

BPA使用手冊OS升級v5.1

- [簡介](#)
 - [主要功能](#)
 - [端到端流](#)
 - [價值主張](#)
 - [支援的控制器和裝置平台](#)
 - [新功能](#)
- [必要條件](#)
- [使用作業系統升級應用程式](#)
 - [軟體映像管理](#)
 - [軟體映像](#)
 - [同步軟體映像後設資料](#)
 - [新增軟體映像後設資料](#)
 - [批次上傳軟體映像後設資料](#)
 - [編輯現有軟體映像後設資料](#)
 - [刪除軟體映像後設資料](#)
 - [影像發佈伺服器管理](#)
 - [影像發佈伺服器](#)
 - [新增映象檔案伺服器詳細資訊](#)
 - [編輯映象檔案伺服器詳細資訊](#)
 - [刪除映象檔案伺服器詳細資訊](#)
 - [軟體洞察](#)
 - [必要條件](#)
 - [將軟體見解資料提取到BPA](#)
 - [檢視和管理安全建議](#)
 - [檢視和管理優先順序錯誤](#)
 - [檢視軟體見解](#)
 - [檢視和選擇供應商建議的軟體版本](#)
 - [識別需要軟體升級的裝置](#)
 - [軟體符合性](#)
 - [必要條件](#)
 - [在引用資料管理應用程式中建立EPLD模組資料](#)
 - [檢視和管理軟體符合性](#)
 - [建立軟體一致性策略](#)
 - [按需執行軟體一致性檢查](#)
 - [安排執行軟體一致性檢查](#)
 - [更新軟體一致性策略](#)
 - [刪除軟體一致性策略](#)
 - [檢視和下載符合性結果](#)
 - [升級策略](#)
 - [必要條件](#)
 - [檢視和管理升級策略](#)
 - [建立升級策略](#)

- [橋接SMU](#)
- [編輯升級策略](#)
- [檢視升級策略](#)
- [刪除升級策略](#)
- [控制對升級策略的訪問](#)
- [升級作業](#)
 - [必要條件](#)
 - [檢視和管理升級作業](#)
 - [計畫升級作業](#)
 - [編輯作業中的批處理](#)
 - [升級作業執行和進度監控](#)
 - [下載軟體升級報告](#)
 - [存檔作業](#)
 - [刪除作業](#)
 - [刪除作業中的批處理](#)
 - [取消作業](#)
 - [回滾已完成的作業或升級](#)
- [設定](#)
 - [軟體符合性](#)
 - [回滾](#)
- [部署配置](#)
- [存取控制](#)
 - [基於角色的訪問控制](#)
 - [資源組](#)
 - [零信任標誌設定](#)
- [作業系統升級問題故障排除](#)
 - [建立一致性策略時看不到目標裝置型號](#)
 - [軟體符合性顯示非運行狀態](#)
 - [某些裝置的軟體一致性結果狀態未知](#)
 - [升級作業完成進度百分比](#)
 - [作業計畫已達到，裝置停滯在「等待」狀態](#)

簡介

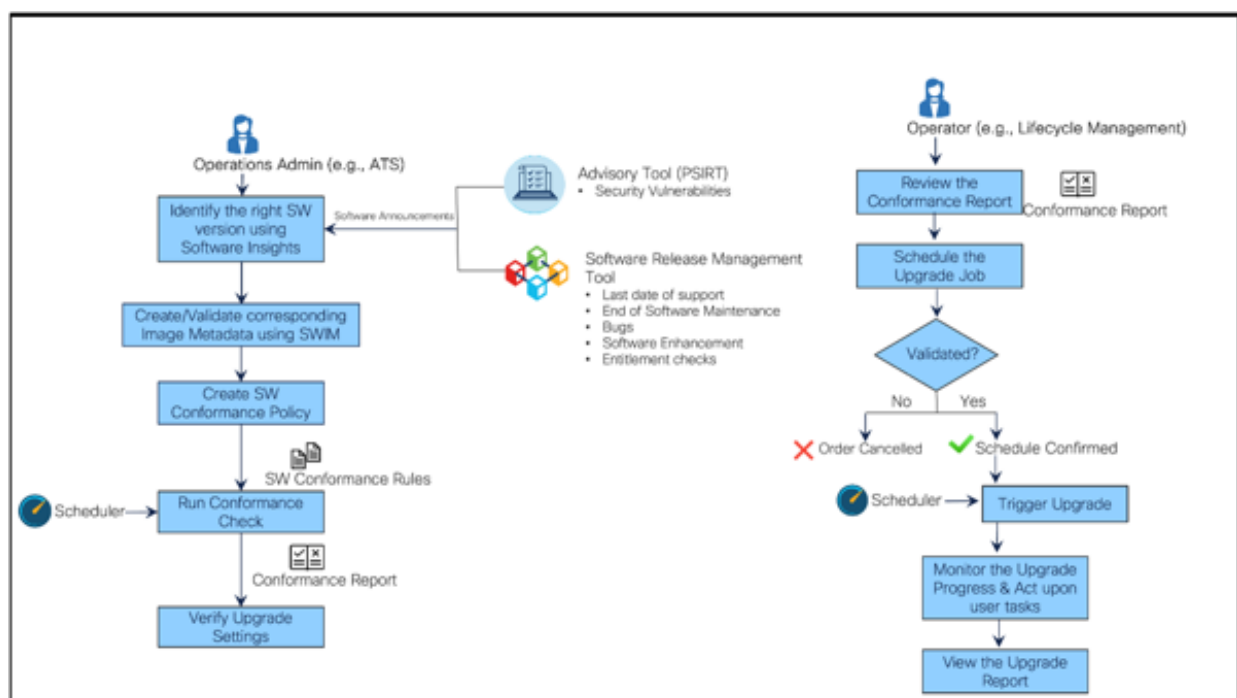
Business Process Automation(BPA)OS Upgrade應用程式提供全面的自動化解決方案，可在不同域間執行網路裝置的軟體一致性和升級。它支援多個域控制器並提供統一的使用者體驗。它支援基本作業系統(OS)升級和軟體維護更新(SMU)或RPM軟體包管理器(RPM)補丁更新。

主要功能

OS升級應用程式提供以下關鍵自動化功能：

- 軟體映像管理:供軟體升級過程使用的軟體映像及其版本（來自所有供應商）的集中清單
- 軟體見解:識別暴露於網路資產的軟體風險和漏洞，並獲取有關供應商推薦軟體版本的見解
- 軟體符合性:標識網路中必須升級其軟體映像的所有資產
- 升級程式方法(MOP)定義:為每個供應商裝置型號或系列預先定義升級過程以及預先檢查和後期檢查
- 升級作業:在跨地理區域的維護時段內安排非一致性資產的升級，監控升級進度，並獲得詳細的報告

端到端流



端到端流

上圖描述了兩種不同使用者角色的OS升級應用程式呼叫流：操作管理員和網路操作員，開箱即用(OOB)。有關OOB角色和相應許可權的詳細資訊，請參閱[訪問控制](#)。

《女神異聞錄》	說明	工作空間
操作管理員	發現影響網路資產的軟體漏洞（例如，諮詢、錯誤、壽命終止公告）	BPA:作業系統升級/軟體映像管理/諮詢
操作管理員	確定受影響的軟體版本和受影響的資產，並根據供應商提供的建議確定正確的目標版本	BPA:作業系統升級/軟體映像管理/洞察
操作管理員	建立所需的軟體映像後設資料	BPA:作業系統升級/軟體映像管理/軟體映像
操作管理員	為受影響的裝置模型建立意圖並按需或按計畫的策略執行策略	BPA:作業系統升級/軟體一致性策略

《女神異聞錄》	說明	工作空間
操作管理員	標識不符合項或受影響的資產	BPA:作業系統升級/軟體一致性/檢視結果
操作管理員	根據升級MOP建立或修改升級策略；這包括預先定義預檢查和後檢查、分發或啟用工作流、流量轉移或逆轉，以及單步或多步升級的回滾	BPA:作業系統升級/升級策略
網路運營商	安排作業以升級所有不符合項裝置	BPA:作業系統升級/升級作業
網路運營商	監視升級作業進度	BPA:作業系統升級/升級作業/作業詳細資訊
網路運營商	執行使用者任務（如果有）以解決問題，並使流程繼續下一步	BPA:作業系統升級/升級作業/作業詳細資訊

價值主張

作業系統升級應用程式提供了以下附加值：

- 一種API — 第一種方法，使北向運營支援系統(OSS)和業務支援系統(BSS)的服務消耗更加輕鬆
- 通過由各種域控制器管理的網路快速驗證網路裝置軟體一致性
- 操作員可以通過使用批處理、排隊和排程機制對升級作業進行更多的控制
- 可以提前建立升級作業以供檢視並在稍後執行
- 一種排隊機制，能夠以最少到零的故障實現更快、更好的吞吐量
- 升級前自動配置備份，在發生故障時實現無縫恢復
- 檢查前和檢查後執行，確保成功升級而不中斷服務
- 一種策略驅動的方法，通過驗證前和驗證後檢查、分發或啟用、流量轉移或反向以及回滾過程，靈活地預先定義升級MOP，允許根據需要對其進行自定義

支援的控制器和裝置平台

以下平台已在BPA中驗證，並且受支援OOB。但是，該框架是通用的，可以擴展到新的平台。未來版本將根據優先順序為其他平台提供OOB支援。

域控制器	裝置平台
Cisco Catalyst中心v2.3.7.5-70434	- Cisco IOS、Cisco IOS-XE
vManage v20.12.4	- Cisco IOS、Cisco IOS-XE
附註：裝置必須是v17.9.x或更高版本，遠端伺服器分發	

域控制器

裝置平台

才能正常工作

Nexus控制面板光纖控制器
(NDFC)v12.1.2e和v12.2.2

- Cisco-NXOS(N9k)

防火牆管理中心(FMC)v7.4.1

- Firepower 3140

- Cisco-IOSXR(NCS540、NCS560、ASR9K)

- Cisco-NXOS(N9K)

網路服務協調器(NSO)v6.3

附註：需要NX-OS NED v5.25.17或更高版本

交叉網路控制器(CNC)v6.0

- Cisco-IOSXR(NCS540、ASR9K)

ANSIBLE v2.9.18(AWX - 17.1.0)

- Cisco-IOSXR(NCS540、ASR9K)

直接到裝置(通過遠端網路(Telnet)和安全
外殼(SSH))

- Cisco-IOSXR(NCS540、ASR9K)

新功能

有關此版本的作業系統升級使用情形可用的增量功能，請參閱[BPA發行說明](#)。

必要條件

在使用作業系統升級應用程式之前，必須滿足以下前提條件：

- 作業系統升級、備份和恢復、計畫程式服務和所有必需的平台服務或控制器代理服務均已啟動並正在運行
- 載入所需的對象（例如，工作流、流程模板、預設升級策略等）
- 新增所需的控制器並成功同步裝置；如需詳細資訊，請參閱[支援的控制器和裝置平台](#)

使用作業系統升級應用程式

作業系統升級應用程式由以下元件組成：

- 軟體映像管理(SWIM)
- 影像發佈伺服器管理
- 軟體洞察
- 軟體符合性
- 升級策略
- 升級作業

- 設定

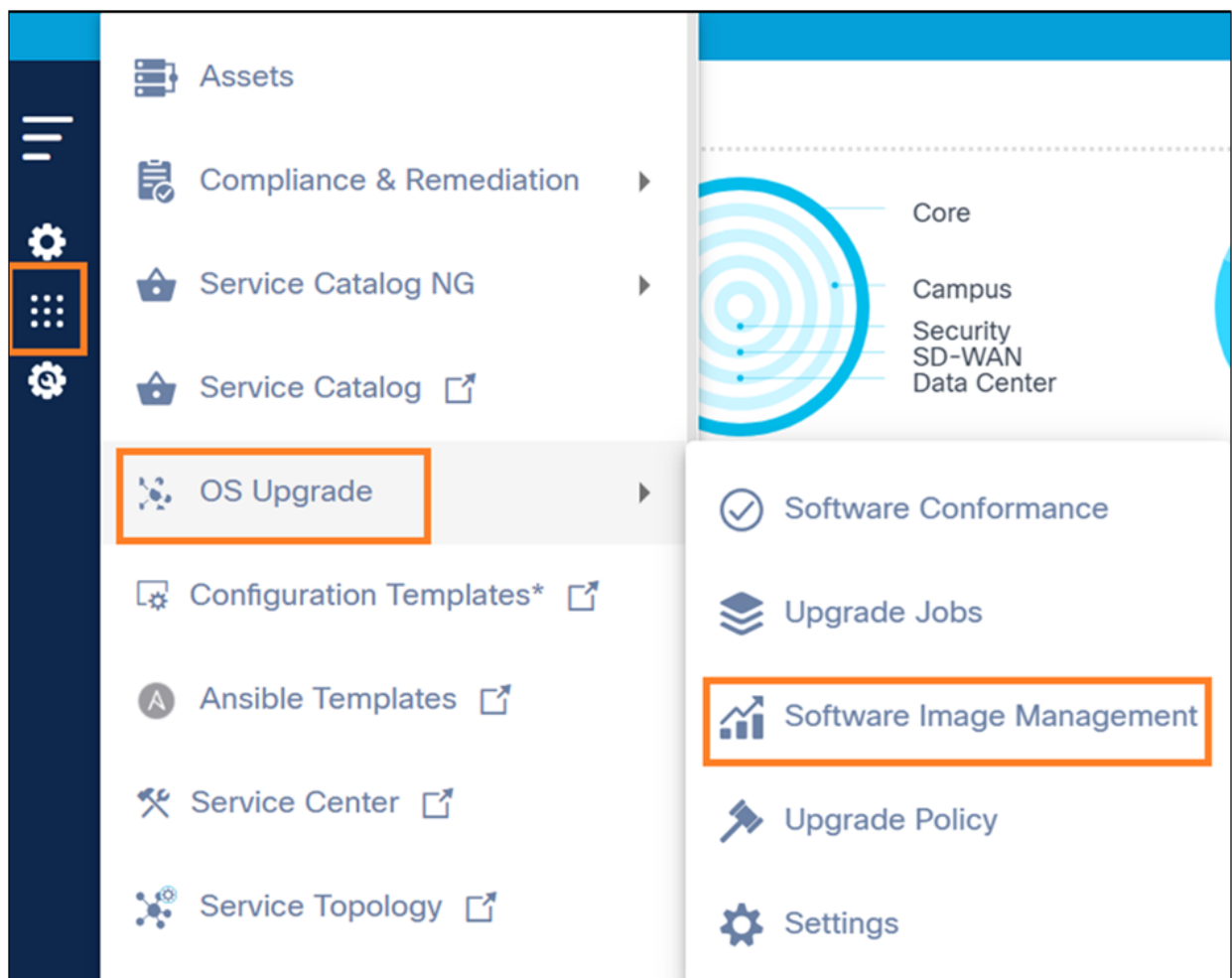
軟體映像管理

SWIM元件允許Operations使用者維護沒有OOB映像管理支援的控制器（如NSO、ANSIBLE、CNC、FMC和直接到裝置）的軟體映像詳細資訊。它還列出由vManage、NDFC和Cisco Catalyst Center等控制器維護的軟體映像詳細資訊，從而提供了在所有域控制器上維護的軟體的集中清單。軟體映像和映像分發伺服器是SWIM模組中的兩個主要子元件。

