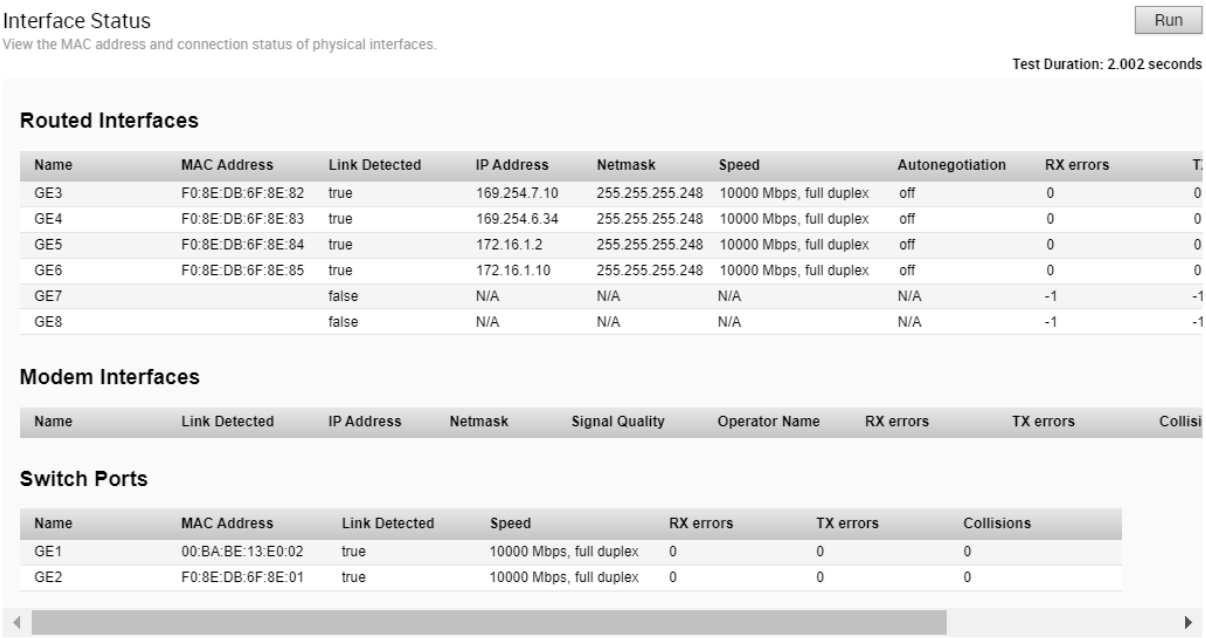
選擇雲端流量是否應使用閘道服務，藉以執行此測試。

備註 這並不會影響 VPN 流量的路由。



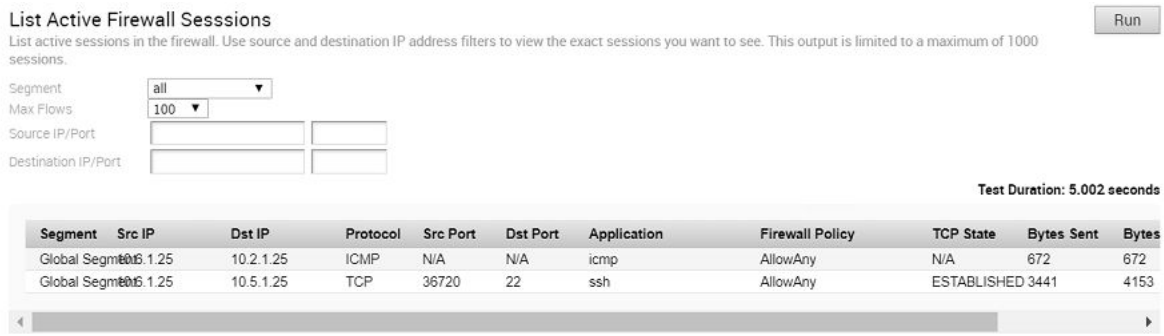
介面狀態

執行此測試，以檢視實體介面的 MAC 位址和連線狀態。



列出作用中防火牆工作階段

執行此測試，以檢視作用中防火牆工作階段的目前狀態 (最多為 1000 個工作階段)。您可以使用篩選器來限制傳回的工作階段數：來源和目的地 IP 位址、來源和目的地連接埠以及區段。



備註 您無法查看遭拒絕的工作階段，因為其並非作用中的工作階段。若要疑難排解這些工作階段，您將需要檢查防火牆記錄。

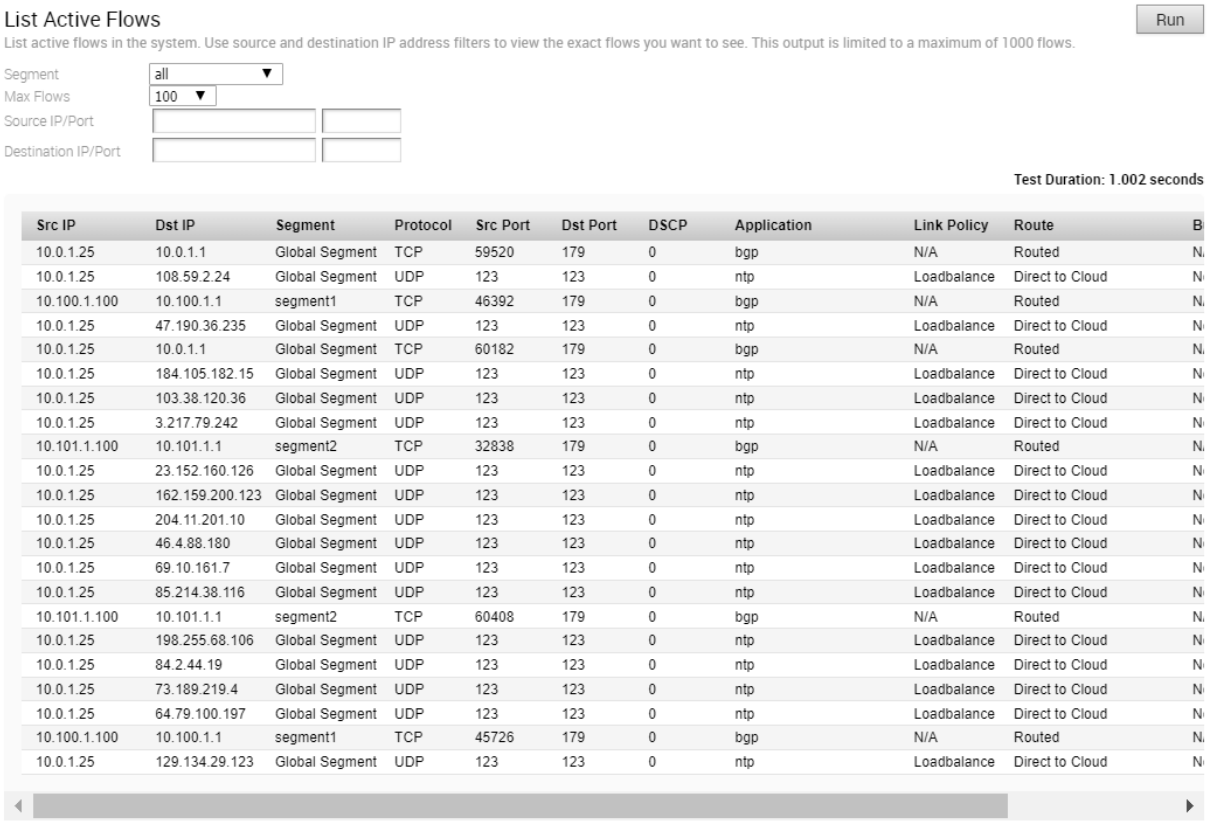
遠端診斷輸出會顯示下列資訊：[區段名稱 (Segment name)]、[來源 IP (Source IP)]、[來源連接埠 (Source Port)]、[目的地 IP (Destination IP)]、[目的地連接埠 (Destination Port)]、[通訊協定 (Protocol)]、[應用程式 (Application)]、[防火牆原則 (Firewall Policy)]、任何流量的目前 TCP 狀態、[已接收/已傳送的位元組 (Bytes Received/Sent)] 以及 [持續時間 (Duration)]。有 11 個不同的 TCP 狀態，如 RFC 793 中所定義：

- LISTEN - 表示正在等待來自任何遠端 TCP 和連接埠的連線要求。(此狀態不會顯示在遠端診斷輸出中)。
- SYN-SENT - 表示在已傳送連線要求後，等待相符的連線要求。

- SYN-RECEIVED - 表示在接收到及傳送連線要求後，等待確認連線要求確認。
- ESTABLISHED - 表示開放式連線，接收到的資料可以傳遞給使用者。連線的資料傳輸階段狀態正常。
- FIN-WAIT-1 - 表示正在等待遠端 TCP 的連線終止要求，或確認先前已傳送的連線終止要求。
- FIN-WAIT-2 - 表示正在等待來自遠端 TCP 的連線終止要求。
- CLOSE-WAIT - 表示正在等待來自本機使用者的連線終止要求。
- CLOSING - 表示正在等待來自遠端 TCP 的連線終止要求確認。
- LAST-ACK - 表示正在等待確認先前已傳送至遠端 TCP 的連線終止要求 (包括確認其連線終止要求的確認)。
- TIME-WAIT - 表示正在等待經過足夠的時間，以確保遠端 TCP 接收到對其連線終止要求的確認。
- CLOSED - 表示根本沒有連線狀態。

列出作用中流量

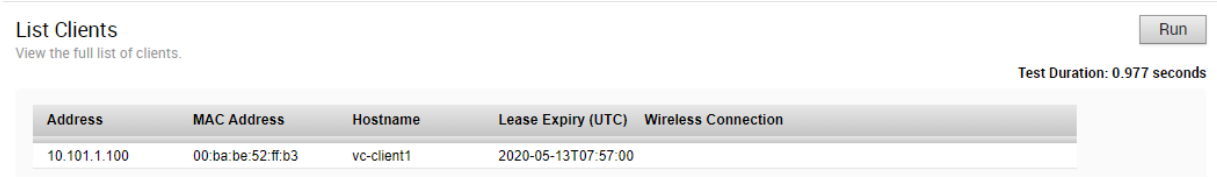
執行此測試以列出系統中的作用中流量。請使用來源和目的地 IP 位址篩選器，檢視您要查看的確切流量。此輸出限定為最多 1000 個流量。



Src IP	Dst IP	Segment	Protocol	Src Port	Dst Port	DSCP	Application	Link Policy	Route	B
10.0.1.25	10.0.1.1	Global Segment	TCP	59520	179	0	bgp	N/A	Routed	N
10.0.1.25	108.59.2.24	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.100.1.100	10.100.1.1	segment1	TCP	46392	179	0	bgp	N/A	Routed	N
10.0.1.25	47.190.36.235	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	10.0.1.1	Global Segment	TCP	60182	179	0	bgp	N/A	Routed	N
10.0.1.25	184.105.182.15	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	103.38.120.36	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	3.217.79.242	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.101.1.100	10.101.1.1	segment2	TCP	32838	179	0	bgp	N/A	Routed	N
10.0.1.25	23.152.160.126	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	162.159.200.123	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	204.11.201.10	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	46.4.88.180	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	69.10.161.7	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	85.214.38.116	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.101.1.100	10.101.1.1	segment2	TCP	60408	179	0	bgp	N/A	Routed	N
10.0.1.25	198.255.68.106	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	84.2.44.19	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	73.189.219.4	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	64.79.100.197	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.100.1.100	10.100.1.1	segment1	TCP	45726	179	0	bgp	N/A	Routed	N
10.0.1.25	129.134.29.123	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N

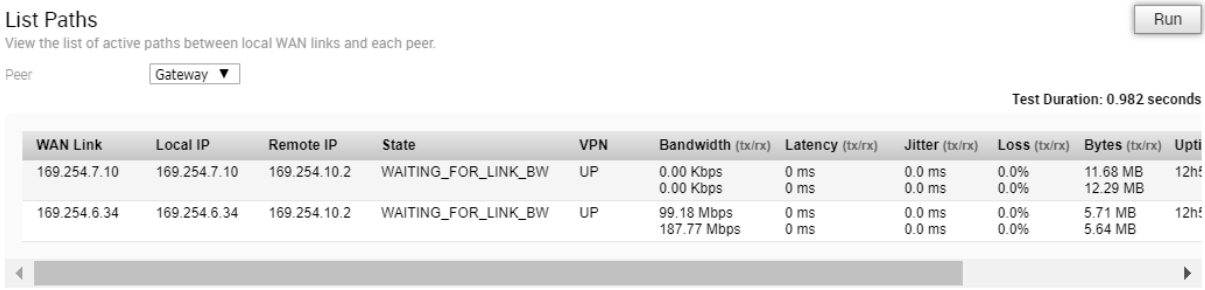
列出用戶端

執行此測試，以檢視完整用戶端清單。



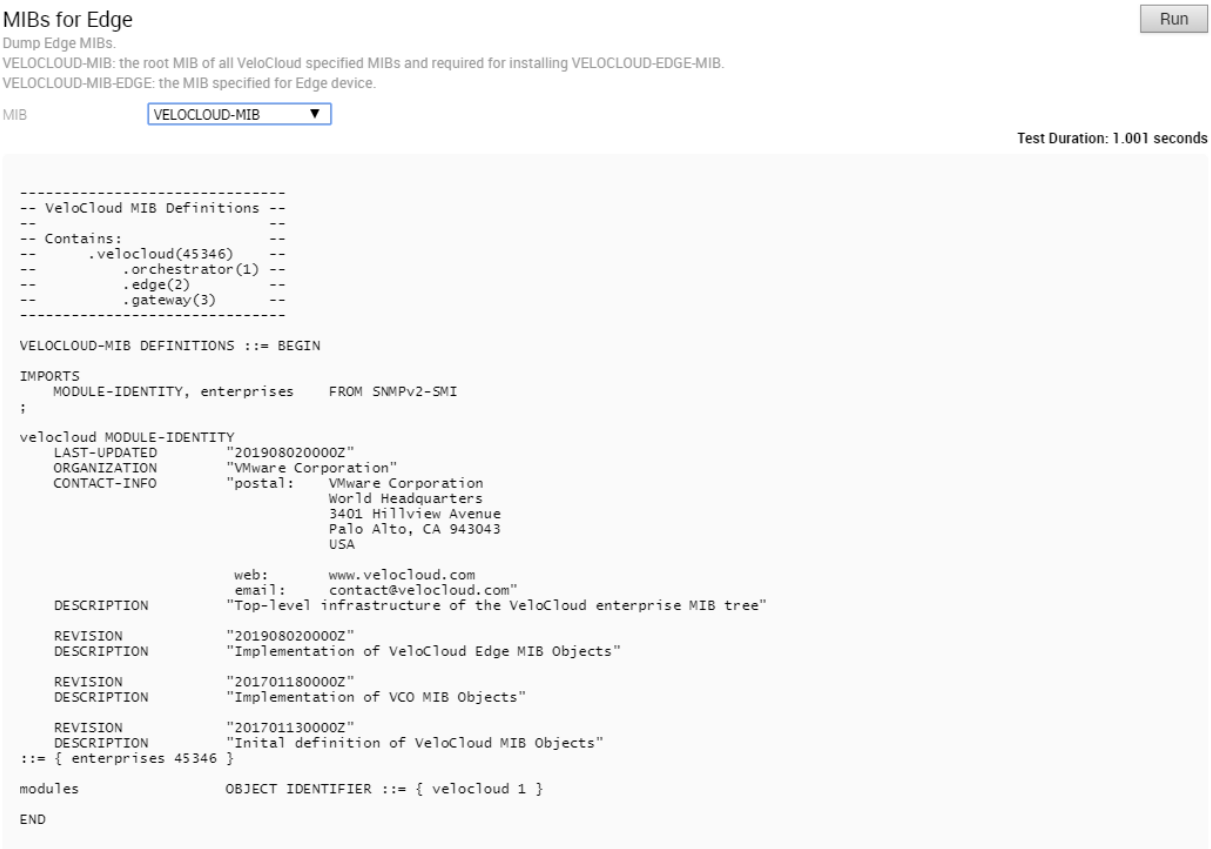
列出路徑

執行此測試，以檢視本機 WAN 連結與每個對等之間的作用中路徑清單。



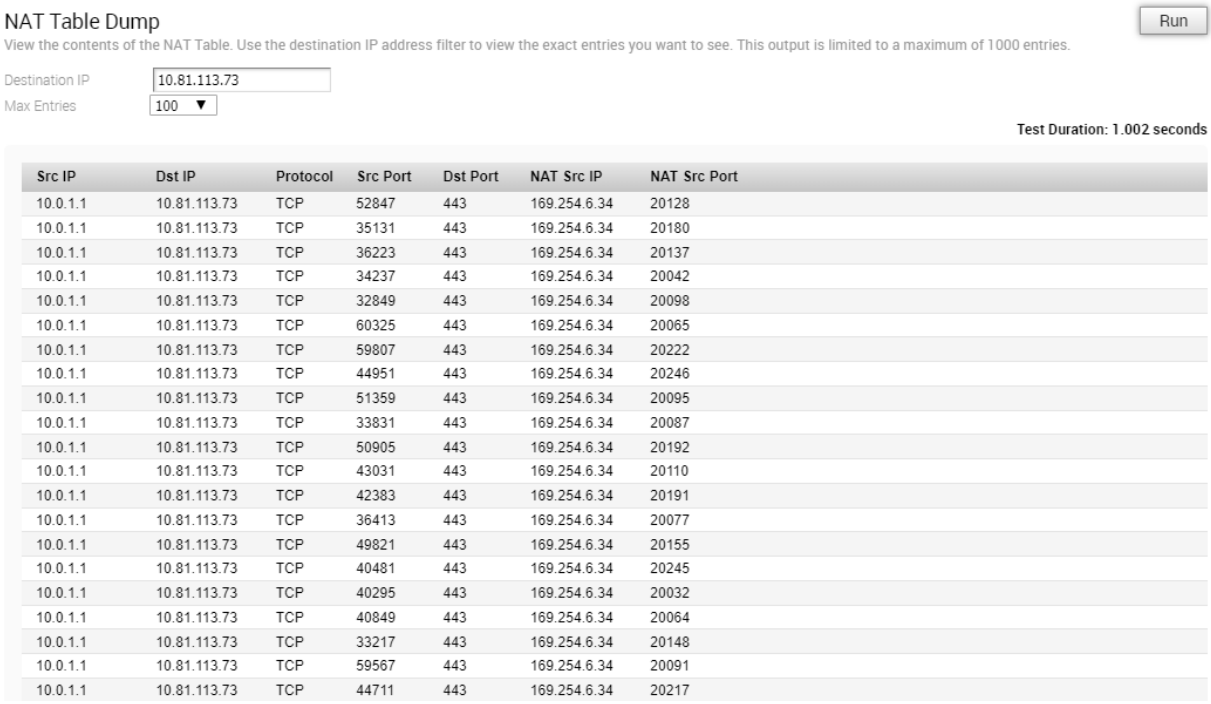
Edge 的 MIB

執行此測試以傾印 Edge MIB。



NAT 資料表傾印

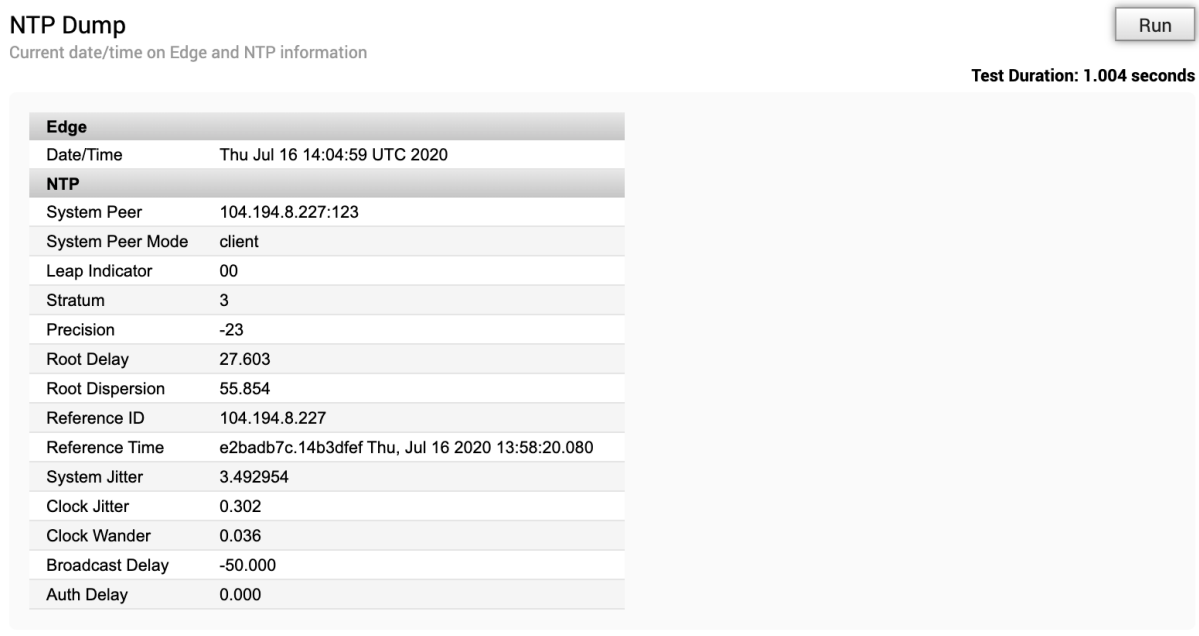
執行此測試，以檢視 NAT 資料表的內容。請使用目的地 IP 位址篩選器，檢視您要檢視的確切項目。此輸出限定為最多 1000 個項目。



Src IP	Dst IP	Protocol	Src Port	Dst Port	NAT Src IP	NAT Src Port
10.0.1.1	10.81.113.73	TCP	52847	443	169.254.6.34	20128
10.0.1.1	10.81.113.73	TCP	35131	443	169.254.6.34	20180
10.0.1.1	10.81.113.73	TCP	36223	443	169.254.6.34	20137
10.0.1.1	10.81.113.73	TCP	34237	443	169.254.6.34	20042
10.0.1.1	10.81.113.73	TCP	32849	443	169.254.6.34	20098
10.0.1.1	10.81.113.73	TCP	60325	443	169.254.6.34	20065
10.0.1.1	10.81.113.73	TCP	59807	443	169.254.6.34	20222
10.0.1.1	10.81.113.73	TCP	44951	443	169.254.6.34	20246
10.0.1.1	10.81.113.73	TCP	51359	443	169.254.6.34	20095
10.0.1.1	10.81.113.73	TCP	33831	443	169.254.6.34	20087
10.0.1.1	10.81.113.73	TCP	50905	443	169.254.6.34	20192
10.0.1.1	10.81.113.73	TCP	43031	443	169.254.6.34	20110
10.0.1.1	10.81.113.73	TCP	42383	443	169.254.6.34	20191
10.0.1.1	10.81.113.73	TCP	36413	443	169.254.6.34	20077
10.0.1.1	10.81.113.73	TCP	49821	443	169.254.6.34	20155
10.0.1.1	10.81.113.73	TCP	40481	443	169.254.6.34	20245
10.0.1.1	10.81.113.73	TCP	40295	443	169.254.6.34	20032
10.0.1.1	10.81.113.73	TCP	40849	443	169.254.6.34	20064
10.0.1.1	10.81.113.73	TCP	33217	443	169.254.6.34	20148
10.0.1.1	10.81.113.73	TCP	59567	443	169.254.6.34	20091
10.0.1.1	10.81.113.73	TCP	44711	443	169.254.6.34	20217

NTP 傾印

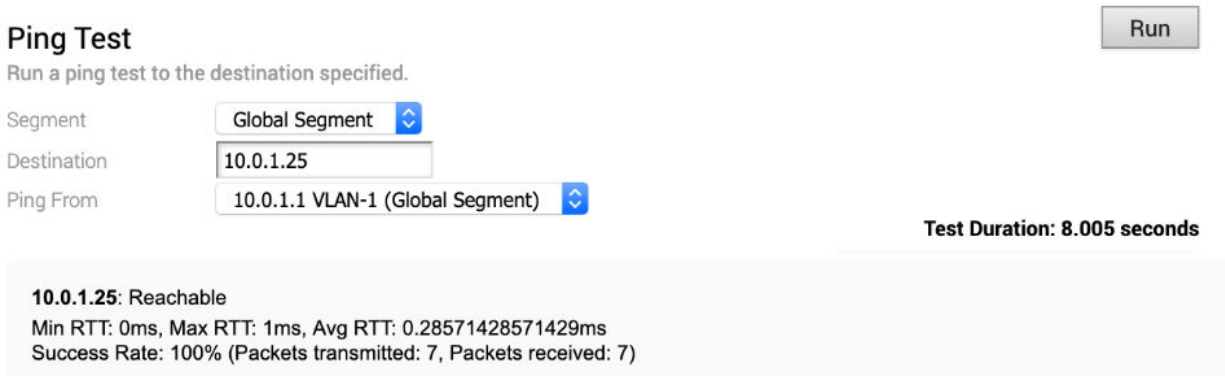
執行此測試，以顯示 Edge 和 NTP 資訊上目前的日期和時間。



Edge	
Date/Time	Thu Jul 16 14:04:59 UTC 2020
NTP	
System Peer	104.194.8.227:123
System Peer Mode	client
Leap Indicator	00
Stratum	3
Precision	-23
Root Delay	27.603
Root Dispersion	55.854
Reference ID	104.194.8.227
Reference Time	e2badb7c.14b3dfef Thu, Jul 16 2020 13:58:20.080
System Jitter	3.492954
Clock Jitter	0.302
Clock Wander	0.036
Broadcast Delay	-50.000
Auth Delay	0.000

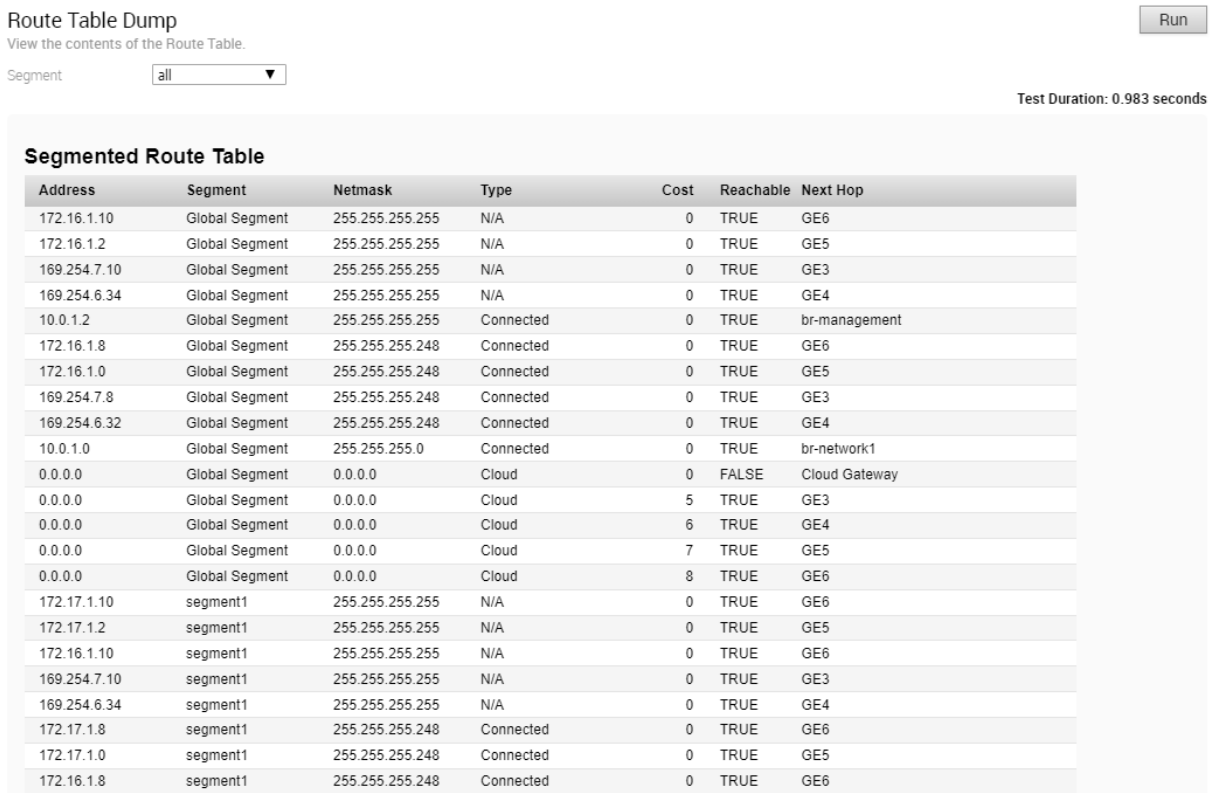
Ping 測試

對指定的目的地執行 Ping 測試。



路由表傾印

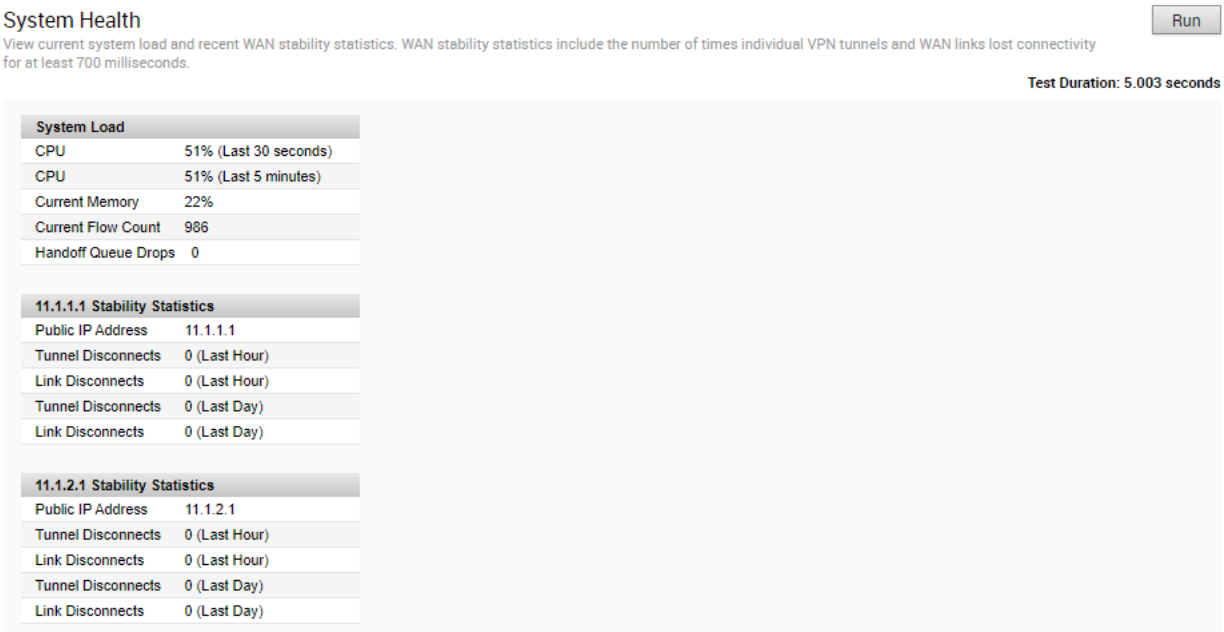
執行此測試，以檢視路由表的內容。



Address	Segment	Netmask	Type	Cost	Reachable	Next Hop
172.16.1.10	Global Segment	255.255.255.255	N/A	0	TRUE	GE6
172.16.1.2	Global Segment	255.255.255.255	N/A	0	TRUE	GE5
169.254.7.10	Global Segment	255.255.255.255	N/A	0	TRUE	GE3
169.254.6.34	Global Segment	255.255.255.255	N/A	0	TRUE	GE4
10.0.1.2	Global Segment	255.255.255.255	Connected	0	TRUE	br-management
172.16.1.8	Global Segment	255.255.255.248	Connected	0	TRUE	GE6
172.16.1.0	Global Segment	255.255.255.248	Connected	0	TRUE	GE5
169.254.7.8	Global Segment	255.255.255.248	Connected	0	TRUE	GE3
169.254.6.32	Global Segment	255.255.255.248	Connected	0	TRUE	GE4
10.0.1.0	Global Segment	255.255.255.0	Connected	0	TRUE	br-network1
0.0.0.0	Global Segment	0.0.0.0	Cloud	0	FALSE	Cloud Gateway
0.0.0.0	Global Segment	0.0.0.0	Cloud	5	TRUE	GE3
0.0.0.0	Global Segment	0.0.0.0	Cloud	6	TRUE	GE4
0.0.0.0	Global Segment	0.0.0.0	Cloud	7	TRUE	GE5
0.0.0.0	Global Segment	0.0.0.0	Cloud	8	TRUE	GE6
172.17.1.10	segment1	255.255.255.255	N/A	0	TRUE	GE6
172.17.1.2	segment1	255.255.255.255	N/A	0	TRUE	GE5
172.16.1.10	segment1	255.255.255.255	N/A	0	TRUE	GE6
169.254.7.10	segment1	255.255.255.255	N/A	0	TRUE	GE3
169.254.6.34	segment1	255.255.255.255	N/A	0	TRUE	GE4
172.17.1.8	segment1	255.255.255.248	Connected	0	TRUE	GE6
172.17.1.0	segment1	255.255.255.248	Connected	0	TRUE	GE5
172.16.1.8	segment1	255.255.255.248	Connected	0	TRUE	GE6

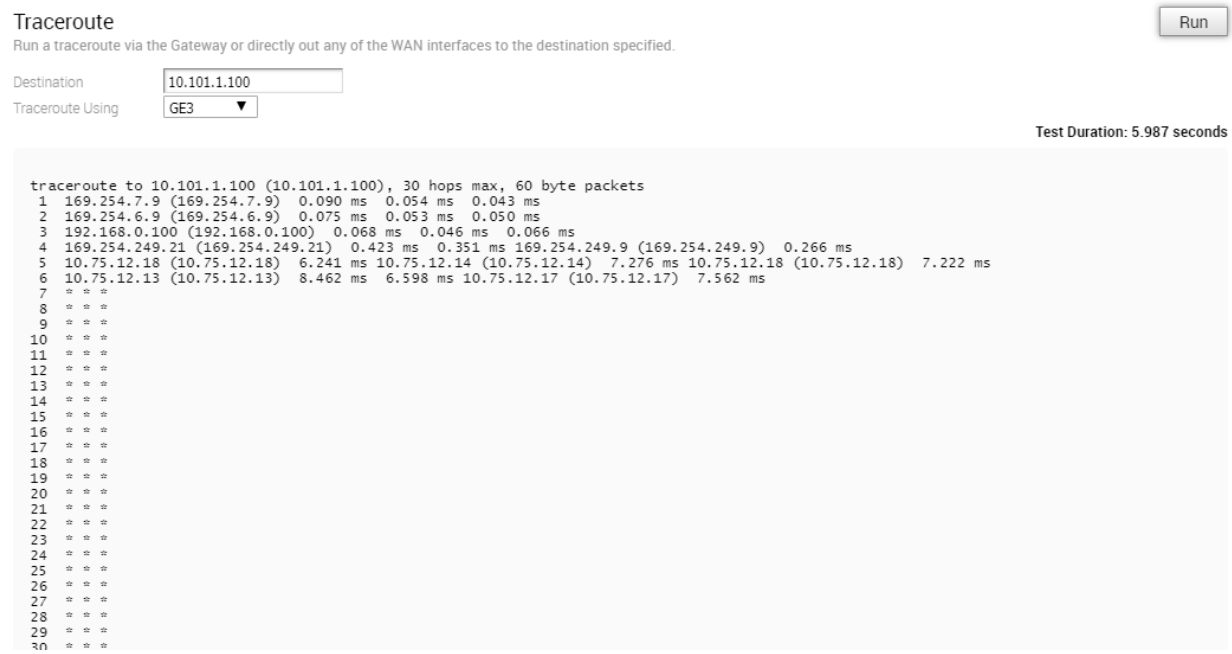
系統健全狀況

執行此測試以檢視系統資訊，例如系統負載、最近的 WAN 穩定性統計資料、監控服務。WAN 穩定性統計資料包含個別 VPN 通道與 WAN 連結中斷連線至少達 700 毫秒的次數。



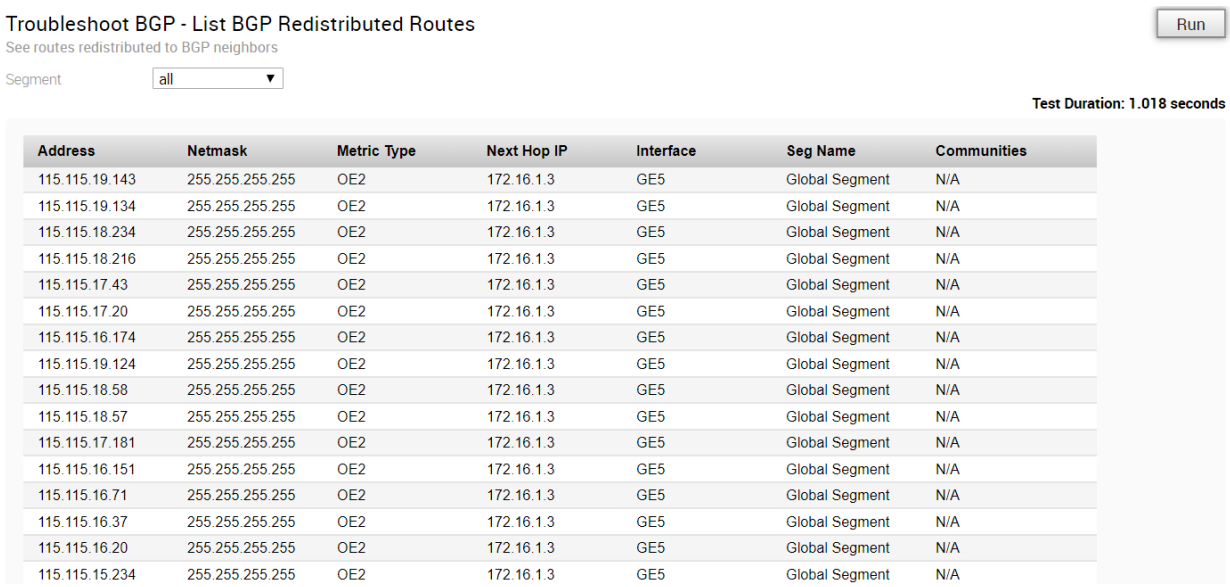
路徑追蹤

執行透過閘道的路徑追蹤，或直接從任何 WAN 介面到指定目的地的路徑追蹤。



疑難排解 BGP - 列出 BGP 重新分配的路由

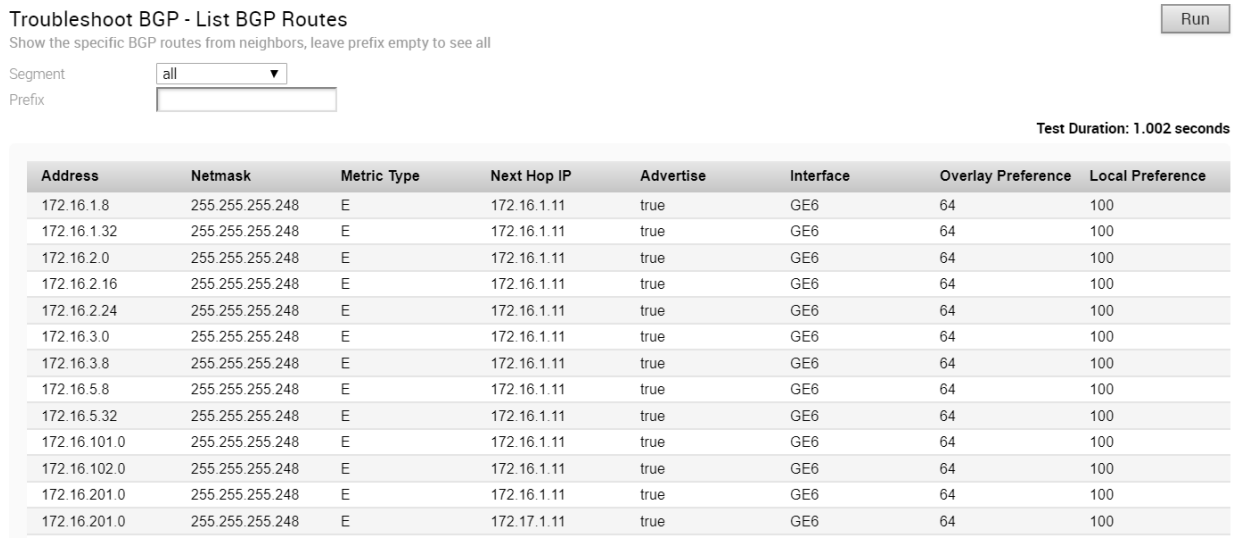
執行此測試，以檢視重新分配至 BGP 芳鄰的路由。



Address	Netmask	Metric Type	Next Hop IP	Interface	Seg Name	Communities
115.115.19.143	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.19.134	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.234	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.216	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.43	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.20	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.174	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.19.124	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.58	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.57	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.181	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.151	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.71	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.37	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.20	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.15.234	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A