軟體映像

要訪問「軟體映像」(Software Images)頁面：

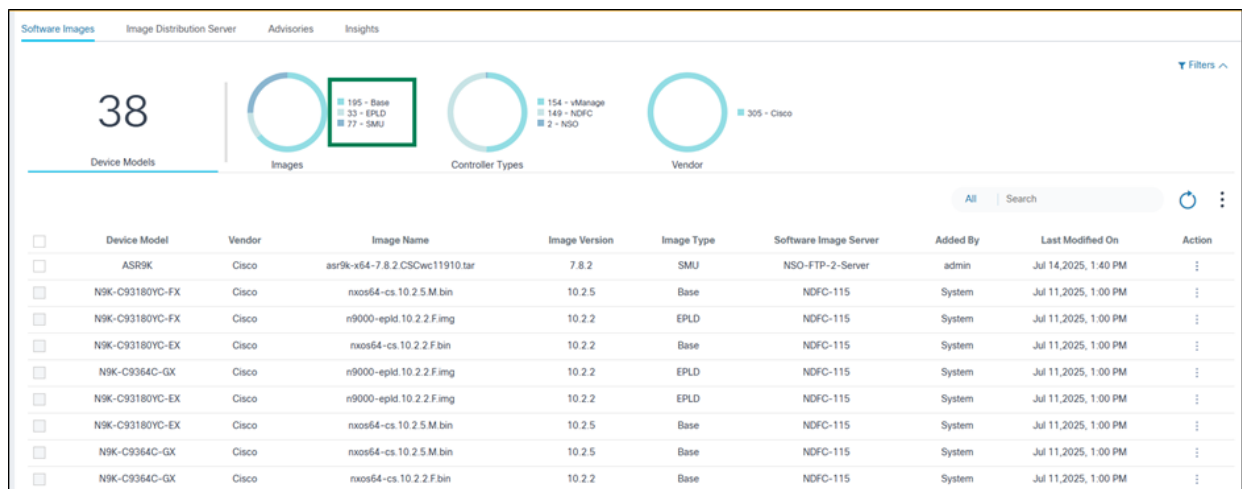
1. 使用具有軟體映像管理訪問許可權的憑據登入到BPA。



軟體映像管理導航

2. 選擇OS Upgrade > Software Image Management。

Image Management頁面顯示以下頁籤：Software Images、Image Distribution Server、Advisories和Insights。



軟體映像頁籤

Software Images頁籤包含以下內容：

- 頂部顯示的分析部分提供以下內容：
 - 裝置型號和相關軟體映像的總數
 - 一種Images快速過濾器，允許根據型別（例如base、SMU）過濾影像；該數字表示與相應影像型別相關聯的影像總數
 - Controller Types快速過濾器，允許根據承載映像的控制器型別（例如Cisco Catalyst Center、vManage、NSO或NDFC、直接到裝置、CNC、ANSIBLE、FMC）過濾映像；該數字表示與相應控制器型別相關聯的影像總數
 - 供應商快速過濾器，允許根據發佈軟體的供應商篩選映像
- More Options圖示提供以下功能：
 - 新增映像詳細資訊:新增新影像後設資料
 - 批次上傳:以.csv格式批次上載影像後設資料
 - 同步映像:同步來自控制器（例如Cisco Catalyst Center、vManage、NDFC和FMC）的映像後設資料
 - 全部刪除:批次刪除選定的映像

 附註：僅允許對NSO、ANSIBLE、CNC和直接到裝置控制器新增、刪除和批次上傳影像詳細資訊。

- Search過濾器可用於搜尋影像，包括以下獨佔搜尋過濾器：
 - All:在所有欄位間搜尋
 - 映像名稱:搜尋具有特定影像名稱的影像
 - 裝置型號:搜尋具有指定模型的影像

- 映像版本:搜尋具有特定軟體版本的映像
- 軟體映像伺服器:搜尋與特定映像檔案伺服器相關聯的映像
- Refresh圖示用於刷新頁面並清除所選過濾器。
- 現有影像顯示在包含以下列的網格表中：
 - 裝置型號：影像詳細資訊適用的裝置型號
 - 供應商:發佈軟體映像的供應商
 - 映像名稱:映像的檔名
 - 映像版本:映像的軟體版本
 - 映像型別:確定映像型別(例如，底座、SMU、電子可程式設計邏輯器件(EPLD))
 - 軟體映像伺服器:當前映像所在的映像伺服器
 - 新增者:新增影像後設資料的使用者
 - 上次修改時間:上次映像詳細資訊更新的時間戳
 - Action:提供更多選項圖示，可從中選擇行特定的操作（例如，編輯、刪除）
- 通過按一下相應的列標題對影像排序

The screenshot displays the Cisco Business Process Automation interface for managing software images. The main dashboard shows a summary of 121 device models and two donut charts representing the distribution of images and controller types. Below this is a table listing various software images, including their device models, vendors, image names, and versions. A 'View Image' modal is open on the right, providing detailed information for a selected image, such as its name, version, device model, vendor, controller type, controller ID, MDS checksum, and the software image server.

檢視映像

- 按一下行將開啟「檢視影像」窗口

同步軟體映像後設資料

要執行軟體映像的按需同步，請執行以下操作：



同步映像

1. 選擇更多選項圖示> 同步影像。從vManage、Cisco Catalyst Center、NDFC和FMC中發現映像後設資料詳細資訊並將其保留在BPA中。



附註：對於FMC控制器，每次執行同步時都會保留現有資料。僅附加新影像。

2. 如果FMC控制器的映像名稱包含單詞「FTD」或「Firepower Threat_Defense」，則該映像的deviceModel將對映為FTD。

或

如果FMC控制器的映像名稱包含單詞「FMC」、「FW_Mgmt_Center」或「Firewall_Management_Center」，則該映像的deviceModel將對映為FMC。

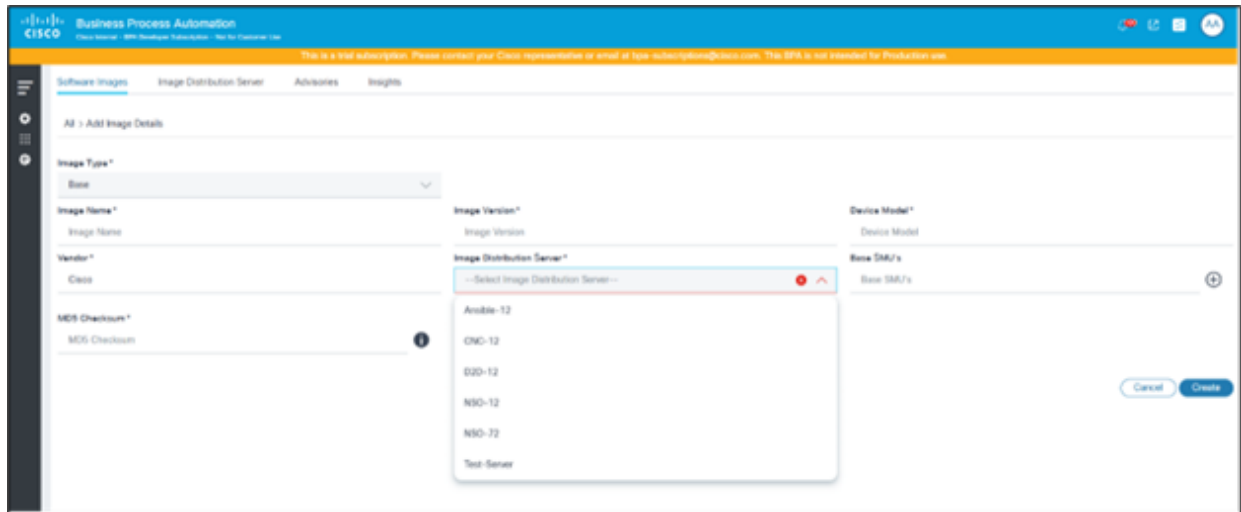


附註：FMC不將模型資訊與影像後設資料相關聯。完成同步後，編輯相應的映像後設資料並根據需要更新模型。如果沒有模型更新，FMC升級過程將無法按預期工作。

3. vManage遠端伺服器的映像在同步操作後，最初會在Version列中對映通用唯一識別符號(UUID)。操作員必須手動編輯所需的遠端伺服器後設資料，並使用適當的映像版本更新該後設資料。如果此對映未完成，則其他OS升級元件（如軟體一致性、升級策略、升級作業等）無法按預期工作。
4. 要計畫定期自動同步SWIM後設資料，請參閱[部署配置](#)。

新增軟體映像後設資料

1. 選擇更多選項圖示> 新增影像詳細資訊。系統隨即會顯示Add Image Details頁面。



新增映像詳細資訊

2. 在以下欄位中輸入資訊：

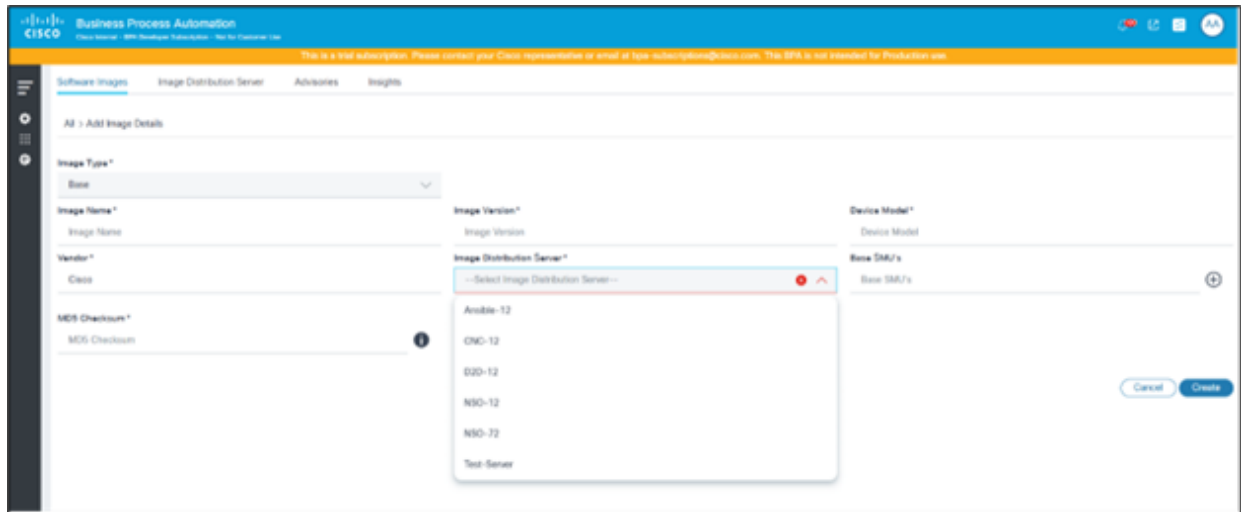
- 映像型別:映像型別（例如，base、SMU、EPLD）
- 映像名稱:影像檔案的名稱；使用者可以在「名稱」欄位中輸入影像的相對或絕對路徑。如果使用者提供一個絕對路徑，系統會直接從該路徑擷取映像；如果使用者提供了相對路徑，則系統會通過在分發過程中新增儲存庫伺服器中定義的基本路徑來解決完整路徑
- 映像版本:映像的軟體版本
- 裝置型號:為其標籤影像的裝置型號

 附註：裝置型號應與適用裝置的CNC、NSO、Direct-To-Device或ANSIBLE控制器提供的型號資訊相匹配。

- 供應商:發佈影像的供應商或提供商；預設值為Cisco，但可以根據需要進行更改
- Image Distribution Server:選擇承載在映像名稱欄位中指示的軟體檔案的映像分發伺服器。在選擇影像分發伺服器時，為與影像分發伺服器中定義的指定控制器型別相關聯的所有控制器ID生成影像。如果使用者在image distribution server下新增或刪除控制器例項，則系統會為這些控制器例項新增或刪除相應的軟體映像。
- 基本SMU:SMU出現在基本黃金映像中；僅當映像型別為Base時，此選項才適用
- MD5總和檢查碼:用於驗證的映像MD5校驗和