疑難排解 BGP - 列出 BGP 路由

執行此測試以檢視來自芳鄰的特定 BGP 路由，將首碼保留為空白可全部檢視。



Address	Netmask	Metric Type	Next Hop IP	Advertise	Interface	Overlay Preference	Local Preference
172.16.1.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.1.32	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.16	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.24	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.3.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.3.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.5.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.5.32	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.101.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.102.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.201.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.201.0	255.255.255.248	E	172.17.1.11	true	GE6	64	100

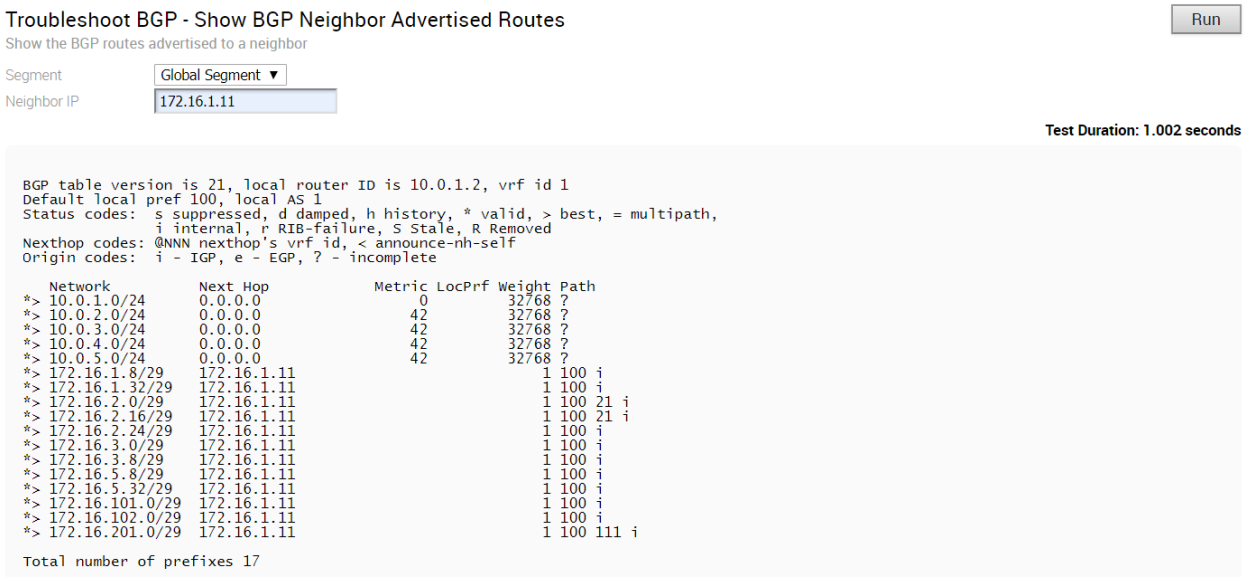
疑難排解 BGP - 列出每個首碼的路由

執行此測試以檢視首碼的所有覆疊和底層路由，以及相關詳細資料。

Address	Netmask	Metric Type	Next Hop IP	Advertise	Interface	Overlay Preference	Local Preference
172.16.3.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100

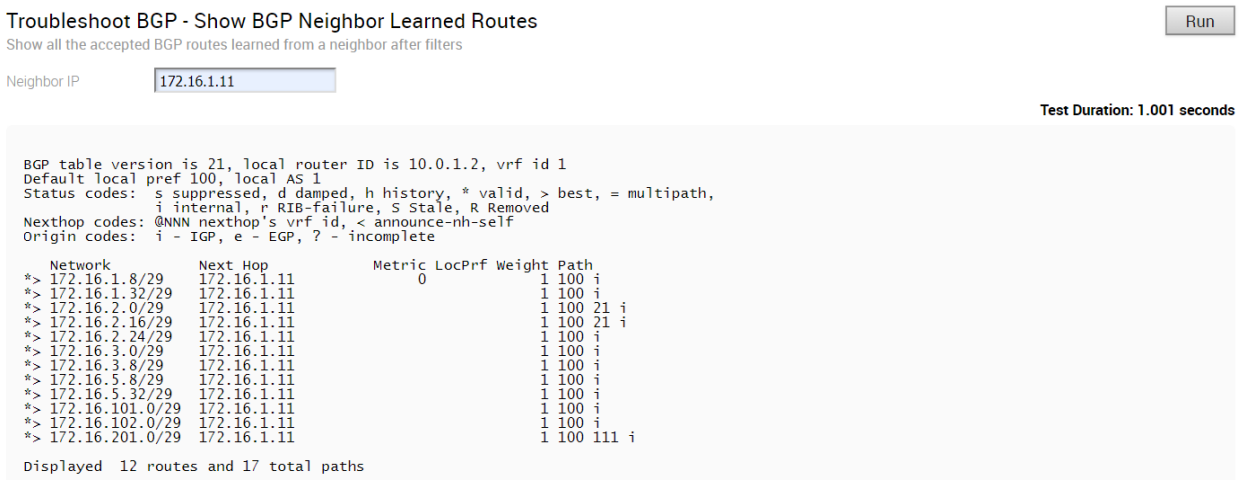
疑難排解 BGP - 顯示 BGP 芳鄰通告的路由

執行此測試，以檢視通告至芳鄰的 BGP 路由。



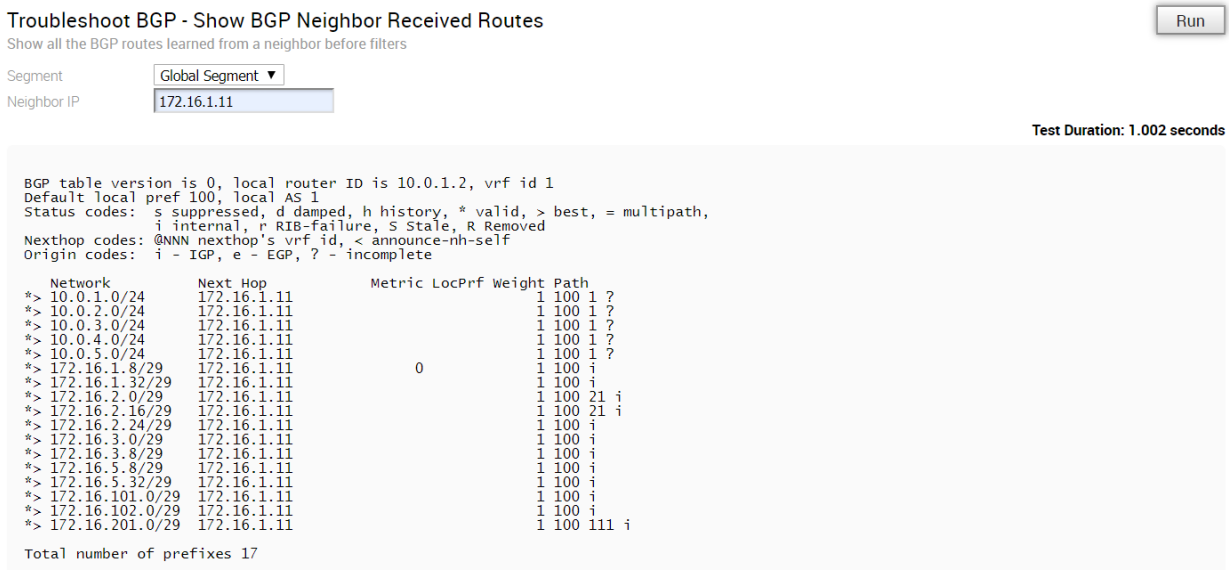
疑難排解 BGP - 顯示 BGP 芳鄰學習的路由

執行此測試，以檢視在篩選後從芳鄰學習的所有已接受的 BGP 路由。



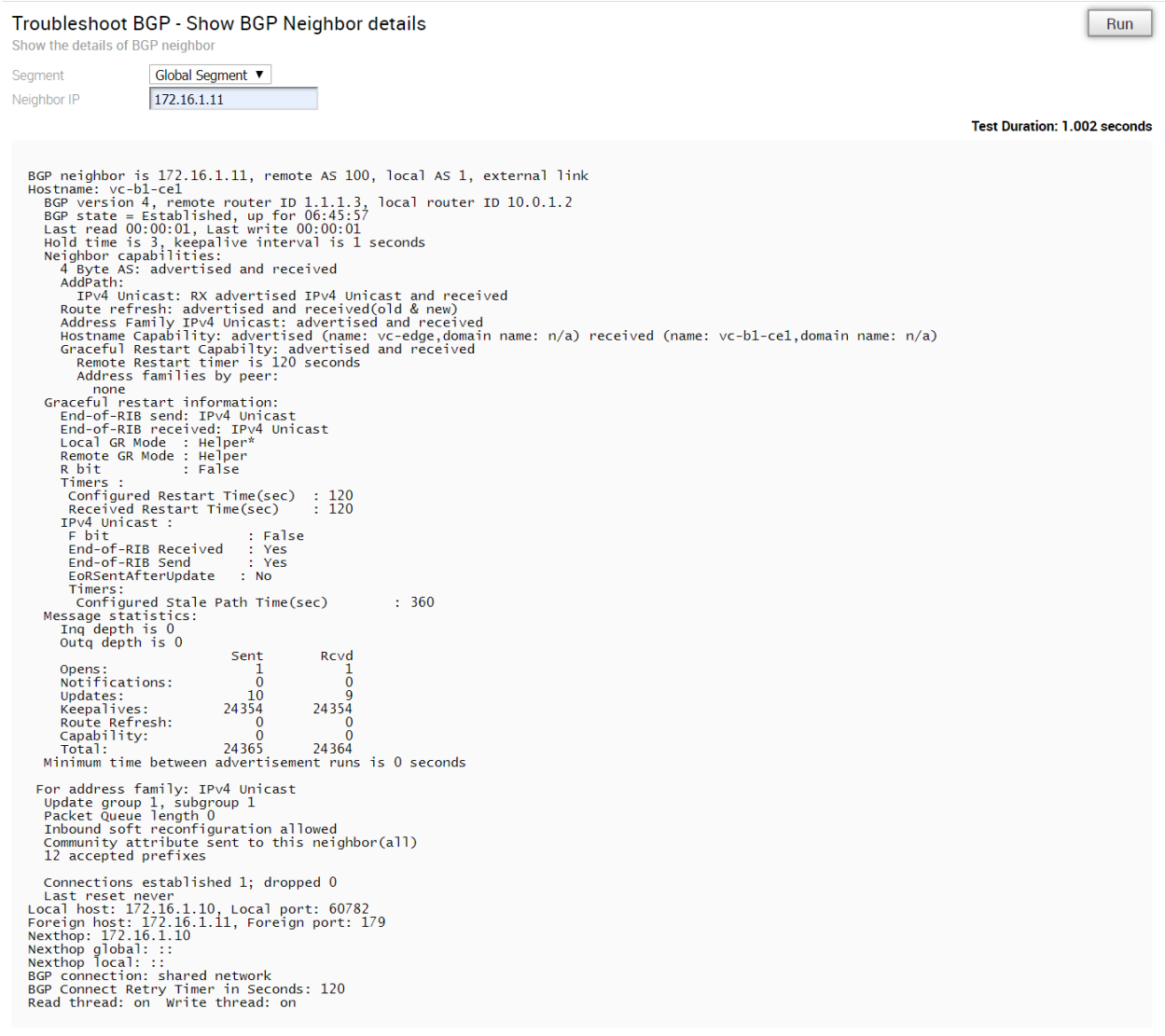
疑難排解 BGP - 顯示 BGP 芳鄰已接收的路由

執行此測試，以檢視在篩選前從芳鄰學習的所有 BGP 路由。



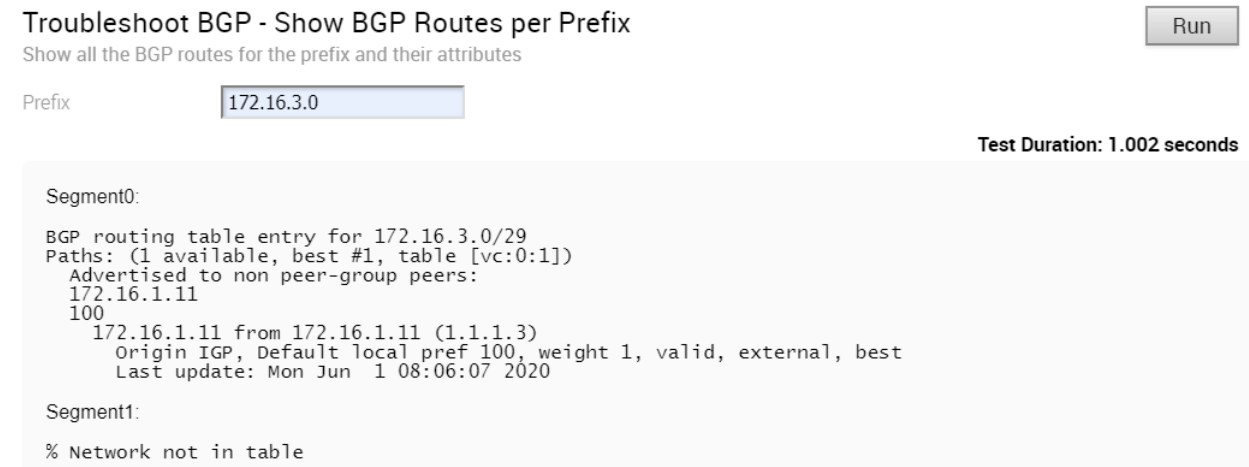
疑難排解 BGP - 顯示 BGP 芳鄰詳細資料

執行此測試，以檢視 BGP 芳鄰的詳細資料。



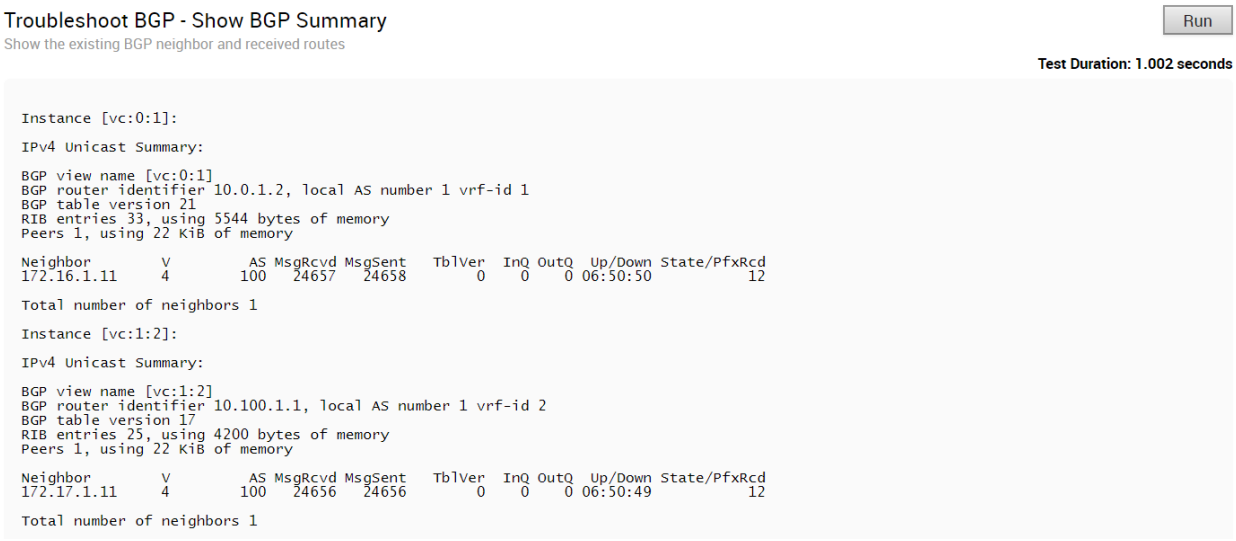
疑難排解 BGP - 顯示每個首碼的 BGP 路由

執行此測試，以檢視指定首碼的所有 BGP 路由及其屬性。



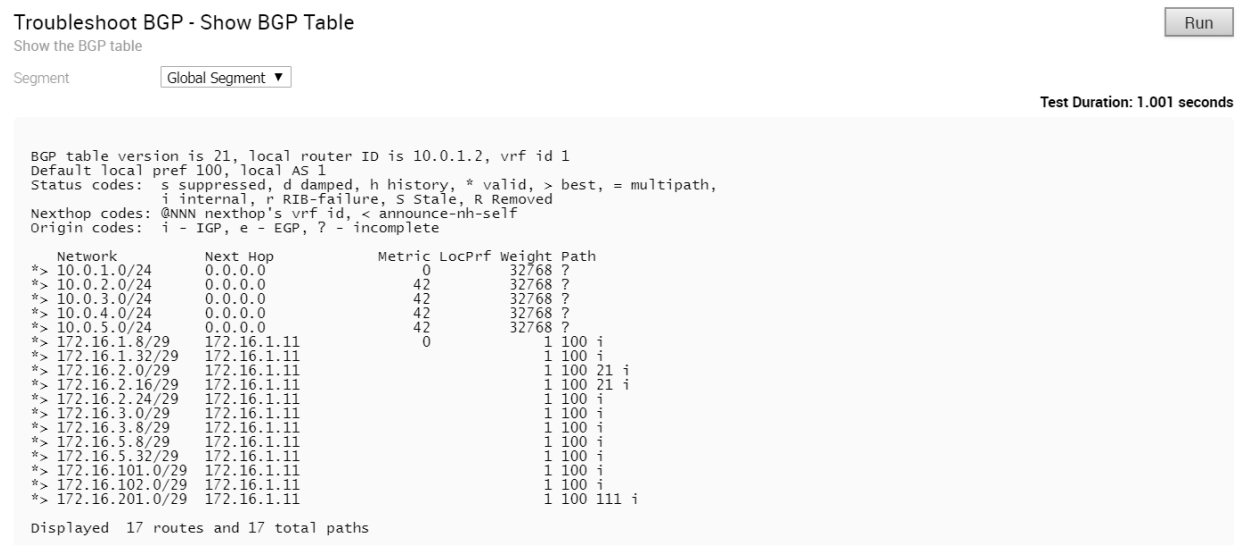
疑難排解 BGP - 顯示 BGP 摘要

執行此測試，以檢視現有的 BGP 芳鄰和已接收的路由。



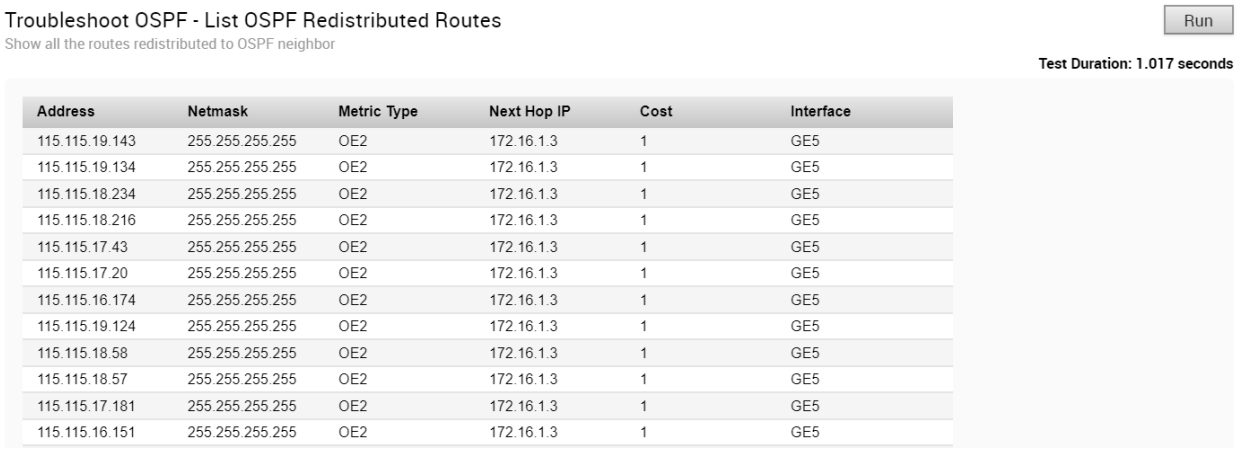
疑難排解 BGP - 顯示 BGP 資料表

執行此測試以檢視 BGP 資料表。



疑難排解 OSPF - 列出 OSPF 重新分配的路由

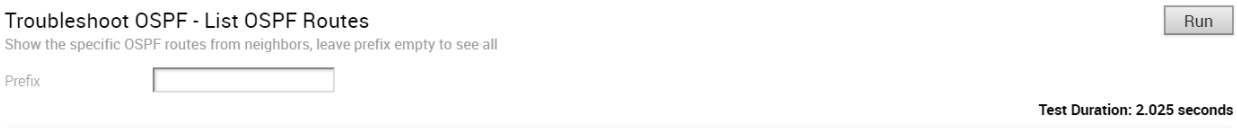
執行此測試，以檢視重新分配至 OSPF 芳鄰的所有路由。



Address	Netmask	Metric Type	Next Hop IP	Cost	Interface
115.115.19.143	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.19.134	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.234	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.216	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.43	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.20	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.16.174	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.19.124	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.58	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.57	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.181	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.16.151	255.255.255.255	OE2	172.16.1.3	1	GE5

疑難排解 OSPF - 列出 OSPF 路由

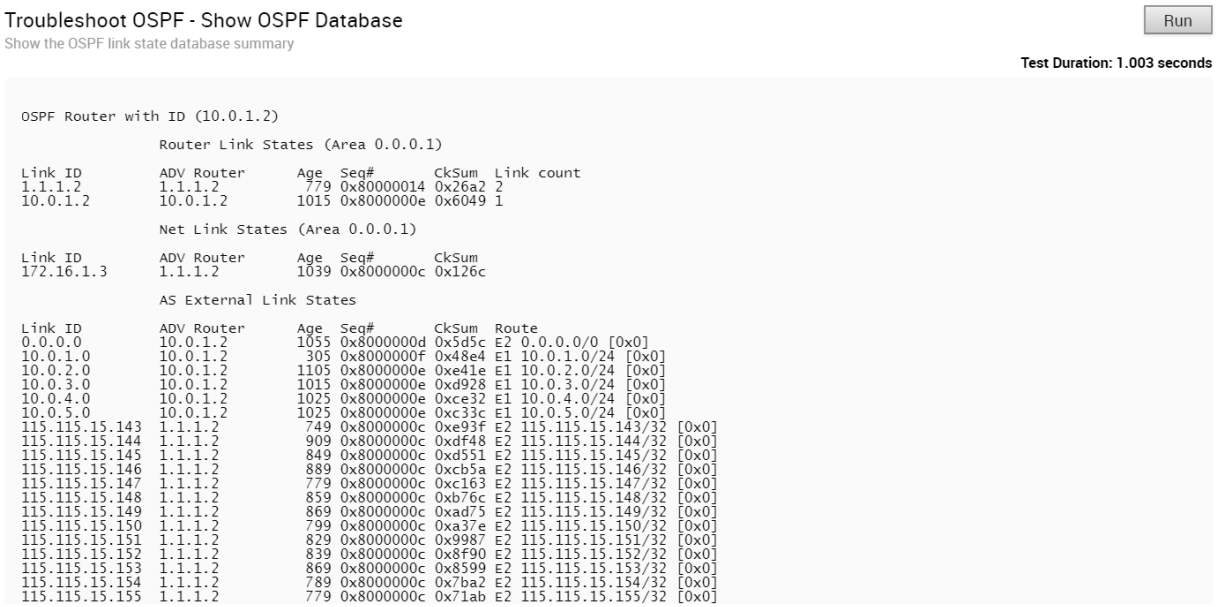
執行此測試，以針對指定的首碼檢視來自芳鄰的 OSPF 路由。顯示未指定首碼時來自芳鄰的所有 OSPF 路由。



Address	Netmask	Metric Type	Nbr ID	OSPF Cost	Overlay Preference	Advertise	Interface
115.115.15.143	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.144	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.145	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.146	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.147	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.148	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.149	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.150	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.151	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.152	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.153	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.154	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.155	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5

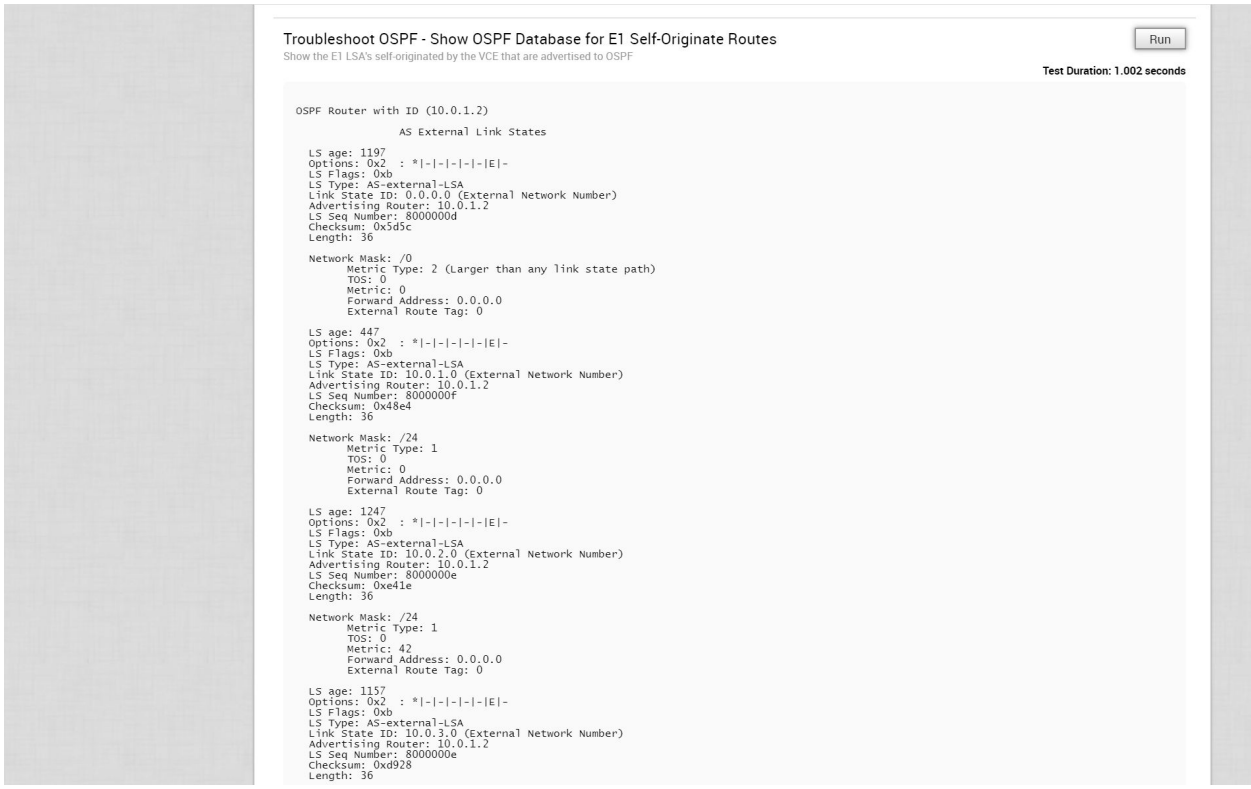
疑難排解 OSPF - 顯示 OSPF 資料庫

執行此測試，以檢視 OSPF 連結狀態資料庫摘要。



疑難排解 OSPF - 顯示 E1 自我產生路由的 OSPF 資料庫

執行此測試，以檢視由 Edge 通告至 OSPF 路由器的 E1 LSA 自我產生路由。

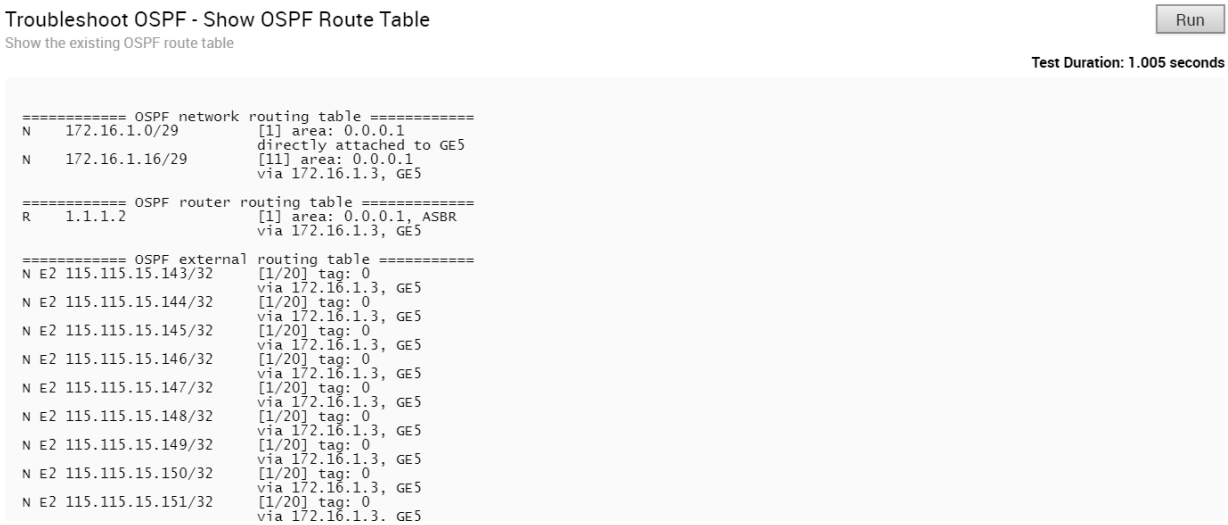


疑難排解 OSPF - 顯示 OSPF 芳鄰

執行此測試，以檢視所有的 OSPF 芳鄰和相關聯的資訊。

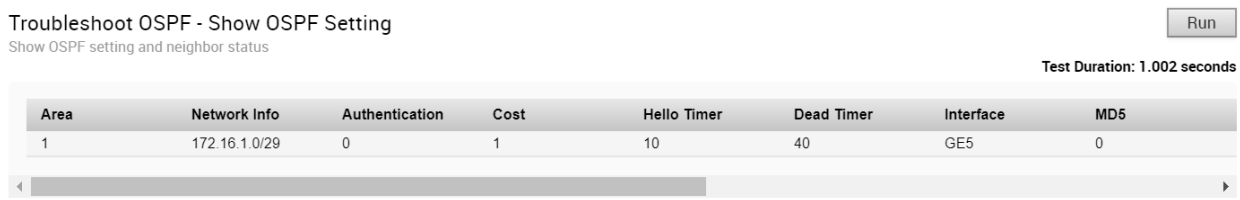
疑難排解 OSPF - 顯示 OSPF 路由表

執行此測試，以檢視現有的 OSPF 路由表。



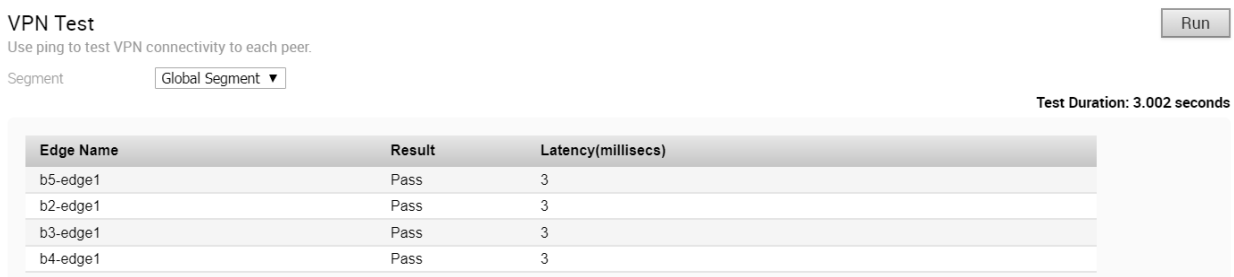
疑難排解 OSPF - 顯示 OSPF 設定

執行此測試，以檢視 OSPF 設定和芳鄰狀態。



VPN 測試

從下拉式功能表選取區段，然後按一下**執行 (Run)** 以測試與每個對等的 VPN 連線。



執行 VPN 測試時，Edge 會選取來源和目的地 IP，並起始通道要求。選取的來源和目的地 IP 應符合下列準則：

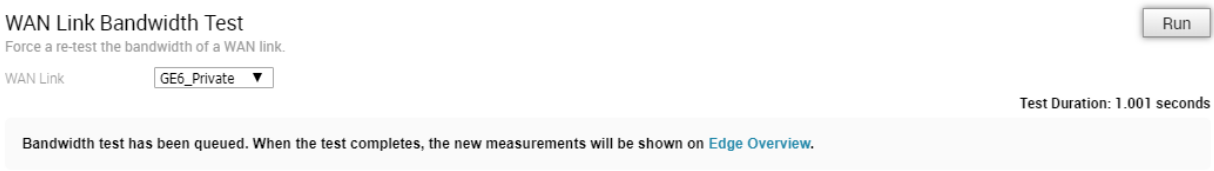
- 它應為連線的路由 IP
- 它應可連線，並且應通告路由

當 Edge 無法選取有效 IP 作為來源 IP 來起始通道要求時，VPN 測試將會失敗，並出現下列錯誤。

```
Branch-to-Branch vpn is disabled. Please enable it before running the test
```

WAN 連結頻寬測試

對指定的 WAN 連結執行頻寬測試。此測試的好處是在多重連結環境中不會中斷。只會對測試中的連結封鎖使用者流量。這表示您可以對特定連結重新執行測試，而其他連結將繼續處理使用者流量。



當通道不穩定達一段時間後重新連線時，系統會執行頻寬測試，有時連結的復原程度已足以進行通道連線，但尚不足以準確測量 WAN 連結的頻寬。為了因應此類情況，如果頻寬測試失敗或測量出明顯減少的值，則會使用上一個已知「良好」的測量，並排程在建立通道後的 30 分鐘重新測試連結，以確保測量的正確性。

備註 對於超過 1 Gbps 的 WAN 連結，建議使用者定義 WAN 連結的頻寬。

遠端動作

您可以從企業入口網站執行動作，例如重新啟動服務、重新啟動或停用 Edge。

您只能在處於**已連線 (Connected)** 狀態的 Edge 上執行遠端動作。

1 在企業入口網站中，按一下**測試和疑難排解 (Test & Troubleshoot) > 遠端動作 (Remote Actions)**。

2 **遠端 Edge 動作 (Remote Edge Actions)** 頁面會顯示所有已連線的 Edge。如有必要，請使用**篩選器 (Filter)** 搜尋 Edge，然後按一下**套用 (Apply)**。

3 按一下已連線 Edge 的連結。

在 **Edge 遠端動作 (Edge Remote Actions)** 視窗中，按一下相關動作。動作會在所選 Edge 上執行。

4 您可以執行下列動作：

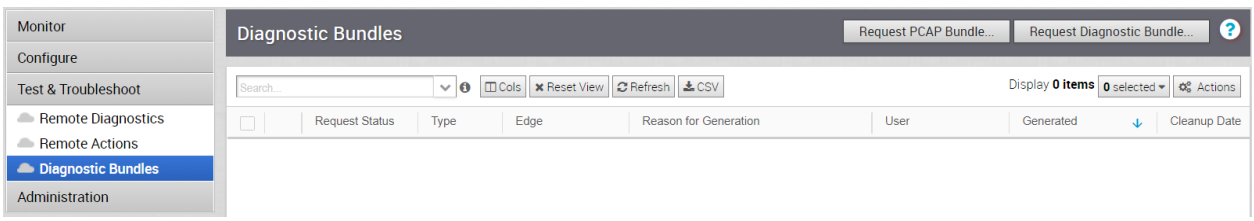
動作	說明
識別 (Identify)	隨機在所選 Edge 上閃燈來識別裝置。
重新啟動服務 (Restart Service)	重新啟動所選 Edge 上的 VMware 服務。
重新開機	將所選 Edge 重新啟動。
關機 (Shutdown)	關閉所選 Edge 的電源。
停用 (Deactivate)	將裝置組態重設回為其原廠預設狀態。

備註 在裝置上執行這些動作最多可能需要一分鐘的時間。

診斷服務包

診斷服務包可讓操作員使用者將所有的組態檔和記錄檔收集到合併的壓縮檔案中。診斷服務包中的可用資料可用於偵錯目的。

在企業入口網站中，按一下**測試和疑難排解 (Test & Troubleshooting) > 診斷服務包 (Diagnostic Bundles)**。



診斷服務包 (Diagnostic Bundles) 視窗可用來要求下列服務包：

- **PCAP 服務包 (PCAP Bundle)** –「封包擷取」服務包是網路封包資料的集合。操作員、標準管理員和客戶支援可要求 PCAP 服務包。請參閱要求封包擷取。

- **診斷服務包 (Diagnostic Bundle)** – 「診斷」服務包是來自特定 Edge 的所有組態和記錄的集合。只有操作員可以要求診斷服務包。請參閱要求診斷服務包。

產生的服務包會顯示在**診斷服務包 (Diagnostic Bundles)** 視窗中。若要下載服務包檔案，請參閱下載服務包。

診斷服務包 (Diagnostic Bundles) 選項僅適用於操作員使用者。如果您是合作夥伴使用者或企業使用者，則可以要求 PCAP 服務包。

在企業入口網站中，按一下**測試和疑難排解 (Test & Troubleshooting) > 封包擷取 (Packet Capture)**。

按一下**要求 PCAP 服務包 (Request PCAP Bundle)** 以產生「封包擷取」服務包，這是網路封包資料的集合。請參閱要求封包擷取。

要求封包擷取

封包擷取功能可用來收集 Edge 裝置的偵錯資訊。

從**測試和疑難排解 (Test & Troubleshoot) > 封包擷取 (Packet Capture)** 存取 [封包擷取 (Packet Capture)]。

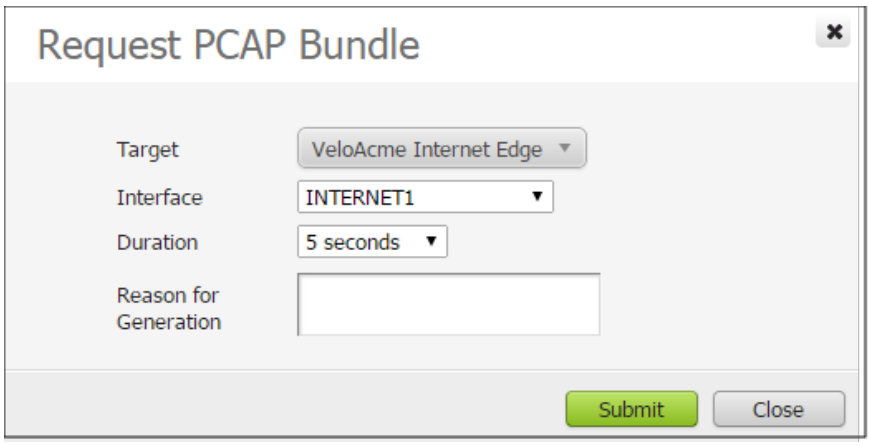
若要要求封包擷取：

1 按一下**測試和疑難排解 (Test & Troubleshoot)** 下的**封包擷取 (Packet Capture)**。

封包擷取 (Packet Capture) 畫面隨即出現。如果適用，就會顯示先前要求的狀態。

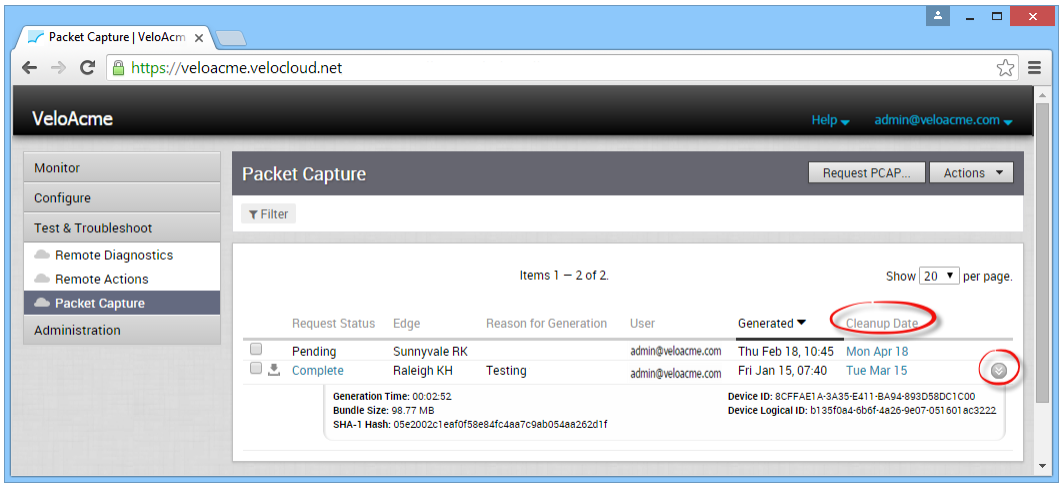
2 按一下畫面右上角的**要求 PCAP (Request PCAP)** 按鈕。

3 在**要求 PCAP 服務包 (Request PCAP Bundle)** 對話方塊中，選擇您的目標、介面和持續時間。如有必要，請輸入產生的原因。



4 按一下**提交 (Submit)**。畫面的右上角會出現快顯訊息 (成功要求)。

封包擷取 (Packet Capture) 畫面會更新，以顯示要求的狀態。重新整理畫面或按一下導覽面板中**封包擷取 (Packet Capture)**，可顯示狀態結果。完成後，您可以取得詳細資訊 (產生時間、服務包大小等)，只要按一下最右邊最後一個資料行旁邊的灰色箭頭即可。



備註 到達**清理日期 (Cleanup Date)** 資料行中顯示的日期時，特定 Edge 的封包擷取資料將會從系統中刪除。按一下**清理日期 (Cleanup Date)** 連結可指定要移除資料的日期，或者，選取**永久保留 (Keep Forever)** 核取方塊，資料就不會刪除；資料將保存到您另行指示為止。

按一下**動作 (Actions)** 按鈕，以下載或刪除服務包。如需詳細資訊，請參閱以下幾節。

要求診斷服務包

只有操作員可以要求診斷服務包。如果您是操作員，您可以在**測試和疑難排解 (Test & Troubleshooting) > 診斷服務包 (Diagnostic Bundles)** 頁面中存取**診斷服務包 (Diagnostic Bundle)** 按鈕。

若要要求診斷服務包：

1 按一下位於**診斷服務包 (Diagnostic Bundles)** 頁面右上角的**要求診斷服務包 (Request Diagnostic Bundle)** 按鈕。

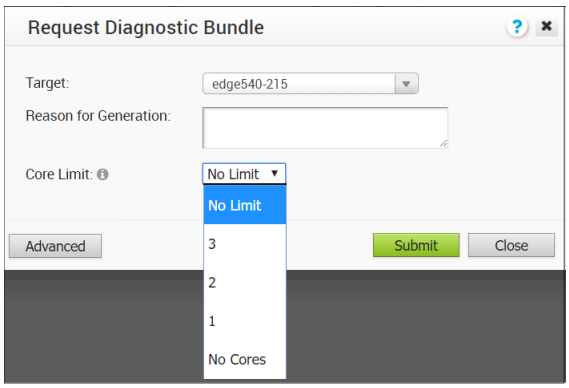
2 在**要求診斷服務包 (Request Diagnostic Bundle)** 對話方塊中：

   a 在**目標 (Target)** 下拉式功能表中，選取您將從中接收資料的特定 Edge。

   b 如果您想要指出要求的原因，請在**產生的原因 (Reason for Generation)** 文字方塊中輸入。

   c 若要進行進階要求，請按一下**進階 (Advanced)** 按鈕，然後從**核心限制 (Core Limit)** 下拉式功能表中選擇限制。當網際網路連線發生錯誤時，核心限制可用來減少已上傳服務包的大小。

   d 按一下 [提交 (Submit)] 按鈕。



所選 Edge 的診斷要求服務包處於擱置中狀態，如 [診斷服務包 (Diagnostic Bundles)] 視窗中的 [要求狀態 (Request Status)] 資料行所示。完成後，狀態會變更為**完成 (Complete)**。**完成 (Complete)** 狀態是一個連結，按一下即可下載服務包。

下載服務包

要求完成後，您可以透過下列其中一種方式下載服務包：

- 在**要求狀態 (Request Status)** 資料行下，按一下已完成的 PCAP 要求旁邊的下載符號。
- 在所選 Edge 的**要求狀態 (Request Status)** 資料行中，按一下**完成 (Complete)** 連結。
- 選取一或多個已完成的 PCAP 要求的核取方塊，然後按一下**動作 (Action)** 按鈕 (螢幕的右上角) 的向下箭頭，然後選擇**下載 (Download)**。

您可以將下載的服務包轉送給 VMware 的網路支援代表。

刪除服務包

如果您想要刪除封包擷取，請從**要求狀態 (Request Status)** 資料行中選取一或多個封包擷取，然後從**動作 (Actions)** 按鈕中選擇**刪除 (Delete)**。

備註 如果封包擷取要求擱置中，您可以在要求完成前刪除該要求。選取要刪除擱置中要求的核取方塊，並按一下**動作 (Action)** 按鈕，然後選擇**刪除 (Delete)**。

企業管理

21

企業入口網站中的**管理 (Administration)** 選項可讓您設定系統設定、驗證資訊，以及建立管理員使用者和管理 Edge 授權。

在企業入口網站中，按一下**管理 (Administration)** 以設定下列項目：

- **系統設定 (System Settings)** – 設定使用者資訊和企業驗證。請參閱系統設定。
- **管理員 (Administrators)** – 建立或修改具有不同角色權限的管理員使用者。請參閱管理管理員使用者。
- **Edge 授權 (Edge Licensing)** – 檢視及產生 Edge 授權的報告。請參閱 Edge 授權。

本章節討論下列主題：

- 系統設定
- 管理管理員使用者
- Edge 授權

系統設定

系統設定 (System Settings) 選項可讓您設定管理員設定以及驗證詳細資料。

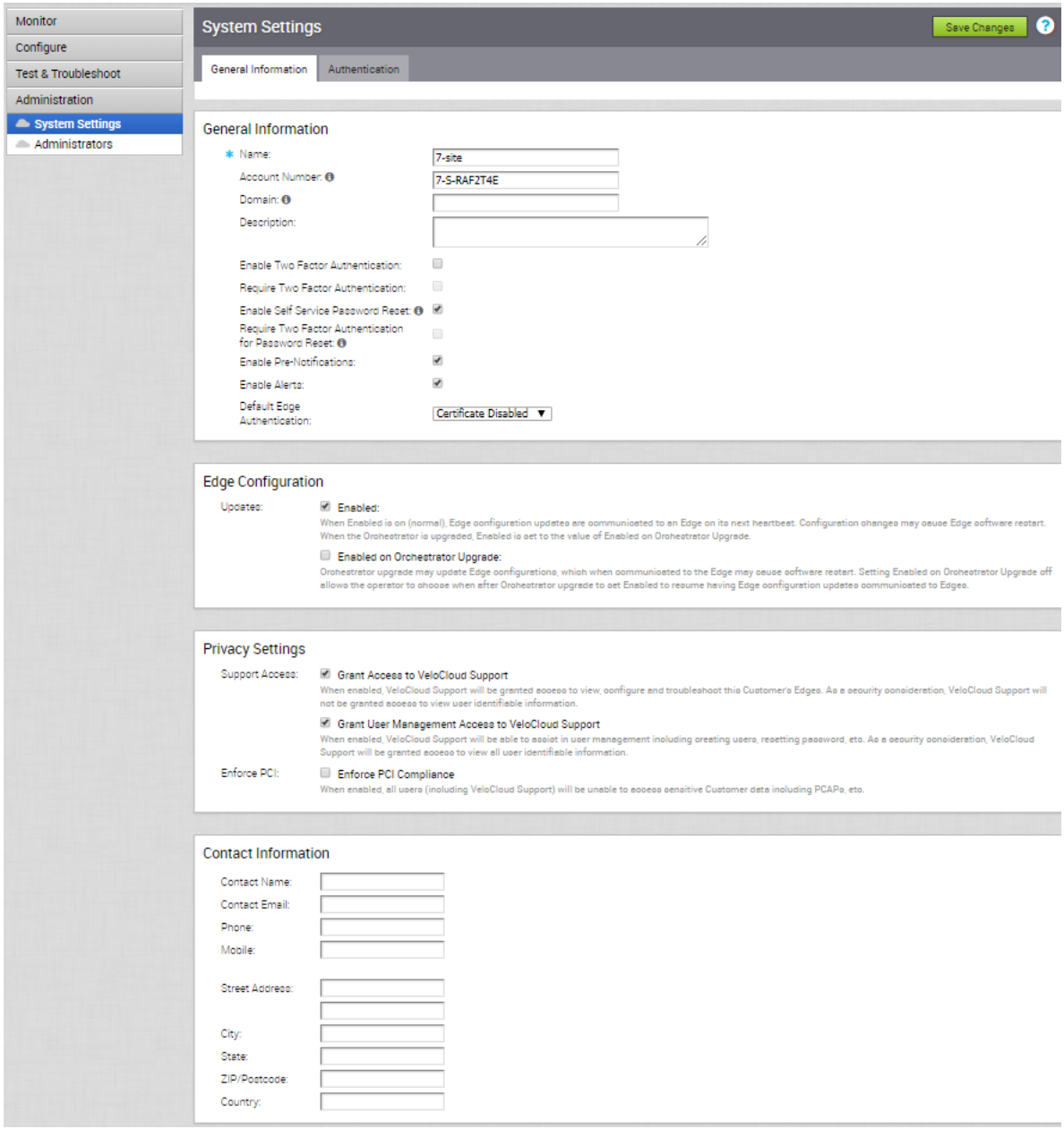
在企業入口網站中，按一下**管理 (Administration) > 系統設定 (System Settings)**，以設定下列項目：

- **一般資訊 (General Information)** – 設定使用者詳細資料、啟用 Edge 組態更新、進行隱私權設定，以及輸入連絡資訊。請參閱設定企業資訊。
- **驗證 (Authentication)** – 設定驗證模式和檢視 API Token。請參閱設定企業驗證。

設定企業資訊

您可以使用**一般資訊 (General Information)** 來設定使用者的使用者資訊、隱私權設定和連絡詳細資料。

在企業入口網站中，按一下**管理 (Administration) > 系統設定 (System Settings)**。您可以在**一般資訊 (General Information)** 索引標籤中設定下列項目。



一般資訊 (General Information)

選項	說明
名稱 (Name)	顯示現有的使用者名稱。如有需要，您可以修改名稱。
帳戶號碼 (Account Number)	顯示現有的帳戶號碼。如有需要，您可以修改號碼。
網域 (Domain)	顯示現有的網域名稱，如有需要，您可以修改網域。
說明	輸入客戶的說明。

選項	說明
啟用雙因素驗證 (Enable Two Factor Authentication)	選取此核取方塊，可為操作員、MSP 和企業啟用使用 SMS 的雙因素驗證。您可以在客戶/MSP 層級或在操作員層級啟用驗證。 在啟用雙因素驗證之前，請確定您已為所有管理員使用者提供有效的行動電話號碼。您可以在**管理 (Administration) > 管理員 (Administrators)** 畫面中選取使用者，以輸入行動電話號碼。另請參閱管理管理員使用者。
需要雙因素驗證 (Require Two Factor Authentication)	選取此核取方塊可強制使用者使用雙因素驗證進行登入。啟用雙因素驗證後，當您嘗試使用您的使用者認證登入時，您也需要輸入在行動電話中以 SMS 的形式收到的六位數 PIN 碼。
啟用自助式密碼重設 (Enable Self Service Password Reset)	依預設會選取此選項，這可讓您在 Orchestrator 的登入頁面中重設密碼。 當您嘗試在登入頁面中重設密碼時，系統會提示您輸入使用者名稱。請確實輸入有效的電子郵件地址作為使用者名稱。提交使用者名稱後，您會收到一則電子郵件，其中包含可重設密碼的連結。按一下該連結即可設定新密碼。
密碼重設需要雙因素驗證 (Require Two Factor Authentication for Password Reset)	選取此選項，可在重設密碼時啟用雙因素驗證。只有在已選取**啟用雙因素驗證 (Enable Two Factor Authentication)** 選項時，才能選取此核取方塊。 如果啟用此選項，當您嘗試在 Orchestrator 的登入頁面中重設密碼時，系統會將您重新導向至 [驗證 (Authentication)] 頁面。[驗證 (Authentication)] 頁面會提示您輸入您在行動裝置中以 SMS 形式接收的一次性代碼。驗證代碼後，系統會將您重新導向至 [密碼 (Password)] 頁面以設定新密碼。
啟用預先通知 (Enable Pre-Notifications)	選取此核取方塊可啟用預先通知警示。
啟用警示 (Enable Alerts)	選取此核取方塊可啟用警示。您可以使用 第 19 章 設定警示 選項來設定警示類型。
預設 Edge 驗證 (Default Edge Authentication)	從下拉式清單中選擇預設選項，以驗證與客戶相關聯的 Edge。

Edge 組態

選擇下列選項，將 Edge 組態的更新傳輸至 Edge：

- **已啟用 (Enabled)** – 選取此選項，可在下一個活動訊號期間將組態更新傳輸至 Edge。組態中的變更可能會重新啟動對應 Edge 中的軟體。依預設會選取此選項。
- **在 Orchestrator 升級時啟用 (Enabled on Orchestrator Upgrade)** – 選取此選項，可在升級 Orchestrator 時將組態中的更新傳輸至 Edge。這可能會使對應 Edge 中的軟體重新啟動。

隱私權設定 (Privacy Settings)

- **支援存取 (Support Access)** – 選擇下列選項可為支援團隊授與存取權。
  - **授與 VeloCloud 支援的存取權 (Grant Access to VeloCloud Support)** – 選取此選項可授與對 VMware 支援的存取權，以檢視、設定連線至客戶的 Edge 並進行疑難排解。基於安全考量，此「支援」無法存取或檢視使用者識別資訊。

- **授與使用者對 VeloCloud 支援的管理存取權 (Grant User Management Access to VeloCloud Support)** – 選取此選項可讓 VMware 支援協助使用者進行管理。使用者管理選項包括建立使用者、重設密碼和進行其他設定。在此情況下，此「支援」可存取使用者識別資訊。

- **強制執行 PCI (Enforce PCI)** - 選取此選項，可阻止基於 PCI 合規性原因而不允許的作業。目前，此選項會阻止的唯一作業是從 Edge 要求 PCAP 診斷服務包。

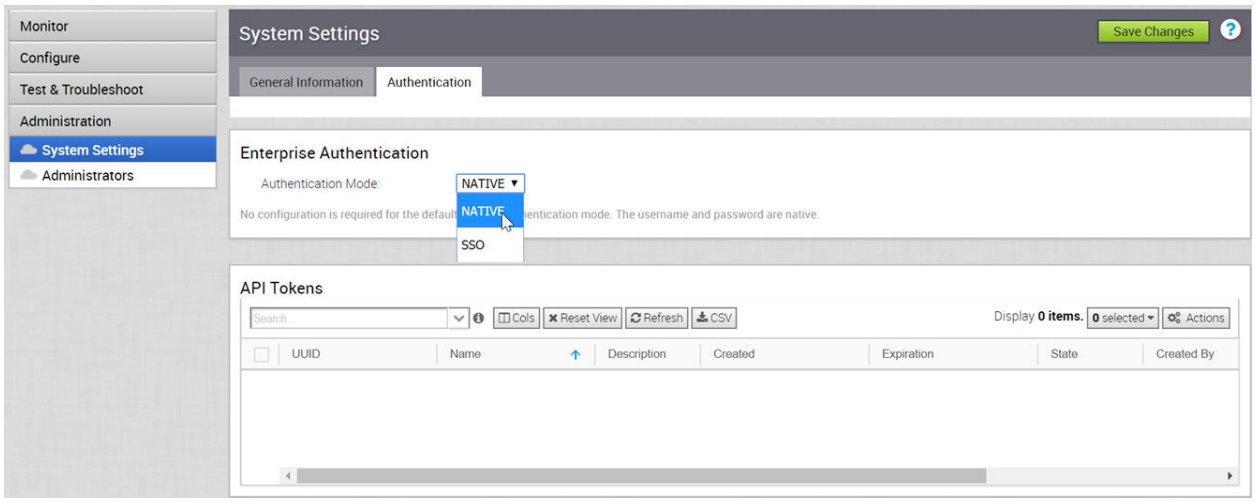
連絡資訊 (Contact Information)

此區段中顯示現有的連絡詳細資料。如有需要，您可以修改詳細資料。

設定企業驗證

在**驗證 (Authentication)** 索引標籤中，您可以設定企業的驗證模式，並檢視現有的 API Token。

在企業入口網站中，按一下**管理 (Administration) > 系統設定 (System Settings) > 驗證 (Authentication)**，以設定下列項目：



企業驗證 (Enterprise Authentication)

從**驗證模式 (Authentication Mode)** 中，選擇下列其中一項。

- **原生 (NATIVE)** – 這是預設驗證模式，您可以使用原生使用者名稱和密碼登入企業。此模式不需要任何設定。
- **SSO** – 單一登入 (SSO) 是一種工作階段和使用者驗證服務，可讓使用者使用一組登入認證登入企業以存取多個應用程式。如需詳細資訊，請參閱單一登入概觀和設定企業使用者的單一登入。

API Token

無論什麼驗證模式，您都可以使用 Token 型驗證來存取 Orchestrator API。您可以在此區段中查看現有的 API Token。

操作員超級使用者或與 API Token 相關聯的使用者可以撤銷 Token。選取 Token，然後按一下**動作 (Actions) > 撤銷 (Revoke)**。若要建立和下載 API Token，請參閱 API Token。

單一登入概觀

SD-WAN Orchestrator 支援一種名為單一登入 (SSO) 的新類型使用者驗證，可用於所有的 Orchestrator 使用者類型：操作員、合作夥伴和企業。

單一登入 (SSO) 是一種工作階段和使用者驗證服務，可讓 SD-WAN Orchestrator 使用者使用一組登入認證登入 SD-WAN Orchestrator 以存取多個應用程式。將 SSO 服務與 SD-WAN Orchestrator 整合，可為 SD-WAN Orchestrator 使用者的使用者驗證提高安全性，並且讓 SD-WAN Orchestrator 可從其他 OpenID Connect (OIDC) 身分識別提供者 (IDP) 驗證使用者。目前支援下列 IDP：

- Okta
- OneLogin
- PingIdentity
- AzureAD
- VMwareCSP

設定企業使用者的單一登入

若要為企業使用者設定單一登入 (SSO) 驗證，請執行此程序中的步驟。

必要條件

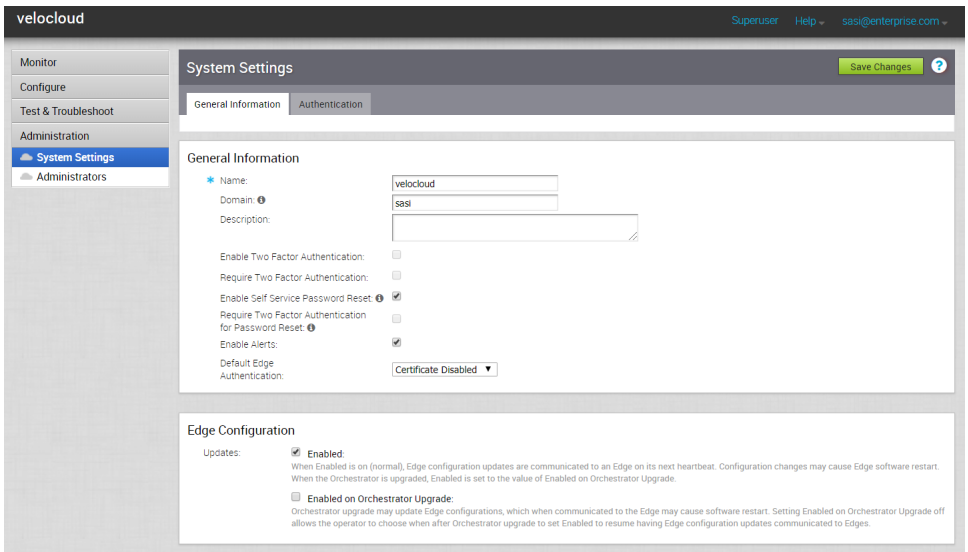
- 確定您具有企業超級使用者權限。
- 在設定 SSO 驗證之前，請確定您已在慣用的身分識別提供者網站中，設定 SD-WAN Orchestrator 的角色、使用者和 OpenID Connect (OIDC) 應用程式。如需詳細資訊，請參閱設定單一登入的 IDP。

程序

1 使用您的登入認證，以企業超級使用者身分登入 SD-WAN Orchestrator 應用程式。

2 按一下**管理 (Administration)** > **系統設定 (System Settings)**

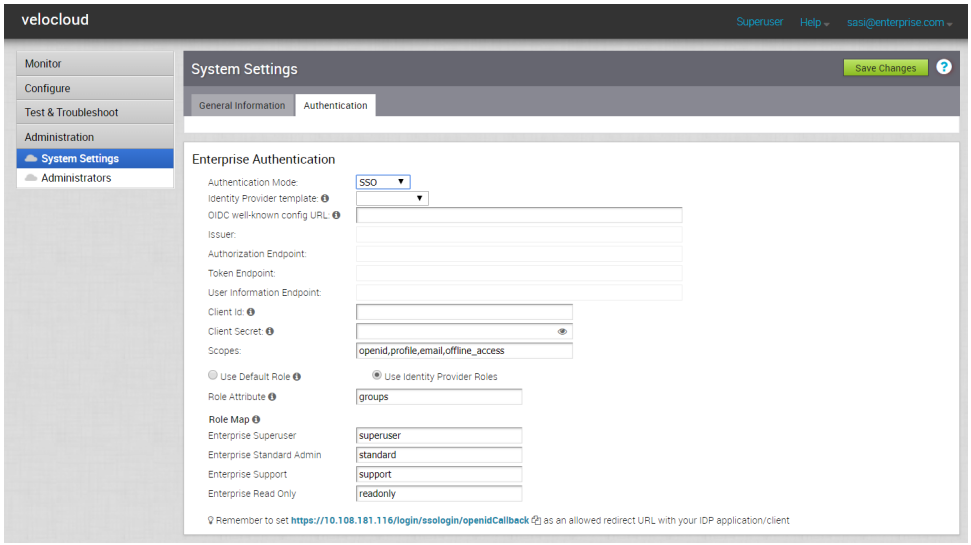
系統設定 (System Settings) 畫面隨即出現。



3 按一下**一般資訊 (General Information)** 索引標籤，然後在**網域 (Domain)** 文字方塊中，輸入企業的網域名稱 (如果尚未設定)。

備註 若要為 SD-WAN Orchestrator 啟用 SSO 驗證，您必須設定企業的網域名稱。

4 按一下**驗證 (Authentication)** 索引標籤，然後從**驗證模式 (Authentication Mode)** 下拉式功能表中，選取 **SSO**。



5 從**身分識別提供者範本 (Identity Provider template)** 下拉式功能表中，選取您為 Single Sign On 設定的慣用身分識別提供者 (IDP)。

備註 當您選取 VMwareCSP 作為慣用的 IDP 時，務必依下列格式提供組織識別碼：/csp/gateway/am/api/orgs/<完整組織識別碼>。

當您登入 VMware CSP 主控台時，您可以按一下使用者名稱來檢視您登入的組織識別碼。組織名稱下方會顯示縮短版本的識別碼。按一下識別碼以顯示完整的組織識別碼。

您也可以從**身分識別提供者範本 (Identity Provider template)** 下拉式功能表中選取**其他 (Others)**，以手動設定自己的 IDP。

6 在 **OIDC 知名組態 URL (OIDC well-known config URL)** 文字方塊中，輸入 IDP 的 OpenID Connect (OIDC) 組態 URL。例如，Okta 的 URL 格式為：https://{oauth-provider-url}/.well-known/openid-configuration。

7 SD-WAN Orchestrator 應用程式會自動填入 IDP 的端點詳細資料，例如簽發人、授權端點、Token 端點及使用者資訊端點。

8 在**用戶端識別碼 (Client Id)** 文字方塊中，輸入 IDP 所提供的用戶端識別碼。

9 在**用戶端密碼 (Client Secret)** 文字方塊中，輸入 IDP 所提供的用戶端密碼，供用戶端將授權碼交換為 Token。

10 若要決定使用者在 SD-WAN Orchestrator 中的角色，請選取下列其中一個選項：

- **使用預設角色 (Use Default Role)** – 可讓使用者使用**預設角色 (Default Role)** 文字方塊 (選取此選項時出現)，將靜態角色設定為預設角色。支援的角色為：企業超級使用者、企業標準管理員、企業支援和企業唯讀。

備註 在 SSO 組態設定中，如果選取**使用預設角色 (Use Default Role)** 選項，並定義預設使用者角色，則系統會為所有 SSO 使用者指派指定的預設角色。標準管理員超級使用者或標準管理員可以在企業入口網站中按一下**管理 (Administration) > 管理員 (Administrators)** 索引標籤，藉此將特定使用者預先登錄為非原生使用者，並定義特定使用者角色，而非指派具有預設角色的使用者。如需設定新管理員使用者的步驟，請參閱建立新的管理員使用者。

- **使用身分識別提供者角色 (Use Identity Provider Roles)** – 使用在 IDP 中設定的角色。

11 選取**使用身分識別提供者角色 (Use Identity Provider Roles)** 選項時，在**角色屬性 (Role Attribute)** 文字方塊中輸入 IDP 中設定的屬性名稱，以傳回角色。

12 在**角色對應 (Role Map)** 區域中，將 IDP 提供的角色對應到每個 SD-WAN Orchestrator 角色，並使用逗號分隔。

VMware CSP 中的角色遵循以下格式：external/<服務定義 UUID>/<建立服務範本期間提及的服務角色名稱>。

13 使用 SD-WAN Orchestrator URL (https://<Orchestrator URL>/login/ssologin/openidCallback) 更新 OIDC 提供者網站中允許的重新導向 URL。

14 按一下**儲存變更 (Save Changes)** 以儲存 SSO 組態。

15 按一下**測試組態 (Test Configuration)**，以驗證輸入的 OpenID Connect (OIDC) 組態。

使用者會導覽至 IDP 網站，且能夠輸入認證。在 IDP 驗證和成功重新導向至 SD-WAN Orchestrator 測試回呼時，將會顯示成功驗證訊息。

結果

SSO 驗證設定已完成。

後續步驟

第 5 章 企業使用者使用 SSO 登入 VMware SD-WAN Orchestrator。

設定單一登入的 IDP

若要為 SD-WAN Orchestrator 啟用單一登入 (SSO)，您必須使用 SD-WAN Orchestrator 的詳細資料設定身分識別合作夥伴 (IDP)。目前支援下列 IDP：Okta、OneLogin、PingIdentity、AzureAD 和 VMware CSP。

如需為各種 IDP 中的 SD-WAN Orchestrator 設定 OpenID Connect (OIDC) 應用程式的逐步指示，請參閱：

- 設定 Okta 的單一登入
- 設定 OneLogin 的單一登入
- 設定 PingIdentity 的單一登入
- 設定單一登入的 Azure Active Directory
- 設定單一登入的 VMware CSP

設定 Okta 的單一登入

若要支援從 Okta 進行的 OpenID Connect (OIDC) 單一登入 (SSO)，您必須先在 Okta 中設定應用程式。若要在 Okta 中設定用於 SSO 的 OIDC 應用程式，請執行此程序的步驟。

必要條件

請確定您有 Okta 帳戶可進行登入。

程序

1 以管理員使用者身分登入您的 Okta 帳戶。

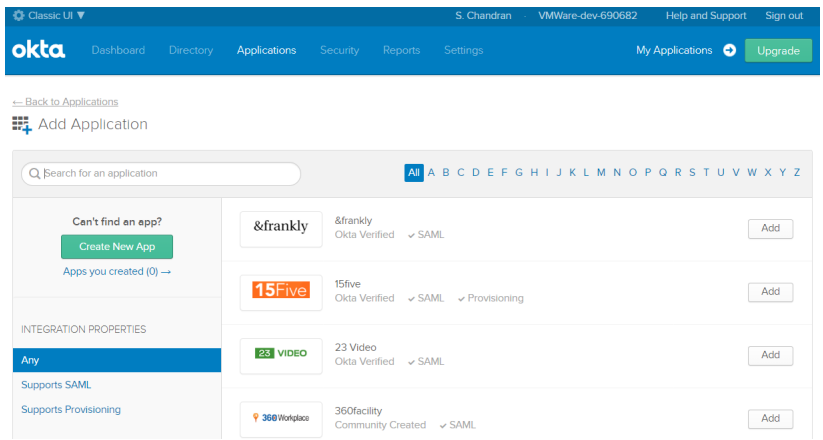
Okta 主畫面隨即出現。

備註 如果您在 [開發人員主控台 (Developer Console)] 視圖中，則必須在**開發人員主控台 (Developer Console)** 下拉式清單中選取**傳統 UI (Classic UI)**，以切換至 [傳統 UI (Classic UI)] 視圖。

2 若要建立新的應用程式：

a 在上方導覽列中，按一下**應用程式 (Applications)** > **新增應用程式 (Add Application)**。

新增應用程式 (Add Application) 畫面隨即出現。



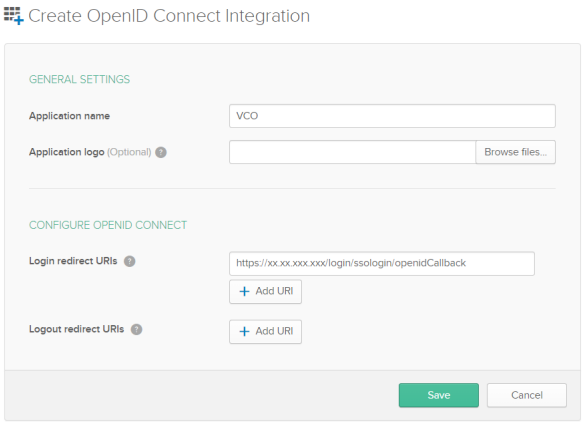
b 按一下**建立新的應用程式 (Create New App)**。

建立新的應用程式整合 (Create a New Application Integration) 對話方塊隨即出現。

c 在**平台 (Platform)** 下拉式功能表中，選取 **Web**。

d 選取 **OpenID Connect** 作為登入方法，然後按一下**建立 (Create)**。

建立 OpenID Connect 整合 (Create OpenID Connect Integration) 畫面隨即出現。



e 在**一般設定 (General Settings)** 區域的**應用程式名稱 (Application name)** 文字方塊中，輸入應用程式的名稱。

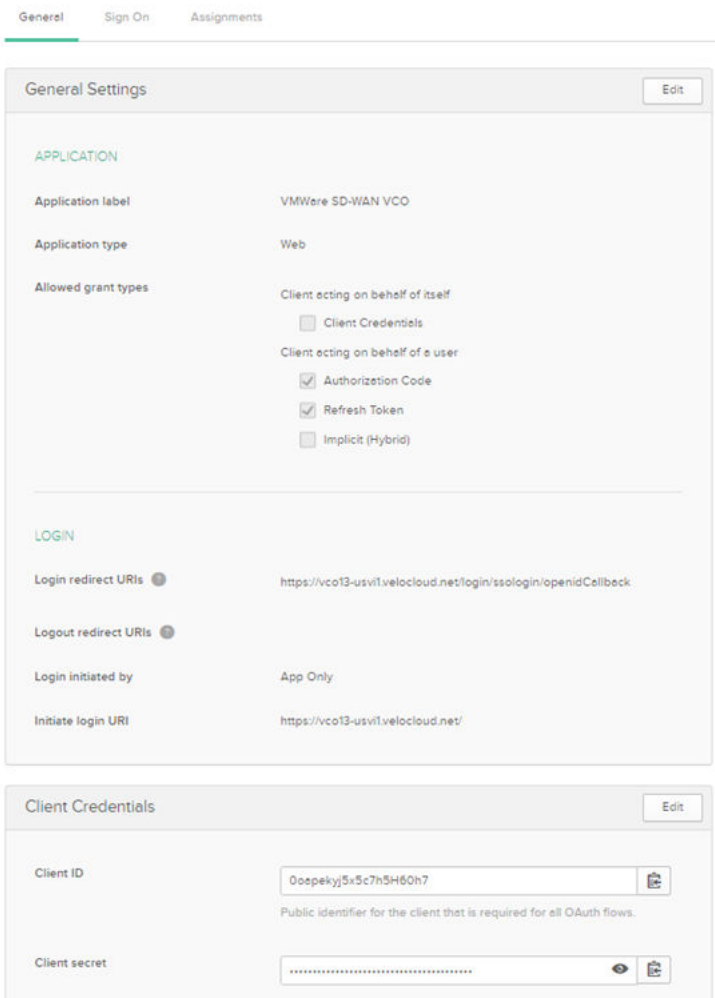
f 在**設定 OPENID CONNECT (CONFIGURE OPENID CONNECT)** 區域下的**登入重新導向 URI (Login redirect URIs)** 文字方塊中，輸入 SD-WAN Orchestrator 應用程式作為回撥端點的重新導向 URL。

在 SD-WAN Orchestrator 應用程式的**設定驗證 (Configure Authentication)** 畫面底部，您可以找到重新導向 URL 連結。理想情況下，SD-WAN Orchestrator 重新導向 URL 將會採用下列格式：https://<Orchestrator URL>/login/ssologin/openidCallback。

g 按一下**儲存 (Save)**。新建立的應用程式頁面隨即出現。

h 在**一般 (General)** 索引標籤上按一下**編輯 (Edit)**，並針對允許的授與類型選取**重新整理 Token (Refresh Token)**，然後按一下**儲存 (Save)**。

請記下 SD-WAN Orchestrator 中 SSO 設定期間所要使用的用戶端認證 (用戶端識別碼和用戶端密碼)。



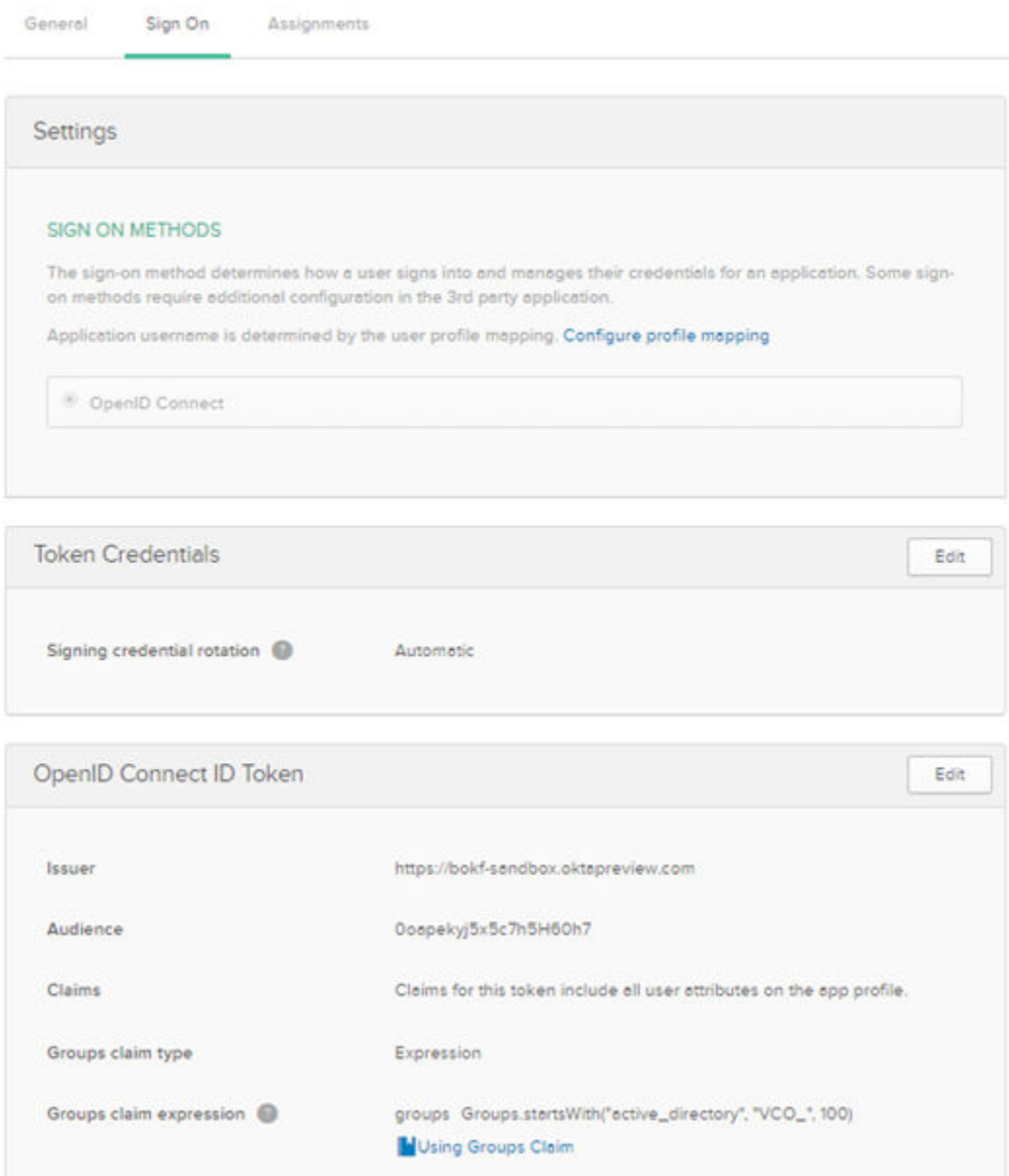
i 按一下**登入 (Sign On)** 索引標籤，然後在 **OpenID Connect ID Token** 區域下方按一下**編輯 (Edit)**。

j 在**群組宣告類型 (Groups claim type)** 下拉式功能表中，選取**運算式 (Expression)**。依預設，群組宣告類型會設定為**篩選器 (Filter)**。

k **群組宣告運算式 (Groups claim expression)** 文字方塊中，輸入將在 Token 中使用的宣告名稱，以及評估 Token 的 Okta 輸入運算式陳述式。

l 按一下**儲存 (Save)**。

應用程式會設定於 IDP 中。您可以將使用者群組和使用者指派給 SD-WAN Orchestrator 應用程式。



3 若要將群組和使用者指派給 SD-WAN Orchestrator 應用程式：

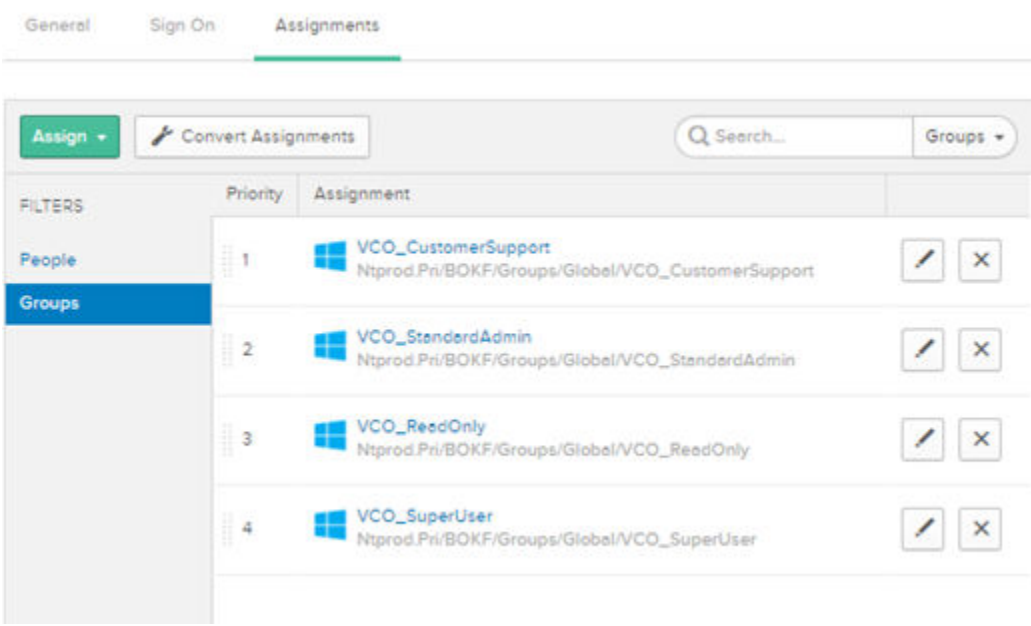
a 移至**應用程式 (Application)** > **應用程式 (Applications)**，然後按一下 SD-WAN Orchestrator 應用程式連結。

b 在**指派 (Assignments)** 索引標籤上，從**指派 (Assign)** 下拉式功能表中選取**指派給群組 (Assign to Groups)** 或**指派給人員 (Assign to People)**。

將 <應用程式名稱> 指派給群組 (Assign <Application Name> to Groups) 或**將 <應用程式名稱> 指派給人員 (Assign <Application Name> to People)** 對話方塊隨即出現。

c 按一下您想要為其指派 SD-WAN Orchestrator 應用程式之可用使用者群組或使用者旁邊的**指派 (Assign)**，然後按一下**完成 (Done)**。

指派給 SD-WAN Orchestrator 應用程式的使用者或使用者群組將會顯示。



結果

您已完成在 Okta 中設定以 OIDC 為基礎的應用程式以用於 SSO 的作業。

後續步驟

在 SD-WAN Orchestrator 中設定單一登入。

在 Okta 中建立新的使用者群組

若要建立新的使用者群組，請執行此程序的步驟。

程序

1 按一下**目錄 (Directory)** > **群組 (Groups)**。

2 按一下**新增群組 (Add Group)**。

新增群組 (Add Group) 對話方塊隨即出現。

3 輸入群組的群組名稱和說明，然後按一下**儲存 (Save)**。

在 Okta 中建立新的使用者

若要新增使用者，請執行此程序的步驟。

程序

1 按一下**目錄 (Directory)** > **人員 (People)**。

2 按一下**新增人員 (Add Person)**。

新增人員 (Add Person) 對話方塊隨即出現。

3 輸入所有必要詳細資料，例如使用者的名字、姓氏和電子郵件識別碼。

4 如果您想要設定密碼，請在**密碼 (Password)** 下拉式功能表中選取**由使用者設定 (Set by user)**，然後啟用**立即將啟用電子郵件傳送給使用者 (Send user activation email now)**。