3. 按一下「Create」。系統隨即會顯示Progress通知，並顯示一條確認消息。

 附註：在升級策略中使用網橋SMU之前，必須新增該映像後設資料。要新增網橋SMU，請從Image Type下拉選單中選擇SMU。



新增網橋SMU映像後設資料

批次上傳軟體映像後設資料

	A	B	C	D	E	F	G
1	Device Model	Vendor	Image Name	Version	Image Type	Image Distribution Server	MD5 Checksum
2	NCS-540	Cisco	test22	1.1.1	Base	Ansible server	680fcd5f9f3558d6fd581edc0835ce2a
3	NCS-540	Cisco	test23	2.2.2	Base	Ansible server	b4ecef95e419c63d8da124d214deaaf
4	NCS-540	Cisco	test33	2.2.2	Base	Ansible server	b4ecef95e419c63d8da124d214deaaf
5	NCS-540	Cisco	test421	2.2.2	Base	Ansible server1	b4ecef95e419c63d8da124d214deaaf

包含影像資訊的CSV檔案示例

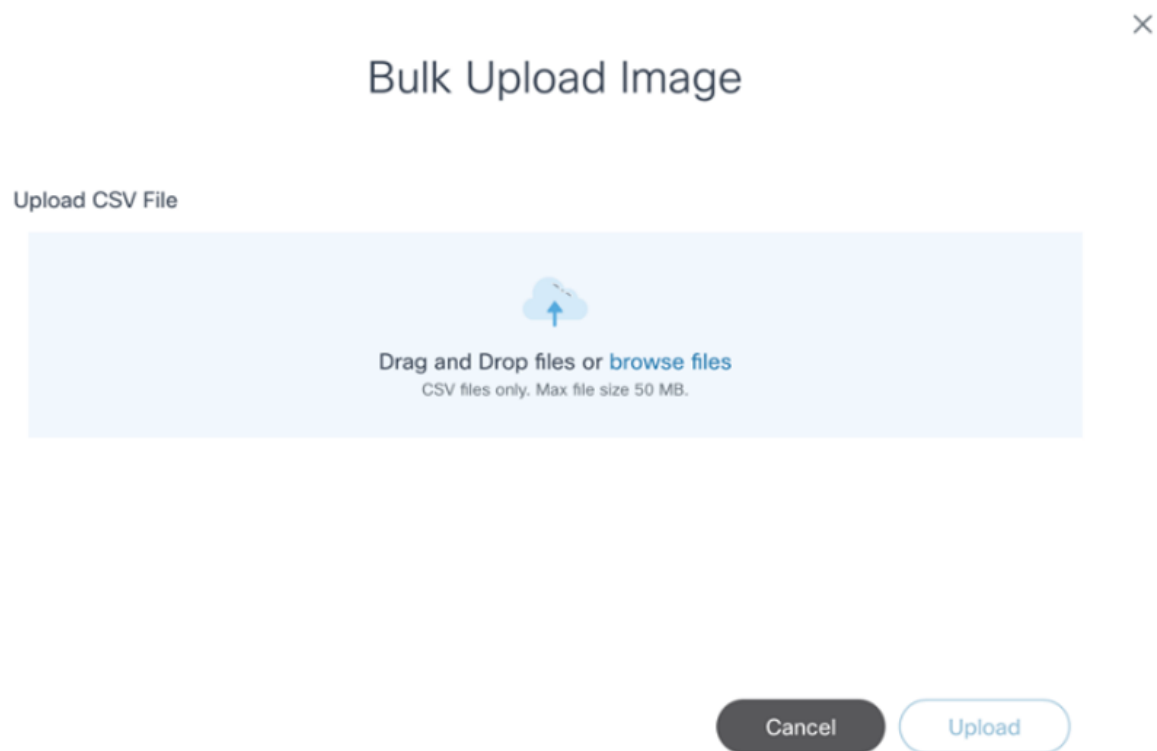
1. 準備一個包含必要的影像詳細資訊和下列列名的.csv檔案：

- 映像名稱
- 版本
- 裝置型號
- 供應商
- 映像型別

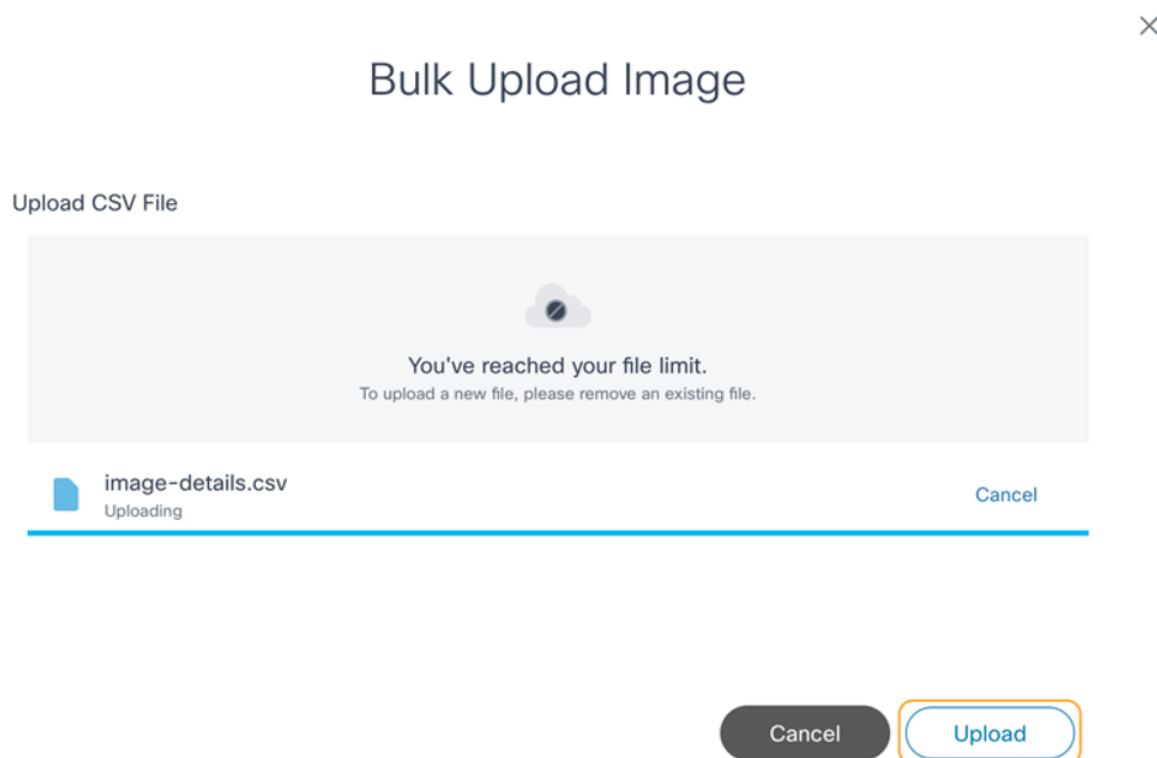
 附註：僅支援Base、SMU和EPLD值。

- 影像發佈伺服器
- MD5校驗和

2. 選擇更多選項圖示>批次上傳。Bulk Upload Image視窗開啟。



批次上傳影像



批次上傳映像 — CSV上傳

3. 選擇準備的.csv檔案，然後按一下Upload。驗證並處理來自.csv的映像詳細資訊。上傳檔案後，系統會顯示最終的批次上傳狀態。



Bulk Upload Image

Upload CSV File

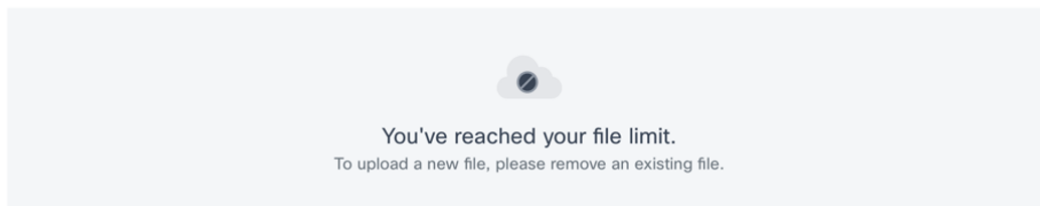


image-details.csv
Uploading

Cancel

Total upload status: Success: 2, Failed: 0

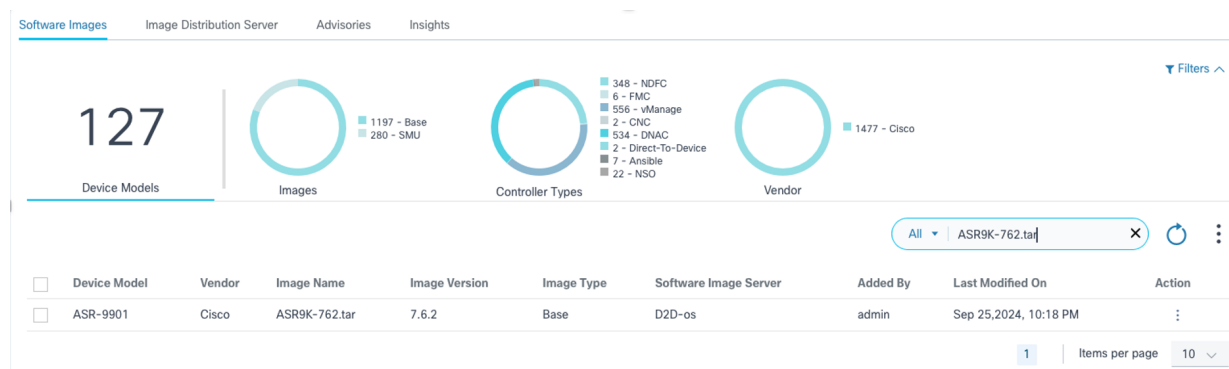
Cancel

Upload

成功批次映像上傳狀態

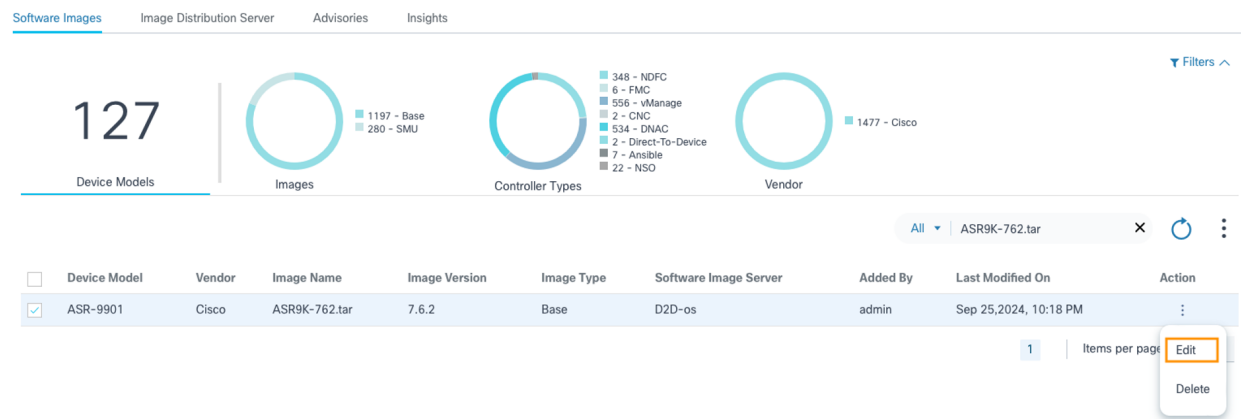
附註：在資料驗證錯誤的情況下（例如重複記錄或無效引數），錯誤消息在「批次上傳影像」視窗中以網格形式顯示。使用者可以更正.csv檔案中的值並重新上傳。

編輯現有軟體映像後設資料



在軟體映像後設資料中搜尋

1. 使用Search過濾器找到需要更新的影像。



編輯

2. 在所需影像的操作列中，選擇更多選項圖示> 編輯。

Software Images | Image Distribution Server | Advisories | Insights

All > asr9k-x64-7.7.2.CSCwe22538.tar

Image Type*: SMU

Image Name*: asr9k-x64-7.7.2.CSCwe22538.tar

Image Version*: 7.7.2

Device Model*: ASR-9901

Vendor*: Cisco

Image Distribution Server*: D2D-12

MDS Checksum*: b70ace4d0813399d11983b17f070d1e7

Cancel Save

編輯軟體映像

3. 更新所需的引數，然後按一下Save儲存更改，或按一下Cancel放棄更改。系統隨即會顯示進度通知，以及影像更新的確認消息。

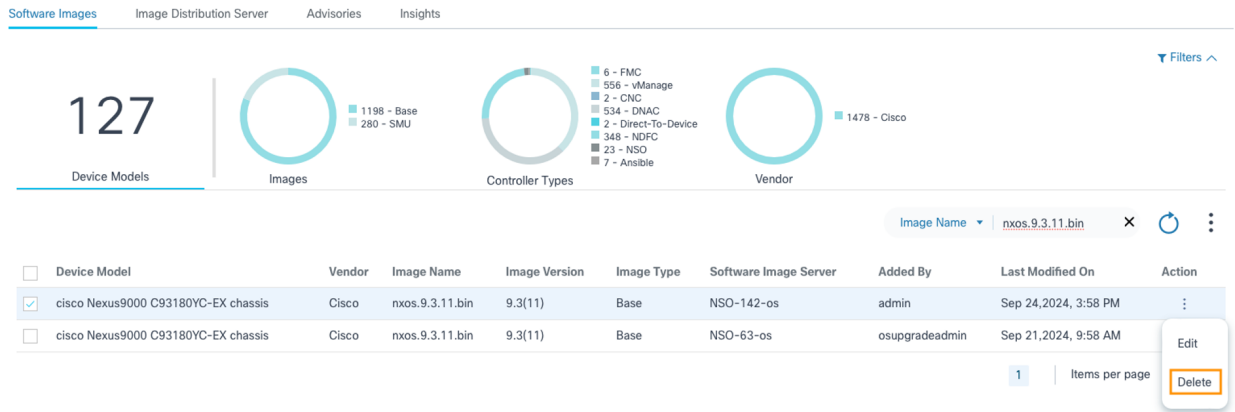
 附註：應註明以下清單。

- 編輯可用於CNC、NSO、D2D、ANSIBLE、FMC和vManage控制器（僅適用於遠端伺服器映像後設資料）
- 僅vManage遠端伺服器映像支援更新裝置模型
- 只能為vManage遠端伺服器映像後設資料更新Software Version欄位
- 對於vManage映像，使用者可以檢視軟體映像伺服器來代替控制器例項