5 按一下**儲存 (Save)**。

啟用連結電子郵件將傳送至您的電子郵件識別碼。按一下電子郵件中的連結，即可啟動您的 Okta 使用者帳戶。

設定 OneLogin 的單一登入

若要在 OneLogin 中設定單一登入 (SSO) 的 OpenID Connect (OIDC) 型應用程式，請執行此程序的步驟。

必要條件

請確定您有 OneLogin 帳戶可進行登入。

程序

1 以管理員使用者身分登入您的 OneLogin 帳戶。

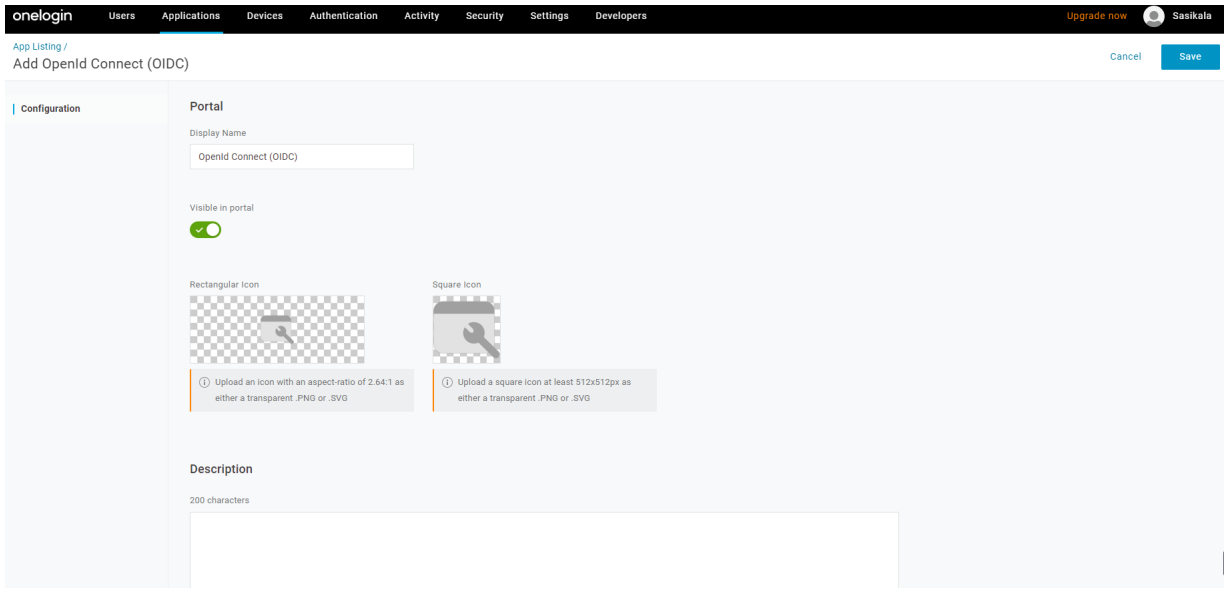
OneLogin 主畫面隨即出現。

2 若要建立新的應用程式：

a 在上方導覽列中，按一下**應用程式 (Apps)** > **新增應用程式 (Add Apps)**。

b 在**尋找應用程式 (Find Applications)** 文字方塊中，搜尋「OpenId Connect」或「oidc」，然後選取 **OpenId Connect (OIDC)** 應用程式。

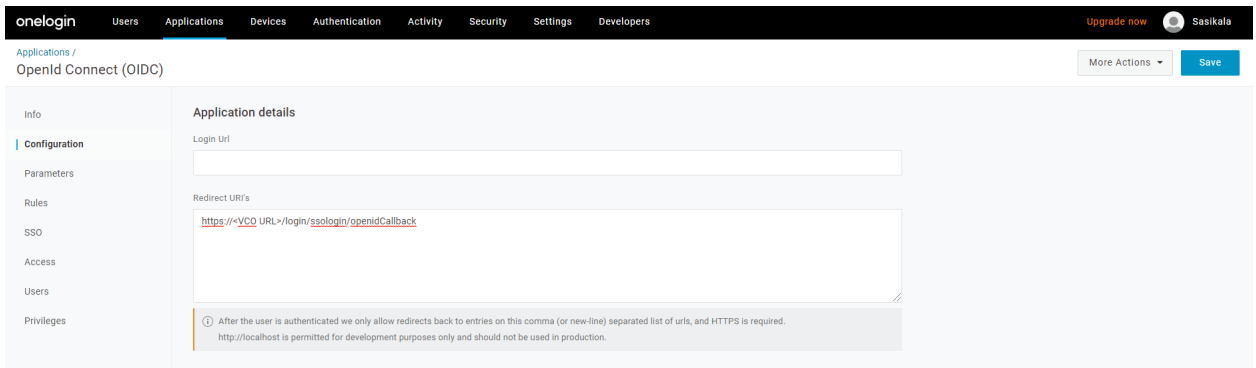
新增 OpenId Connect (OIDC) 畫面隨即出現。



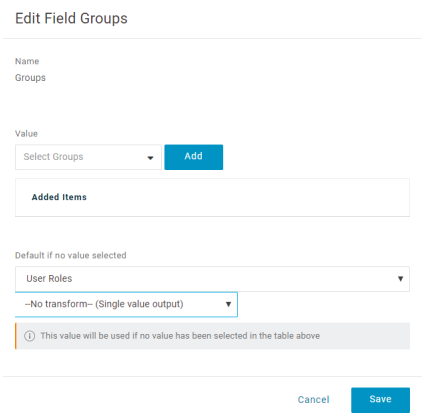
c 在**顯示名稱 (Display Name)** 文字方塊中輸入應用程式的名稱，然後按一下**儲存 (Save)**。

d 在**組態 (Configuration)** 索引標籤上，輸入 SD-WAN Orchestrator 作為回撥端點的重新導向 URI，然後按一下**儲存 (Save)**。

在 SD-WAN Orchestrator 應用程式的**驗證 (Authentication)** 畫面底部，您可以找到重新導向 URL 連結。理想情況下，SD-WAN Orchestrator 重新導向 URL 將會採用下列格式：https://<Orchestrator URL>/login/ssologin/openidCallback。



e 在**參數 (Parameters)** 索引標籤的 **OpenId Connect (OIDC)** 下，按兩下**群組 (Groups)**。**編輯欄位群組 (Edit Field Groups)** 快顯視窗隨即出現。

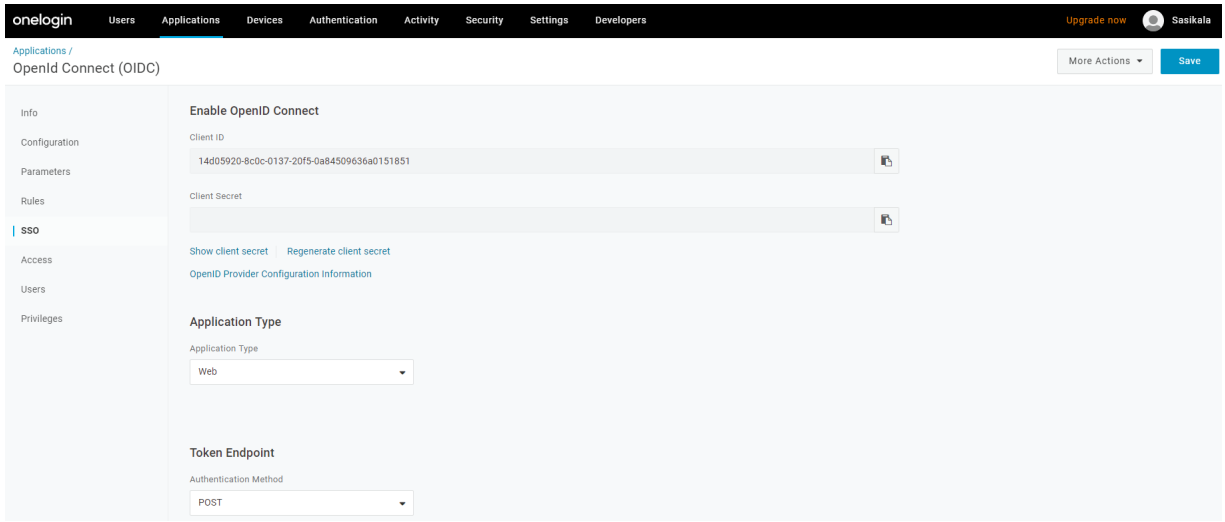


f 設定值為「--無轉換-- (單一值輸出)」的使用者角色以在群組屬性中傳送，然後按一下**儲存 (Save)**。

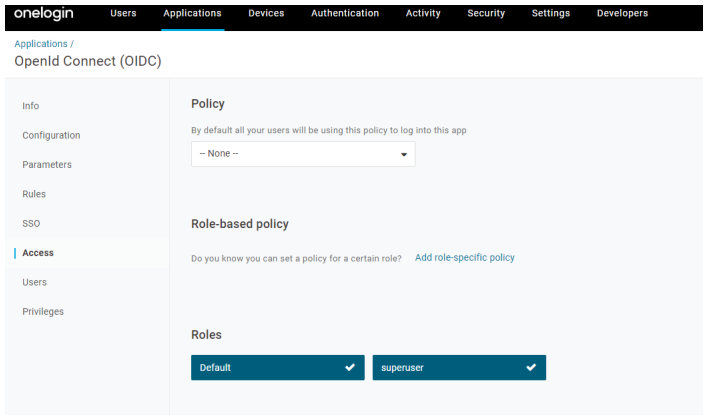
g 在 **SSO** 索引標籤上，從**應用程式類型 (Application Type)** 下拉式功能表中選取 **Web**。

h 在**驗證方法 (Authentication Method)** 下拉式功能表中選取 **POST** 作為 Token 端點，然後按一下**儲存 (Save)**。

此外，請記下 SD-WAN Orchestrator 中的 SSO 設定期間所要使用的用戶端認證 (用戶端識別碼和用戶端密碼)。



i 在**存取 (Access)** 索引標籤上選擇將可登入的角色，然後按一下**儲存 (Save)**。



3 若要將角色和使用者新增至您的 SD-WAN Orchestrator 應用程式：

a 按一下**使用者 (Users)** > **使用者 (Users)**，然後選取使用者。

b 在**應用程式 (Application)** 索引標籤上，從左側的**角色 (Role)** 下拉式功能表中，選取要對應至使用者的角色。

c 按一下**儲存使用者 (Save Users)**。

結果

您已完成在 OneLogin 中設定以 OIDC 為基礎的應用程式以用於 SSO 的作業。

後續步驟

在 SD-WAN Orchestrator 中設定單一登入。

在 OneLogin 中建立新的角色

若要建立新的角色，請執行此程序的步驟。

程序

1 按一下**使用者 (Users)** > **角色 (Role)**。

2 按一下**新增角色 (New Role)**。

3 輸入角色的名稱。

當您第一次設定角色時，**應用程式 (Applications)** 索引標籤會顯示您公司目錄中的所有應用程式。

4 按一下應用程式加以選取，然後按一下**儲存 (Save)**，將選取的應用程式新增至角色。

在 OneLogin 中建立新的使用者

若要建立新的使用者，請執行此程序的步驟。

程序

1 按一下**使用者 (Users)** > **使用者 (Users)** > **新增使用者 (New User)**。

新增使用者 (New User) 畫面隨即出現

2 輸入所有必要詳細資料，例如使用者的名字、姓氏和電子郵件識別碼，然後按一下**儲存使用者 (Save User)**。

設定 PingIdentity 的單一登入

若要在 PingIdentity 中設定單一登入 (SSO) 的 OpenID Connect (OIDC) 型應用程式，請執行此程序的步驟。

必要條件

請確定您有 PingOne 帳戶可進行登入。

備註 目前，SD-WAN Orchestrator 支援以 PingOne 作為身分識別合作夥伴 (IDP)；但您可以輕鬆設定任何支援 OIDC 的 PingIdentity 產品。

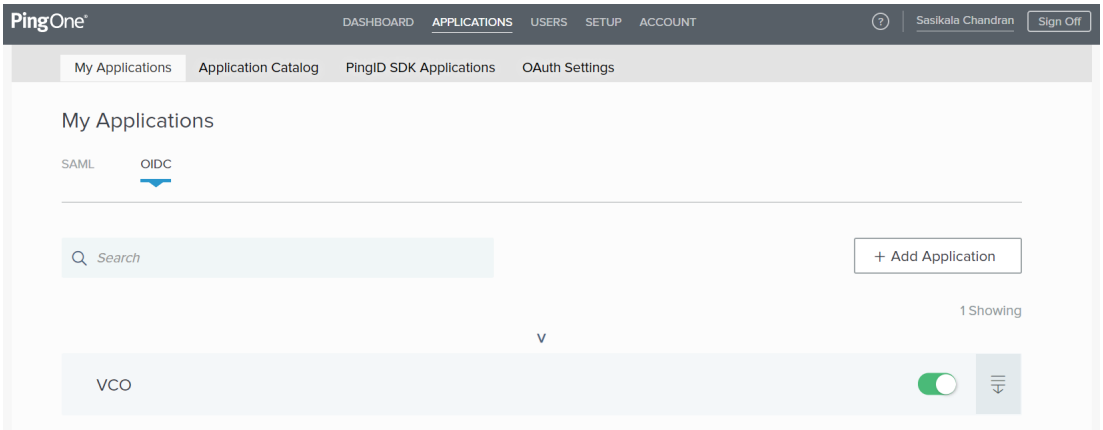
程序

1 以管理員使用者身分登入您的 PingOne 帳戶。

PingOne 主畫面隨即出現。

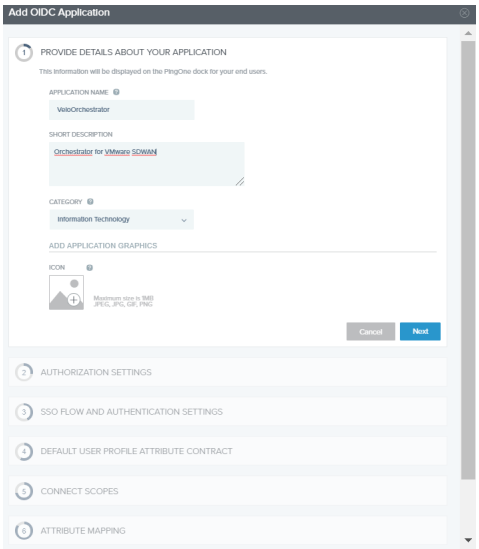
2 若要建立新的應用程式：

a 在上方導覽列中，按一下**應用程式 (Applications)**。



b 在**我的應用程式 (My Applications)** 索引標籤上選取 OIDC，然後按一下**新增應用程式 (Add Application)**。

新增 OIDC 應用程式 (Add OIDC Application) 快顯視窗隨即出現。



c 提供應用程式的名稱、簡短說明和類別等基本詳細資料，然後按**下一步 (Next)**。

d 在**授權設定 (AUTHORIZATION SETTINGS)** 下，選取**授權碼 (Authorization Code)** 作為允許的授與類型，然後按**下一步 (Next)**。

此外，請記下 SD-WAN Orchestrator 中的 SSO 設定期間所要使用的探索 URL 和用戶端認證 (用戶端識別碼和用戶端密碼)。

e 在 **SSO 流程和驗證設定 (SSO FLOW AND AUTHENTICATION SETTINGS)** 下，提供起始 SSO URL 和重新導向 URL 的有效值，然後按**下一步 (Next)**。

在 SD-WAN Orchestrator 應用程式的**設定驗證 (Configure Authentication)** 畫面底部，您可以找到重新導向 URL 連結。理想情況下，SD-WAN Orchestrator 重新導向 URL 將會採用下列格式：https://<Orchestrator URL>/login/ssologin/openidCallback。起始 SSO URL 將採用以下格式：https://<Orchestrator URL>/<domain name>/login/doEnterpriseSsoLogin。

f 在**預設的使用者設定檔屬性合約 (DEFAULT USER PROFILE ATTRIBUTE CONTRACT)** 下，按一下**新增屬性 (Add Attribute)**，以新增其他使用者設定檔屬性。

g 在**屬性名稱 (Attribute Name)** 文字方塊中輸入 *group_membership*，並選取**必要 (Required)** 核取方塊，然後選取**下一步 (Next)**。

備註 必須要有 *group_membership* 屬性才能從 PingOne 擷取角色。

h 在**連線範圍 (CONNECT SCOPES)** 下，選取在驗證期間可為 SD-WAN Orchestrator 應用程式要求的範圍，然後按**下一步 (Next)**。

i 在**屬性對應 (Attribute Mapping)** 下，將您的身分識別存放庫屬性對應至 SD-WAN Orchestrator 應用程式可用的宣告。

備註 要讓整合正常運作所需的最低對應為 email、given_name、family_name、phone_number、sub 和 group_membership (對應至 memberOf)。

j 在**群組存取 (Group Access)** 下，選取應可存取 SD-WAN Orchestrator 應用程式的所有使用者群組，然後按一下**完成 (Done)**。

應用程式將新增至您的帳戶，且將在**我的應用程式 (My Application)** 畫面中提供。

結果

您已完成在 PingOne 中設定以 OIDC 為基礎的應用程式以用於 SSO 的作業。

後續步驟

在 SD-WAN Orchestrator 中設定單一登入。

在 PingIdentity 中建立新的使用者群組

若要建立新的使用者群組，請執行此程序的步驟。

程序

1 按一下**使用者 (Users)** > **使用者目錄 (User Directory)**。

2 在**群組 (Groups)** 索引標籤上，按一下**新增群組 (Add Group)**

新增群組 (New Group) 畫面隨即出現。

3 在**名稱 (Name)** 文字方塊中，輸入群組的名稱，然後按一下**儲存 (Save)**。

在 PingIdentity 中建立新的使用者

若要新增使用者，請執行此程序的步驟。

程序

1 按一下**使用者 (Users)** > **使用者目錄 (User Directory)**。

2 在**使用者 (Users)** 索引標籤上，按一下**新增使用者 (Add Users)** 下拉式功能表，然後選取**建立新的使用者 (Create New User)**。

使用者 (User) 畫面隨即出現。

3 輸入所有必要詳細資料，例如使用者的使用者名稱、密碼和電子郵件識別碼。

4 在**群組成員資格 (Group Memberships)** 下，按一下**新增 (Add)**。

新增群組成員資格 (Add Group Membership) 快顯視窗隨即出現。

5 搜尋使用者並將其新增至群組，然後按一下**儲存 (Save)**。

設定單一登入的 Azure Active Directory

若要在 Microsoft Azure Active Directory (AzureAD) 中設定單一登入 (SSO) 的 OpenID Connect (OIDC) 型應用程式，請執行此程序的步驟。

必要條件

請確定您有 AzureAD 帳戶可進行登入。

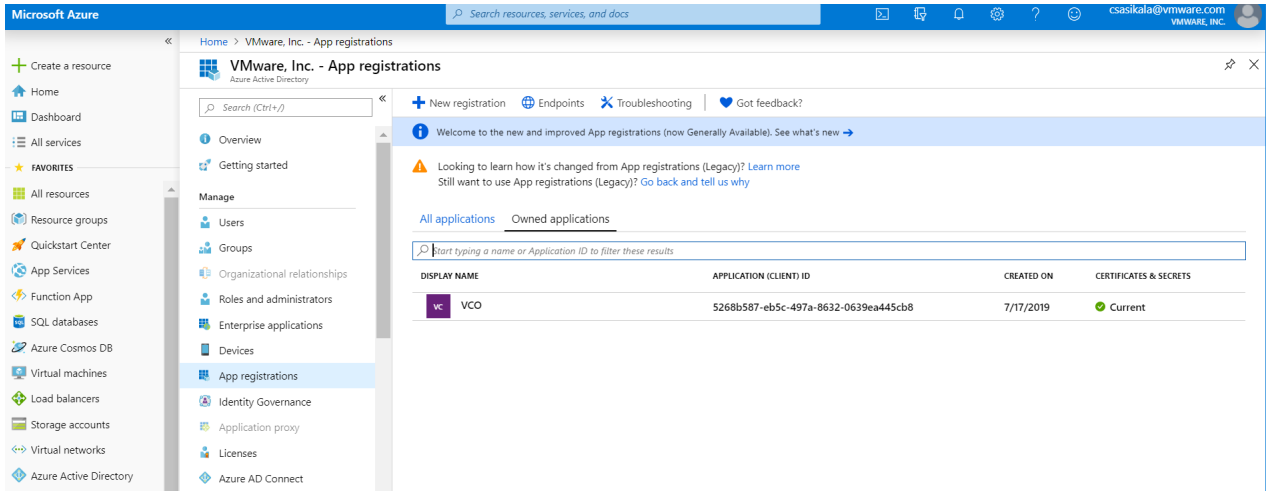
程序

1 以管理員使用者身分登入您的 Microsoft Azure 帳戶。

Microsoft Azure 主畫面隨即出現。

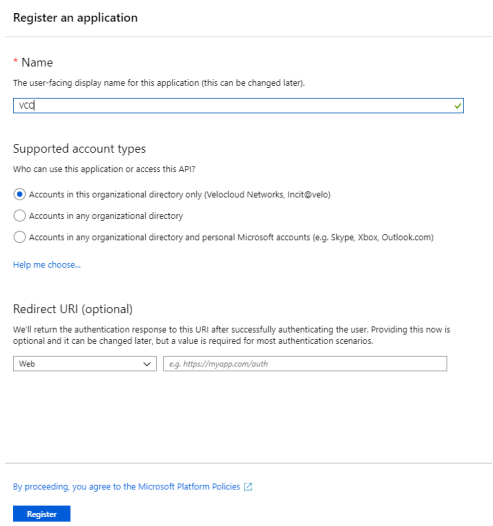
2 若要建立新的應用程式：

a 搜尋並選取 **Azure Active Directory** 服務。



b 移至**應用程式登錄 (App registration)** > **新增登錄 (New registration)**。

登錄應用程式 (Register an application) 畫面隨即出現。



c 在**名稱 (Name)** 欄位中，輸入 SD-WAN Orchestrator 應用程式的名稱。

d 在**重新導向 URL (Redirect URL)** 欄位中，輸入 SD-WAN Orchestrator 應用程式作為回撥端點的重新導向 URL。

在 SD-WAN Orchestrator 應用程式的**設定驗證 (Configure Authentication)** 畫面底部，您可以找到重新導向 URL 連結。理想情況下，SD-WAN Orchestrator 重新導向 URL 將會採用下列格式：https://<Orchestrator URL>/login/ssologin/openidCallback。

e 按一下**登錄 (Register)**。

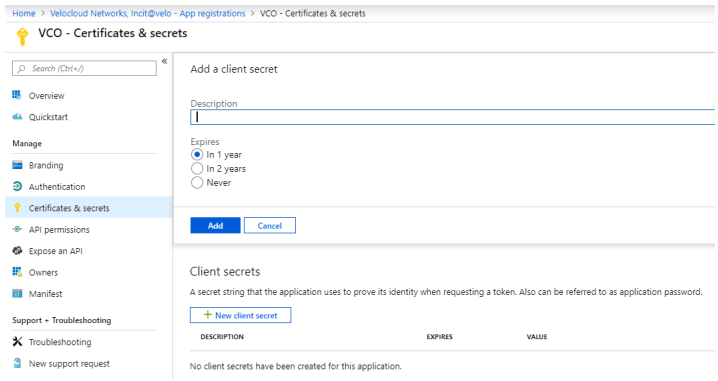
您的 SD-WAN Orchestrator 應用程式將登錄並顯示在**所有應用程式 (All applications)** 和**擁有的應用程式 (Owned applications)** 索引標籤中。請務必記下在 SD-WAN Orchestrator 中 SSO 設定期間所要使用的用戶端識別碼/應用程式識別碼。

f 按一下**端點 (Endpoints)**，然後複製在 SD-WAN Orchestrator 中 SSO 設定期間所要使用的已知 OIDC 組態 URL。

g 若要為 SD-WAN Orchestrator 應用程式建立用戶端密碼，請在**擁有的應用程式 (Owned Applications)** 索引標籤上，按一下您的 SD-WAN Orchestrator 應用程式。

h 移至**憑證和密碼 (Certificates & secrets)** > **新增用戶端密碼 (New client secret)**。

新增用戶端密碼 (Add a client secret) 畫面隨即出現。

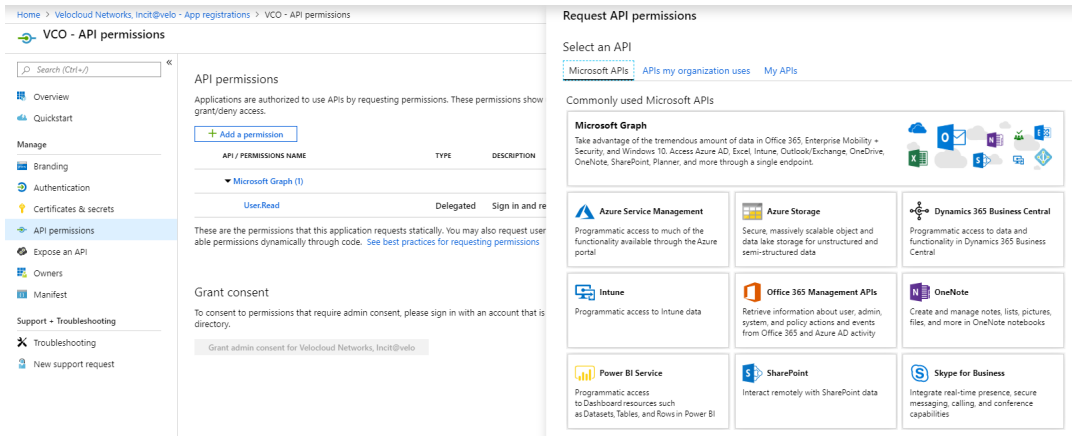


i 提供密碼的說明和到期值等詳細資料，然後按一下**新增 (Add)**。

系統會為應用程式建立用戶端密碼。請記下在 SD-WAN Orchestrator 中 SSO 設定期間所要使用的新用戶端密碼值。

j 若要設定 SD-WAN Orchestrator 應用程式的權限，請按一下您的 SD-WAN Orchestrator 應用程式，然後移至 **API 權限 (API permissions)** > **新增權限 (Add a permission)**。

要求 API 權限 (Request API permissions) 畫面隨即出現。



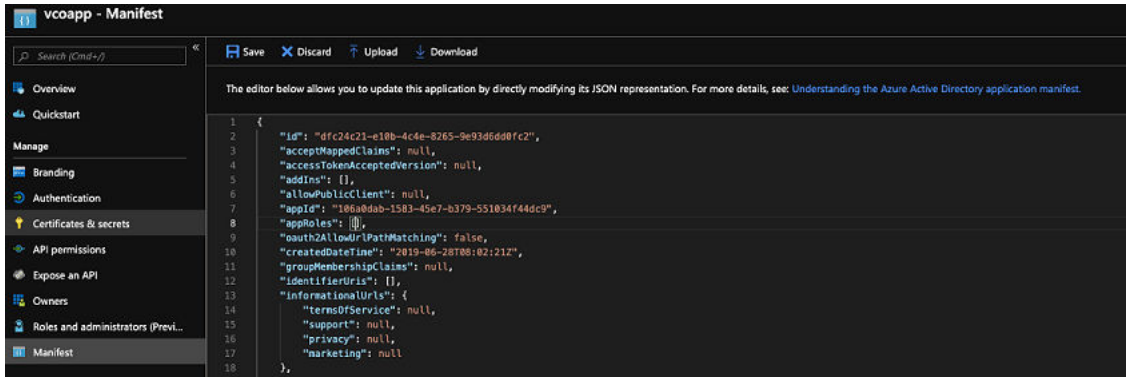
k 按一下 **Microsoft Graph**，然後選取**應用程式權限 (Application permissions)** 作為應用程式的權限類型。

l 在**選取權限 (Select permissions)** 下，從**目錄 (Directory)** 下拉式功能表中選取 **Directory.Read.All**，然後從**使用者 (User)** 下拉式功能表中選取 **User.Read.All**。

m 按一下**新增權限 (Add permissions)**。

- 若要在資訊清單中新增和儲存角色，請按一下 SD-WAN Orchestrator 應用程式，然後在應用程式的**概觀 (Overview)** 畫面中，按一下**資訊清單 (Manifest)**。

  此時會開啟以 Web 為基礎的資訊清單編輯器，可讓您在入口網站內編輯資訊清單。您可以選擇性地選取**下載 (Download)** 以在本機編輯資訊清單，然後使用**上傳 (Upload)** 將其重新套用至應用程式。



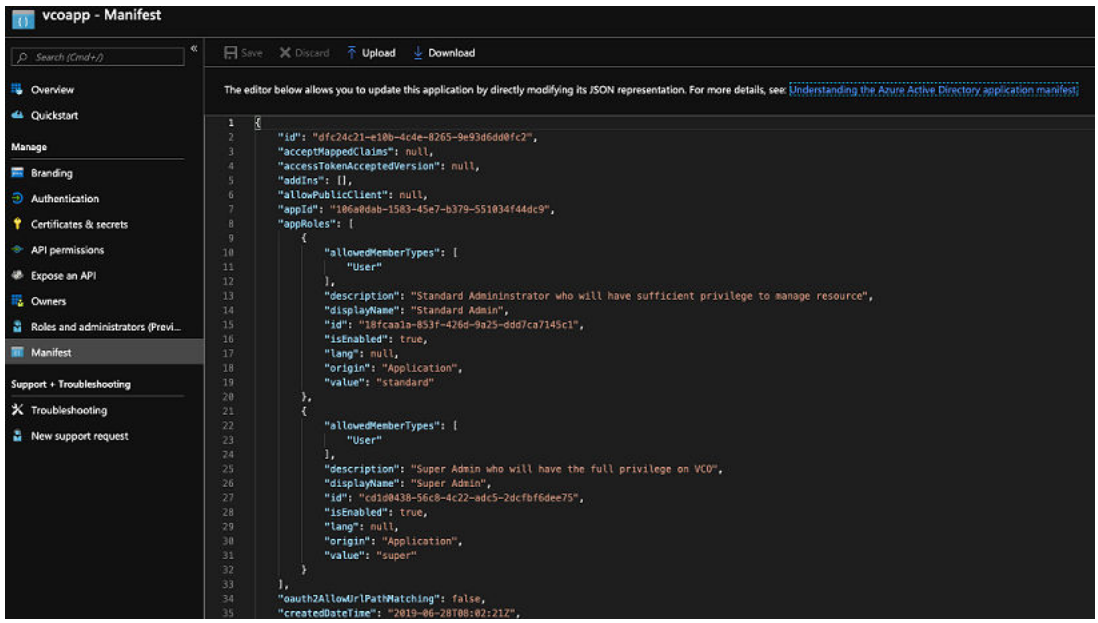
- 在資訊清單中搜尋 `appRoles` 陣列，並新增一或多個角色物件 (如下列範例所示)，然後按一下**儲存 (Save)**。

  範例角色物件

```
{
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Standard Administrator who will have sufficient privilege
to manage resource",
            "displayName": "Standard Admin",
            "id": "18fcaa1a-853f-426d-9a25-ddd7ca7145c1",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "standard"
        },
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Super Admin who will have the full privilege on SD-WAN
Orchestrator",
            "displayName": "Super Admin",
            "id": "cd1d0438-56c8-4c22-adc5-2dcfbf6dee75",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "superuser"
        }
```

備註 請確定已將 `id` 設為新產生的全域唯一識別碼 (Global Unique Identifier, GUID) 值。您可以使用 Web 型工具 (例如，https://www.guidgen.com/) 或執行以下命令，在線上產生 GUID：

- Linux/OSX - `uuidgen`
- Windows - `powershell [guid]::NewGuid()`



3 若要將群組和使用者指派給 SD-WAN Orchestrator 應用程式：

a 移至 **Azure Active Directory** > **企業應用程式 (Enterprise applications)**。

b 搜尋並選取您的 SD-WAN Orchestrator 應用程式。

c 按一下**使用者和群組 (Users and groups)**，然後將使用者和群組指派給應用程式。

d 按一下**提交 (Submit)**。

結果

您已完成在 AzureAD 中設定以 OIDC 為基礎的應用程式以進行 SSO 的作業。

後續步驟

在 SD-WAN Orchestrator 中設定單一登入。

在 AzureAD 中建立新的客體使用者

若要建立新的客體使用者，請執行此程序的步驟。

程序

1 移至 **Azure Active Directory** > **使用者 (Users)** > **所有使用者 (All users)**。

2 按一下**新增客體使用者 (New guest user)**。

新增客體使用者 (New Guest User) 快顯視窗隨即出現。

3 在**電子郵件地址 (Email address)** 文字方塊中，輸入客體使用者的電子郵件地址，然後按一下**邀請 (Invite)**。

客體使用者會立即收到可自訂的邀請，讓他們能夠登入其存取面板。

4 目錄中的客體使用者可指派給應用程式或群組。

設定單一登入的 VMware CSP

若要設定單一登入 (SSO) 的 VMware Cloud Services Platform (CSP)，請執行此程序的步驟。

必要條件

使用您的 VMware 帳戶識別碼登入 VMware CSP 主控台 (預備或生產環境)。如果您開始接觸 VMware Cloud，且沒有 VMware 帳戶，則可以在註冊時建立一個。如需詳細資訊，請參閱使用 VMware Cloud 說明文件中的〈如何註冊 VMware CSP〉一節。

程序

1 請連絡 VMware 支援提供者，以取得向 VMware CSP 登錄 SD-WAN Orchestrator 應用程式的服務邀請 URL 連結。如需如何聯絡支援提供者的相關資訊，請參閱 https://kb.vmware.com/s/article/53907 和 https://www.vmware.com/support/contacts/us_support.html。

VMware 支援提供者將會建立和共用：

- 需要兌換給客戶組織的服務邀請 URL
- 用於 Orchestrator 中角色對應的服務定義 UUID 和服務角色名稱

2 請依照 UI 畫面中的步驟，將服務邀請 URL 兌換給您現有的客戶組織，或建立新的客戶組織。

您必須是組織擁有者，才能將服務邀請 URL 兌換給您現有的客戶組織。

3 兌換服務邀請後，當您登入 VMware CSP 主控台時，您可以在 **VMware Cloud Services** 頁面中的**我的服務 (My Services)** 區域下檢視應用程式動態磚。

您登入的組織會顯示在功能表列上的使用者名稱下。請按一下您的使用者名稱以記下組織識別碼，以便在 Orchestrator 設定期間使用。組織名稱下方會顯示縮短版本的識別碼。按一下識別碼以顯示完整的組織識別碼。

4 登入 VMware CSP 主控台，並建立 OAuth 應用程式。如需步驟，請參閱使用適用於 Web 應用程式的 OAuth 2.0。請務必將重新導向 URI 設定為在 Orchestrator 的**設定驗證 (Configure Authentication)** 畫面中顯示的 URL。

在 VMware CSP 主控台中建立 OAuth 應用程式後，請記下 IDP 整合詳細資料，例如用戶端識別碼和用戶端密碼。在 Orchestrator 中設定 SSO 時將需要這些詳細資料。

5 以超級管理員使用者身分登入 SD-WAN Orchestrator 應用程式，並使用 IDP 整合詳細資料設定 SSO，如下所示。

a 按一下**管理 (Administration)** > **系統設定 (System Settings)**

系統設定 (System Settings) 畫面隨即出現。

b 按一下**一般資訊 (General Information)** 索引標籤，然後在**網域 (Domain)** 文字方塊中，輸入企業的網域名稱 (如果尚未設定)。

備註 若要為 SD-WAN Orchestrator 啟用 SSO 驗證，您必須設定企業的網域名稱。

c 按一下**驗證 (Authentication)** 索引標籤，然後從**驗證模式 (Authentication Mode)** 下拉式功能表中，選取 **SSO**。

d 在**身分識別提供者範本 (Identity Provider template)** 下拉式功能表中，選取 **VMwareCSP**。

e 在**組織識別碼 (Organization Id)** 文字方塊中，以下列格式輸入 (您在步驟 3 中記下的) 組織識別碼：/csp/gateway/am/api/orgs/<full organization ID>。

f 在 **OIDC 知名組態 URL (OIDC well-known config URL)** 文字方塊中，輸入 IDP 的 OpenID Connect (OIDC) 組態 URL (https://console.cloud.vmware.com/csp/gateway/am/api/.well-known/openid-configuration)。

SD-WAN Orchestrator 應用程式會自動填入 IDP 的端點詳細資料，例如簽發人、授權端點、Token 端點及使用者資訊端點。

g 在**用戶端識別碼 (Client Id)** 文字方塊中，輸入您在 OAuth 應用程式建立步驟中記下的用戶端識別碼。

h 在**用戶端密碼 (Client Secret)** 文字方塊中，輸入您在 OAuth 應用程式建立步驟中記下的用戶端密碼。

i 若要決定使用者在 SD-WAN Orchestrator 中的角色，請選取**使用預設角色 (Use Default Role)** 或**使用身分識別提供者角色 (Use Identity Provider Roles)**。

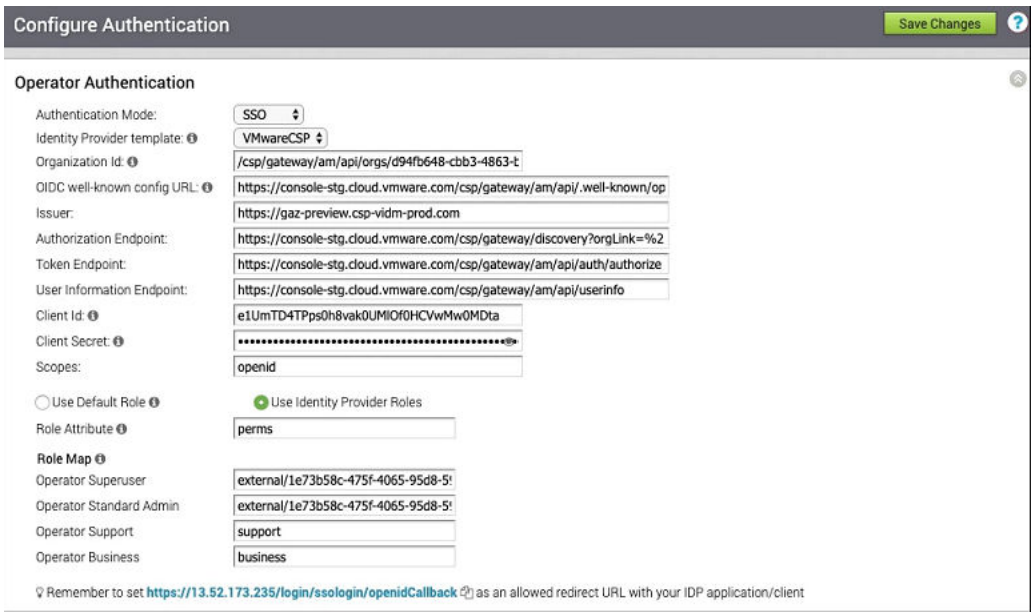
j 選取**使用身分識別提供者角色 (Use Identity Provider Roles)** 選項時，在**角色屬性 (Role Attribute)** 文字方塊中輸入 VMware CSP 中設定的屬性名稱，以傳回角色。

k 在**角色對應 (Role Map)** 區域中，將 VMwareCSP 提供的角色對應至每個 SD-WAN Orchestrator 角色，並使用逗點分隔。

VMware CSP 中的角色遵循以下格式：external/<服務定義 UUID>/<建立服務範本期間提及的服務角色名稱>。請使用您從支援提供者收到的相同服務定義 UUID 和服務角色名稱。

6 按一下**儲存變更 (Save Changes)** 以儲存 SSO 組態。

7 按一下**測試組態 (Test Configuration)**，以驗證輸入的 OpenID Connect (OIDC) 組態。



使用者會導覽至 VMware CSP 站台，並且能夠輸入認證。在 IDP 驗證和成功重新導向至 SD-WAN Orchestrator 測試回呼時，將會顯示成功驗證訊息。

結果

您已在 VMware CSP 中完成 SSO 的 SD-WAN Orchestrator 應用程式整合，並且可以存取登入 VMware CSP 主控台的 SD-WAN Orchestrator 應用程式。

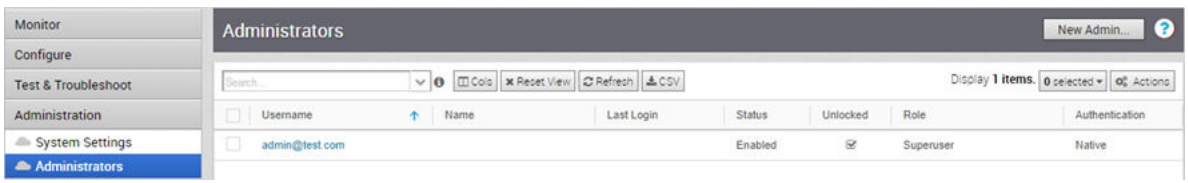
後續步驟

- 在組織內，藉由新增使用者並且為使用者指派適當的角色以管理使用者。如需詳細資訊，請參閱使用 VMware Cloud 說明文件中的〈身分識別與存取管理〉一節。

管理管理員使用者

管理員 (Administrators) 頁面會顯示現有的管理員使用者。標準管理員超級使用者和標準管理員可使用不同的角色權限建立新的管理員使用者，並為每個管理員使用者設定 API Token。

在企業入口網站中，按一下**管理 (Administration) > 管理員 (Administrators)**。



按一下**動作 (Actions)**，以執行下列活動：

- **新增管理員 (New Admin)**：建立新的管理員使用者。請參閱建立新的管理員使用者。
- **修改管理員 (Modify Admin)**：修改所選管理員使用者的內容。您也可以按一下使用者名稱的連結以修改內容。請參閱設定管理員使用者。

- **密碼重設 (Password Reset)**：傳送電子郵件給所選的使用者，並附上重設密碼的連結。
- **刪除管理員 (Delete Admin)**：刪除所選的使用者。

建立新的管理員使用者

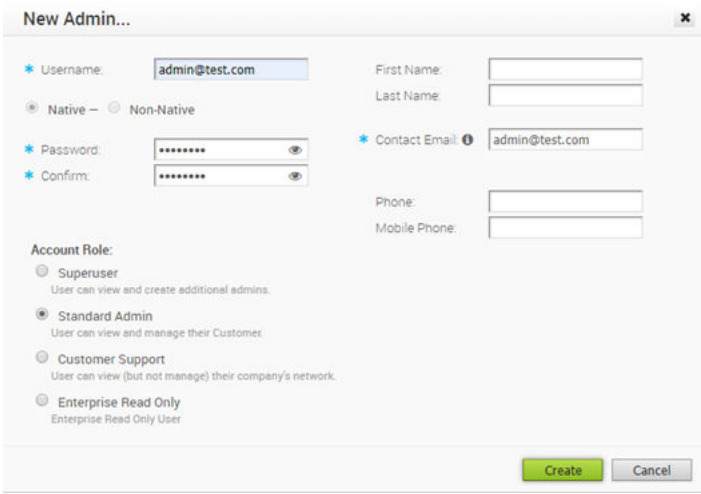
標準管理員超級使用者和標準管理員可建立新的管理員使用者。

在企業入口網站中，按一下**管理 (Administration) > 管理員 (Administrators)**。

程序

1 您可以按一下**新增管理員 (New Admin)**，或**動作 (Actions) > 新增管理員 (New Admin)**，以建立新的 Admin 使用者。

2 在**新增管理員 (New Admin)** 視窗中，輸入下列詳細資料：



a 輸入使用者詳細資料，例如：使用者名稱、密碼、名稱、電子郵件和電話號碼。使用者名稱應採用電子郵件地址格式，例如 user@example.com。密碼必須符合以下需求：

- 字元數必須在 8 到 32 的範圍內。
- 必須至少有一個小寫字元。
- 必須至少有一個數字。

b 如果您已在設定企業驗證 中選擇 [原生] (Native) 作為驗證模式，則系統會選取 [原生] (Native) 作為使用者的類型。如果您選擇不同的驗證模式，則可以選擇使用者的類型。如果您選擇使用者為 [非原生] (Non-Native)，則無法使用密碼選項，因為此選項是繼承自驗證模式。

c **帳戶角色 (Account Role)**：從可用選項中選擇使用者角色。

3 按一下**建立 (Create)**。

結果

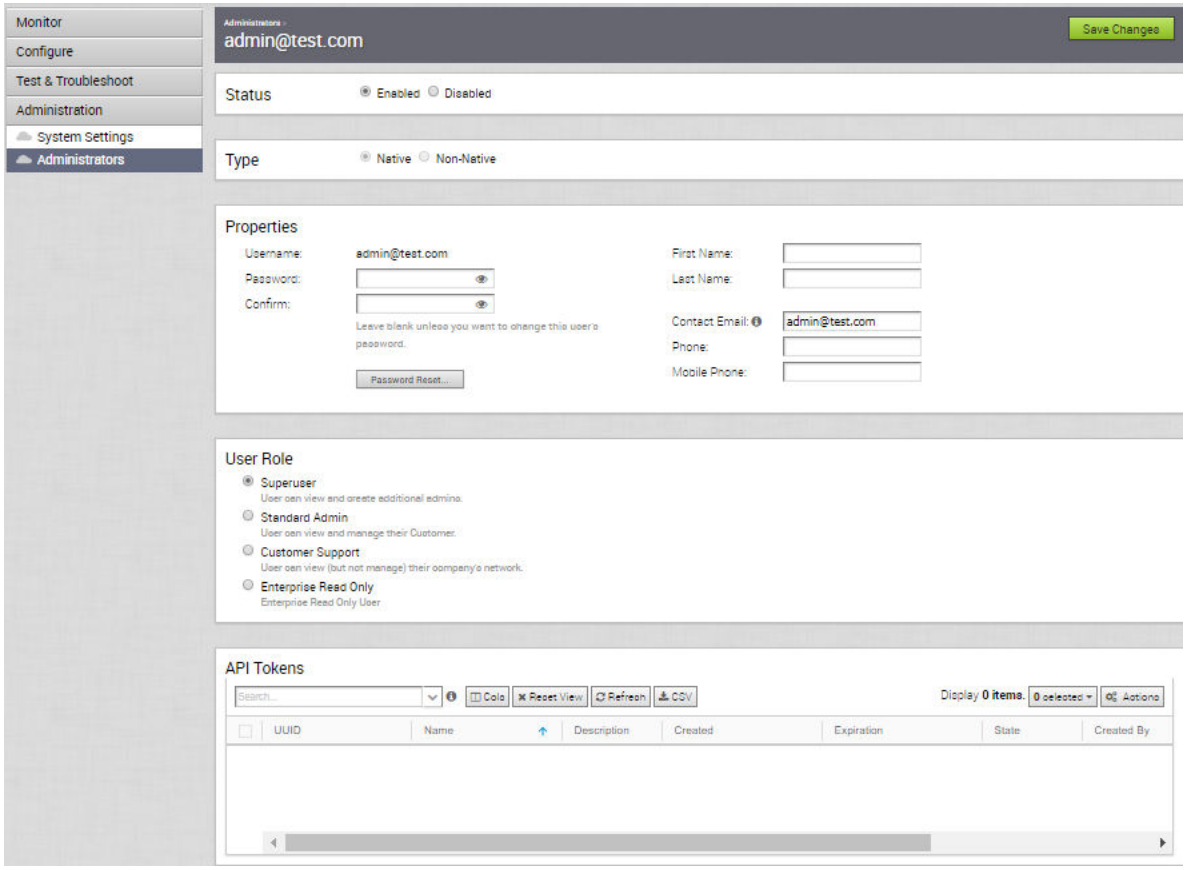
使用者詳細資料會顯示在**管理員 (Administrators)** 頁面中。

設定管理員使用者

您可以為 Admin 使用者設定其他內容並建立 API Token。

在企業入口網站中，**管理 (Administration) > 管理員 (Administrators)**。若要設定 Admin 使用者，請按一下使用者名稱的連結，或選取使用者並按一下**動作 (Actions) > 修改管理員 (Modify Admin)**。

系統會顯示所選使用者的現有內容，如有需要，您可以新增或修改下列項目：



狀態 (Status)

依預設，狀態處於**已啟用 (Enabled)** 狀態。如果您選擇**已停用 (Disabled)**，則使用者會登出所有作用中工作階段。

類型 (Type)

如果您已在設定企業驗證中選擇**原生 (Native)** 作為驗證模式，則系統會選取**原生 (Native)** 作為使用者的類型。如果您選擇不同的驗證模式，則可以選擇使用者的類型。如果您選擇使用者為**非原生 (Non-Native)**，則無法重設密碼或修改使用者角色。

Properties (內容)

顯示使用者的現有連絡詳細資料。如有需要，您可以修改詳細資料並選擇重設密碼。如果您按一下**密碼重設 (Password Reset)**，則會傳送電子郵件給使用者，並附上重設密碼的連結。

角色 (Role)

顯示現有的使用者角色類型。如有需要，您可以為使用者選擇不同的角色。角色權限會相應地變更。

API Token

使用者可以使用 Token (而非工作階段型驗證) 來存取 Orchestrator API。身為操作員超級使用者，您可以管理客戶的 API Token。您可以為使用者建立多個 API Token。

對於企業唯讀使用者和 MSP 商務專員使用者時不會啟用 Token 型驗證。

設定 API Token (Configure API Tokens)

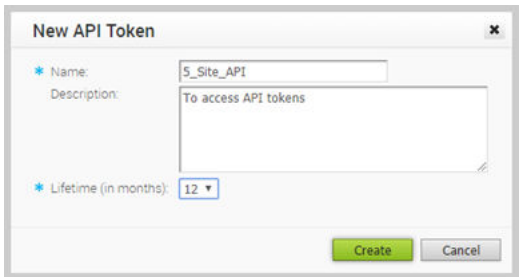
任何使用者都可以根據其使用者角色獲指派的權限來建立 Token，但企業唯讀使用者和 MSP 商務專員使用者除外。

使用者可根據其角色執行下列動作：

- 企業使用者可以為自己建立、下載和撤銷 Token。
- 如果企業使用者已將使用者權限委派給操作員，則操作員超級使用者可管理其他操作員使用者和企業使用者的 Token。
- 企業超級使用者可管理該企業內所有使用者的 Token。
- 使用者只能下載自己的 Token，無法下載其他使用者的 Token。
- 超級使用者僅能為其他使用者建立和撤銷 Token。

若要管理 API Token：

- 在 **API Token** 區段中，按一下**動作 (Actions) > 新增 API Token (New API Token)**，以建立新的 Token。
- 在**新增 API Token (New API Token)** 視窗中，輸入 Token 的**名稱 (Name)** 和**說明 (Description)**，然後從下拉式功能表中選取**存留時間 (Lifetime)**。



- 按一下**建立 (Create)**，新 Token 會顯示在 **API Token** 網格中。
- 一開始，Token 的狀態會顯示為**擱置中 (Pending)**。若要下載 Token，請選取 Token，然後按一下**動作 (Actions) > 下載 API Token (Download API Token)**。狀態會變更為**已啟用 (Enabled)**，這表示 API Token 可用於 API 存取。
- 若要停用 Token，請選取 Token，然後按一下**動作 (Actions) > 撤銷 API Token (Revoke API Token)**。Token 的狀態會顯示為**已撤銷 (Revoked)**。
- 當 Token 的存留期結束時，狀態會變更為**已到期 (Expired)** 狀態。

只有與 Token 相關聯的使用者能夠下載 Token，而在下載後，系統僅會顯示 Token 的識別碼。一個 Token 只能下載一次。

下載 Token 後，使用者可以在要求的授權標頭中傳送 Token 存取 Orchestrator API。

下列範例顯示用來存取 API 的範例程式碼片段。

```
curl -k -H "Authorization: Token <Token>"
  -X POST https://vco/portal/
  -d '{ "id": 1, "jsonrpc": "2.0", "method": "enterprise/getEnterpriseUsers", "params":
{ "enterpriseId": 1 }}'
```

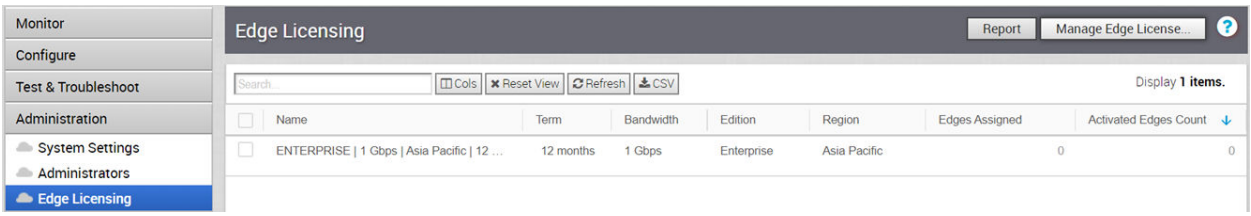
修改設定和 API Token 後，按一下**儲存變更 (Save Changes)**。

Edge 授權

SD-WAN Orchestrator 為 Edge 提供不同類型的授權。標準管理員超級使用者、標準管理員、商務專員和客戶支援使用者可以檢視及產生指派給他們之授權的報告。

在企業入口網站中，按一下**管理 (Administration) > Edge 授權 (Edge Licensing)**。

備註 只有在操作員已啟用 Edge 授權並將授權指派給企業客戶時，才能使用 **Edge 授權 (Edge Licensing)** 索引標籤。



按一下**報告 (Report)**，以 MS Excel 格式產生授權與相關聯 Edge 的報告。

若要將授權指派給 Edge：

- 在企業入口網站中，按一下**設定 (Configure) > Edge**。
- 若要將授權指派給每個 Edge，請按一下 Edge 的連結，然後在 **Edge 概觀 (Edge Overview)** 頁面中選取授權。您也可以選取 Edge，然後按一下**動作 (Actions) > 指派 Edge 授權 (Assign Edge License)** 來指派授權。
- 若要將授權指派給多個 Edge，請選取適當的 Edge，接著按一下**動作 (Actions) > 指派 Edge 授權 (Assign Edge License)**，然後選取授權。

如需詳細資訊，請參閱第 14 章 Edge 概觀索引標籤。

設定 SD-WAN Edge 高可用性

22

本節說明如何在 SD-WAN Edge 上啟用高可用性。

本章節討論下列主題：

SD-WAN Edge HA 的概觀

SD-WAN Edge 是在使用者之分支位置部署的 VMware 資料平面元件。在高可用性 (HA) 模式下設定的 SD-WAN Edges 是其彼此的鏡像映像，且會在 SD-WAN Orchestrator 上顯示為單一 SD-WAN Edge。

在 HA 模式中進行設定時，有兩個選項。

1 HA 選項 1

2 HA 選項 2

如需這兩個選項的說明，請參閱〈高可用性 (HA) 選項〉。

本文件說明要啟用高可用性 (HA)，以及將第二個 SD-WAN Edge 設為已啟用 Edge 的備用裝置時的所需步驟。

必要條件

本節說明將 SD-WAN Edge 設定為備用之前必須符合的 HA 需求。

- 兩個 SD-WAN Edges 必須是相同的型號。
- 只有一個 SD-WAN Edge 應佈建在 SD-WAN Orchestrator 上。
- 備用 SD-WAN Edge 不可有現有的組態。

高可用性選項

Edge 可安裝為單一獨立裝置，或與另一個 Edge 配對，以提供高可用性 (HA) 支援。不過，僅支援將 HA 組態用於有線 WAN 連線。

HA 選項

當您在 HA 模式下設定 Edge 時，Edge 會自動選取下列其中一個選項：

- **標準 HA (Standard HA)** – 當作用中和待命 Edge 連線至相同的 WAN 連結時，就會選取此選項。
- **增強型 HA (Enhanced HA)** – 當 Edge 連線至不同的 WAN 連結時，就會選取此選項。

以下 SD-WAN Edge 平台支援 HA 選項：510、510N、520、520v、540、610、610N、620、620N、640、640N、680、680N、840、2000、3400、3800 和虛擬 Edge。

備註 僅在相同的 SD-WAN Edge 平台型號之間支援 HA。如需 Edge 平台型號的詳細資訊，請參閱 https://sdwan.vmware.com/get-started。

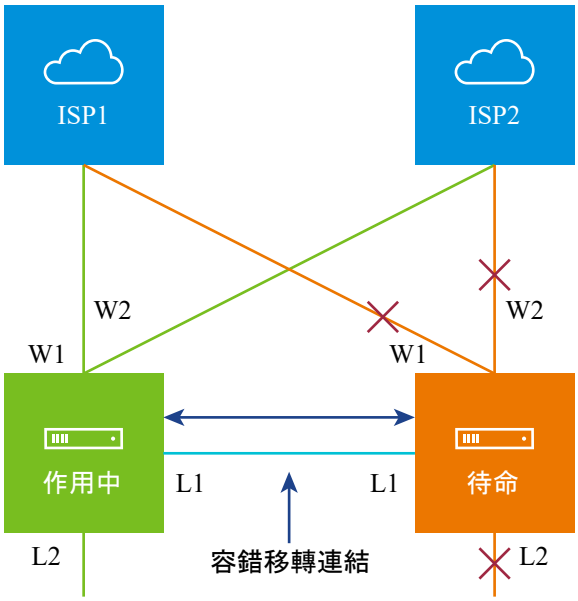
備註 在高可用性部署中，不支援混合使用支援 Wi-Fi 和不支援 Wi-Fi 的 Edge。雖然 Edge 型號 510N、610N、620N、640N 和 680N 看起來與支援 Wi-Fi 的對應型號相同，但不支援將支援 Wi-Fi 和不支援 Wi-Fi 的相同型號 Edge (例如，Edge 640 和 Edge 640N) 部署為高可用性配對。客戶應確保部署為高可用性配對的 Edge 為相同的類型：同時支援 Wi-Fi，或同時不支援 Wi-Fi。

標準 HA

本節說明標準 HA。

標準 HA 的拓撲概觀

下圖顯示標準 HA 的概念性概觀。



Edge (一個作用中，一個待命) 透過 L1 連接埠連線，以建立容錯移轉連結。待命 SD-WAN Edge 會封鎖 L1 連接埠以外的所有連接埠，使其無法用於容錯移轉連結。

標準 HA 的必要條件

- 下列組態說明中的 LAN 端交換器必須具有 STP 功能，並且設定了 STP。
- 此外，SD-WAN Edge LAN 和 WAN 連接埠必須連線至不同的 L2 交換器。如果有必要將連接埠連線至相同的交換器，則必須隔離 LAN 和 WAN 連接埠。
- 兩個 SD-WAN Edges 必須具有鏡像實體 WAN 和 LAN 連線。

標準 HA 的部署類型

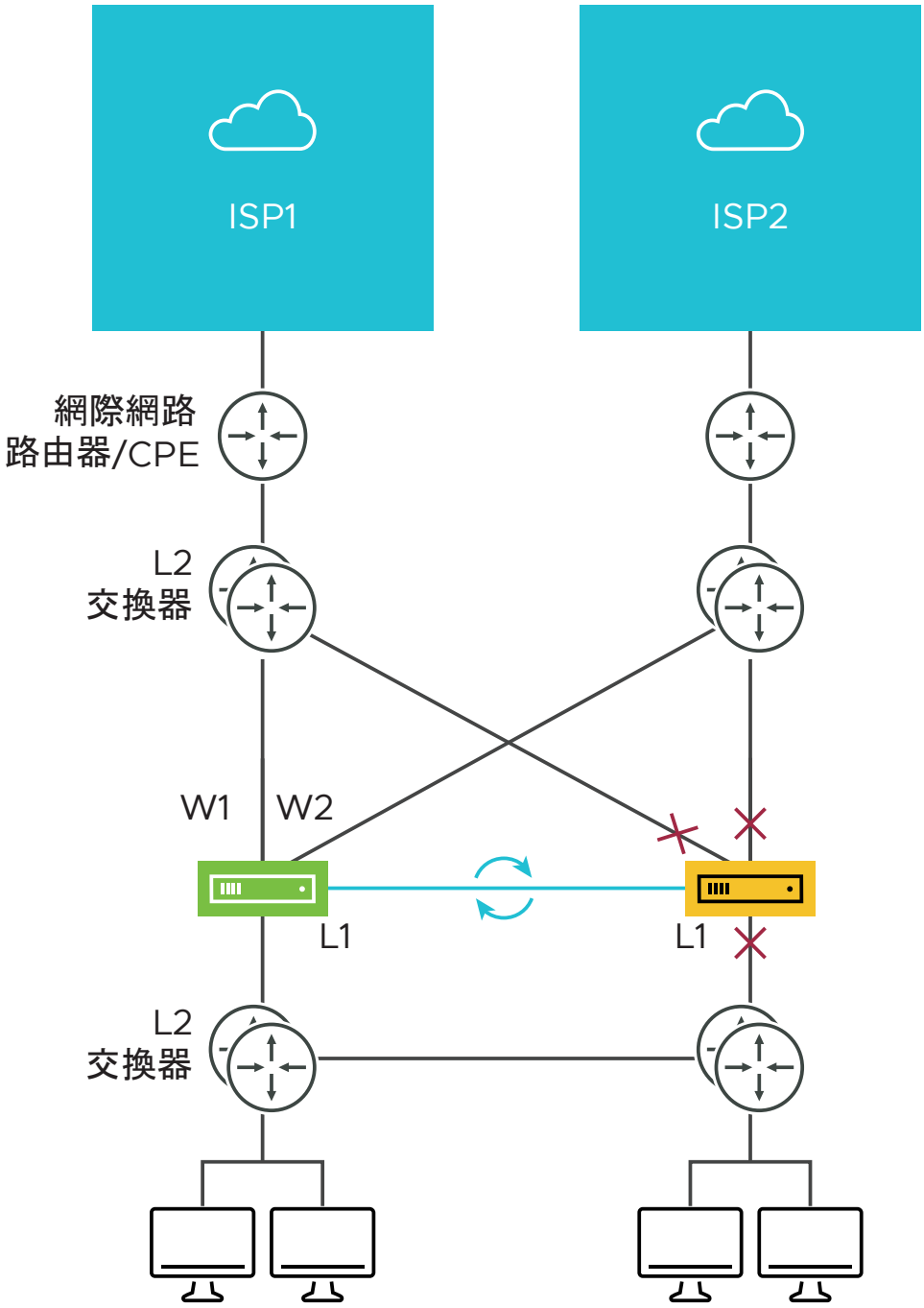
標準 HA 有兩種可能的部署類型：

- 部署類型 1：使用 L2 交換器的高可用性 (HA)
- 部署類型 2：使用 L2 和 L3 交換器的高可用性 (HA)

以下幾節將說明這兩種部署類型。

部署類型 1：使用 L2 交換器的 HA

下圖顯示僅使用 L2 交換器的網路連線。



W1 和 W2 是 WAN 連線，用來連線至 L2 交換器，以為兩個 ISP 提供 WAN 連線性。L1 連結會將兩個 SD-WAN Edges 連線，並用於「保持運作」，以及 HA 支援所需 SD-WAN Edges 之間的相互通訊。SD-WAN Edge 的 LAN 連線可用來連線至存取層 L2 交換器。

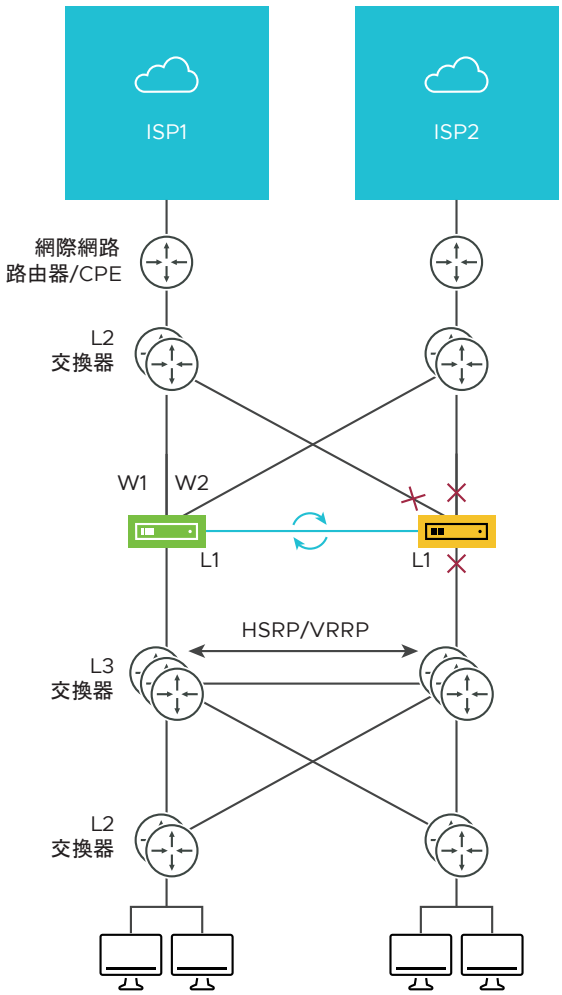
使用 L2 交換器的 HA 部署考量事項

- 相同的 ISP 連結必須連線至兩個 Edge 上的相同連接埠。
- 使用 L2 交換器可讓相同的 ISP 連結同時可供兩個 Edge 使用。

- 待命 SD-WAN Edge 不會封鎖除容錯移轉連結 (L1 連接埠) 以外的所有連接埠，因此不會干擾到任何流量。
- 工作階段資訊會透過容錯移轉連結，在作用中和待命 SD-WAN Edges 之間同步。
- 作用中 Edge 在偵測到 LAN 連結遺失時，它也會容錯移轉至待命 Edge (如果它有主動 LAN 連結)。

部署類型 2：使用 L2 和 L3 交換器的 HA

下圖顯示使用 L2 和 L3 交換器的網路連線。



SD-WAN Edge WAN 連線 (W1-stvc 和為) 用來連線至 L2 交換器，以分別提供與 ISP1 和 ISP2 的 WAN 連線。SD-WAN Edges 上的 L1 連線用來提供 HA 支援所需的容錯移轉連結。VMware Edge LAN 連線用來連線已連接數個使用者裝置 L2 交換器。

使用 L2 和 L3 交換器的 HA 部署考量事項

- L3 交換器配對必須要有 HSRP/VRRP。
- SD-WAN Edge 的靜態路由會指向 L3 交換器的 HSRP VIP，作為下一個躍點以到達 L2 交換器後方的終點站。

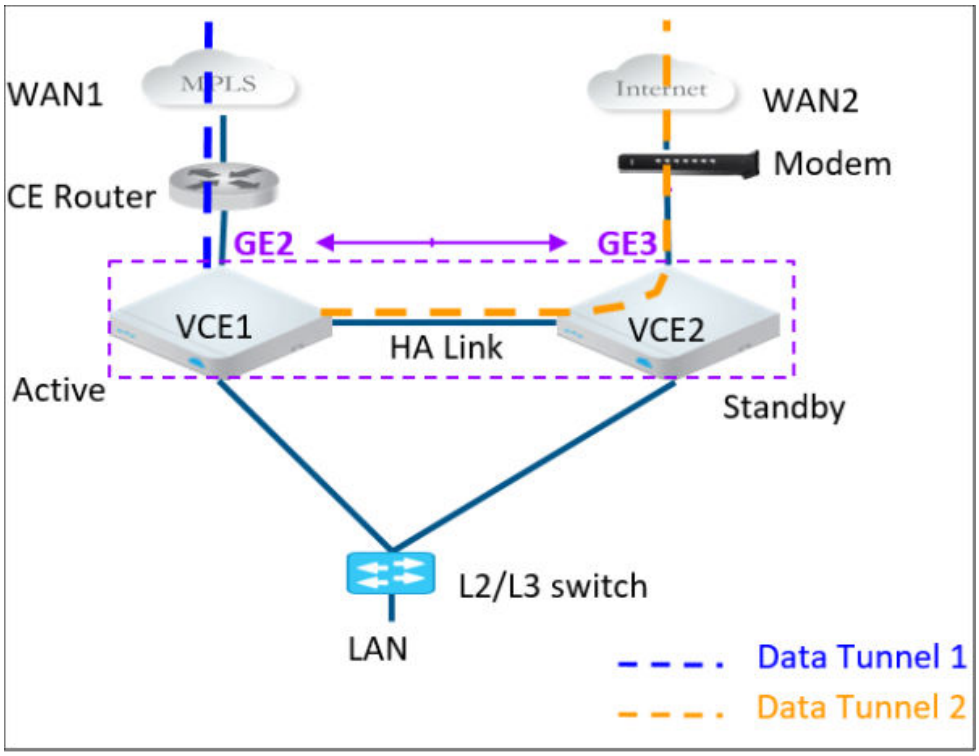
- 相同的 ISP 連結必須連線至兩個 SD-WAN Edges 上的相同連接埠。L2 交換器可讓相同的 ISP 連結同時可供兩個 Edge 使用。
- 待命 SD-WAN Edge 不會封鎖除容錯移轉連結 (L1 連接埠) 以外的所有連接埠，因此不會干擾到任何流量。
- 工作階段資訊會透過容錯移轉連結，在作用中和待命 SD-WAN Edges 之間同步。
- HA 配對也會在偵測到 L1 遺失 LAN/WAN 連結時，執行從作用中到待命的容錯移轉。
  - 如果作用中和待命具有相同數量的已啟動 LAN 連結，但待命有較多啟動的 WAN 連結，則系統會切換至待命。
  - 如果待命 Edge 有較多啟動的 LAN 連結，且至少有一個啟動的 WAN 連結，則系統會容錯移轉至待命。在此情況下，系統會假設待命 Edge 在 LAN 端有比作用中 Edge 更多的使用者，且待命將允許較多的 LAN 端使用者連線至 WAN，前提是有某些 WAN 連線可供使用。

HA 選項 2：增強型 HA

本節說明高可用性 (HA) 選項 2：增強型 HA 的選項

使用 HA 選項 2 時，Edge 的 WAN 端就不再需要 L2 交換器。如果主動 Edge 偵測到某些 WAN 連結連線至備用 Edge，而非像其他連結一樣連線至主動 Edge 本身，就會選取此選項。

下圖顯示 HA 選項 2 的概念性概觀。



Edge (一個主動，一個備用) 透過 L1 連接埠連線，以建立容錯移轉連結。備用 SD-WAN Edge 會封鎖 L1 連接埠以外的所有連接埠，使其無法用於容錯移轉連結。如圖所示，主動 Edge 會在兩個 WAN 連結上建立覆疊通道 (連線至自身和備用 Edge)。

備註 兩個 SD-WAN Edges 不應具有鏡像實體 WAN 連線。如圖所示，如果 VCE1 以 GE2 作為 WAN 連結，則 VCE2 即無法以 GE2 作為其 WAN 連結。

為了利用連線至備用 Edge 的 WAN 連結，主動 Edge 會透過 HA 連結建立覆疊通道。來自 LAN 的流量會轉送至主動 Edge。分支的商務原則可定義覆疊通道間的流量分配。

叢集分裂狀況

當 HA 連結中斷連線，或主動和備用 Edge 無法彼此通訊時，兩個 Edge 都會承擔主動角色。因此，兩個 Edge 都會開始回應對其 LAN 介面的 ARP 要求。這會導致 LAN 流量同時轉送至兩個 Edge，進而可能導致在 LAN 上出現跨距樹狀目錄迴圈。

交換器通常會執行跨距樹狀目錄通訊協定，以防止網路中出現迴圈。在此情況下，交換器會封鎖一或兩個 Edge 的流量。這會導致流經 Edge 配對的流量總數下降。

備註 需要通往主要閘道的通道才能偵測叢集分裂狀況。因此，在 WAN 2 中應要有通往 SD-WAN Gateway 的通道。

核心分裂偵測和防護

本節介紹在使用高可用性拓撲的 Edge 部署中，用來偵測及防止核心分裂狀態的機制。

在高可用性部署中，有兩種機制可用來偵測及防止核心分裂狀況 (在此情況下，兩個 HA Edge 都會變為作用中)。

第一種機制是，當裝置之間的 HA 活動訊號連結遺失時，會在兩個 HA Edge 之間傳送第 2 層廣播活動訊號。第 2 層廣播 (EtherType 0x9999) 活動訊號會從其所有 WAN 介面上的作用中 Edge 送出，以便在該廣播網路中找到待命 Edge。當待命 Edge 收到此封包時，它會將封包解譯成「維護其目前待命狀態」指示。舊版高可用性部署採用此機制，在這種部署中，兩個 HA Edge 的 WAN 連接埠都會連線至相同的第 2 層交換器。

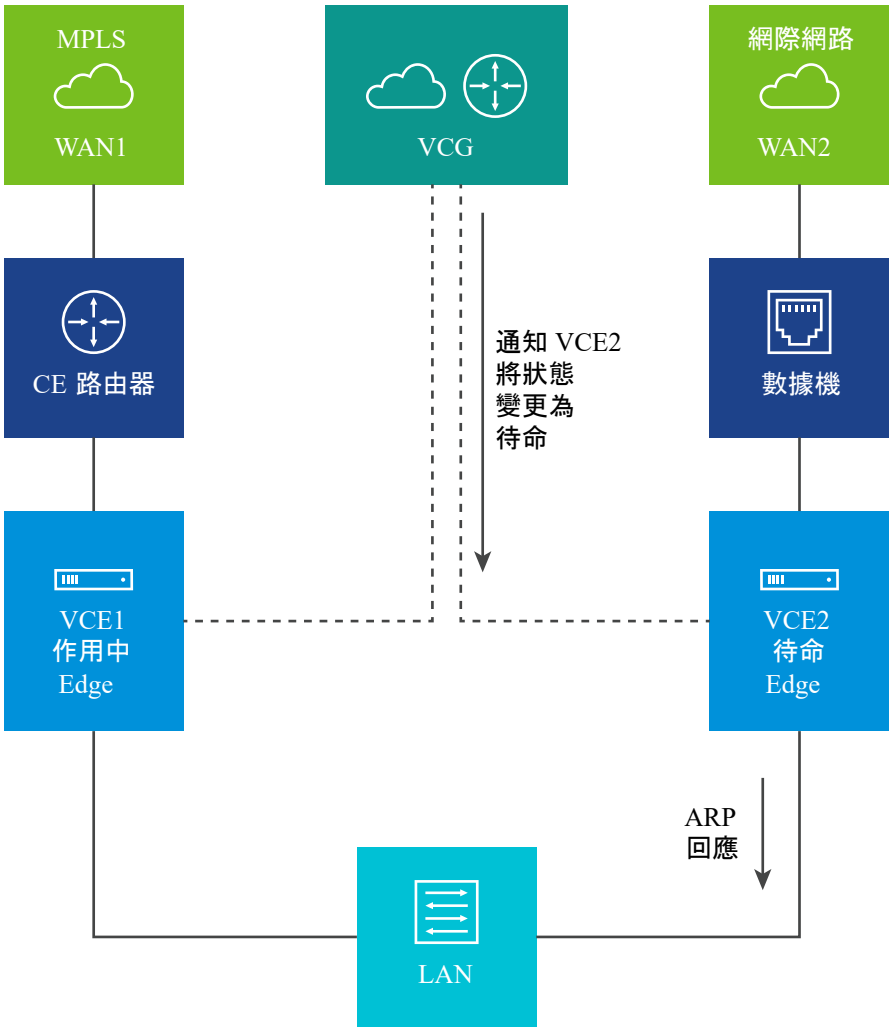
用來偵測及防止核心分裂狀況的第二種機制是，利用 HA Edge 使用的主要閘道。在增強型高可用性部署中，若要偵測及防止核心分裂，唯一的作法是使用此機制，因為此拓撲不會將兩個 HA Edge 都連線至上游第 2 層交換器。

主要閘道原本即已連線至作用中 Edge (VCE1)。發生核心分裂狀況時，待命 Edge (VCE2) 的狀態會變更為作用中，並嘗試對主要閘道 (VCG) 建立通道。閘道會將回應傳回至待命 Edge (VCE2)，對其指示應回復為待命狀態，並且不會允許建立通道。主要閘道將一律只會有來自作用中 Edge 的通道。

一旦 HA 連結失敗，VCE2 會變成作用中狀態，並啟用 LAN/WAN 連接埠，然後嘗試與主要閘道建立通道。如果 VCE1 仍具有通道，則主要閘道會指示 VCE2 還原為待命狀態，因此 VCE2 會封鎖其 LAN 連接埠。只有 LAN 介面仍會受到封鎖 (只要 HA 纜線已中斷)。如下圖所示，閘道指示 VCE2 進入待命狀態。這在邏輯上將可防止核心分裂情況的發生。

備註 在核心分裂情況下，從作用中 Edge 至待命 Edge 的容錯移轉，不同於在作用中 Edge 關閉時所進行的正常容錯移轉。若為更正核心分裂情況而進行容錯移轉，可能還需要額外的幾毫秒/秒才能聚合。

備註 為 Edge 設定 WAN 介面設定時，如果從 [定址類型 (Addressing Type)] 欄位中選取 [PPPoE]，則 Edge 無法藉由從設定為 [PPPoE] 的 WAN 介面廣播，來傳送活動訊號封包。



失敗案例

本節說明下列可能觸發作用中 Edge 容錯移轉至待命 Edge 的案例。

- WAN 連結失敗
- LAN 連結失敗

- Edge 功能沒有回應
- Edge 當機、重新開機或沒有回應

支援透過 HA 連結的 BGP

如果 Edge 切換為增強型 HA 選項，主動 SD-WAN Edge 將透過 HA 連結交換 BGP 路由。主動 Edge 上的 BGP 現在可以與僅連線至備用 Edge WAN 連結的對等建立芳鄰關係。

這可以讓主動的 Edge 從連線至備用 Edge 的 WAN 連結學習路由。備用的路由精靈不會涉及任何功能。備用 Edge 本身只會執行傳遞。

備註 路由不會在主動和備用 Edge 之間同步。因此，在上述案例中，如果發生容錯移轉且備用 Edge 變成主動狀態，則新的主動 Edge 上的 BGP 精靈將會與相同的 BGP 對等建立新的芳鄰關係。

判斷作用中和待命狀態的選取準則

本節說明用來判斷作用中和待命狀態的選取準則。

- 檢查是否有 Edge 具有較高號碼 (L2 和 L3) 的 LAN 介面。LAN 介面號碼較高的 Edge 會被選為作用中 Edge。請注意，用於 HA 連結的介面不計為 LAN 介面。
- 如果兩個 Edge 具有相同號碼的 LAN 介面，則 WAN 介面號碼較高的 Edge 會被選為作用中 Edge。

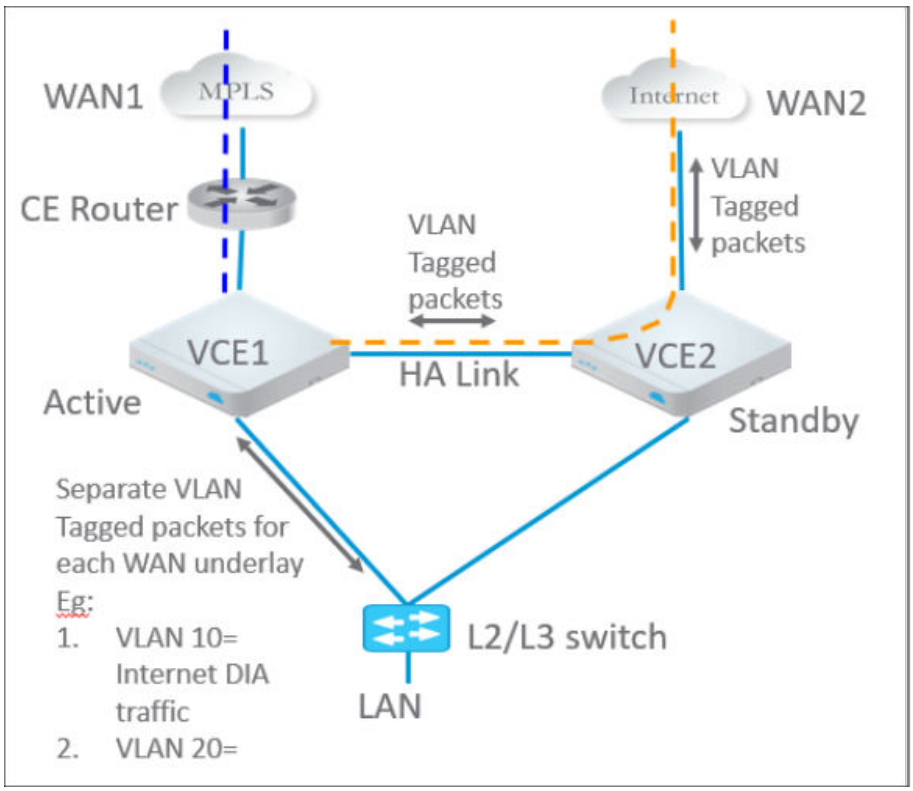
備註 如果兩個 Edge 的 LAN 和 WAN 介面號碼都相同，則不會有任一方先佔。

- 其他支援對照表：
  - 支援靜態/DHCP/PPPoE 連結。
  - 支援在單一介面 (例如子介面) 上以個別的 VLAN 識別碼標記多個 WAN 連結。
  - 不建議將 USB 數據機用於 HA。介面存在於待命 Edge 時，將不會使用。

透過 HA 連結的 VLAN 標記流量

本節說明透過 HA 連結的 VLAN 標記流量。

- 來自 ISP2 的網際網路流量會標記 VLAN。
- 客戶會將個別的 VLAN 用於企業流量與 DIA 流量。
- 待命的 WAN 連結具有可承載網際網路流量的子介面。
- 多個區段



設定 HA

若要設定高可用性，請設定作用中和待命 Edge。

啟用高可用性 (HA)

若要在 SD-WAN Orchestrator 上啟用 HA 功能：

1 在導覽面板中，移至**設定 (Configure) > Edge**。

2 選取您的 SD-WAN Edge，然後按一下**裝置 (Device)** 索引標籤。

3 在**高可用性 (High Availability)** 區域中，按一下**主動備用配對 (Active Standby Pair)**。

依預設將會使用 GE1 或 LAN1 介面作為 HA 介面，以根據 SD-WAN Edge 型號連線配對。

備註 此項目會以 Edge 覆寫的形式提供，且無法在設定檔層級上進行設定。請勿連線備用 SD-WAN Edge。

等待 SD-WAN Edge 進入作用中狀態

在 SD-WAN Orchestrator 上啟用高可用性功能後，請等待現有的 SD-WAN Edge 成為「作用中」角色，並等待 SD-WAN Orchestrator 事件顯示**高可用性處於作用中狀態 (High Availability Going Active)**。