刪除軟體映像後設資料

在軟體映像後設資料中搜尋

1. 使用Search欄位可定位所需的映像。



刪除

2. 在所需影象的操作列中，選擇更多選項圖示> 刪除以刪除影象。

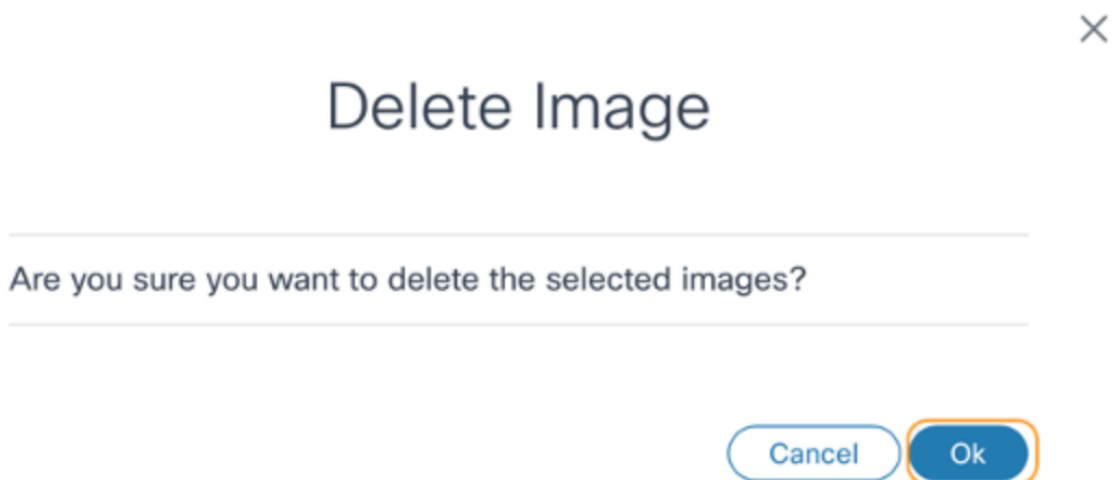
或



全部刪除

選擇所需的影象，然後選擇更多選項圖示> 全部刪除以刪除多個影象。

系統會顯示確認。



確認

3. 按一下「OK」（確定）。系統將顯示進度通知，然後顯示確認消息。

 附註：應註明以下清單。

- 只能為NSO、ANSIBLE、Direct-to-Device和CNC控制器新增影像後設資料。對於所有其他企業控制器，利用內建SWIM功能，並從各個控制器中發現映像
- NSO、ANSIBLE、直接到裝置和CNC控制器的映像伺服器不支援映像發現功能。
- 預設情況下，vManage remote server image metadata包含UUID for version parameter post-sync。使用者必須編輯後設資料並使用相應的版本更新UUID。相應的映像版本可以通過vManage控制器或登入到映像存在的裝置來識別。

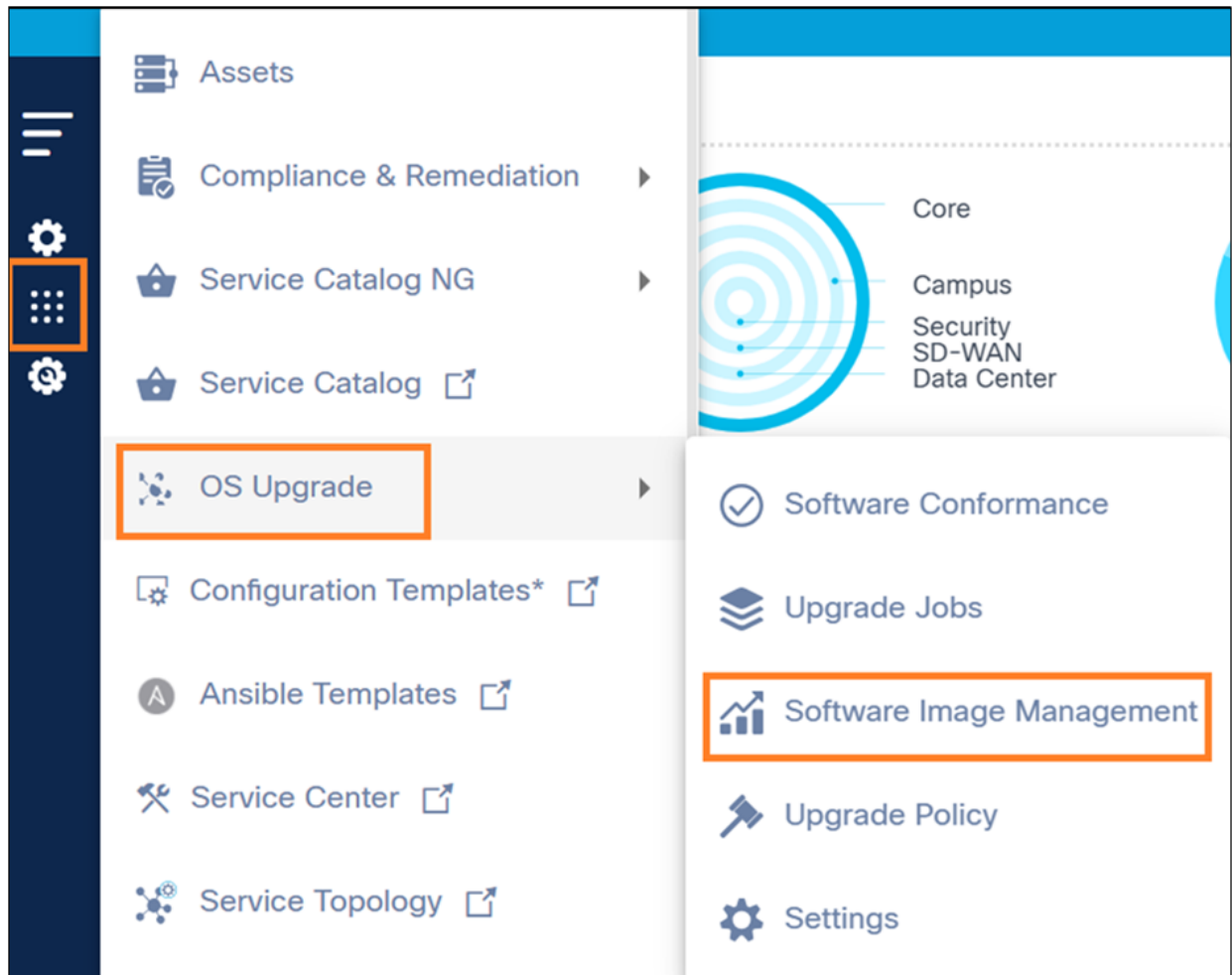
影像發佈伺服器管理

影像發佈伺服器

該元件允許Operations使用者維護沒有OOB映像儲存庫管理支援的CNC、NSO、ANSIBLE、FMC和直接到裝置控制器的映像儲存庫伺服器詳細資訊。

要訪問「Image Distribution Server」，請執行以下操作：

1. 使用具有對映像分發伺服器管理訪問許可權的憑據登入到BPA。



軟體映像管理

2. 選擇OS Upgrade > Software Image Management。

SW Images Image Distribution Server

2

Image Servers

CONTROLLER TYPE

1 - Direct-To-Device
1 - NSO

All Search

Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐ chennai	NSO	FTP	NSO-15	admin	Aug 2,2023, 3:48 PM	⋮
☐ Bangalore	Direct-To-Device	FTP	All	admin	Aug 2,2023, 3:43 PM	⋮

1 Items per page 10

Image Distribution Server頁籤

3. 按一下Image Distribution Server頁籤。

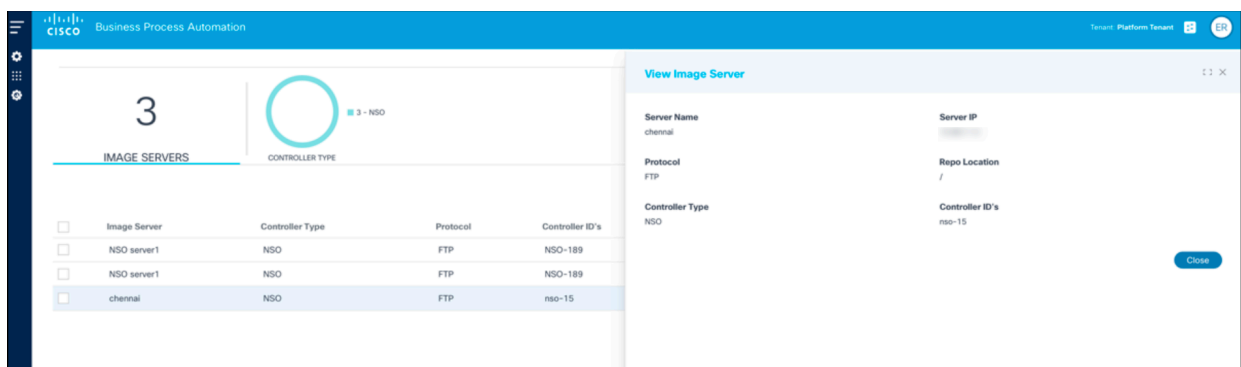
Image Distribution Server頁籤包含以下內容：

- 頂部顯示的分析部分提供以下內容：

- 此BPA例項上已加入的映像檔案伺服器總數
- Controller Type快速過濾器，允許根據控制器型別 (例如NSO、直接到裝置、CNC、ANSIBLE、FMC) 過濾影像伺服器；該數字表示與該控制器型別關聯的影像分發伺服器的總數
- 一個More Options圖示，提供以下功能：
 - 新增映像伺服器:新增新的影像分發伺服器
 - 全部刪除:批次刪除選定的分發伺服器
- 可用於搜尋分發伺服器的搜尋過濾器，它包括以下獨佔搜尋過濾器：
 - All:跨所有欄位搜尋
 - Image Server:搜尋具有特定伺服器名稱的伺服器
 - 控制器ID:搜尋與特定控制器ID關聯的伺服器
- 一個Refresh圖示，可用於刷新頁面和清除所選篩選器
- 現有分發伺服器顯示在包含以下列的網格表中：
- Image Server:儲存庫伺服器的唯一名稱
 - 控制器型別:此影像伺服器適用的控制器型別
 - 通訊協定：儲存庫伺服器支援的複製協定

 附註：僅支援FTP、SCP和安全檔案傳輸協定(SFTP)

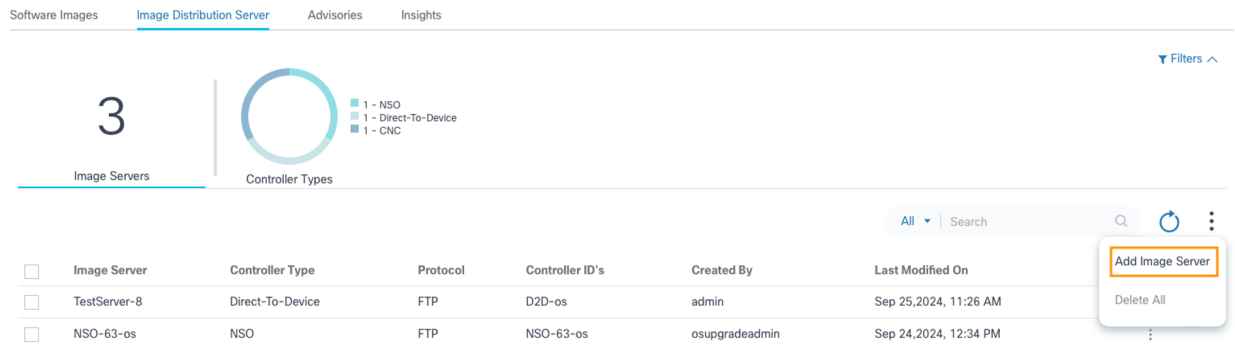
- 控制器ID:當前儲存庫伺服器可用或適用的控制器例項；控制器例項是指通過該控制器管理的裝置
- 建立者:登入儲存庫伺服器的使用者
- 上次修改時間:上次更新伺服器詳細資訊的時間戳
- Action:提供行特定的操作，如編輯和刪除



檢視映像檔案伺服器面板

- 按一下某一行將開啟「檢視影像伺服器」視窗

新增映像檔案伺服器詳細資訊



新增映像檔案伺服器

4. 選擇更多選項圖示> 新增影像伺服器。系統隨即會顯示Add Image Server頁面。

Software Images | **Image Distribution Server** | Advisories | Insights

All > Add Image Server

Server Name *	Server IP *	Protocol *
Server Name	Server IP	Select option
Root Location *	Controller Type *	Controller Instances *
Root Location	Select option	
User Name *	Password *	
Username		