Sun Jul 10, 23:00	High Availability Going Active	DC1 - Hub1	Notice	Velocloud Edge going active, peer has not been detected
Sun Jul 10, 23:00	Edge service startup	DC1 - Hub1	Notice	VeloCloud edge service started
Sun Jul 10, 23:00	Edge online	DC1 - Hub1	Info	Management Daemon Started, version 2.1.0 build R21-
Sun Jul 10, 22:56	ENDPOINT_ACCEPTED_CERTIFICATE	DC1 - Hub1	Info	AE18A7B61185ABE827DBD8B98556C5AACA36C3ED
Sun Jul 10, 22:56	EDGE_OSPF_NSM	DC1 - Hub1	Notice	Edge NSM event: interface=172.31.2.1 nbr=172.31.2.2 router_id=172.31.2.2 status=Full
Sun Jul 10, 22:56	Link alive	DC1 - Hub1	Info	Link GE4 is no longer DEAD
Sun Jul 10, 22:56	Edge Interface Up	DC1 - Hub1	Info	Interface GE4 is up
Sun Jul 10, 22:56	Edge Interface Up	DC1 - Hub1	Info	Interface GE3 is up

將備用 SD-WAN Edge 連線至主動 Edge

1 開啟備用 SD-WAN Edge 的電源，而不進行任何網路連線。

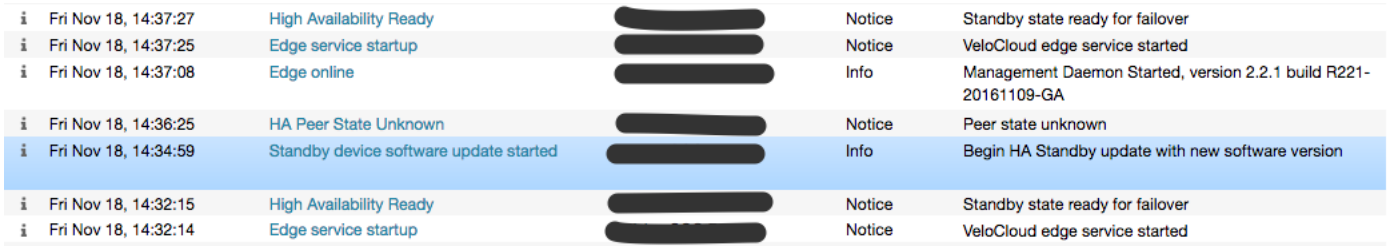
2 在其啟動後，將 LAN1/GE1 介面 (如**裝置 (Device)** 索引標籤上所示) 連線至主動 SD-WAN Edge 上的相同介面。

3 等待主動 SD-WAN Edge 偵測並啟動備用 SD-WAN Edge。當 SD-WAN Orchestrator 成功啟動備用 SD-WAN Edge 時，SD-WAN Orchestrator 事件會顯示**已啟動 HA 備用 (HA Standby Activated)**。

Fri Nov 18, 14:31:54	Edge service startup	[redacted]	Notice	VeloCloud edge service started
Fri Nov 18, 14:31:07	HA Standby Activated	[redacted]	Notice	Standby has been detected

備用 Edge 隨後會開始與主動 SD-WAN Edge 同步，並在此程序期間自動重新開機。

備註 最多可能需要 10 分鐘的時間，備用 SD-WAN Edge 才能與主動 Edge 同步並升級其軟體。



Fri Nov 18, 14:37:27	High Availability Ready	[redacted]	Notice	Standby state ready for failover
Fri Nov 18, 14:37:25	Edge service startup	[redacted]	Notice	VeloCloud edge service started
Fri Nov 18, 14:37:08	Edge online	[redacted]	Info	Management Daemon Started, version 2.2.1 build R221-20161109-GA
Fri Nov 18, 14:36:25	HA Peer State Unknown	[redacted]	Notice	Peer state unknown
Fri Nov 18, 14:34:59	Standby device software update started	[redacted]	Info	Begin HA Standby update with new software version
Fri Nov 18, 14:32:15	High Availability Ready	[redacted]	Notice	Standby state ready for failover
Fri Nov 18, 14:32:14	Edge service startup	[redacted]	Notice	VeloCloud edge service started

連線備用 SD-WAN Edge 上的 LAN 和 WAN 介面

連線在主動 Edge 上鏡像網路連線之備用 SD-WAN Edge 上的 LAN 和 WAN 介面。

SD-WAN Orchestrator 事件會顯示**備用裝置軟體更新已完成 (Standby device software update completed)**。**監控 (Monitor) > Edge** 頁面中的 **HA 狀態 (HA State)** 在準備就緒時會顯示為綠色。

HA 事件詳細資料

本節說明 HA 事件。

HA 事件	說明
HA_GOING_ACTIVE	備用 SD-WAN Edge 因未接收來自對等的活動訊號，而將接管成為主動 Edge。
HA_STANDBY_ACTIVATED	當主動 Edge 偵測到新的備用 Edge 時，主動 Edge 會嘗試向 SD-WAN Orchestrator 傳送此事件以啟動 Edge。收到成功回應時，主動 Edge 將會同步組態和資料。
HA_FAILED	通常發生在 HA 配對已形成，而主動 SD-WAN Edge 已不再接收來自備用 SD-WAN Edge 的訊號時。例如，如果備用 SD-WAN Edge 重新開機，您就會收到此訊息。
HA_READY	表示主動 SD-WAN Edge 目前會接收來自備用 SD-WAN Edge 的訊號。備用 SD-WAN Edge 恢復啟動狀態並重新建立活動訊號時，您就會收到此訊息。
HA_TERMINATED	當 HA 組態已停用，且在 Edge 上成功套用時，就會產生此事件。
HA_ACTIVATION_FAILURE	如果 SD-WAN Orchestrator 無法驗證 HA 啟用，它將產生此事件。範例包括： ■ SD-WAN Orchestrator 無法產生憑證 ■ HA 已停用 (罕見)

在 VMware ESXi 上部署 HA

您可以使用支援的拓撲在 VMware ESXi 上部署 VMware SD-WAN HA。

在 VMware ESXi 上部署 HA 時，請考慮下列限制：

VMware ESXi 的限制

- vSwitch 不支援**連結損失轉送**功能。此功能可確保實體介面上的故障會傳播到 vSwitch 的虛擬介面，並因此支援連結層級故障。由於 vSwitch 不支援此選項，即使實體介面卡關閉，VMware Edge 仍會顯示連結已開啟，且不會進行容錯移轉。
- 如果您想要允許多個 VLAN，則 vSwitch 不允許在連接埠群組上設定特定的 VLAN。不需設定特定 VLAN，而是您需要設定 4095，這表示允許所有 VLAN。

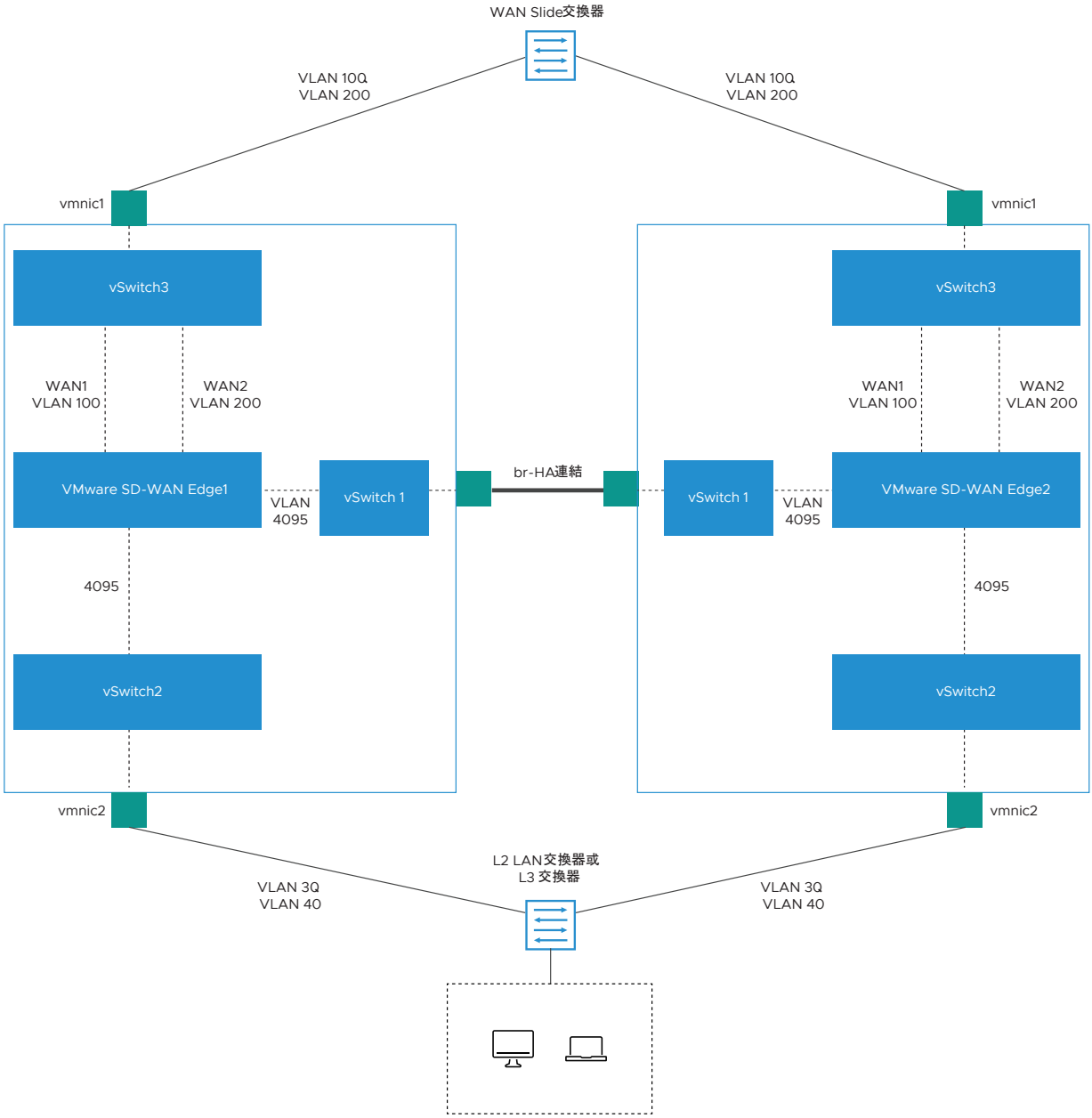
VMware SD-WAN HA 的限制

- 沒有在所有硬體、虛擬和 uCPE 平台上都可運作的一般故障偵測方法。

在 VMware ESXi 上部署 HA 時，VMware SD-WAN 支援下列拓撲：

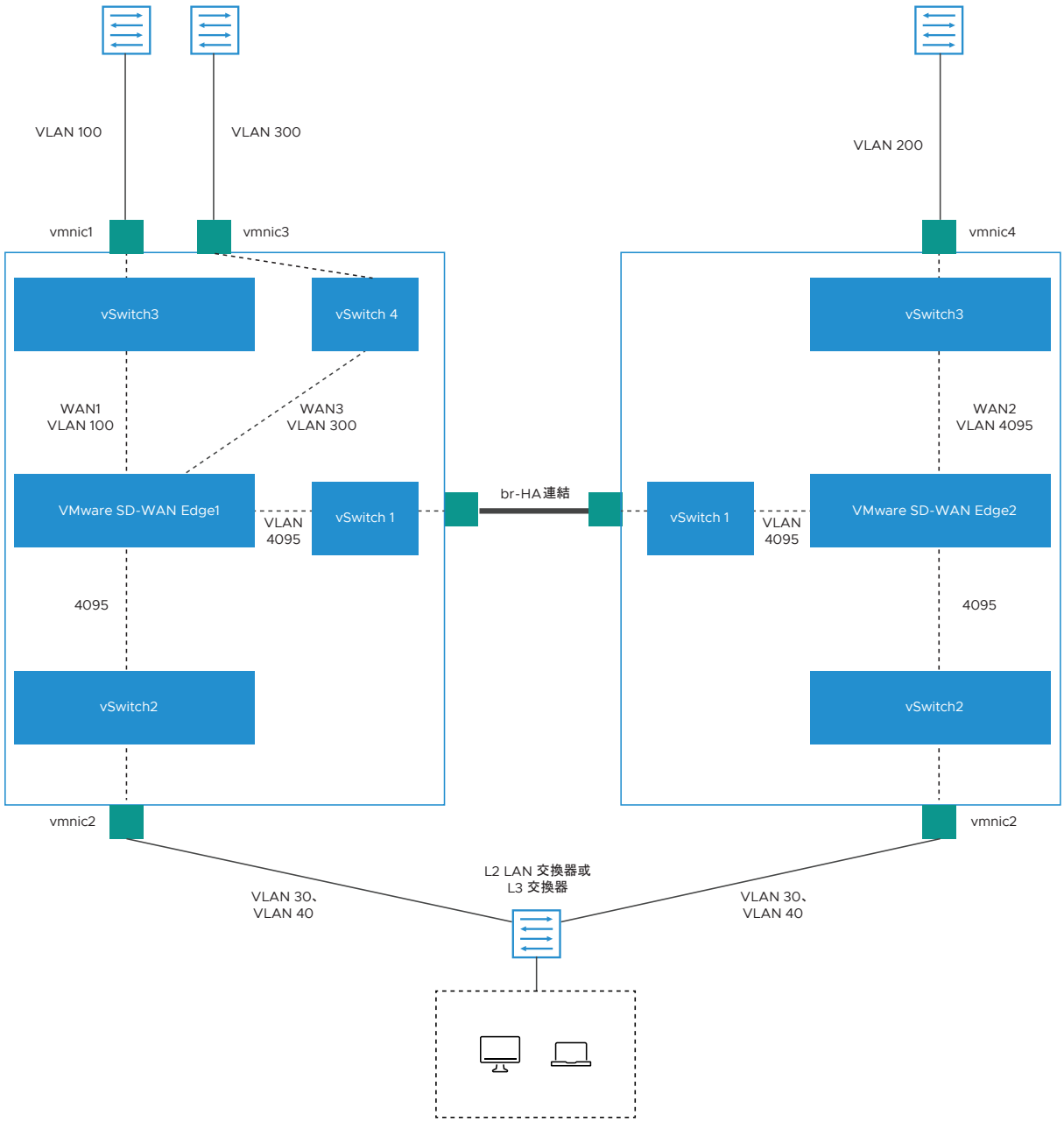
拓撲 1：具有 WAN 連結的舊版 HA

下圖說明的拓撲具有舊版 HA 以及已使用單一實體介面卡上行連結的 WAN 連結，以及透過單一實體介面卡的路由 LAN 或主幹 LAN。



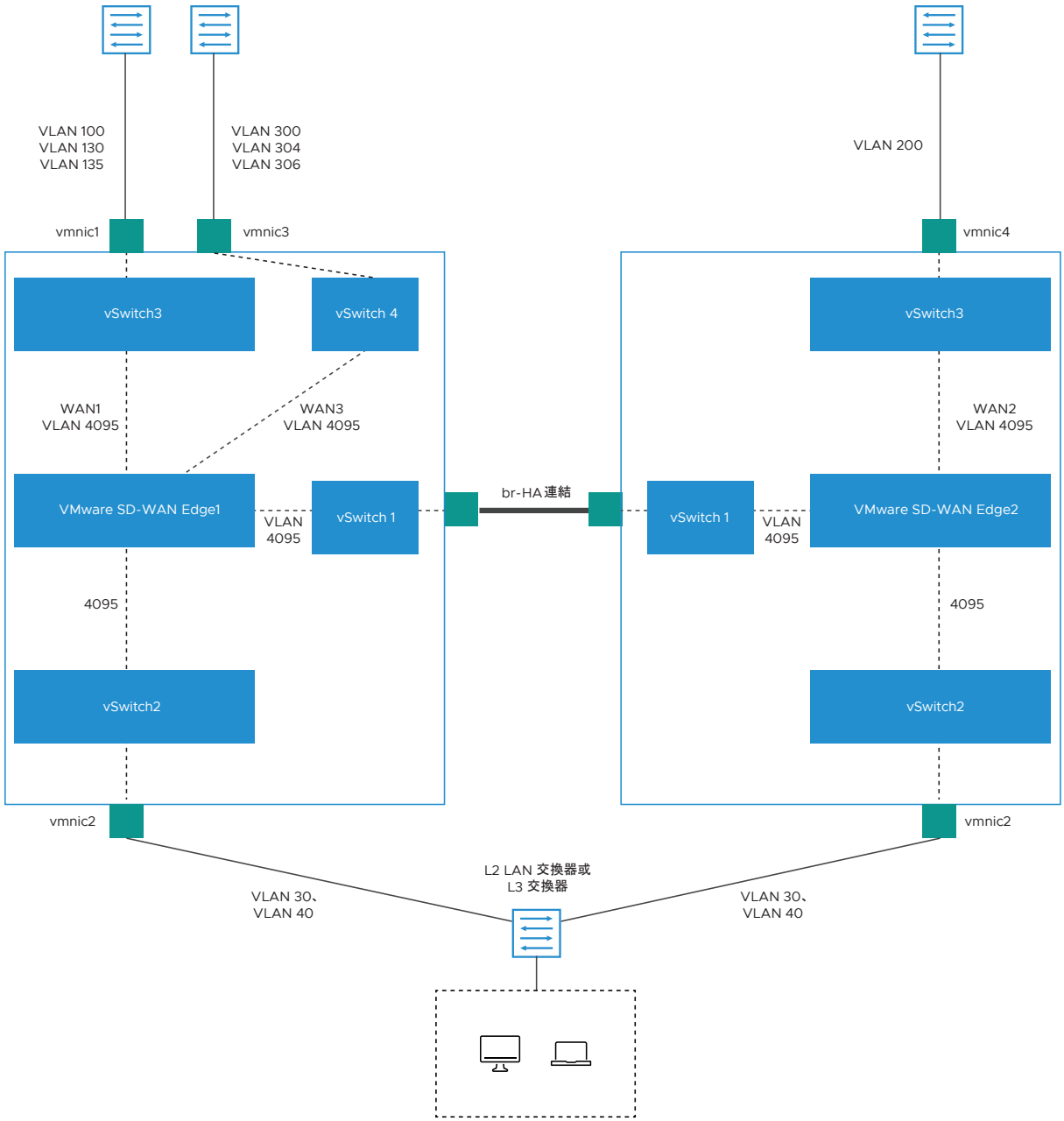
拓撲 2：具有 WAN 連結的增強型 HA

下列拓撲顯示具有三個 WAN 連結的增強型 HA。



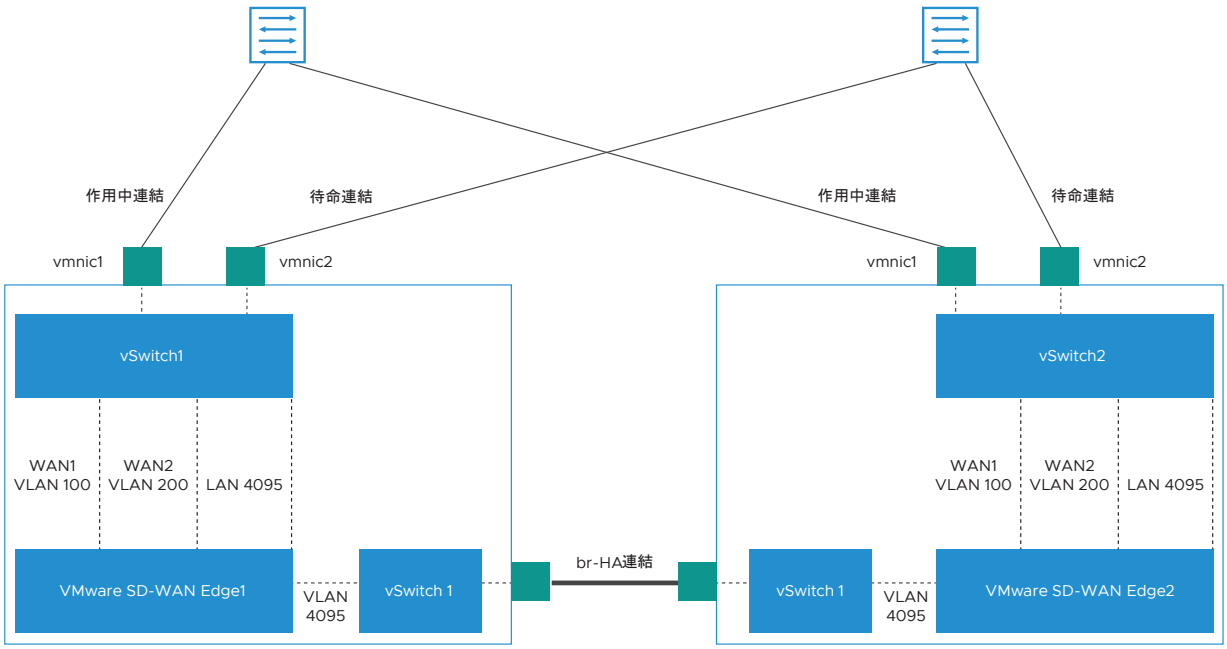
拓撲 3：具有子介面的增強型 HA

下圖顯示的增強型 HA，在 WAN 介面上具有子介面，並在連接埠群組上的 VLAN 識別碼為 4095。



拓撲 4：Dell IT

下圖顯示使用 VEP 硬體的 Dell IT。


作用中連結
待命連結
作用中連結
待命連結
vmnic1
vmnic2
vmnic1
vmnic2
vSwitch1
vSwitch2
WAN1
VLAN 100
WAN2
VLAN 200
LAN 4095
WAN1
VLAN 100
WAN2
VLAN 200
LAN 4095
VMware SD-WAN Edge1
VLAN
4095
vSwitch 1
br-HA連結
vSwitch 1
VLAN
4095
VMware SD-WAN Edge2

VMware 虛擬 Edge 部署

23

虛擬 Edge 可作為安裝在標準 Hypervisor 上的虛擬機器。本節說明在 KVM 和 VMware ESXi Hypervisor 上部署 VMware 虛擬 Edge 的必要條件和安裝程序。

本章節討論下列主題：

- VMware 虛擬 Edge 的部署必要條件
- VMware 虛擬 Edge 部署的特殊考量事項
- 建立 Cloud-Init
- 安裝 VMware 虛擬 Edge

VMware 虛擬 Edge 的部署必要條件

說明 VMware 虛擬 Edge 部署的需求。

虛擬 Edge 需求

部署虛擬 Edge 之前請注意下列需求：

- 支援 2、4、8 和 10 vCPU 指派。

	2 個 vCPU	4 個 vCPU	8 個 vCPU	10 個 vCPU
記憶體下限 (DRAM)	8 GB	16 GB	32 GB	32 GB
儲存區下限 (虛擬磁碟)	8 GB	8 GB	16 GB	16 GB

- AES-NI CPU 功能必須傳遞至虛擬 Edge 應用裝置。
- 最多 8 個 vNIC (預設值為 GE1 和 GE2 LAN 連接埠，以及 GE3-GE8 WAN 連接埠)。

注意 不支援過度訂閱虛擬 Edge 資源，例如 CPU、記憶體和儲存區。

建議的伺服器規格

NIC 晶片組	硬體	規格
Intel 82599/82599ES	HP DL380G9	http://www.hp.com/hpinfo/newsroom/press_kits/2014/ComputeEra/HP_ProLiantDL380_DataSheet.pdf
Intel X710/XL710	Dell PowerEdge R640	https://www.dell.com/en-us/work/shop/povw/poweredge-r640 ■ CPU 型號和核心 - 雙插槽 Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz，各 16 個核心 ■ 記憶體 - 384 GB RAM
Intel X710/XL710	Supermicro SYS-6018U-TRTP+	https://www.supermicro.com/en/products/system/1U/6018/SYS-6018U-TRTP_.cfm ■ CPU 型號和核心 - 雙插槽 Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz，各 10 個核心 ■ 記憶體 - 256 GB RAM

建議的 NIC 規格

硬體製造商	韌體版本	適用於 Ubuntu 16.04/18.04 的主機驅動程式	適用於 ESXi 6.7 的主機驅動程式
適用於 40GbE QSFP+ 的雙埠 Intel Corporation 乙太網路控制卡 XL710	6.80	2.7.11	1.7.17
適用於 10GbE SFP+ 的雙埠 Intel Corporation 乙太網路控制卡 X710	6.80	2.7.11	1.7.17
適用於 10GbE SFP+ 的四埠 Intel Corporation 乙太網路控制卡 X710	6.80	2.7.11	1.7.17

支援的作業系統

- Ubuntu 16.04
- VMware vSphere ESXi 6.7，從 4.3 版和更高版本開始，為 VMware vSphere ESXi 6.7 和 7.0

防火牆/NAT 需求

如果 VMware 虛擬 Edge 部署在防火牆和/或 NAT 裝置後方，則須符合下列需求：

- 防火牆必須允許從 VMware 虛擬 Edge 到 TCP/443 的輸出流量 (為了與 SD-WAN Orchestrator 通訊)。
- 防火牆必須允許流量從連接埠 UDP/2426 (VCMP) 輸出至網際網路。

CPU 旗標需求

如需部署虛擬 Edge 所需的 CPU 旗標需求的詳細資訊，請參閱 VMware 虛擬 Edge 部署的特殊考量事項。

VMware 虛擬 Edge 部署的特殊考量事項

說明 VMware 虛擬 Edge 部署的特殊考量事項。

- SD-WAN Edge 是對延遲很敏感的應用程式。請參閱 VMware 說明文件，以將虛擬機器 (VM) 調整為對延遲敏感的應用程式。
- 建議的主機設定：
  - 要達到最高效能的 BIOS 設定：
    - 2.0 GHz 或更高的 CPU
    - 啟用 Intel Virtualization Technology (Intel VT)
    - 停用超執行緒
    - 虛擬 Edge 支援半虛擬化 vNIC VMXNET 3 和傳遞 vNIC SR-IOV：
      - 使用 VMXNET3 時，請在主機 BIOS 和 ESXi 上停用 SR-IOV
      - 使用 SR-IOV 時，請在主機 BIOS 和 ESXi 上啟用 SR-IOV
      - 若要在 VMware 和 KVM 上啟用 SR-IOV，請參閱：
        - KVM - 在 KVM 上啟用 SR-IOV
        - VMware - 在 VMware 上啟用 SR-IOV
    - 在 CPU BIOS 上停用省電功能，以達到最佳效能
    - 啟用 CPU Turbo
    - CPU 必須支援 AES-NI、SSSE3、SSE4、RDTSC、RDSEED、RDRAND 指令集
    - 建議為 Hypervisor 工作負載保留 2 個核心

      例如，對於 10 核心的 CPU 系統，建議執行一個 8 核心虛擬 Edge 或兩個 4 核心虛擬 Edge，並且為 Hypervisor 處理程序保留 2 個核心。
  - 對於雙通訊端主機系統，請確定 Hypervisor 所指派的網路介面卡、記憶體和 CPU 資源與 vCPU 指派的位於相同的通訊端 (NUMA) 界限內。
- 建議的虛擬機器設定：
  - CPU 應設定為「100% 保留」
  - CPU 共用率應設為「高」
  - 記憶體應設定為「100% 保留」
  - 必須將延遲敏感度設定為「高」
- SD-WAN Edge SSH 主控台的預設使用者名稱為 `root`。

建立 Cloud-Init

cloud-init 是一個 Linux 套件，負責處理執行個體的早期初始化。如果在發行版中可用，它可讓您在安裝後直接設定執行個體的許多一般參數。這會建立根據一系列輸入進行設定的完整功能執行個體。Cloud-init 組態由兩個主要組態檔組成，即中繼資料檔案和使用者資料檔案。中繼資料包含 Edge 的網路組態，而使用者資料則包含 Edge 軟體組態。cloud-init 檔案所提供的資訊可識別要安裝的 VMware 虛擬 Edge 執行個體。

cloud-init 的行為可透過 user-data 進行設定。使用者可在啟動執行個體時指定使用者資料。這通常是透過連結 cloud-init 將在第一次開機時所尋找 ISO 格式的次要磁碟來完成。此磁碟包含將在當時套用的所有早期組態資料。

VMware 虛擬 Edge 支援 cloud-init 和封裝在 ISO 映像中的所有必要組態。

建立 cloud-init 中繼資料和使用者資料檔案

最終安裝組態選項是使用一對 cloud-init 設定檔進行設定。第一個安裝組態檔案包含中繼資料。請使用文字編輯器建立此檔案，並將其命名為 `meta-data`。此檔案所提供的資訊可識別要安裝的 VMware 虛擬 Edge 執行個體。執行個體識別碼可以是任何識別名稱，且本機主機名稱應為符合站台標準的主機名稱。

1 建立包含執行個體的中繼資料檔案：

```
name.instance-id: vedge1

local-hostname: vedge1
```

2 新增以下顯示的 `network-interfaces` 區段以指定 WAN 組態。在此只需指定需要靜態 IP 定址的 WAN 介面。依預設會為 DHCP 設定所有 SD-WAN Edge WAN 介面。您可以指定多個介面。

```
root@ubuntu# cat meta-data
instance-id: Virtual-Edge
local-hostname: Virtual-Edge
network-interfaces:
      GE1:
         mac_address: 52:54:00:79:19:3d
      GE2:
         mac_address: 52:54:00:67:a2:53
      GE3:
         type: static
         ipaddr: 11.32.33.1
         mac_address: 52:54:00:e4:a4:3d
         netmask: 255.255.255.0
         gateway: 11.32.33.254
      GE4:
         type: static
         ipaddr: 11.32.34.1
         mac_address: 52:54:00:14:e5:bd
         netmask: 255.255.255.0
         gateway: 11.32.34.254
```

3 建立 user-data 檔案。此檔案包含三個主要模組：SD-WAN Orchestrator、啟動碼和忽略憑證錯誤。

模組	說明
vco	SD-WAN Orchestrator 的 IP 位址/URL。
activation_code	虛擬 Edge 的啟動碼。在 SD-WAN Orchestrator 上建立 Edge 執行個體時，會產生啟動碼。
vco_ignore_cert_errors	確認或忽略任何憑證有效性錯誤的選項。

在 SD-WAN Orchestrator 上建立 Edge 執行個體時，會產生啟動碼。

重要 SD-WAN Edge 映像中沒有預設密碼。必須在 cloud-config 中提供密碼：

```
#cloud-config
password: passw0rd
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
      vce:
            vco: 10.32.0.3
            activation_code: F54F-GG4S-XGFI
            vco_ignore_cert_errors: true
```

建立 ISO 檔案

完成檔案後，您必須將其封裝為 ISO 映像。此 ISO 映像用作虛擬機器的虛擬組態 CD。此 ISO 映像 (在以下範例中稱為 seed.iso) 可使用下列命令建立於 Linux 系統上：

```
genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data network-data
```

您可以選擇是否包含 network-interfaces 區段。如果該區段不存在，則依預設會使用 DHCP 選項。

ISO 映像產生後，請將映像傳輸到主機電腦上的資料存放區。

安裝 VMware 虛擬 Edge

您可以使用 cloud-init 設定檔，在 KVM 和 VMware ESXi 上安裝 VMware 虛擬 Edge。cloud-init 組態包含 Edge 的介面組態和啟用金鑰。

必要條件

請確定您已建立 cloud-init 中繼資料和使用者資料檔案，並已將檔案封裝為 ISO 映像檔。如需相關步驟，請參閱建立 Cloud-Init。

KVM 有多種方式可提供虛擬機器的網路。VMware 建議下列選項：

- SR-IOV
- Linux 橋接器

- OpenVSwitch 橋接器

如果您決定使用 SR-IOV 模式，請在 KVM 和 VMware 上啟用 SR-IOV。如需相關步驟，請參閱：

- 在 KVM 上啟用 SR-IOV
- 在 VMware 上啟用 SR-IOV

若要安裝 VMware 虛擬 Edge：

- 在 KVM 上，請參閱在 KVM 上安裝虛擬 Edge。
- 在 VMware ESXi 上，請參閱在 VMware ESXi 上安裝虛擬 Edge。

在 KVM 上啟用 SR-IOV

若要在 KVM 上啟用 SR-IOV 模式，請執行下列步驟。

必要條件

這需要特定的 NIC 卡。下列晶片組已通過 VMware 認證，可與 SD-WAN Gateway 和 SD-WAN Edge 搭配使用。

- Intel 82599/82599ES
- Intel X710/XL710

備註 在 KVM 上以 SR-IOV 模式使用 Intel X710/XL710 卡之前，請確定已正確安裝〈部署必要條件〉一節中指定的支援韌體和驅動程式版本。

備註 如果 KVM 虛擬 Edge 部署了高可用性拓撲，則不支援 SR-IOV 模式。對於高可用性部署，請確保沒有針對該 KVM Edge 配對啟用 SR-IOV。

若要在 KVM 上啟用 SR-IOV：

1 在 BIOS 中啟用 SR-IOV。這將取決於您的 BIOS。登入 BIOS 主控台並尋找 SR-IOV 支援/DMA。您可以檢查 Intel 是否有正確的 CPU 旗標，以確認提示上的支援。

```
cat /proc/cpuinfo | grep vmx
```

2 在 Bboot 上新增選項 (在 `/etc/default/grub` 中)。

```
GRUB_CMDLINE_LINUX="intel_iommu=on"
```

a 執行下列命令：`update-grub` 和 `update-initramfs -u`。

b 重新開機

c 確定 iommu 已啟用。

```
velocloud@KVMperf3:~$ dmesg | grep -i IOMMU
 [ 0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/mapper/qa--
multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
 [ 0.000000] Kernel command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/
```

```
mapper/qa--multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
 [ 0.000000] Intel-IOMMU: enabled
 ….
 velocloud@KVMperf3:~$
```

3 根據使用的 NIC 晶片組，依照下列方式新增驅動程式：

- 對於 SR-IOV 模式下的 **Intel 82599/82599ES** 卡：
  1. 從 Intel 網站下載並安裝 **ixgbe** 驅動程式。
  2. 設定 ixgbe 組態 (tar 和 sudo make install)。

     ```
     velocloud@KVMperf1:~$ cat /etc/modprobe.d/ixgbe.conf
     ```

  3. 如果 ixgbe 組態檔不存在，您必須依照下列方式建立該檔案。

     ```
     options ixgbe max_vfs=32,32
     options ixgbe allow_unsupported_sfp=1
     options ixgbe MDD=0,0
     blacklist ixgbevf
     ```

  4. 執行 `update-initramfs -u` 命令，然後將伺服器重新開機。
  5. 使用 `modinfo` 命令確認安裝是否成功。

     ```
     velocloud@KVMperf1:~$ modinfo ixgbe and ip link
      filename: /lib/modules/4.4.0-62-generic/updates/drivers/net/ethernet/intel/ixgbe/
     ixgbe.ko
      version: 5.0.4
      license: GPL
      description: Intel(R) 10GbE PCI Express Linux Network Driver
      author: Intel Corporation, <linux.nics@intel.com>
      srcversion: BA7E024DFE57A92C4F1DC93
     ```

- 對於 SR-IOV 模式下的 **Intel X710/XL710** 卡：
  1. 從 Intel 網站下載並安裝 **i40e** 驅動程式。
  2. 建立虛擬函式 (VF)。

     ```
     echo 4 > /sys/class/net/device name/device/sriov_numvfs
     ```

  3. 若要讓 VF 在重新開機後持續保存，請將上一個步驟中的命令新增至 `"/etc/rc.d/rc.local"` 檔案。
  4. 拒絕列出 VF 驅動程式

     ```
     echo “blacklist i40evf” >> /etc/modprobe.d/blacklist.conf
     ```

  5. 執行 `update-initramfs -u` 命令，然後將伺服器重新開機。

驗證 SR-IOV (選用)

您可以使用下列命令快速確認主機是否已啟用 SR-IOV：

```
lspci | grep -i Ethernet
```

確認您是否擁有虛擬函式：

```
01:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function(rev
01)
```

在 KVM 上安裝虛擬 Edge

說明如何使用 cloud-init 組態檔在 KVM 上安裝和啟動虛擬 Edge。

如果您決定使用 SR-IOV 模式，請在 KVM 上啟用 SR-IOV。如需相關步驟，請參閱在 KVM 上啟用 SR-IOV。

備註 如果 KVM 虛擬 Edge 部署了高可用性拓撲，則不支援 SR-IOV 模式。對於高可用性部署，請確保沒有針對該 KVM Edge 配對啟用 SR-IOV。

若要使用 libvirt 在 KVM 上執行 VMware 虛擬 Edge：

1 使用 gunzip 將 `qcow2` 檔案解壓縮到映像位置 (例如 `/var/lib/libvirt/images`)。

2 使用 SR-IOV 和 OpenVswitch 建立要用於裝置的網路集區。

使用 SR-IOV

以下是使用 SR-IOV 的 Intel X710/XL710 NIC 卡專用的網路介面範本範例。

```
    <interface type='hostdev' managed='yes'>
        <mac address='52:54:00:79:19:3d'/>
        <driver name='vfio'/>
        <source>
            <address type='pci' domain='0x0000' bus='0x83' slot='0x0a' function='0x0'/>
        </source>
        <model type='virtio'/>
    </interface>
```

使用 OpenVSwitch

```
<network>
 <name>passthrough</name>
 <model type='virtio'/>
 <forward mode="bridge"/>
 <bridge name="passthrough"/>
 <virtualport type='openvswitch'>
 </virtualport>
 <vlan trunk='yes'>
 <tag id='33' nativeMode='untagged'/>
 <tag id='200'/>
 <tag id='201'/>
```

```
 <tag id='202'/>
 </vlan>
 </network>
 Bridge
 <network>
 <name>passthrough</name>
 <model type='virtio'/>
 <forward mode="bridge"/>
 </network>
<domain type='kvm'>
 <name>vedge1</name>
 <memory unit='KiB'>4194304</memory>
 <currentMemory unit='KiB'>4194304</currentMemory>
 <vcpu placement='static'>2</vcpu>
 <resource>
 <partition>/machine</partition>
 </resource>
 <os>
 <type arch='x86_64' machine='pc-i440fx-trusty'>hvm</type>
 <boot dev='hd'/>
 </os>
 <features>
 <acpi/>
 <apic/>
 <pae/>
 </features>
<!--
Set the CPU mode to host model to leverage all the available features on the host CPU
-->
 <cpu mode='host-model'>
 <model fallback='allow'/>
 </cpu>
 <clock offset='utc'/>
 <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot>
 <on_crash>restart</on_crash>
 <devices>
 <emulator>/usr/bin/kvm-spice</emulator>
 <!--
 Below is the location of the qcow2 disk image
 -->
 <disk type='file' device='disk'>
 <driver name='qemu' type='qcow2'/>
 <source file='/var/lib/libvirt/images/edge-VC_KVM_GUEST-x86_64-2.3.0-18- R23-20161114-GA-
updatable-ext4.qcow2'/>
 <target dev='sda' bus='sata'/>
 <address type='drive' controller='0' bus='0' target='0' unit='0'/>
 </disk>
 <!--
 If using cloud-init to boot up virtual edge, attach the 2nd disk as CD-ROM
 -->
 <disk type='file' device='cdrom'>
 <driver name='qemu' type='raw'/>
 <source file='/home/vcadmin/cloud-init/vedge1/seed.iso'/>
 <target dev='sdb' bus='sata'/>
```

```
 <readonly/>
 <address type='drive' controller='1' bus='0' target='0' unit='0'/>
 </disk>
 <controller type='usb' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
 </controller>
 <controller type='pci' index='0' model='pci-root'/>
 <controller type='sata' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
 </controller>
 <controller type='ide' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
 </controller>
 <!--
 The first two interfaces are for the default L2 interfaces, NOTE VLAN support just for SR-
IOV and OpenvSwitch
 -->
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork='LAN1'/>
 < vlan>< tagid='#hole2_vlan#'/></ vlan>
 < aliasname=LAN1/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0'/>
 </ interface>
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork=LAN2/>
 < vlan>< tagid='#LAN2_VLAN#'/></ vlan>
 < aliasname='hostdev1'/>
 < addresstype='pci' domain='0x0000' bus=' 0x00' slot='0x13' function='0x0'/>
 </ interface>
<!--
 The next two interfaces are for the default L3 interfaces. Note that additional 6 routed
interfaces
are supported for a combination of 8 interfaces total
 -->
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork=WAN1/>
 < vlan>< tagid='#hole2_vlan#'/></ vlan>
 < aliasname=LAN1/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0'/>
 </ interface>
 < interfacetype='network'>
 < modeltype='virtio'/>
 < source network=LAN2/>
 < vlan>< tag id='#LAN2_VLAN#'/></ vlan>
 < aliasname='hostdev1'/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0'/>
 </ interface>
 <serial type='pty'>
 <target port='0'/>
 </serial>
 <console type='pty'>
 <target type='serial' port='0'/>
```

```
</console>
<input type='mouse' bus='ps2'/>
<input type='keyboard' bus='ps2'/>
<graphics type='vnc' port='-1' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1'/>
</graphics>
<sound model='ich6'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</sound>
<video>
<model type='cirrus' vram='9216' heads='1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
</video>
<memballoon model='virtio'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
</memballoon>
</devices>
</domain>
```