Cancel Create

新增映像檔案伺服器詳細資訊

Software Images | **Image Distribution Server** | Advisories | Insights

All > Add Image Server

Server Name *	Server IP *	Protocol *
Demo-server	1.2.3.4	FTP
Root Location *	Controller Type *	Controller Instances *
/	NSO	NSO-142-OS
User Name *	Password *	
calo	*****	

Cancel Create

新增包含示例詳細資訊的映像伺服器

5. 在以下欄位中輸入資訊：

- 伺服器名稱:映像儲存庫伺服器的唯一名稱
- 伺服器IP:儲存庫伺服器的IPv4地址

 附註：在新增之前，請確保此IP可從網路裝置訪問。

- 通訊協定：映像副本受映像儲存庫伺服器支援

 附註：僅支援FTP、SCP和SFTP協定。

- 回購地點：儲存庫伺服器中映像檔案的基本路徑

 附註：如果映像檔案存在於映像檔案伺服器資料檔案庫資料夾的根目錄中，則「/」作為一個值使用。

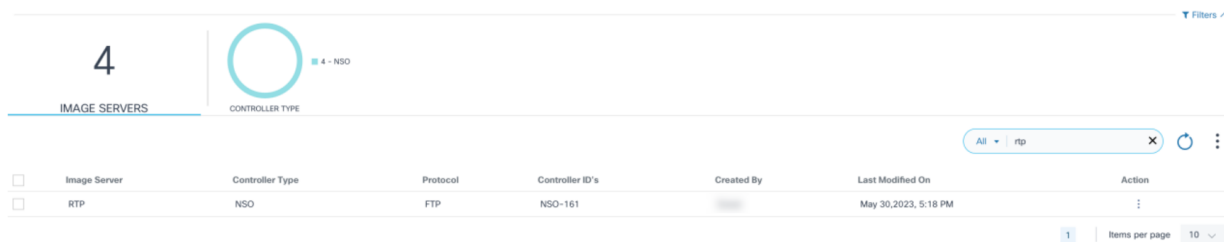
- 控制器型別:當前映像檔案伺服器適用的控制器型別

 附註：僅支援NSO、直接到裝置、CNC和ANSIBLE。

- 控制器實例：一個或多個適用的控制器例項，基於它們管理的裝置，給定的映像儲存庫伺服器應該用於複製映像
- 使用者:用於訪問儲存庫中的映像檔案的自定義憑據

6. 按一下「Create」。系統隨即會顯示進度通知，然後是一條確認消息。

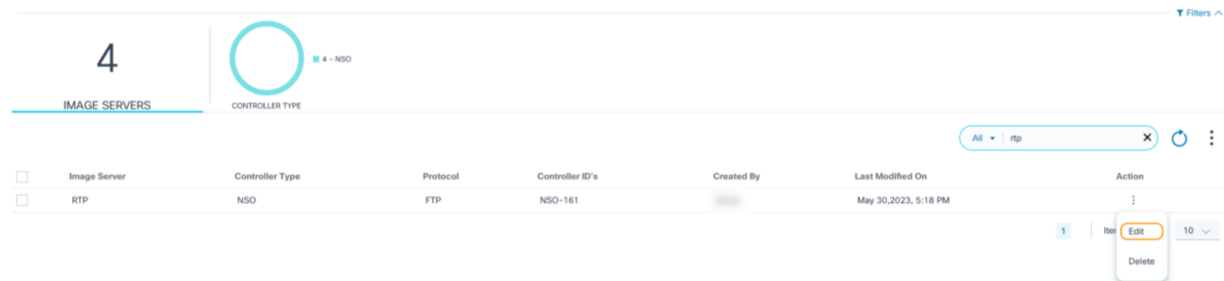
編輯映像檔案伺服器詳細資訊



☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐	RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	

影像伺服器搜尋

7. 使用Search欄位，找到需要更新的分發伺服器。



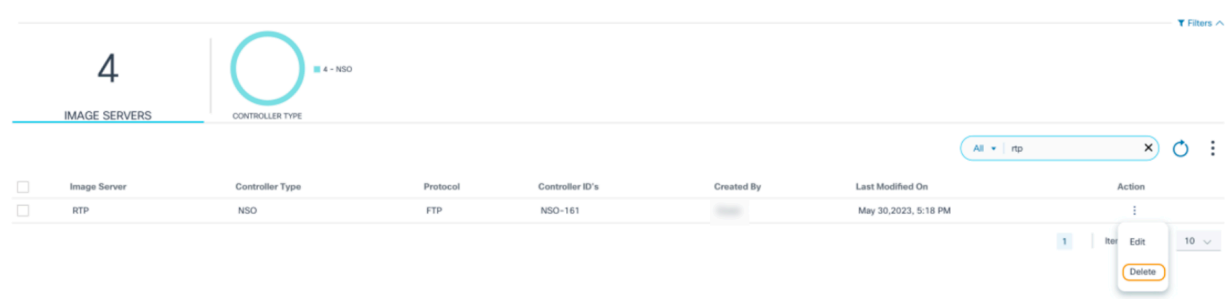
☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐	RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	Edit

編輯影像伺服器

8. 在「Action」列中，選擇More Options圖示> Edit。
9. 更新所需的引數。
10. 按一下「Save」。系統隨即會顯示進度通知，然後是一條確認消息。

刪除映像檔案伺服器詳細資訊

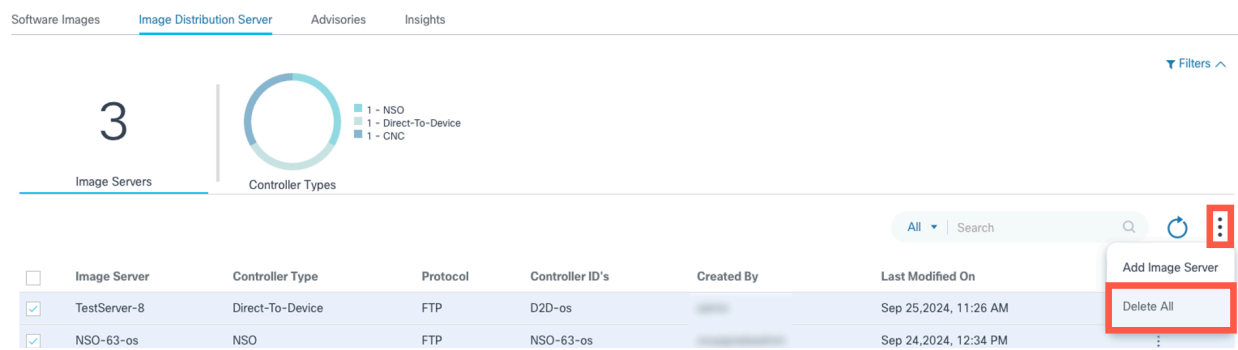
1. 使用Search過濾器找到所需的伺服器。



刪除映像檔案伺服器

2. 在操作列中，選擇更多選項圖示> 刪除以刪除單個分發伺服器。

或



刪除多個映像檔案伺服器

選擇所需的伺服器，然後選擇更多選項圖示> 全部刪除以刪除多個分發伺服器。

系統會顯示確認。



Delete Image Server

Are you sure you want to delete the selected server images?

Cancel

Ok

刪除確認

3. 按一下「OK」(確定)。系統隨即會顯示進度通知，然後是一條確認消息。

軟體洞察

Software Insights會發現所有安全漏洞，如網路資產所暴露的安全公告、錯誤和軟體壽命終止等。它還為由Cisco Catalyst Center和NDFC控制器管理的裝置型號提供軟體建議。它允許管理員使用者選擇網路資產的建議軟體版本，並為裝置模型建立一致性策略 (如果建議可用)。

必要條件

- 啟用介面卡以便獲得見解。Cisco Insights伺服器的介面卡 (名稱為「Cisco-Insights-Adapter」) 在OOB中提供。要與某些外部第三方Insights伺服器整合，需要構建相應的介面卡。有關詳細資訊，請參閱[BPA Developer Guide](#)中的Configuring Insights Adapter。
- BPA系統需要網際網路連線才能連線到思科雲。
- 繼續同步操作之前，請驗證client_id和client_secret是否位於介面卡配置中。
- 如果需要，可以按照以下步驟配置Internet的Proxy。
- 對於IOS-XR OS型別，可以根據需要在Reference Data Management(RefD)中完成自定義裝置系列到型號的對映。有關自定義系列到型號對映的詳細資訊，請參閱[BPA開發人員指南](#)。
- BPA Kubernetes Pods需要訪問網際網路，以便從思科收集公告、錯誤和壽命終止詳細資訊。如果BPA網路沒有直接網際網路訪問，但可通過代理訪問，請使用以下步驟使Kubernetes Pods使用網際網路代理。

1. 用實際的代理地址代替<<http://proxy-domain.com:port>>更新指令碼。
2. 針對部署YAML或掌舵圖表中的每個Pod配置環境引數。
3. 通過在NO_PROXY或no_proxy配置中新增所有部署名稱，在Kubernetes節點中執行以下指令碼。

```
#!/bin/bash
# Define the environment variables
HTTP_PROXY=""<

>"
HTTPS_PROXY=""<< http://proxy-domain.com:port>>"
http_proxy=""<

>"
https_proxy=""<

>"

NO_PROXY="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana

no_proxy="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana
# Get the list of deployments
deployments=$(kubectl get deployments -n bpa-ns | grep -v NAME | awk '{print $1}')

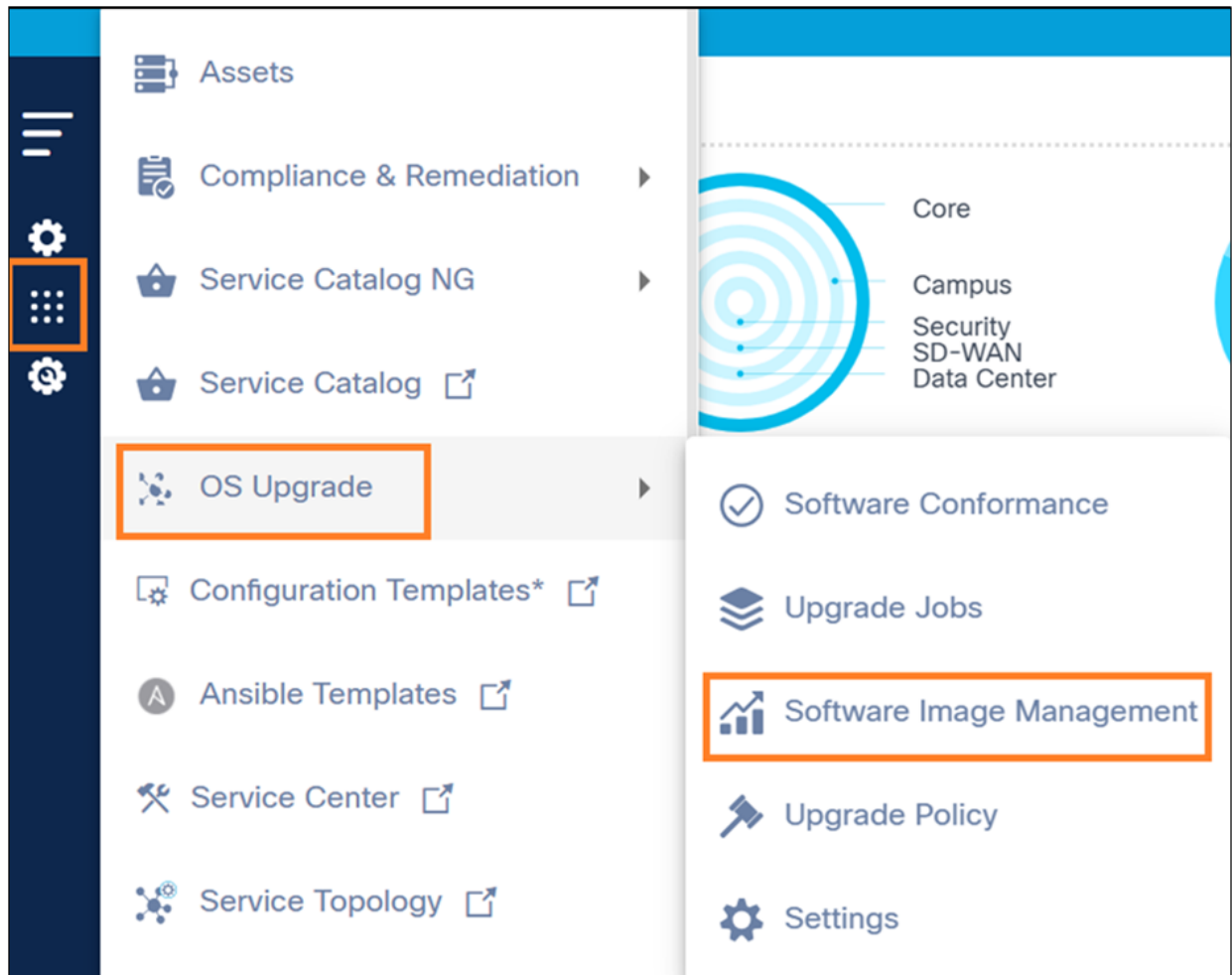
# Loop through each deployment and set the environment variables
for dp in $deployments;do
    kubectl set env deployment/$dp\
        HTTP_PROXY=$HTTP_PROXY \
        HTTPS_PROXY=$HTTPS_PROXY \
        http_proxy=$http_proxy \
        https_proxy=$https_proxy \
        NO_PROXY=$NO_PROXY \
        no_proxy=$no_proxy \
        -n bpa-ns
done
```