3 儲存定義虛擬機器的網域 XML 檔案 (例如，在步驟 2 中建立的 `vedge1.xml`)。

4 執行下列步驟來啟動虛擬機器：

a 建立虛擬機器。

```
virsh define vedge1.xml
```

b 啟動虛擬機器。

```
virsh start vedge1
```

備註 `vedge1` 是在網域 XML 檔案的 `<name>` 元素中定義之虛擬機器的名稱。請將 `vedge1` 取代為您在 `<name>` 元素中指定的名稱。

5 如果您使用 SR-IOV 模式，則在啟動虛擬機器後，請在使用的虛擬功能 (VF) 上設定下列項目：

a 將 spoofcheck 設定為關閉。

```
ip link set eth1 vf 0 spoofchk off
```

b 將信任模式設定為開啟。

```
ip link set dev eth1 vf 0 trust on
```

c 如有需要，請設定 VLAN。

```
ip link set eth1 vf 0 vlan 3500
```

備註 虛擬功能設定步驟不適用於 OpenVSwitch (OVS) 模式。

6 透過主控台進入虛擬機器。

```
virsh list
Id Name State
----------------------------------------------------
25 test_vcg running
velocloud@KVMperf2$ virsh console 25
Connected to domain test_vcg
Escape character is ^]
```

cloud-init 已包含在 SD-WAN Orchestrator 上建立新的虛擬 Edge 時產生的啟用金鑰。虛擬 Edge 會使用 cloud-init 檔案中的組態設定進行設定。這將在虛擬 Edge 已開啟電源時設定介面。虛擬 Edge 連線後，它會透過 SD-WAN Orchestrator 使用啟用金鑰來啟動。SD-WAN Orchestrator IP 位址和啟用金鑰已定義在 cloud-init 檔案中。

在 VMware 上啟用 SR-IOV

在 VMware 上啟用 SR-IOV 是選擇性的，但必須要實現 DPDK 的所有效益，才能提升封包處理效能。

必要條件

這需要特定的 NIC 卡。下列晶片組已通過 VMware 認證，可與 SD-WAN Gateway 搭配使用。

- Intel 82599/82599ES
- Intel X710/XL710

備註 在 VMware 上以 SR-IOV 模式使用 Intel X710/XL710 卡之前，請確定已正確安裝〈部署必要條件〉一節中說明的支援韌體和驅動程式版本。

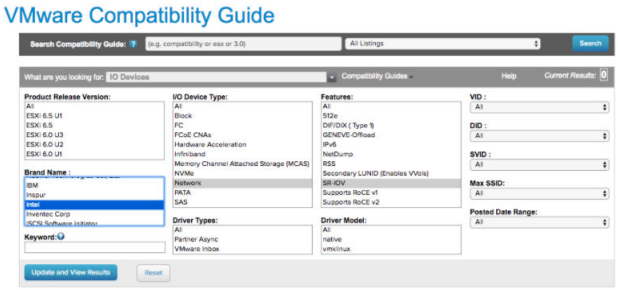
若要在 VMware 上啟用 SR-IOV：

1 確定您的 NIC 卡支援 SR-IOV。查看 https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io 上的 VMware 硬體相容性清單 (HCL)

品牌名稱：(Brand Name:) Intel

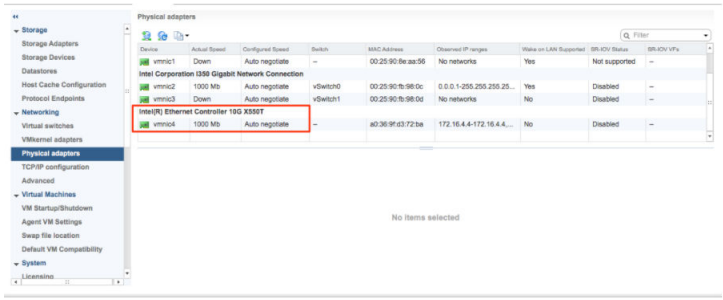
I/O 裝置類型：(I/O Device Type:) 網路

功能：(Features:) SR-IOV



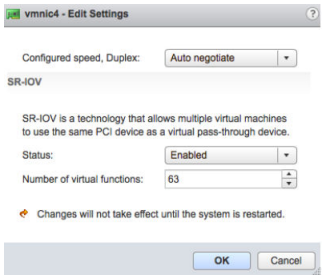
下列 VMware 知識庫文章提供如何在支援的 NIC 上啟用 SR-IOV 的詳細資料：https://kb.vmware.com/s/article/2038739

2 如果您已有支援 NIC 卡，請移至特定的 VMware 主機，選取**設定 (Configure)** 索引標籤，然後選擇**實體介面卡 (Physical adapters)**。



3 選取**編輯設定 (Edit Settings)**。將**狀態 (Status)** 變更為**已啟用 (Enabled)**，並指定所需的虛擬函式數目。此數目會根據 NIC 卡類型而有所不同。

4 將 Hypervisor 重新開機。



5 如果 SR-IOV 已成功啟用，則在 ESXi 重新開機後，虛擬函式 (VF) 數目將會顯示在特定 NIC 下。

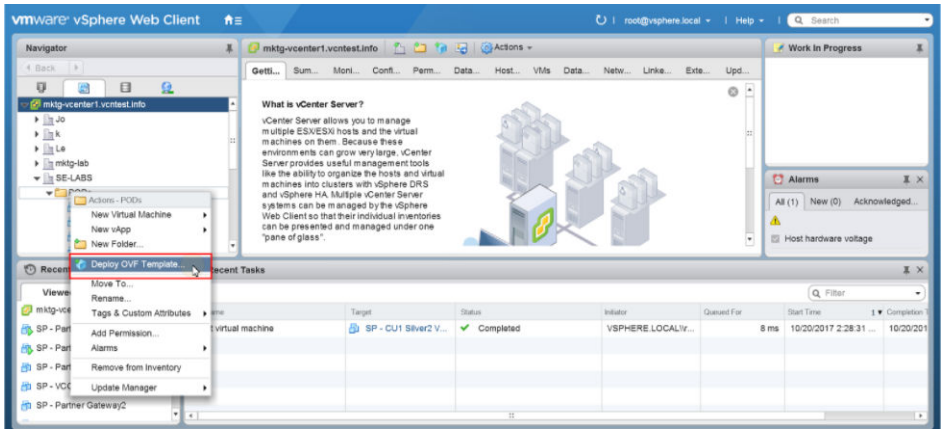
在 VMware ESXi 上安裝虛擬 Edge

說明如何在 VMware ESXi 上安裝虛擬 Edge。

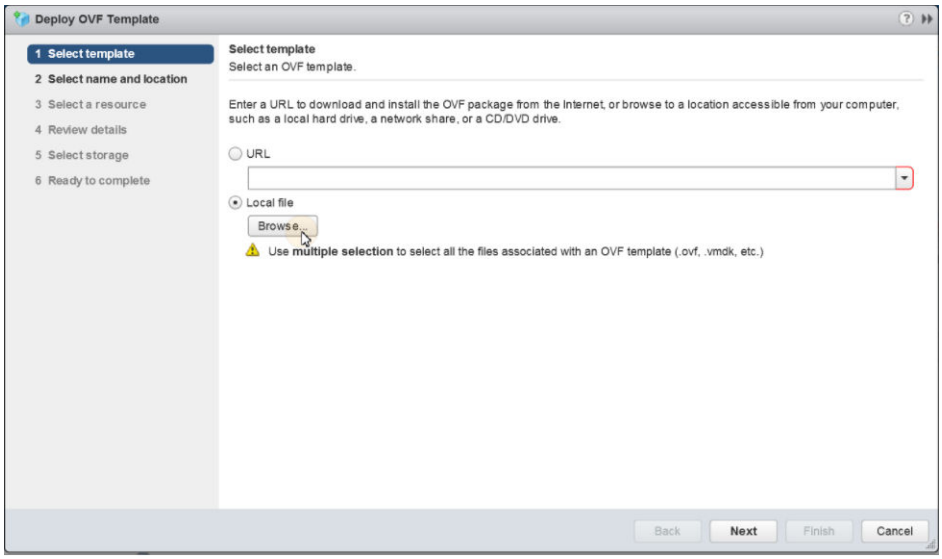
如果您決定使用 SR-IOV 模式，請在 VMware 上啟用 SR-IOV。如需相關步驟，請參閱在 VMware 上啟用 SR-IOV。

若要在 VMware ESXi 上安裝虛擬 Edge：

1 使用 vSphere Client 部署 OVF 範本，然後選取 Edge OVA 檔案。



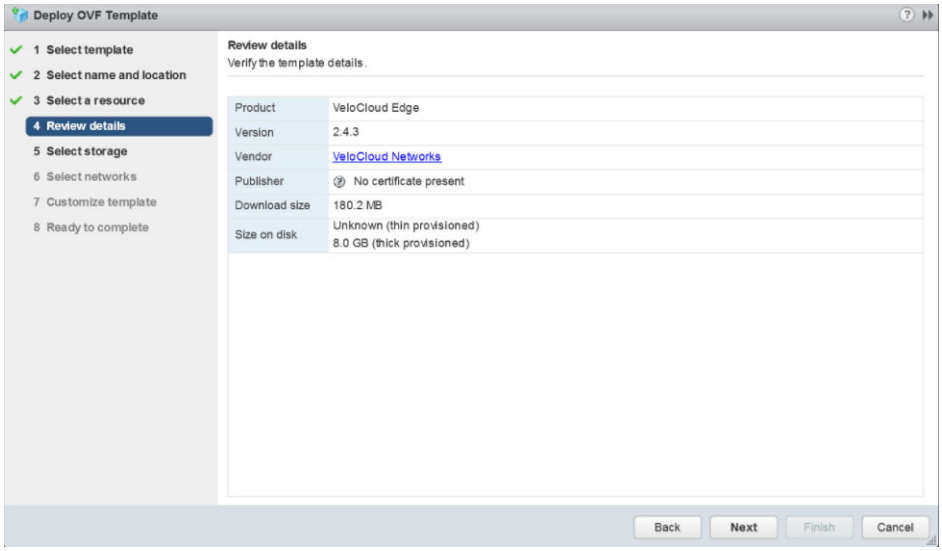
2 從 URL 或本機檔案中選取 OVF 範本。



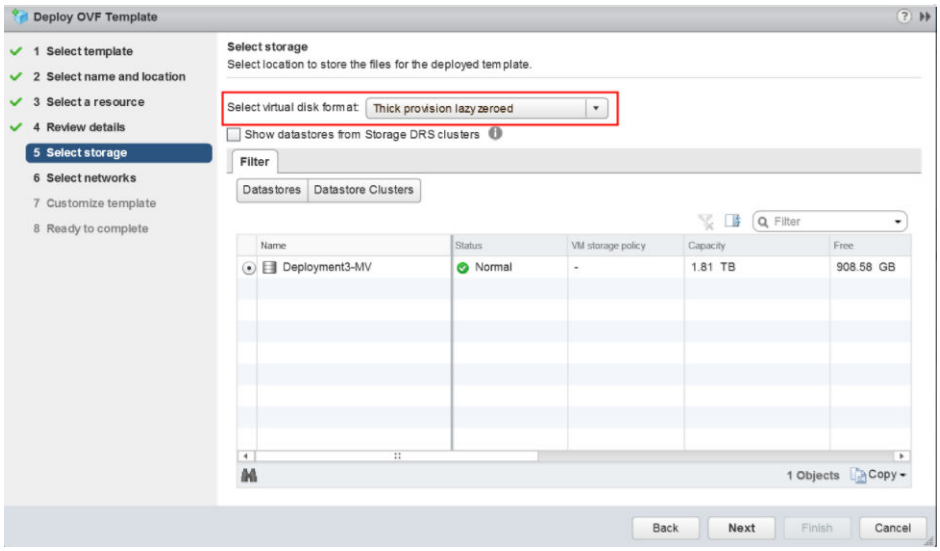
3 選取虛擬機器的名稱和位置。

4 選取資源。

5 確認範本詳細資料。

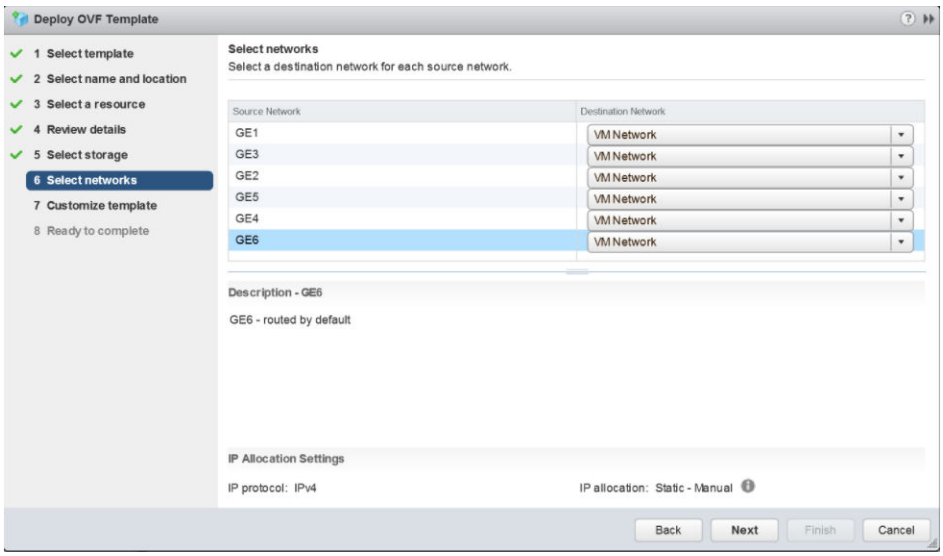


6 選取用來儲存部署範本檔案的儲存位置。



7 設定每個介面的網路。

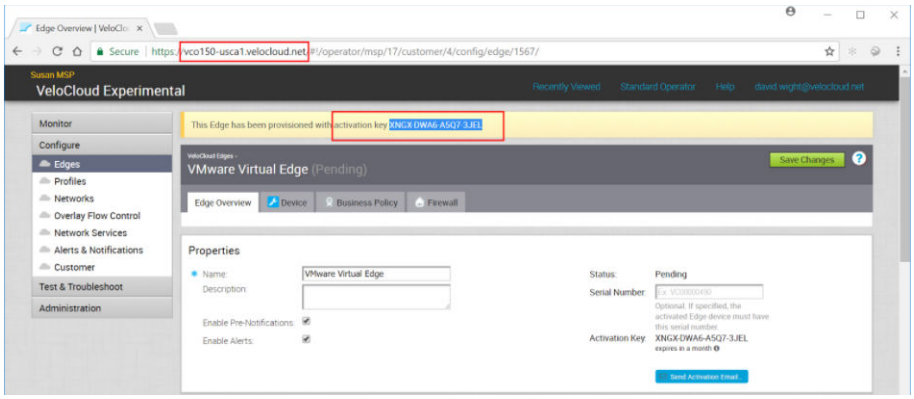
備註 如果您要使用 cloud-init 檔案在 ESXi 上佈建虛擬 Edge，請略過此步驟。



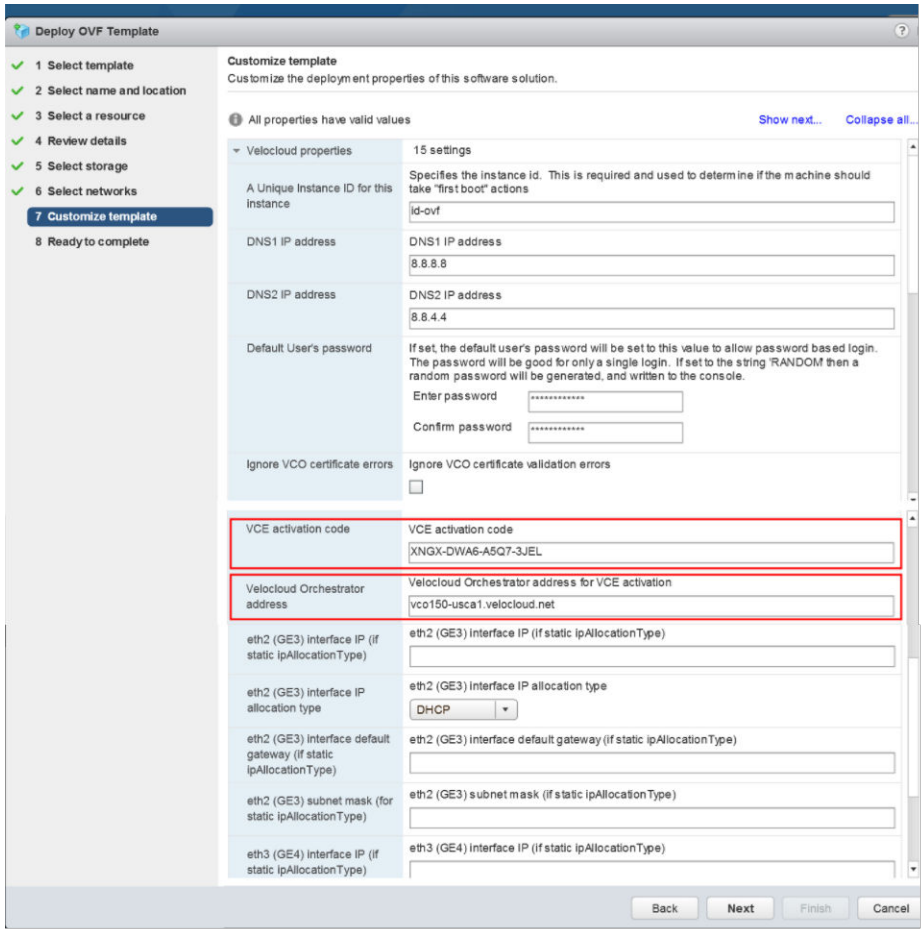
8 指定部署內容以自訂範本。下圖會反白顯示：

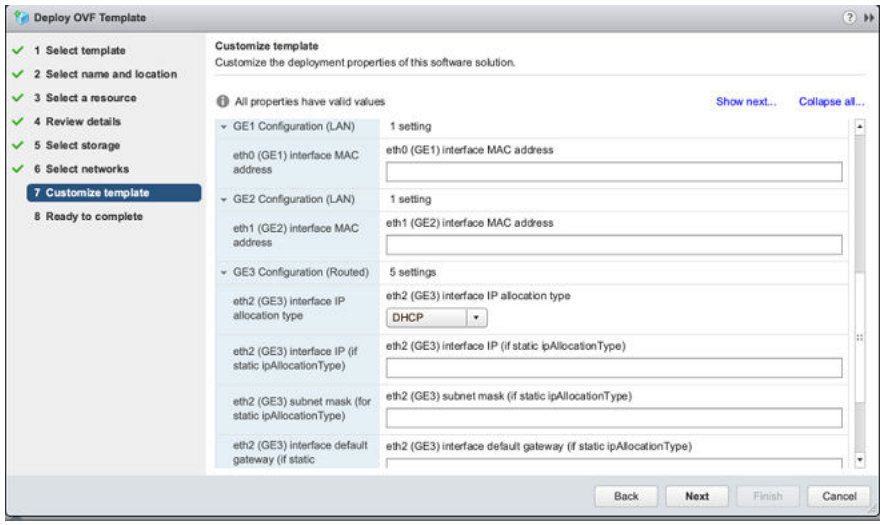
a 從 SD-WAN Orchestrator UI 擷取 URL/IP 位址。您在後續的步驟 c 中將需要此位址。

b 為企業建立新的虛擬 Edge。建立 Edge 後，請複製啟用金鑰。後續的步驟 c 將需要此啟用金鑰。

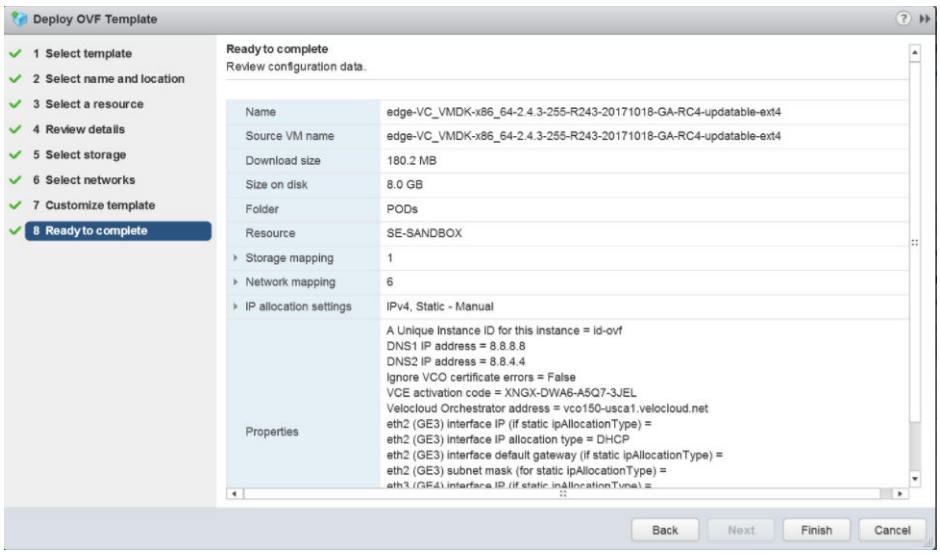


c 在下圖中顯示的自訂範本頁面上，將您在上述步驟 b 中擷取的啟動碼，以及在上述步驟 a 中擷取的 SD-WAN Orchestrator URL/IP 位址，輸入到對應的欄位中。

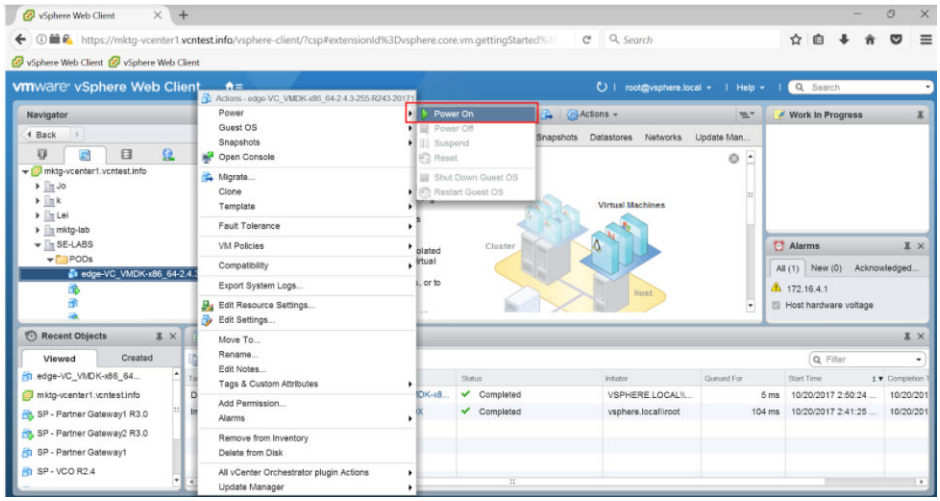

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Show next...
Collapse all...
Velocloud properties
15 settings
A Unique Instance ID for this instance
Specifies the instance id. This is required and used to determine if the machine should take "first boot" actions
id-ovf
DNS1 IP address
8.8.8.8
DNS2 IP address
8.8.4.4
Default User's password
If set, the default user's password will be set to this value to allow password based login. The password will be good for only a single login. If set to the string 'RANDOM' then a random password will be generated, and written to the console.
Enter password
Confirm password
Ignore VCO certificate errors
Ignore VCO certificate validation errors
VCE activation code
XNGX-DWA6-A5Q7-3JEL
Velocloud Orchestrator address
vco150-usca1.velocloud.net
eth2 (GE3) interface IP (if static ipAllocationType)
eth2 (GE3) interface IP allocation type
DHCP
eth2 (GE3) interface default gateway (if static ipAllocationType)
eth2 (GE3) subnet mask (for static ipAllocationType)
eth3 (GE4) interface IP (if static ipAllocationType)
Back
Next
Finish
Cancel


Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Show next...
Collapse all...
GE1 Configuration (LAN)
1 setting
eth0 (GE1) interface MAC address
GE2 Configuration (LAN)
1 setting
eth1 (GE2) interface MAC address
GE3 Configuration (Routed)
5 settings
eth2 (GE3) interface IP allocation type
DHCP
eth2 (GE3) interface IP (if static ipAllocationType)
eth2 (GE3) subnet mask (if static ipAllocationType)
eth2 (GE3) interface default gateway (if static
Back
Next
Finish
Cancel

9 檢閱組態資料。



10 開啟虛擬 Edge 的電源。



Edge 的電源開啟後，將建立對 SD-WAN Orchestrator 的連線。

Azure Virtual WAN SD-WAN Gateway 自動化

24

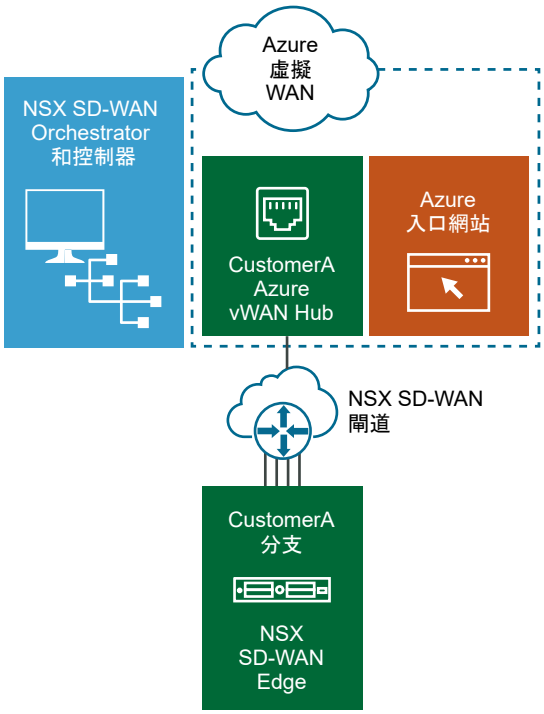
SD-WAN Orchestrator 支援 Azure Virtual WAN 和 SD-WAN Gateway 的整合和自動化，以啟用分支到 VPN 的連線。

本章節討論下列主題：

Azure Virtual WAN SD-WAN Gateway 自動化概觀

Azure Virtual WAN 是一項網路服務，可促使從企業分支位置通往或透過 Microsoft Azure 的虛擬私人網路 (VPN) 連線達到最佳化和自動化。Azure 訂閱者可佈建對應於 Azure 區域的虛擬中樞，並透過 IP 安全性 (IPSec) VPN 連線來連接分支 (不一定已啟用 SD-WAN)。

SD-WAN Orchestrator 可利用 Azure 主幹透過 SD-WAN Gateway 建立分支到 Azure VPN 的連線，以支援 Azure Virtual WAN 與 SD-WAN Gateway 的整合及自動化，如下圖所示。



以下幾節說明如何設定 SD-WAN Orchestrator 和 Azure 以透過 SD-WAN Gateway 啟用分支到 Azure VPN 的連線：

- 設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線
- 設定 SD-WAN Orchestrator 以建立分支到 Azure VPN 的連線

必要的 Azure 組態

企業網路管理員必須在 Azure 入口網站上完成下列必要的組態工作，以確保 SD-WAN Orchestrator 應用程式可作為服務主體 (應用程式的身分識別) 正常運作，以進行 Azure Virtual WAN 與 SD-WAN Gateway 的整合。

- 登錄 SD-WAN Orchestrator 應用程式
- 將 SD-WAN Orchestrator 應用程式指派給參與者角色
- 登錄資源提供者
- 建立用戶端密碼

登錄 SD-WAN Orchestrator 應用程式

說明如何在 Azure Active Directory (AD) 中登錄新的應用程式。

若要在 Azure AD 中登錄新的應用程式：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

程序

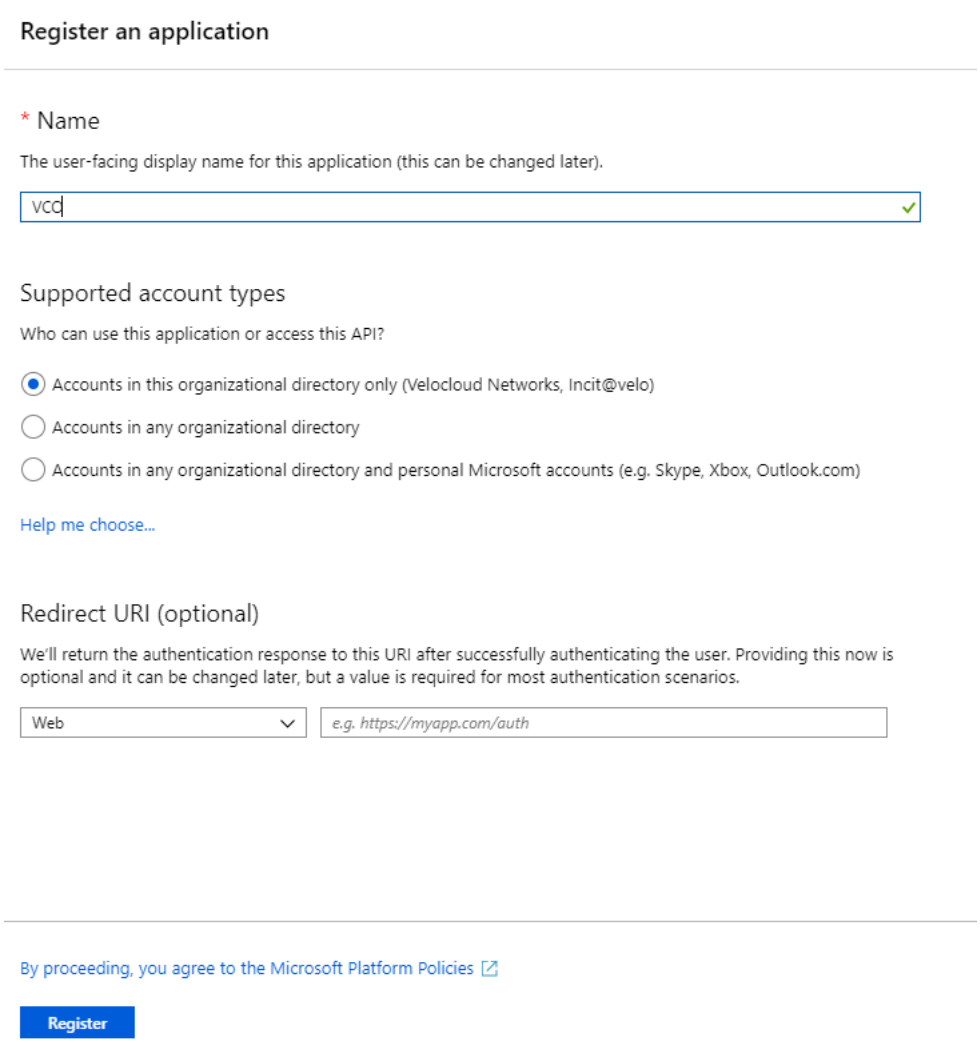
1 登入您的 Microsoft Azure 帳戶。

Microsoft Azure 主畫面隨即出現。

2 按一下**所有服務 (All Services)**，然後搜尋 **Azure Active Directory**。

3 選取 **Azure Active Directory**，然後移至**應用程式登錄 (App registrations)** > **新增登錄 (New registration)**。

登錄應用程式 (Register an application) 畫面隨即出現。



4 在**名稱 (Name)** 欄位中，輸入 SD-WAN Orchestrator 應用程式的名稱。

5 選取支援的帳戶類型，以判斷哪些人可使用該應用程式。

6 按一下**登錄 (Register)**。

結果

您的 SD-WAN Orchestrator 應用程式將登錄並顯示在**所有應用程式 (All applications)** 和**擁有的應用程式 (Owned applications)** 索引標籤中。

請務必記下在 IaaS 訂閱之 SD-WAN Orchestrator 設定期間將會使用的目錄 (承租人) 識別碼和應用程式 (用戶端) 識別碼。

後續步驟

- 將 SD-WAN Orchestrator 應用程式指派給參與者角色
- 建立用戶端密碼

將 SD-WAN Orchestrator 應用程式指派給參與者角色

若要存取 Azure 訂閱中的資源，您必須將應用程式指派給某個角色。您可以將範圍設定為訂閱、資源群組或資源層級。權限會沿用至較低層級的範圍。

若要在訂閱範圍指派參與者角色：

必要條件

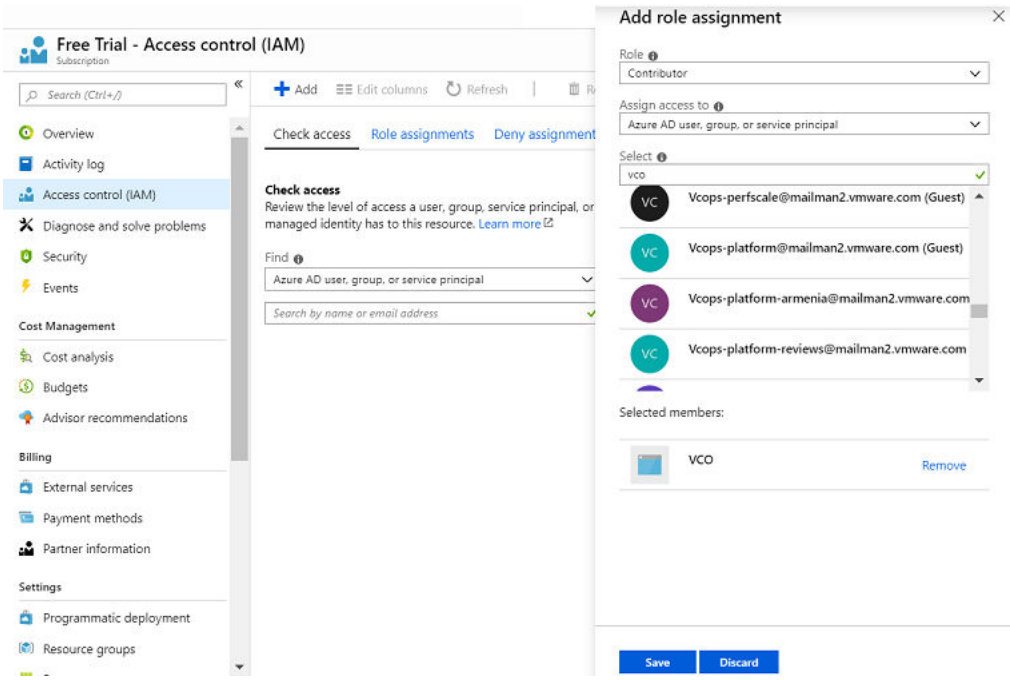
- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

程序

1. 按一下**所有服務 (All Services)** 並搜尋**訂閱 (Subscriptions)**。
2. 在訂閱清單中，選取您要為其指派應用程式的訂閱。如果看不到您要尋找的訂閱，請選取**全域訂閱篩選器 (global subscriptions filter)**。確定已為入口網站選取您所需的訂閱。
3. 按一下**存取控制 (IAM) (Access control (IAM))**。

4 按一下 **+新增 (+Add)** > **新增角色指派 (Add role assignment)**。

新增角色指派 (Add role assignment) 對話方塊隨即出現。



5 在**角色 (Role)** 下拉式功能表中，選取要指派給應用程式的**參與者 (Contributor)** 角色。

若要允許應用程式執行**重新開機**、**啟動**和**停止**執行個體之類的動作，建議使用者將**參與者 (Contributor)** 角色指派給應用程式登錄。

6 在**將存取權指派給 (Assign access to)** 下拉式功能表中，選取 **Azure AD 使用者、群組或服務主體 (Azure AD user, group, or service principal)**。

依預設，Azure AD 應用程式不會顯示在可用的選項中。若要尋找應用程式，請搜尋名稱並加以選取。

7 選取**儲存 (Save)**。

結果

應用程式會指派給參與者角色，並顯示於在該範圍內指派給角色的使用者清單中。

後續步驟

- 建立用戶端密碼
- 設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線

登錄資源提供者

若要下載 Virtual WAN 虛擬私人網路 (VPN) 組態，SD-WAN Orchestrator 需要 Blob 儲存區帳戶作為可下載組態的中間資料存放區。SD-WAN Orchestrator 的目標是要為每個下載工作佈建暫時性的儲存區帳戶，以建立順暢的使用者體驗。若要下載 VPN 站台組態，您必須在 Azure 訂閱上手動登錄

Microsoft.Storage 資源提供者。依預設，系統不會在 Azure 訂閱上登錄 **Microsoft.Storage** 資源提供者。

若要為您的訂閱登錄資源提供者：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。
- 確定您具有參與者或擁有者角色權限。

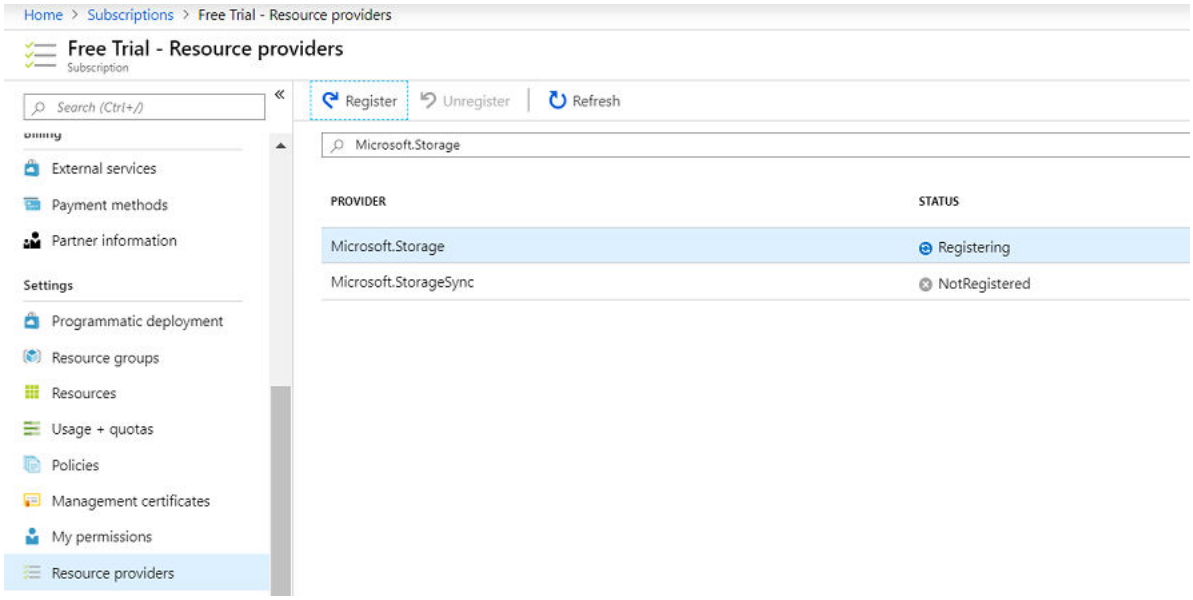
程序

1 登入您的 Microsoft Azure 帳戶。

2 按一下**所有服務 (All Services)** 並搜尋**訂閱 (Subscriptions)**。

3 從訂閱清單中選取您的訂閱。

4 在**設定 (Settings)** 索引標籤下，選取**資源提供者 (Resource providers)**。



5 從可用資源提供者的清單中，選取 **Microsoft.Storage**。然後，按一下**登錄 (Register)**。

結果

資源提供者會隨即登錄，並將您的訂閱設定為與資源提供者搭配使用。

後續步驟

您可以在 Azure 中建立資源，如需相關步驟，請參閱設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線。

建立用戶端密碼

說明如何在 Azure AD 中建立新的用戶端密碼以用於驗證。

若要在 Azure AD 中建立新的用戶端密碼：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

程序

1 登入您的 Microsoft Azure 帳戶。

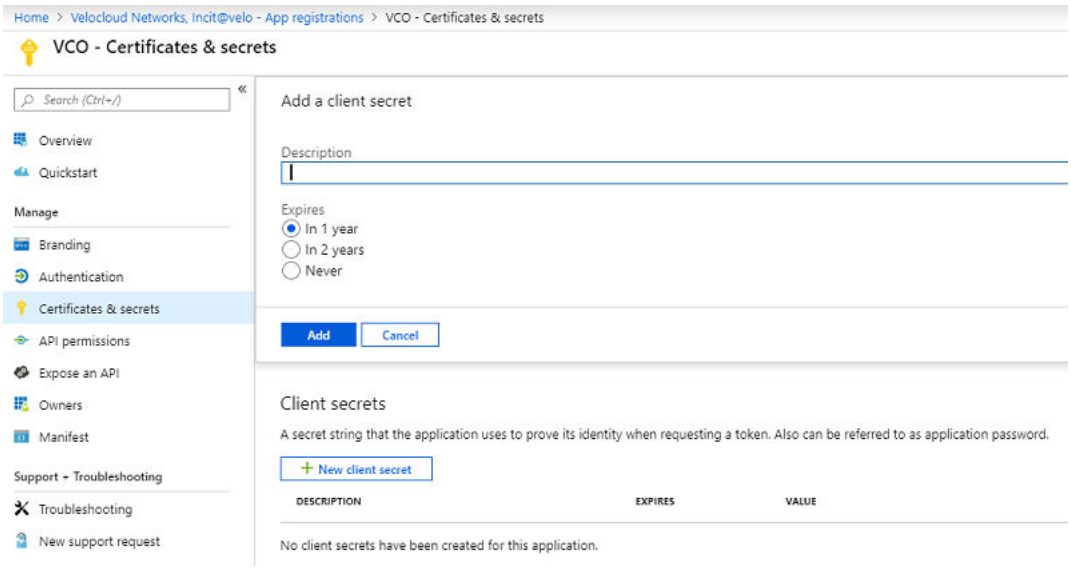
Microsoft Azure 主畫面隨即出現。

2 選取 **Azure Active Directory** > **應用程式登錄 (App registrations)**。

3 在**擁有的應用程式 (Owned applications)** 索引標籤上，按一下已登錄的 SD-WAN Orchestrator 應用程式。

4 移至**憑證和密碼 (Certificates & secrets)** > **新增用戶端密碼 (New client secret)**。

新增用戶端密碼 (Add a client secret) 畫面隨即出現。



5 提供密碼的說明和到期值等詳細資料，然後按一下**新增 (Add)**。

結果

系統會為已登錄的應用程式建立用戶端密碼。

備註 請複製並儲存在 SD-WAN Orchestrator 中的 IaaS 訂閱期間所要使用的新用戶端密碼值。

後續步驟

- 設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線
- 設定 SD-WAN Orchestrator 以建立分支到 Azure VPN 的連線