 附註：通過按上述方式設定代理，洞察介面卡可以訪問思科網路並將所需的軟體洞察資料下載到BPA。要直接連線到任何其他外部Insights伺服器而不使用代理，請確保將其新增到no_proxy變數中。

將軟體見解資料提取到BPA

要將軟體見解資料同步到BPA，請執行以下操作：

1. 使用有權訪問同步軟體洞察資料的憑據登入到BPA。



軟體映像管理導航

2. 從側面板中選擇OS Upgrade > Software Image Management。



「指導」頁籤

3. 按一下Advisories頁籤。

同步以將軟體見解提取到BPA



同步以將軟體見解提取到BPA

4. 按一下「Sync」。

此指令會發現與清單中現有資產相關的所有資安諮詢、優先順序錯誤、壽命終止公告和軟體建議。

系統會根據作業系統型別和軟體版本確定安全建議和軟體壽命終止日期。優先順序錯誤和軟體建議取決於產品ID和軟體版本。

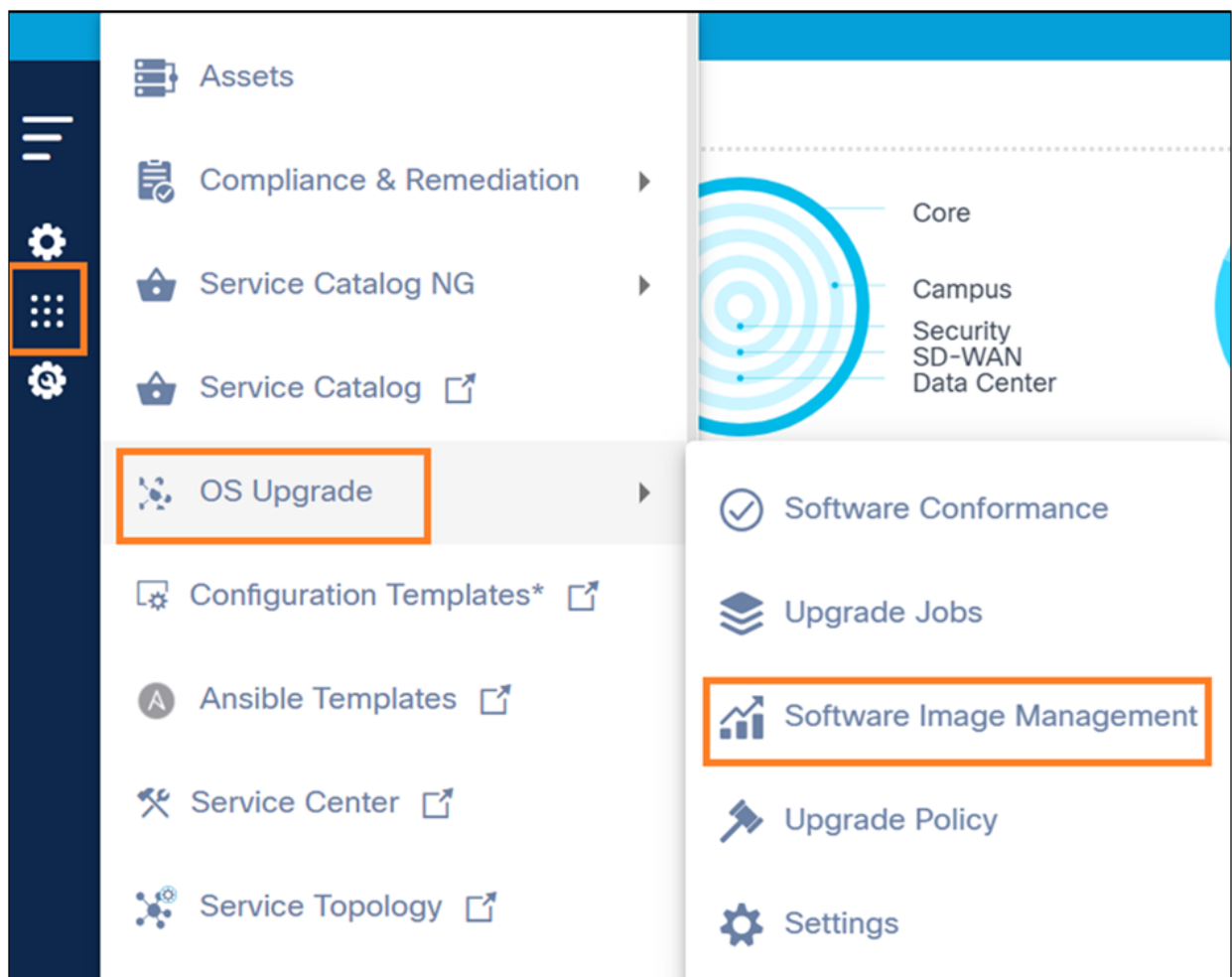
「上次更新」顯示上次同步見解資料的日期和時間，「同步狀態」字段顯示上次同步狀態。

 附註：所有適用的諮詢、錯誤、版本說明和建議均通過「Cisco-Insights-Adapter」檔案從思科雲獲取。

檢視和管理安全建議

要訪問Advisories頁面：

1. 使用具有管理諮詢訪問許可權的憑據登入到BPA。



軟體映像管理導航

2. 選擇OS Upgrade > Software Image Management。

Software Images Image Distribution Server **Advisories** Insights

Security Advisories are determined by matching the OS Type and SW version of the devices **Last Updated**: Dec 20, 2023, 1:17:06 PM **Sync Status**: Completed **Sync**

Security Advisories 214 Total **All** Search

Advisory	Impact	CVE	Softwares Versions	Last Updated	Version	Potentially Affected Assets
Vulnerability in NVIDIA Data Plane Development Kit	High	CVE-2022-28199	IOS-XE:17.6.2,IOS-XE:17.6.3a	1 year ago	1.0	4
Telnet Vulnerability Affecting Cisco Products: Ju	High	CVE-2020-10188	IOS-XE:16.9.2s	3 years ago	1.1	1
SNMP Remote Code Execution Vulnerabilities in Cts	High	CVE-2017-6736,CVE-2017-6737,CVE-2017-6738,CVE-201	IOS:15.2(4)E1,IOS:15.0(2)SE	8 months ago	1.10	2
OpenSSL RSA Temporary Key Cryptographic Downgrade	Medium	CVE-2015-0204	IOS:15.0(2)SE	8 years ago	14.0	1
OSPF LSA Manipulation Vulnerability in Multiple C	Medium	CVE-2013-0149	IOS:15.0(2)SE	6 years ago	1.4	1
Multiple Vulnerabilities in ntpd (April 2015) Aff	Medium	CVE-2015-1798,CVE-2015-1799	IOS:15.0(2)SE	8 years ago	1.11	1
Multiple Vulnerabilities in OpenSSL		CVE-2010-5298,CVE-2014-0076,CVE-				

參考指南

3. 按一下Advisories頁籤。預設情況下，會開啟Security Advisories頁面。

將顯示以下選項以過濾諮詢資料：

- 影響允許根據建議嚴重性進行過濾；預設情況下會選擇全部
- Last Updated允許基於顧問的上次更新日期進行過濾；預設情況下會選擇全部
- 清除全部重置所選過濾器
- Search篩選條件用於搜尋諮詢，包括下列獨佔搜尋篩選條件：
- All:在Advisory、CVE和Software Versions等列之間搜尋
- 建議:使用搜尋中指定的術語搜尋建議
- CVE:搜尋具有特定常見漏洞和洩露(CVE)的建議
- 軟體版本:搜尋與特定作業系統型別或軟體版本相關的諮詢
- Refresh圖示用於刷新頁面並清除所選過濾器
- 顯示以下列中的現有建議：
 - 建議：諮詢摘要
 - 影響:建議嚴重性
 - CVE:已分配CVE
 - 軟體版本：受影響的作業系統型別和軟體版本
 - 上次更新日期：上次更新顧問的日期和時間
 - 版本:建議版本
 - 可能受影響的資產：可能受諮詢影響的資產數量
- 按一下標題欄位可對建議進行排序



附註：排序不是潛在受影響的資產的選項。

Filters

Impacts

All

Critical

High

Medium

Low

Last Updated

All

<30 Days

31-60 Days

61-90 Days

>90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
...		
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
...		
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
...		
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
...		
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
...		
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
...		
Cisco IOx for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
...		
Cisco IOx for IOS XE Software Command Injection V	Medium	CVE-2021-1384
...		
Cisco IOx Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2022-20718,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE

CVE-2022-20823

Published

Aug 24,2022, 9:30 PM(1 year ago)

Last Updated

Aug 24,2022, 9:30 PM(1 year ago)

Version

1.0

View Security Advisory

Summary

Affected Assets (2)

A vulnerability in the OSPF version 3 (OSPFv3) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to incomplete input validation of specific OSPFv3 packets. An attacker could exploit this vulnerability by sending a malicious OSPFv3 link-state advertisement (LSA) to an affected device. A successful exploit could allow the attacker to cause the OSPFv3 process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.

建議詳細資訊檢視

- 選擇顧問行將開啟顧問的詳細資訊檢視，其中包括以下頁籤：
 - 摘要:顯示所選顧問的摘要；預設顯示
 - 受影響的資產：顯示可能受影響的資產詳細資訊，例如資產名稱、序列號、型號名稱、軟體版本、IP地址和控制器ID;可以在此頁籤中對資產進行排序和搜尋

Filters

Impacts

All

Critical

High

Medium

Low

Last Updated

All

<30 Days

31-60 Days

61-90 Days

>90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
...		
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
...		
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
...		
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
...		
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
...		
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
...		
Cisco IOx for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
...		
Cisco IOx for IOS XE Software Command Injection V	Medium	CVE-2021-1384
...		
Cisco IOx Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2022-20718,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE

CVE-2022-20823

Published

Aug 24,2022, 9:30 PM(1 year ago)

Last Updated

Aug 24,2022, 9:30 PM(1 year ago)

Version

1.0

View Security Advisory

Summary

Affected Assets (2)

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

2 Total Assets

All

Search

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93180-2		N9K-C93180YC-FX	9.3(7)	super spine		NDFC
CNXS-N93600CD-2		N9K-C93600CD-GX	9.3(7)	border		NDFC

1Items per page10

檢視資安諮詢

- 檢視安全建議連結：導航到「官方建議」頁面

檢視和管理優先順序錯誤

Software ImagesImage Distribution ServerAdvisoriesInsights

Security Advisories

Priority Bugs

Filters

Impacts

All

Critical

High

Medium

Low

Security Advisories 214 Total

All

Search

Advisory	Impact	CVE	Softwares Versions	Last Updated	Version	Potentially Affected Assets
----------	--------	-----	--------------------	--------------	---------	-----------------------------

選擇優先順序錯誤

按上一節所述開啟「Advisories」頁面後，按一下「Priority Bugs」頁籤。系統隨即會顯示優先順序

錯誤頁面。

Software ImagesImage Distribution ServerAdvisoriesInsights

Security Advisories

Priority Bugs

Filters

Severity

All

Sev 1

Sev 2

Sev 3

Sev 4

Sev 5

Sev 6

Clear All

Priority Bugs 73 Total

AllSearch

Bug ID	Severity	Summary	Product Versions	Potentially Affected Assets
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vp ...	N9K-C93360YC-FX2:10.2(5)	2
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2021-3593 ...	N9K-C93360YC-FX2:10.2(5)	2
CSCwi43066	3	DOC: Update N9K SFlow documentation for tah sampl ...	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi40943	3	/32 route is not getting installed in the RIB on ...	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi52972	2	Multicast traffic forwarding issues for random fl ...	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi15483	3	Interface UP without cable, only QSPF interted	N9K-C93180YC-FX:9.3(7)	1
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from 9.3(7 ...	N9K-C93180YC-FX:9.3(7)	1
CSCwi26553	6	Web UI on 17.9.4 performance/response is slow	C9300-24T:17.9.4,C9300-24UX:17.9.4	0
CSCwh99413	4	Console Logging for some XPATH isco-IOS-XE-instal ...	C9300-24T:17.9.4,C9300-24UX:17.9.4	0
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset Attack v ...	C9300-24T:17.9.4,C9300-24UX:17.9.4	0

123...8NextItems per page10

優先順序錯誤

優先順序錯誤頁面上有以下選項：

- 允許根據錯誤嚴重性進行篩選的嚴重性篩選條件;預設情況下會選擇全部
- Search篩選條件可用於搜尋錯誤，並包括下列獨佔搜尋篩選條件：
 - All:跨所有欄位搜尋
 - 錯誤ID:搜尋具有指定錯誤ID的錯誤
 - 摘要:搜尋摘要中存在特定關鍵字的錯誤
 - 產品版本：搜尋與特定產品ID或軟體版本相關的錯誤
- Refresh圖示可用於刷新頁面和清除所選過濾器
- 優先順序錯誤顯示在包含以下列的表中：
 - 錯誤ID
 - 嚴重性:錯誤嚴重性
 - 摘要:錯誤的摘要詳細資訊
 - 產品版本:產品ID和軟體版本受到影響
 - 可能受影響的資產：可能受錯誤影響的資產數量
- 可通過按一下除「可能受影響的資產」之外的任何列標題完成排序

Software Images Image Distribution Server **Advisories** Insights

Security Advisories

Priority Bugs

Filters

Severity

- All
- Sev 1
- Sev 2
- Sev 3
- Sev 4
- Sev 5
- Sev 6

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2020-15176
CSCwi43066	3	DOC: Update N9K SFlow documentation for N9K 9504
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for random
CSCwi15483	3	Interface UP without cable, only QSPF interface
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from 7.0(3) to 7.0(4)
CSCwi26553	6	Web UI on 17.9.4 performance/response issues
CSCwh99413	4	Console Logging for some XPATH Isco-IOCs
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset Attacks

Sev 6

CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

View Priority Bugs

Summary Affected Assets (2)

Bug Severity

Sev 6

Description:

Symptom:

OSPF stuck in exstart state.