設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線

本節說明如何設定 Azure 以整合 Azure Virtual WAN 與 SD-WAN Gateway，進而啟用分支到 Azure VPN 的連線。

在您開始設定 Azure Virtual WAN 和其他 Azure 資源之前：

- 確認您的內部部署網路的子網路皆未與要連線的現有虛擬網路重疊。您的虛擬網路不需要閘道子網路，且不可有任何虛擬網路閘道。如需建立虛擬網路的步驟，請參閱建立虛擬網路。
- 取得中樞區域的 IP 位址範圍，並確定您為中樞區域指定的位址範圍未與您所連線的任何現有虛擬網路重疊。
- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

如需在 Azure 入口網站端中需要完成以整合 Azure Virtual WAN 與 SD-WAN Gateway 時各種程序的逐步說明，請參閱：

- 建立資源群組
- 建立虛擬 WAN
- 建立虛擬中樞
- 建立虛擬網路
- 在 VNet 與中樞之間建立虛擬連線

建立資源群組

說明如何在 Azure 中建立資源群組。

若要在 Azure 中建立資源群組：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

程序

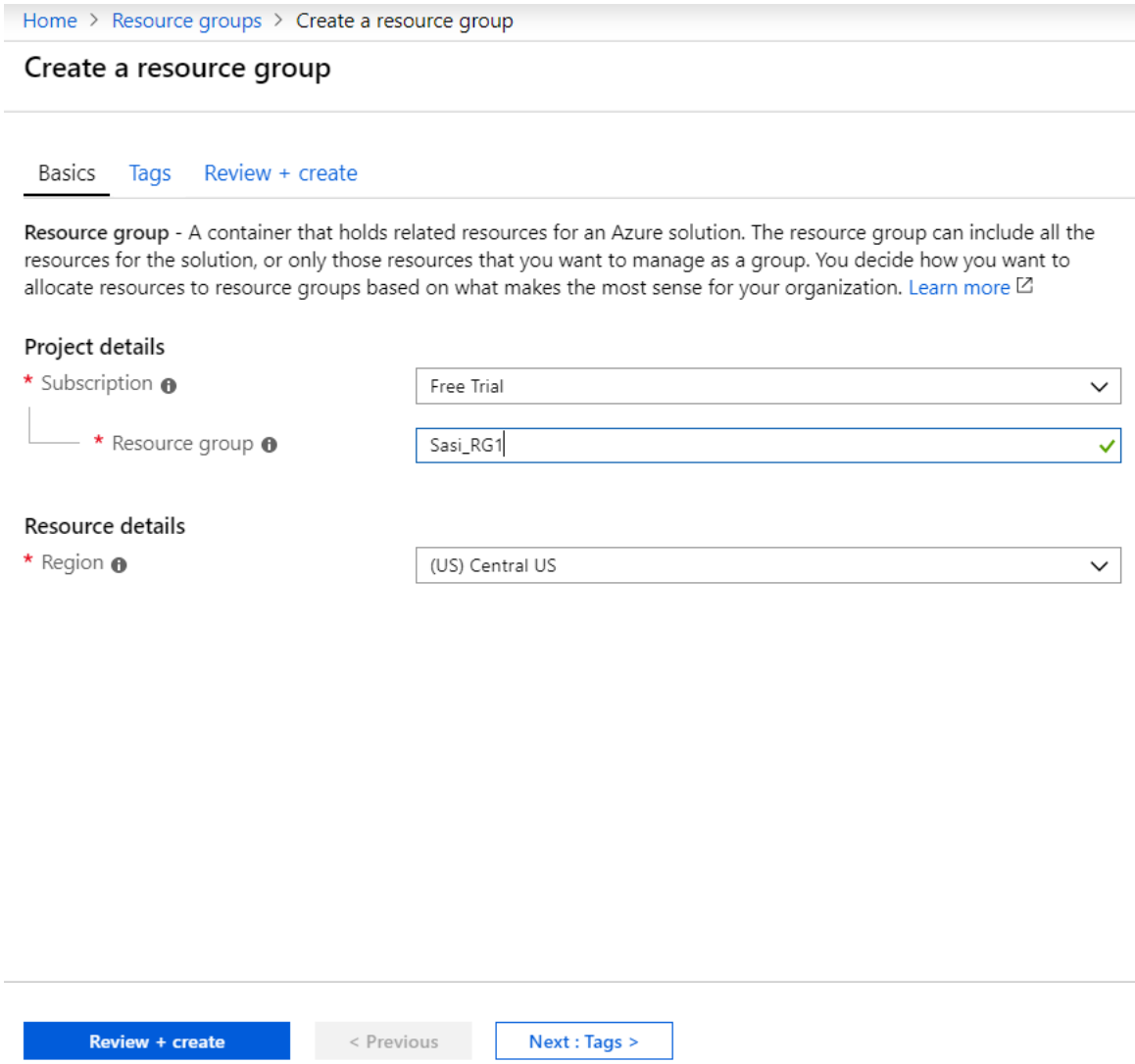
1 登入您的 Microsoft Azure 帳戶。

Microsoft Azure 主畫面隨即出現。

2 按一下**所有服務 (All Services)**，然後搜尋**資源群組 (Resource group)**。

3 選取**資源群組 (Resource group)**，然後按一下 **+新增 (+Add)**。

建立資源群組 (Create a resource group) 畫面隨即出現。



4 在**訂閱 (Subscription)** 下拉式功能表中，選取您的 Microsoft Azure 訂閱。

5 在**資源群組 (Resource group)** 文字方塊中，輸入新資源群組的唯一名稱。

資源群組名稱可以包含英數字元、句號 (.)、底線 (_)、連字號 (-) 和括弧 ()，但名稱不能以句號結尾。

6 在**區域 (Region)** 下拉式功能表中選取您資源群組的位置，您多數的資源都將位於該處。

7 按一下**檢閱+建立 (Review+create)**，然後按一下**建立 (Create)**。

結果

資源群組隨即建立，並顯示在 Azure 入口網站儀表板上。

後續步驟

建立 Azure 虛擬 WAN。如需相關步驟，請參閱建立虛擬 WAN。

建立虛擬 WAN

說明如何在 Azure 中建立虛擬 WAN。

若要在 Azure 中建立虛擬 WAN：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。
- 確定您已建立資源群組以新增虛擬 WAN。

程序

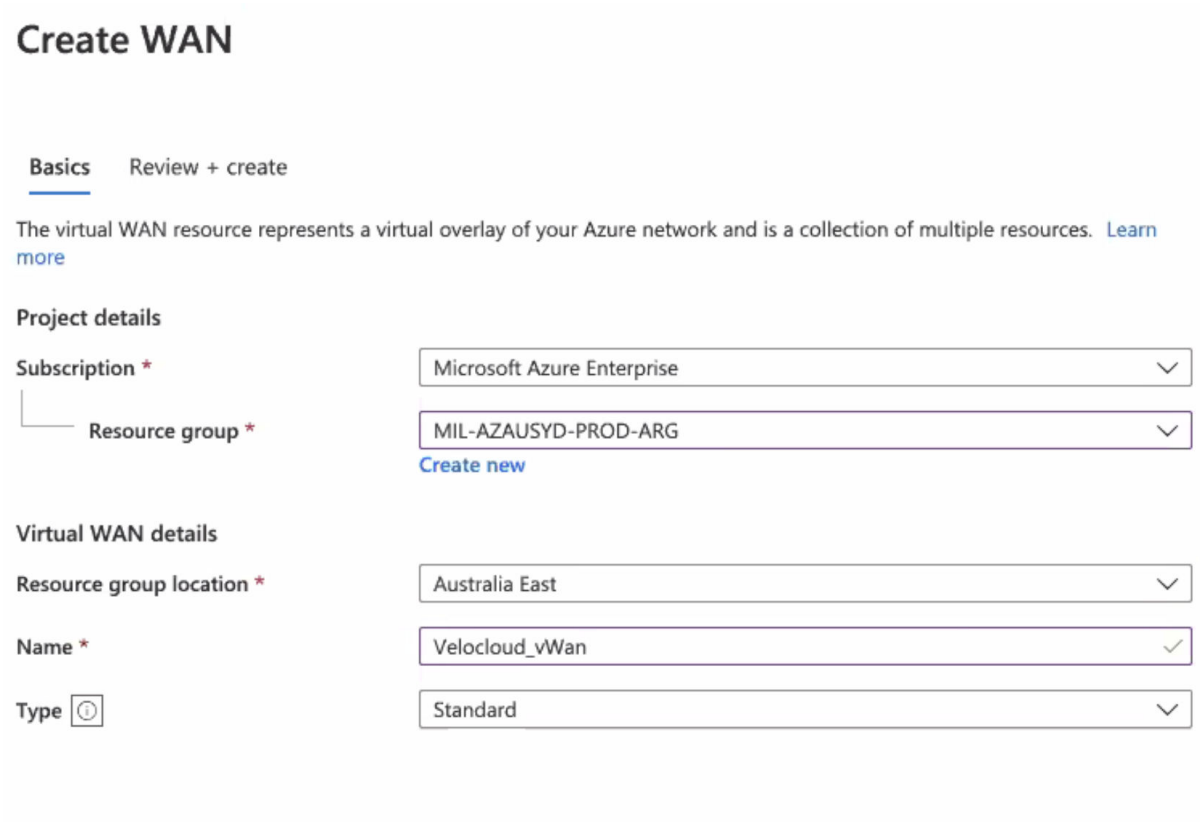
1 登入您的 Microsoft Azure 帳戶。

Microsoft Azure 主畫面隨即出現。

2 按一下**所有服務 (All Services)**，然後搜尋**虛擬 WAN (Virtual WAN)**。

3 選取**虛擬 WAN (Virtual WAN)**，然後按一下 **+新增 (+Add)**。

建立 WAN (Create WAN) 畫面隨即出現。



4 在**訂閱 (Subscription)** 下拉式功能表中，選取您的 Microsoft Azure 訂閱。

5 在**資源群組 (Resource group)** 下拉式功能表中，選取要新增虛擬 WAN 的資源群組。

6 在**資源群組位置 (Resource group location)** 下拉式功能表中，選取與虛擬 WAN 相關聯中繼資料所在的位置。

7 在**名稱 (Name)** 文字方塊中，輸入虛擬 WAN 的唯一名稱。

8 從**類型 (Type)** 下拉式功能表中，選取**標準 (Standard)** 作為虛擬 WAN 類型。

9 按一下**建立 (Create)**。

結果

虛擬 WAN 隨即建立，並顯示在 Azure 入口網站儀表板上。

後續步驟

建立虛擬中樞。如需相關步驟，請參閱建立虛擬中樞。

建立虛擬中樞

說明如何在 Azure 中建立虛擬中樞。

若要在 Azure 中建立虛擬中樞：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。
- 確定您已建立資源群組以新增 Azure 資源。

程序

1 登入您的 Microsoft Azure 帳戶。

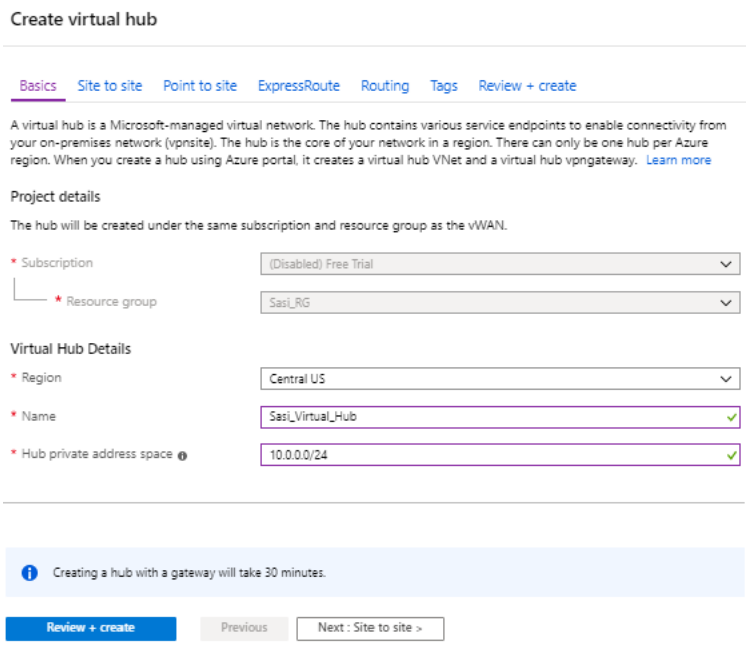
Microsoft Azure 主畫面隨即出現。

2 移至**所有資源 (All resources)**，然後從可用資源清單中選取您已建立的 Virtual WAN。

3 在 **Virtual WAN 架構 (Virtual WAN architecture)** 區域下，按一下**中樞 (Hubs)**。

4 按一下 **+新增中樞 (+New Hub)**。

建立虛擬中樞 (Create virtual hub) 畫面隨即出現。



5 在**基礎 (Basics)** 索引標籤中，輸入下列虛擬中樞詳細資料。

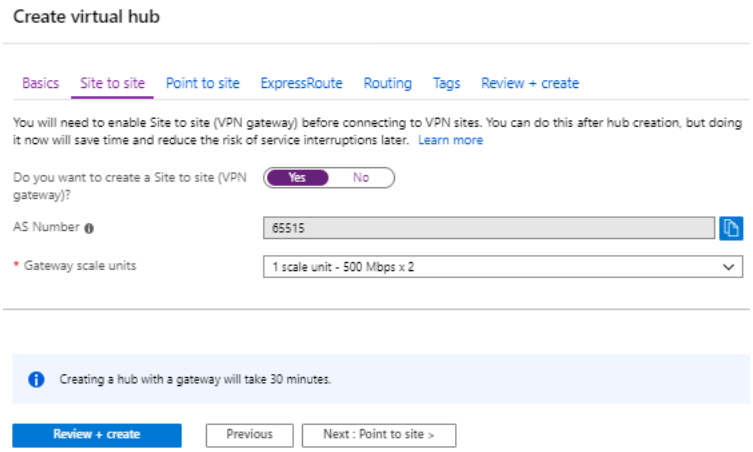
a 在**區域 (Region)** 下拉式功能表中，選取虛擬中樞所在的位置。

b 在**名稱 (Name)** 文字方塊中，輸入中樞的唯一名稱。

c 在**中樞私人位址空間 (Hub private address space)** 文字方塊中，輸入中樞的位址範圍 (採用無類別網域間路由 (CIDR) 表示法)。

6 若要連線至 VPN 站台，請按**下一步：站台對站台 (Next: Site to site)** 並啟用站對站 (VPN 閘道)，然後選取**是 (Yes)** 連線至 VPN 站台。

備註 必須要有 VPN 閘道，通道自動化才能正常運作，否則將無法建立 VPN 連線。



a 在**閘道縮放單位 (Gateway scale units)** 下拉式功能表中，選取調整值。

7 按一下**檢閱 + 建立 (Review + Create)**。

結果

虛擬中樞隨即建立，並顯示在 Azure 入口網站儀表板上。

後續步驟

- 在中樞與虛擬網路 (VNet) 之間建立虛擬連線。如需相關步驟，請參閱在 VNet 與中樞之間建立虛擬連線。
- 如果您沒有現有的 VNet，則可以依照建立虛擬網路中的步驟建立一個。

建立虛擬網路

說明如何在 Azure 中建立虛擬網路。

若要在 Azure 中建立虛擬網路：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。

程序

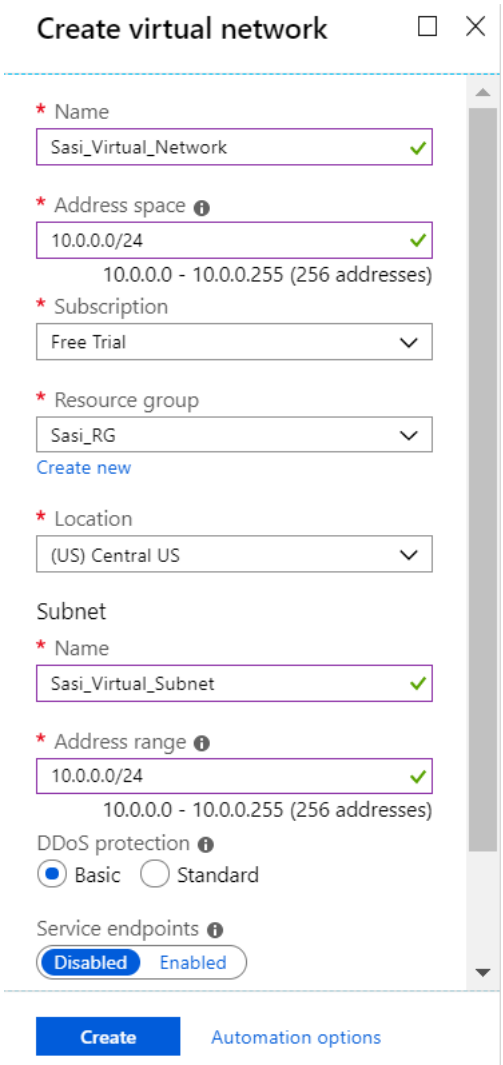
1 登入您的 Microsoft Azure 帳戶。

Microsoft Azure 主畫面隨即出現。

2 按一下**所有服務 (All Services)**，然後搜尋**虛擬網路 (Virtual networks)**。

3 選取**虛擬網路 (Virtual networks)**，然後按一下 **+新增 (+Add)**。

建立虛擬網路 (Create virtual network) 畫面隨即出現。



4 在**名稱 (Name)** 文字方塊中，輸入虛擬網路的唯一名稱。

5 在**位址空間 (Address space)** 文字方塊中，輸入虛擬網路的位址範圍 (採用無類別網域間路由 (CIDR) 表示法)。

6 在**訂閱 (Subscription)** 下拉式功能表中，選取您的 Microsoft Azure 訂閱。

7 在**資源群組 (Resource group)** 下拉式功能表中，選取要新增虛擬網路的資源群組。

8 在**位置 (Location)** 下拉式功能表中，選取虛擬網路所在的位置。

9 在**子網路 (Subnet)** 區域下，輸入子網路的名稱和位址範圍。

請勿對 DDoS 保護、服務端點和防火牆的其他預設設定進行任何變更。

10 按一下**建立 (Create)**。

結果

虛擬網路隨即建立，並顯示在 Azure 入口網站儀表板上。

後續步驟

在中樞與虛擬網路 (VNet) 之間建立虛擬連線。如需相關步驟，請參閱在 VNet 與中樞之間建立虛擬連線。

在 VNet 與中樞之間建立虛擬連線

說明如何在特定 Azure 區域中的虛擬網路 (VNet) 與虛擬中樞之間建立虛擬連線。

若要在特定 Azure 區域中的 VNet 與虛擬中樞之間建立虛擬網路連線：

必要條件

- 確定您具有 Azure 訂閱。如果沒有，請建立免費帳戶。
- 確定您已建立虛擬中樞和虛擬網路。

程序

1 登入您的 Microsoft Azure 帳戶。

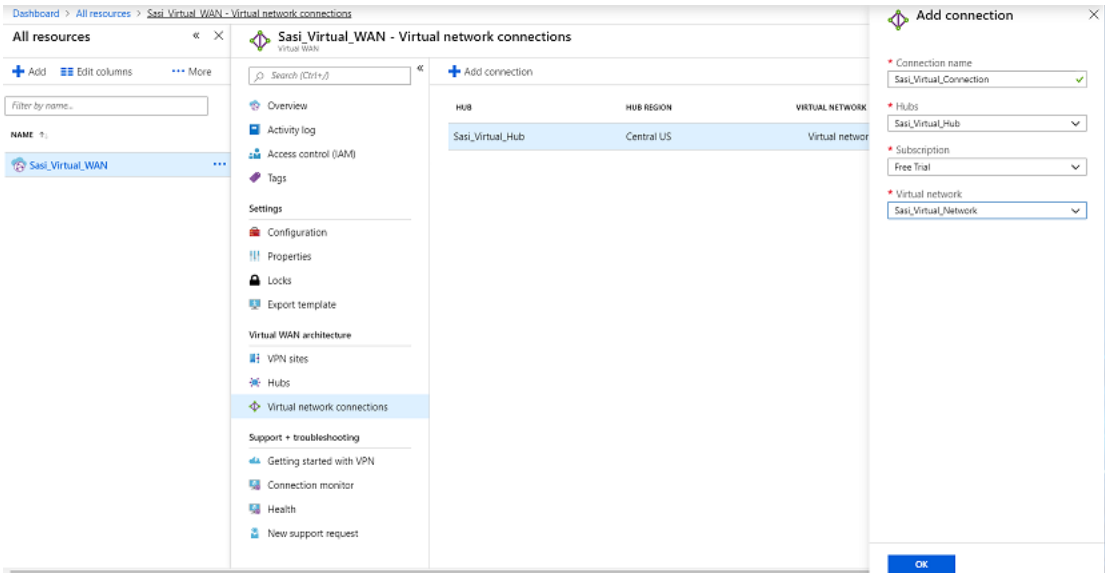
Microsoft Azure 主畫面隨即出現。

2 移至**所有資源 (All resources)**，然後從可用資源清單中選取您已建立的 Virtual WAN。

3 在 **Virtual WAN 架構 (Virtual WAN architecture)** 區域下，按一下**虛擬網路連線 (Virtual network connections)**。

4 按一下 **+新增連線 (+Add connection)**。

新增連線 (Add connection) 畫面隨即出現。



5 在**連線名稱 (Connection name)** 文字方塊中，輸入虛擬連線的唯一名稱。

6 在**中樞 (Hubs)** 下拉式功能表中，選取要與此連線相關聯的中樞。

7 在**訂閱 (Subscription)** 下拉式功能表中，選取您的 Microsoft Azure 訂閱。

8 在**虛擬網路 (Virtual network)** 下拉式功能表中，選取要連線至此中樞的虛擬網路。

9 按一下**確定 (OK)**。

結果

將在選取的 VNet 與中樞之間會建立對等連線。

後續步驟

- 設定 SD-WAN Orchestrator 以建立分支到 Azure VPN 的連線

設定 SD-WAN Orchestrator 以建立分支到 Azure VPN 的連線

您可以設定 SD-WAN Orchestrator 以整合 Azure Virtual WAN 與 SD-WAN Gateway，進而啟用分支到 Azure VPN 的連線。

備註 依預設，會停用 Azure Virtual WAN 功能。若要啟用此功能，您必須將 `session.options.enableAzureVirtualWAN` 系統內容設定為 `true`。

在您開始進行 Azure Virtual WAN SD-WAN Gateway 自動化的 SD-WAN Orchestrator 設定之前，請先確定您已完成必要的 Azure 組態和設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線小節中說明的所有步驟。

如需在 SD-WAN Orchestrator 端中需要完成以整合 Azure Virtual WAN 與 SD-WAN Gateway 的各種程序的逐步說明，請參閱：

- 設定 IaaS 訂閱網路服務
- 設定 Microsoft Azure Non VMware SD-WAN Site
- 同步 VPN 組態

設定 IaaS 訂閱網路服務

說明如何在 SD-WAN Orchestrator 中設定基礎結構即服務提供者 (IaaS) 訂閱。

若要在 SD-WAN Orchestrator 中設定 IaaS 訂閱：

必要條件

請確定您已在 Azure 入口網站中登錄 SD-WAN Orchestrator 應用程式和建立的用戶端密碼。如需相關步驟，請參閱必要的 Azure 組態。

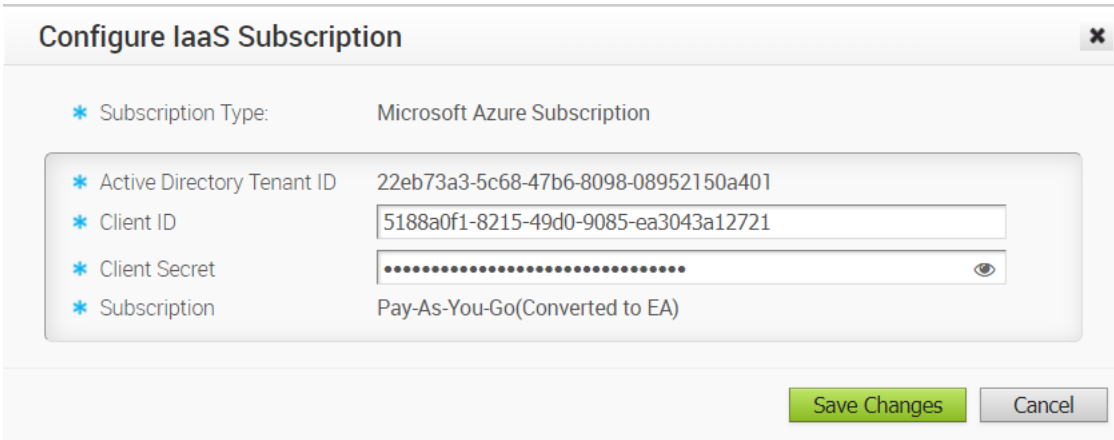
程序

1 在 SD-WAN Orchestrator 的導覽面板中，移至**設定 (Configure)** > **網路服務 (Network Services)**。

服務 (Services) 畫面隨即出現。

2 在 **Iaas 訂閱 (Iaas Subscriptions)** 區域中，按一下**新增 (New)** 按鈕。

設定 IaaS 訂閱 (Configure IaaS Subscription) 對話方塊隨即出現。



3 在 **訂閱類型 (Subscription Type)** 下拉式功能表中，選取 **Microsoft Azure 訂閱 (Microsoft Azure Subscription)**。

4 輸入與您的 SD-WAN Orchestrator 應用程式登錄相對應的 Active Directory 承租人識別碼、用戶端識別碼和用戶端密碼。

5 按一下**取得訂閱 (Get Subscriptions)** 按鈕，以擷取已為應用程式登錄配置 IAM 角色的 Azure 訂閱清單。

6 按一下**儲存變更 (Save Changes)**。

後續步驟

設定 Microsoft Azure 虛擬中樞類型的 Non VMware SD-WAN Site。如需詳細資訊，請參閱設定 Microsoft Azure Non VMware SD-WAN Site。

設定 Microsoft Azure Non VMware SD-WAN Site

說明如何在 SD-WAN Orchestrator 中設定 **Microsoft Azure 虛擬中樞**類型的 Non VMware SD-WAN Site。

若要在 SD-WAN Orchestrator 中設定 **Microsoft Azure 虛擬中樞**類型的 NVS：

必要條件

- 確定您已設定 IaaS 訂閱。如需相關步驟，請參閱設定 IaaS 訂閱網路服務。
- 確定您已在 Azure 中建立 Virtual WAN 和中樞。如需相關步驟，請參閱設定 Azure Virtual WAN 以建立分支到 Azure VPN 的連線。

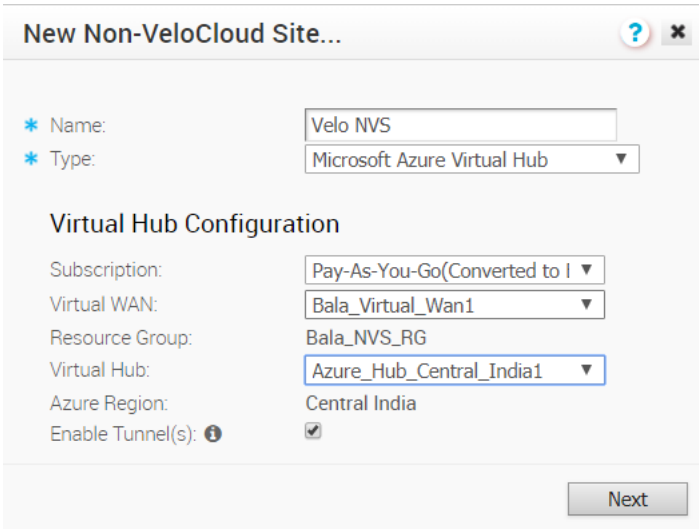
程序

1 在 SD-WAN Orchestrator 的導覽面板中，移至**設定 (Configure)** > **網路服務 (Network Services)**。

服務 (Services) 畫面隨即出現。

2 在 [非 VeloCloud 站台 (Non-VeloCloud Sites)] 區域中，按一下**新增 (New)** 按鈕。

新增非 VeloCloud 站台 (New Non-VeloCloud Site) 對話方塊隨即出現。



3 在**名稱 (Name)** 文字方塊中，輸入 Non VMware SD-WAN Site 的名稱。

4 在**類型 (Type)** 下拉式功能表中，選取 **Microsoft Azure 虛擬中樞 (Microsoft Azure Virtual Hub)**。

5 在**訂閱 (Subscription)** 下拉式功能表中，選取訂閱。

應用程式會從 Azure 動態擷取所有可用的 Virtual WAN。

6 在 **Virtual WAN** 下拉式功能表中，選取 Virtual WAN。

應用程式會自動填入與 Virtual WAN 相關聯的資源群組。

7 在**虛擬中樞 (Virtual Hub)** 下拉式功能表中，選取虛擬中樞。

應用程式會自動填入與中樞對應的 Azure 區域

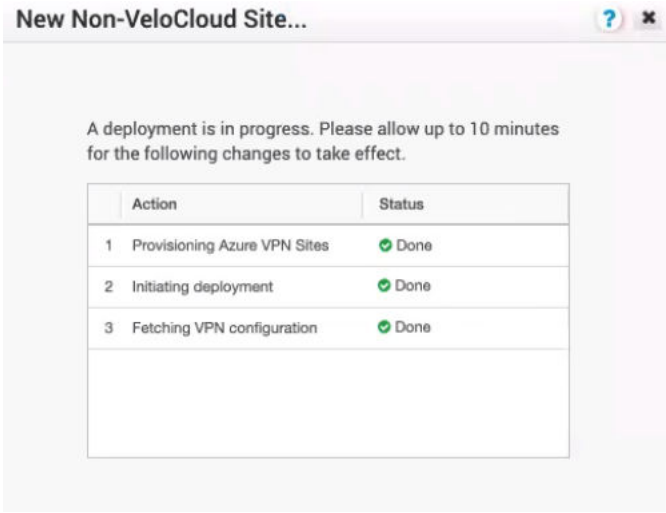
8 選取**啟用通道 (Enable Tunnel(s))** 核取方塊，使 VMware VPN 閘道在站台成功佈建後隨即起始對目標虛擬中樞的 VPN 連線。

備註 在至少一個設定檔上設定此 Non VMware SD-WAN Site 之前，VMware VPN 閘道將不會起始 IKE 交涉。

備註 依預設，針對 Microsoft Azure Non VMware SD-WAN Site 使用的本機驗證識別碼值為 SD-WAN Gateway 介面公用 IP。

9 按**下一步 (Next)**。

SD-WAN Orchestrator 會自動起始部署、佈建 Azure VPN 站台、下載新設定站台的 VPN 站台組態，並將組態儲存在 SD-WAN OrchestratorSD-WAN Orchestrator 的 Non VMware SD-WAN Site 組態資料庫中。



結果

在 SD-WAN Orchestrator 端佈建 Azure VPN 站台之後，您可以導覽至 **Virtual WAN** 頁面 > **Virtual WAN 架構 (Virtual WAN architecture)** > **VPN 站台 (VPN sites)**，在 Azure 入口網站中檢視 VPN 站台 (主要和備援)。

後續步驟

- 將 Microsoft Azure Non VMware SD-WAN Site 與設定檔相關聯，以便在分支與 Azure 虛擬中樞之間建立通道。如需詳細資訊，請參閱將 Non VMware SD-WAN Site 與設定檔相關聯。
- 您必須手動將 SD-WAN 路由新增至 Azure 網路。如需詳細資訊，請參閱編輯 VPN 站台。

將 Non VMware SD-WAN Site 與設定檔相關聯

在 SD-WAN Orchestrator 中設定 **Microsoft Azure 虛擬中樞 (Microsoft Azure Virtual Hub)** 類型的 Non VMware SD-WAN Site 之後，您必須將 Non VMware SD-WAN Site 與所需的設定檔相關聯，才能建立 SD-WAN Gateways 與 Microsoft Azure 虛擬中樞之間的通道。

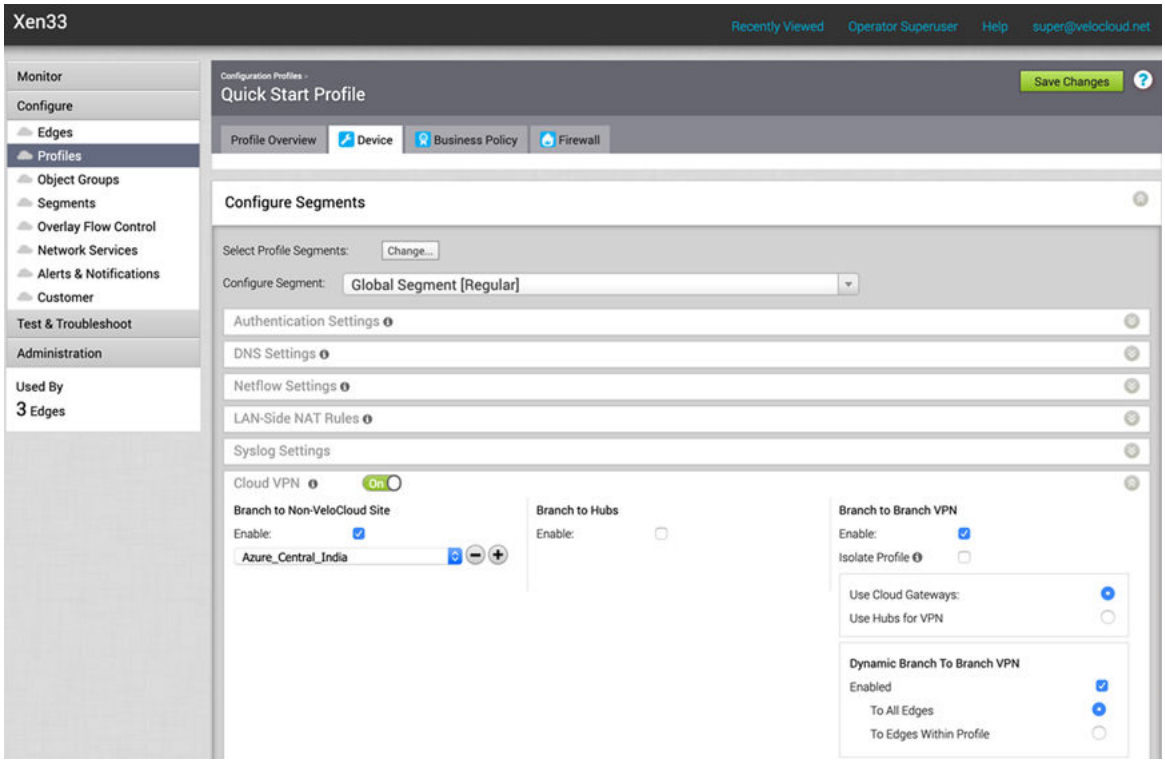
若要將 Non VMware SD-WAN Site 與設定檔相關聯，請執行下列步驟：

程序

1 在 SD-WAN Orchestrator 導覽面板中，移至**設定 (Configure)** > **設定檔 (Profiles)**。

組態設定檔 (Configuration Profiles) 頁面隨即出現。

2 選取您想要與 **Microsoft Azure 虛擬中樞 (Microsoft Azure Virtual Hub)** 類型的 Non VMware SD-WAN Site 相關聯的設定檔，然後按一下**裝置 (Device)** 資料行下的圖示。



所選設定檔的**裝置設定 (Device Settings)** 頁面隨即出現。

3 移至**雲端 VPN (Cloud VPN)** 區域，並藉由**開啟**切換按鈕來啟用雲端 VPN。

4 在**分支到非 VeloCloud 站台 (Branch to Non-VeloCloud Site)** 下方，選取**啟用 (Enable)** 核取方塊。

5 從下拉式功能表中，選取 **Microsoft Azure 虛擬中樞 (Microsoft Azure Virtual Hub)** 類型的 Non VMware SD-WAN Site，以建立分支與 Microsoft Azure Non VMware SD-WAN Site 之間的 VPN 連線。

6 按一下**儲存變更 (Save Changes)**。

結果

分支與 Microsoft Azure Non VMware SD-WAN Site 之間會建立通道。如需詳細資訊，請參閱設定分支到 Non VMware SD-WAN Site VPN。

編輯 VPN 站台

說明如何手動將 SD-WAN 路由新增至 Azure 網路中。

若要將 SD-WAN 路由手動新增至 Azure 網路中：

必要條件

請確定您已在 SD-WAN Orchestrator 端完成 Azure VPN 站台的佈建。

程序

1 登入您的 Microsoft Azure 帳戶。

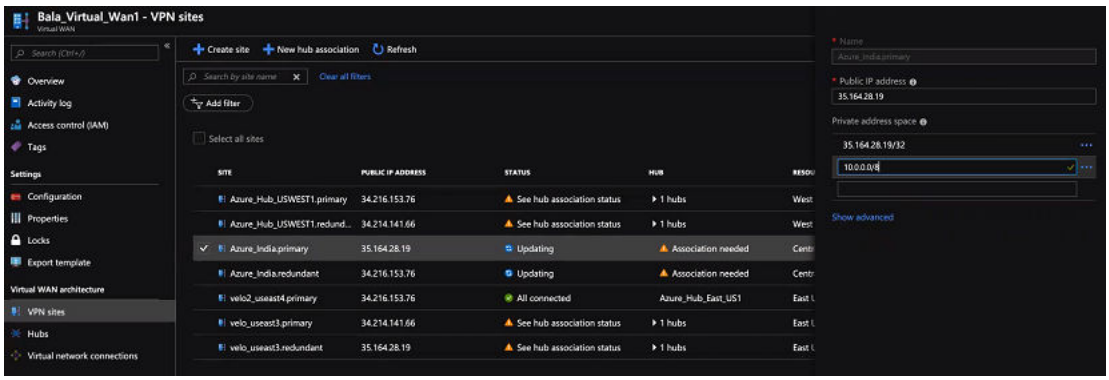
Microsoft Azure 主畫面隨即出現。

2 移至**所有資源 (All resources)**，然後從可用資源清單中選取您已建立的 Virtual WAN。

3 在 **Virtual WAN 架構 (Virtual WAN architecture)** 區域下，按一下 **VPN 站台 (VPN sites)**。

4 從可用的 VPN 站台清單中，選取您因使用 SD-WAN Orchestrator 完成 Non VMware SD-WAN Site 佈建步驟而新增的 VPN 站台 (例如 Non VMware SD-WAN Site name.primary)。

5 按一下所選 VPN 站台的名稱，然後從下一個畫面的頂端選取**編輯站台 (Edit site)**。



6 在**私人位址空間 (Private address space)** 文字方塊中，輸入 SD-WAN 路由的位址範圍。

7 按一下**確認 (Confirm)**。

同樣地，您也可以依照上述步驟來編輯備援 VPN 站台。

同步 VPN 組態

成功佈建 Non VMware SD-WAN Site 後，每當 Azure 中樞或靜態路由的端點 IP 位址發生變更，您就必須重新同步 Azure 虛擬中樞與 Non VMware SD-WAN Site 組態。按一下**非 VeloCloud 站台 (Non-VeloCloud Sites)** 區域中的**重新同步組態 (Resync configuration)** 按鈕，將會自動從 Azure 入口網站擷取 VPN 組態詳細資料，並更新 SD-WAN Orchestrator 本機組態。

刪除 Non VMware SD-WAN Site

說明若要刪除與 Azure 虛擬中樞對應的 Non VMware SD-WAN Site，藉以確保 SD-WAN Orchestrator 與 Azure 在刪除後的 Virtual WAN 部署狀態能夠保持一致，則必須執行的相關步驟。

程序

1 刪除與預計要刪除之 VPN 站台相關聯的 Azure VPN 連線。

2 使用 Azure API，刪除代表為該虛擬中樞所選取之 Non VMware SD-WAN Site SD-WAN Gateways 佈建的 Azure VPN 站台。

備註 如果未移除與 VPN 站台 (預計要刪除) 相關聯的 VPN 連線，則刪除 Azure VPN 站台將會失敗。