Conditions:

VPC Orphan port connected L3 device establishing OSPF adjacency in non-vpc vlan carried on L2 trunk between vpc peers.

Workaround:

N/A

Further Problem Description:

錯誤詳細資訊檢視

- 按一下錯誤會開啟錯誤的詳細檢視，包括以下各項：
 - Summary選項卡：顯示錯誤嚴重性、說明和因應措施詳細資訊

Software Images Image Distribution Server **Advisories** Insights

Security Advisories

Priority Bugs

Filters

Severity

- All
- Sev 1
- Sev 2
- Sev 3
- Sev 4
- Sev 5
- Sev 6

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2020-15176
CSCwi43066	3	DOC: Update N9K SFlow documentation for N9K 9504
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for random
CSCwi15483	3	Interface UP without cable, only QSPF interface
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from 7.0(3) to 7.0(4)
CSCwi26553	6	Web UI on 17.9.4 performance/response issues
CSCwh99413	4	Console Logging for some XPATH Isco-IOCs
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset Attacks

Sev 6

CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

View Priority Bugs

Summary **Affected Assets (2)**

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

2 Total Assets

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXX-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXX-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151

1 Items per page 10

受影響的資產頁籤

- 受影響的資產頁籤：顯示所有可能受影響的資產詳細資訊，例如資產名稱、序列號、型號名稱、軟體版本、IP地址和控制器ID;可以在此頁籤中對資產進行排序和搜尋

Software Images Image Distribution Server **Advisories** Insights

Security Advisories

Priority Bugs

Filters

Severity

- All
- Sev 1
- Sev 2
- Sev 3
- Sev 4
- Sev 5
- Sev 6

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2020-15176
CSCwi43066	3	DOC: Update N9K SFlow documentation for N9K 9504
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for random
CSCwi15483	3	Interface UP without cable, only QSPF interface
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from 7.0(3) to 7.0(4)
CSCwi26553	6	Web UI on 17.9.4 performance/response issues
CSCwh99413	4	Console Logging for some XPATH Isco-IOCs
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset Attacks

Sev 6

CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

View Priority Bugs

Summary **Affected Assets (2)**

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

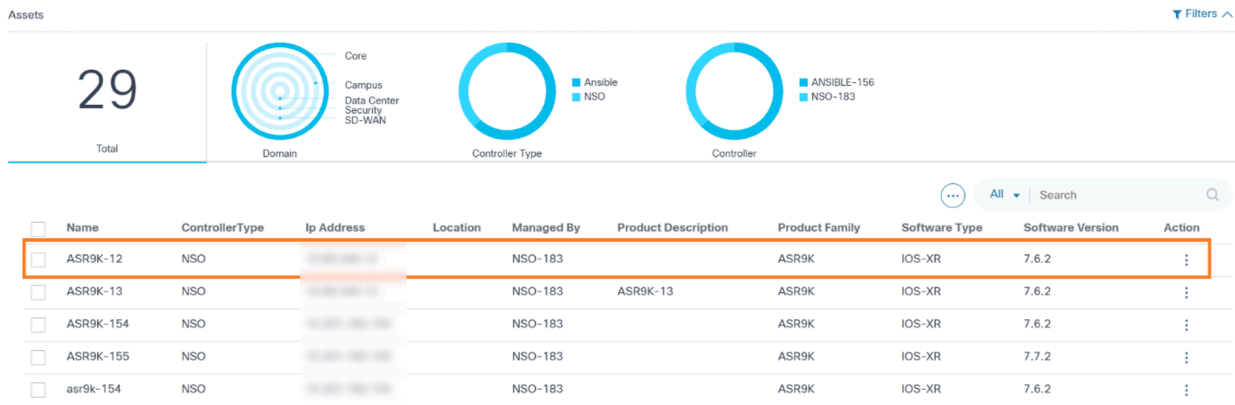
2 Total Assets

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXX-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXX-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151

1 Items per page 10

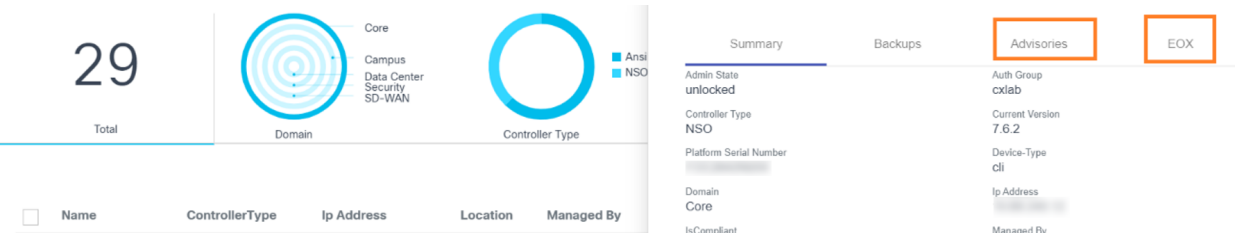
檢視優先順序錯誤

- 檢視優先順序錯誤連結：導覽至官方Bug Search Tool



資產

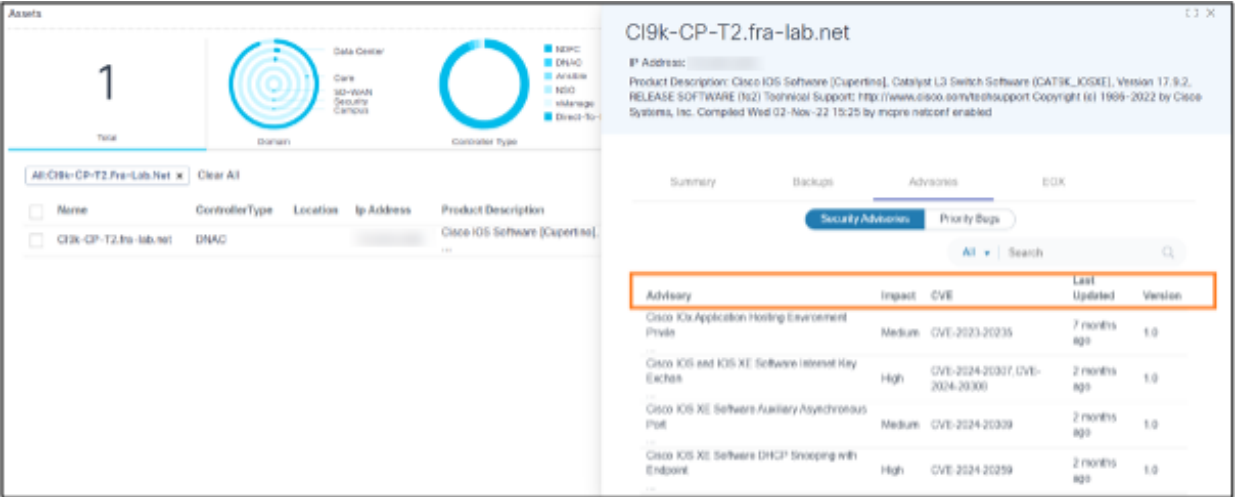
在Asset Manager中，使用者可以檢視所有資產的清單。選擇任何資產後，面板將顯示資產級別資訊，其中包括按兩個頁籤組織的資產軟體漏洞詳細資訊：諮詢和EOX。



諮詢和EOX

Advisories索引標籤包含兩個子索引標籤，Security Advisories和Priority Bug。有關這些頁籤的更多詳細資訊在下面的部分中提供。

參考指南



選定資產的安全諮詢

在「Security Advisories」子頁籤上，使用者可以檢視影響選定資產的所有安全公告。Security Advisories表中的列包括Advisories、Impact、CVE、Last Updated和Version。

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDFC, DNAC, Ansible, NSO, vManage, Direct-To

Alt: CI9k-CP-T2.Fra-Lab.Net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address: [redacted]

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

Security Advisories Priority Bugs

All ASR x

Advisory	Impact	CVE	Last Updated	Version
Cisco IOS XE Software for ASR 1000 Series Aggrega	High	CVE-2023-20187	8 months ago	1.0

1 Items per page 10

參考指南

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDFC, DNAC, Ansible, NSO, vManage, Direct-To

Alt: CI9k-CP-T2.Fra-Lab.Net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address: [redacted]

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

Security Advisories Priority Bugs

Impact Critical x

Advisory	Impact	CVE	Last Updated	Version
Multiple Vulnerabilities in Cisco IOS XE Software	Critical	CVE-2023-20198, CVE-2023-20273	6 months ago	2.6

1 Items per page 10

「安全諮詢」搜尋 — 「影響」選項

使用者可根據Advisories、Impact、CVE、Last Updated和Version列中的值搜索建議。分頁允許使用者在頁面之間導航。

優先順序錯誤

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDFC, DNAC, Ansible, NSO, vManage, Direct-To

Alt: CI9k-CP-T2.Fra-Lab.Net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address: [redacted]

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

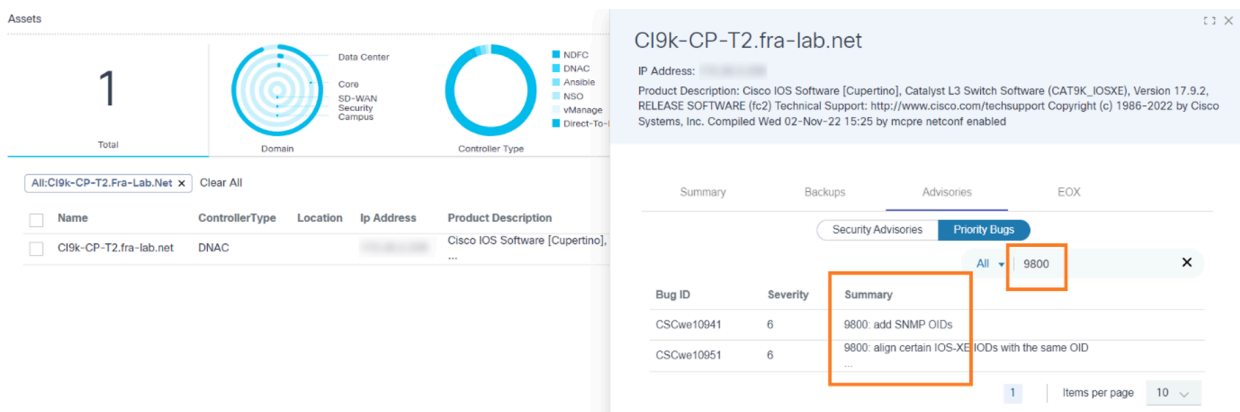
Security Advisories Priority Bugs

All Search

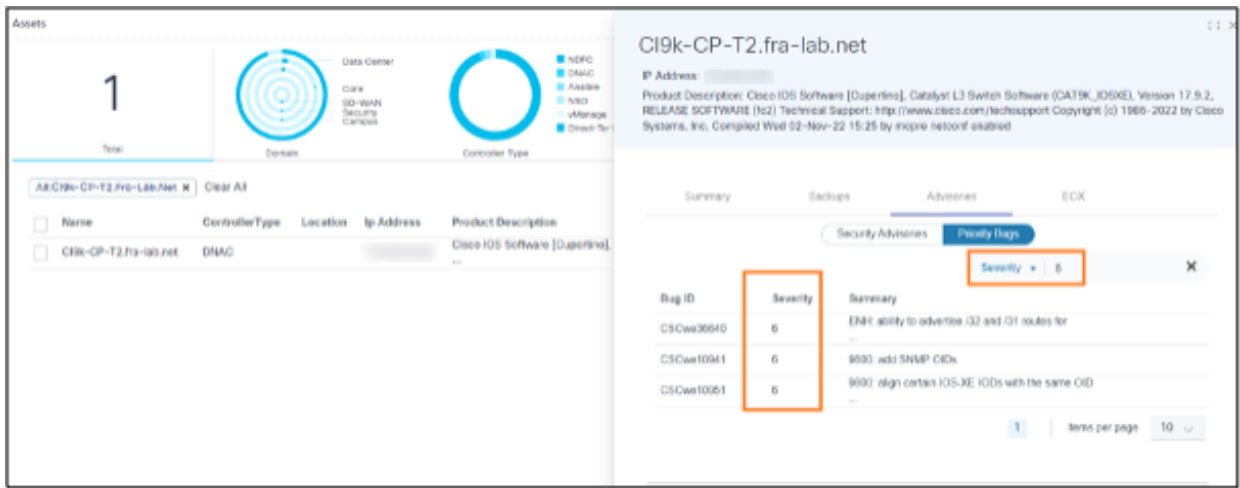
Bug ID	Severity	Summary
CSOwd60753	4	CCO flow does not support forward slash in the pa

影響選定資產的優先順序錯誤

在「Priority Bug」子索引標籤上，使用者可以存取影響指定資產的所有優先順序錯誤。此索引標籤中的列包括錯誤ID、嚴重性和摘要。



優先順序錯誤搜尋（按摘要）



優先順序錯誤按嚴重性搜尋

使用者可以根據錯誤ID、嚴重性和摘要列中的值搜尋優先順序錯誤。分頁便於在頁面之間輕鬆導航。

EOX

CI9k-CP-T1.fra-lab.net

IP Address: 192.168.1.100

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary

Backups

Advisories

EOX

End of SW Maintenance
Mar 30, 2025

End of Security Support
Sep 30, 2026

Last Date of Support
Mar 31, 2027

EOX頁籤

EOX頁籤顯示特定於資產的軟體壽命終止資料，其中包括三個重要日期：

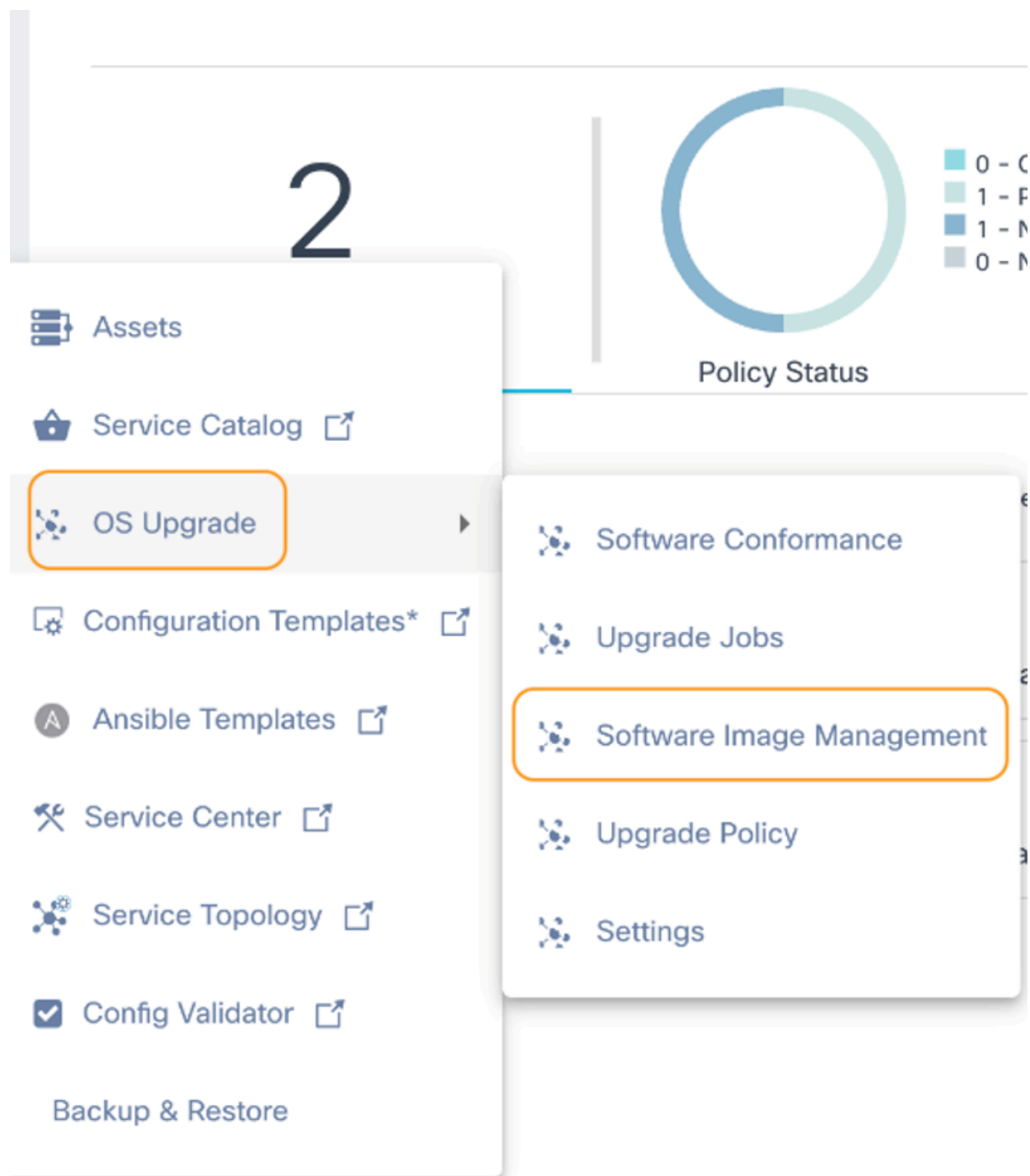
- 軟體維護結束
- 安全支援結束
- 最後支援日期

檢視軟體見解

Software Insights為Cisco Catalyst Center和NDFC控制器管理的裝置型號提供軟體建議，允許管理員使用者為裝置型號建立一致性策略（如果建議可用）。

要訪問Software Insights:

1. 使用具有管理見解訪問許可權的憑據登入到BPA。



軟體映像管理

2. 從側面板中選擇OS Upgrade > Software Image Management。

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

Device Model	Product Family	Software Type	Current Releases	Selected Release	Assets	Suggestions	Action
WS-C3850-48P-E	Cisco Catalyst 3850 Series Ethernet Stackable Swi	IOS-XE	16.12.6		1	Yes	⋮
N9K-C9300v	Data Center Switches	NX-OS	9.3(9)		7	No	⋮
WS-C2960S-48FPD-L	Cisco Catalyst 2960-X/XR Series Switches	IOS	15.0(2)SE		1	Yes	⋮
WS-C3750X-48PF-S	Cisco Catalyst 3750 Series Switches	IOS	15.2(4)E1		1	Yes	⋮
C9300-24T	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2		1	Yes	⋮
C9800-CL-K9	Cisco Catalyst 9800 Wireless Controllers for Cloud	IOS-XE	17.9.2		1	Yes	⋮
C9300-24UX	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2		1	Yes	⋮
N9K-C9364C-GX	Data Center Switches	NX-OS	9.3(10)		1	Yes	⋮
C9500-24Y4C	Cisco Catalyst 9500 Series Switches	IOS-XE	17.9.2		1	Yes	⋮
C9500-48Y4C	Cisco Catalyst 9500 Series Switches	IOS-XE	17.5.1		1	Yes	⋮

1 2 3 Next Items per page 10

Insights頁籤

3. 按一下Insights頁籤。

Insights頁籤包含以下內容：

- 允許使用者根據建議篩選資料的篩選器。預設情況下會選擇全部。
 - 是過濾裝置型號的資料，並提供建議
 - No在沒有建議的情況下過濾裝置型號的資料

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

29 Total Device Models

Device Model	Product Family	Software Type	Current Releases	Selected Release	Assets	Suggestions	Action
WS-C3850-48P-E	Cisco Catalyst 3850 Series Ethernet Stackable Swi	IOS-XE	16.12.6		1	No	⋮
C9500-48Y4C	Cisco Catalyst 9500 Series Switches	IOS-XE	17.5.1		1	No	⋮
N9K-C93180YC-EX	Data Center Switches	NX-OS	10.2(2)		2	No	⋮
N9K-C9500v	N9K	NX-OS	9.3(5)		1	No	⋮
WS-C4500X-32	Cisco Catalyst 4500-X Series Switches	IOS-XE	03.11.02.E		1	No	⋮

Export to CSV

匯出到CSV

- More Options圖示提供Export to CSV選項以匯出頁面中顯示的資料
 - Refresh圖示用於刷新頁面並清除所選過濾器
 - Search篩選條件用於搜尋資料，包括下列獨佔搜尋篩選條件：
- All:在所有列中進行搜尋(例如Device Model、Product Family和Software Type)
- 裝置型號:搜尋具有特定裝置型號名稱的資料
- 產品系列:搜尋具有特定產品系列名稱的資料
- 軟體型別:搜尋具有特定軟體型別名稱的資料
 - 現有裝置型號顯示如下列：
 - 裝置型號:裝置型號的名稱
 - 產品系列:裝置模型所屬的產品系列的名稱
 - 軟體型別:裝置模型所屬軟體型別的名稱

- 目前版本:裝置型號的清單中當前存在的唯一軟體版本的清單
- 所選版本:根據思科提供的建議選為可選版本的建議版本版本
- 資產:裝置型號的Asset Manager中存在的資產數量
- 建議:對於可用於裝置型號的任何建議，顯示Yes或No

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

Device Model	Product Family	Software Type	Current Releases	Selected Release	Assets	Suggestions	Action
ASR1001-X	Cisco ASR 1000 Series Aggregation Services Routers	IOS-XE	17.9.2a, 17.6.5		2	Yes	⋮
C9300-48U	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2, 17.6.4		4	Yes	⋮
N9K-C93600CD-GX	Data Center Switches	NX-OS	10.2(6)		1	Yes	⋮
C9500-40X	Cisco Catalyst 9500 Series Switches	IOS-XE	17.9.2		2	Yes	⋮
WS-C4500X-32	Cisco Catalyst 4500-X Series Switches	IOS-XE	03.11.02.E		1	No	⋮
C9300-48P	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2, 17.5.1		3	Yes	⋮
N9K-C93180YC-EX	Data Center Switches	NX-OS	9.3(10), 10.2(2)	10.2(6)	4	Yes	⋮
N9K-C93180YC-FX	Data Center Switches	NX-OS	9.3(10), 9.3(7)		2	Yes	⋮
WS-C3750X-48PF-L	Cisco Catalyst 3750 Series Switches	IOS	15.2(4)E10		1	Yes	⋮
ASR1002-X	Cisco ASR 1000 Series Aggregation Services Routers	IOS-XE	17.6.5, 17.9.3a		2	Yes	⋮

Prev 1 2 3 Next Items per page 10

檢視建議導航

- Action:通過More Options圖示(例如View Suggestions和View Assets)提供特定於行的操作



附註：如果裝置型號沒有任何建議，則禁用「檢視建議」。

檢視和選擇供應商建議的軟體版本

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

Device Model	Product Family
ASR1001-X	Cisco ASR 1000 Series Aggregation Services Routers
C9300-48U	Cisco Catalyst 9300 Series Switches
N9K-C93600CD-GX	Data Center Switches
C9500-40X	Cisco Catalyst 9500 Series Switches
WS-C4500X-32	Cisco Catalyst 4500-X Series Switches
C9300-48P	Cisco Catalyst 9300 Series Switches
N9K-C93180YC-EX	Data Center Switches
N9K-C93180YC-FX	Data Center Switches
WS-C3750X-48PF-L	Cisco Catalyst 3750 Series Switches
ASR1002-X	Cisco ASR 1000 Series Aggregation Services Routers

Device Model: N9K-C93600CD-GX
Product Family: Data Center Switches

Suggestions Affected Assets (1)

② Select one of the Cisco suggested software releases as the standard or policy while taking into consideration known issues and any workaround Last Suggestion Date :Dec 20, 2023

Release Version & Date	CURRENT	OPTIMAL - 1
	10.2(6) Sep 1, 2023 Release Notes	10.2(6) Sep 1, 2023 Release Notes

Conformance Policy Create

Bugs	Current Exposure : 7	Future Exposure : 7
	sev1 0	sev1 0
	sev2 1	sev2 1
	sev3 4	sev3 4
	sev4 1	sev4 1
	sev5 0	sev5 0
	sev6 1	sev6 1

Security Advisories	Current Exposure : 0	Future Exposure : 0
	Critical 0	Critical 0
	High 0	High 0
	Informational 0	Informational 0
	Low 0	Low 0
	Medium 0	Medium 0

EoX	End of SW Maintenance	End of SW Maintenance
	Nov 30, 2023	Nov 30, 2023
	End of Security Support	End of Security Support
	Feb 28, 2025	Feb 28, 2025
	Last date of Support	Last date of Support
	Aug 31, 2025	Aug 31, 2025

「建議」頁籤

從操作列中選擇更多選項圖示> 檢視建議將開啟包含所有深入分析詳細資訊的側面板。
 Suggestions索引標籤包含所選裝置型號的當前版本和建議版本詳細資訊；一個裝置型號可以有許多建議。以下資料可用：

- 發行版本和日期:如果思科雲中提供了當前版本和建議版本的發行版本、日期和註釋詳細資訊；如果資產屬於多個版本，則所有適用版本在當前列中顯示為逗號分隔值
- 建立一致性策略:允許管理員為裝置角色為Any的特定版本建立一致性策略

 附註：僅支援NDFC控制器裝置型號建立一致性策略

Device Model : N9K-C93180YC-EX
Product Family : Data Center Switches

Suggestions

Affected Assets (4)

 Select one of the Cisco suggested software releases as the standard or policy while taking into consideration known issues and any workaround

Last Suggestion Date :Dec 20, 2023

Release Version & Date	CURRENT 9.3(10),10.2(2) Dec 16, 2021 Release Notes	OPTIMAL - 1 10.2(6) Sep 1, 2023 Release Notes
Conformance Policy		Insights-policy-for-N9K-C93180YC-EX  Created On : Dec 20, 2023

刪除策略選項

 附註：如果裝置模型已存在任何策略，則會顯示錯誤。如果不存在任何策略，則在Enabled狀態下建立策略。如果策略是通過Insights建立的，則使用者可以選擇刪除該策略。

- 錯誤:顯示每個版本的整合錯誤計數
- 參考指南:顯示每個版本的合併建議計數
- EoX:顯示每個版本的軟體維護結束、安全支援結束和支援最後日期

Device Model : N9K-C93360YC-FX2 Product Family : Data Center Switches						
Suggestions		Affected Assets (2)				
2 Total Assets		All ▾ Search				
Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXS-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
		1 Items per page 10 ▾				

受影響的資產頁籤

從操作列中選擇更多選項圖示> 檢視資產將開啟一個側面板，預設情況下會顯示受影響的資產頁籤。「受影響的資產」頁籤在「資產名稱」、「序列號」、「型號名稱」、「軟體版本」、「IP地址」和「控制器ID」等列中顯示可能受影響的資產詳細資訊。可以在此頁籤中對資產進行排序和搜尋。

識別需要軟體升級的裝置

有關詳細資訊，請參閱[軟體一致性](#)。

軟體符合性

軟體一致性幫助識別網路中不符合目標軟體版本的資產。驗證基於用於定義軟體合規意圖的策略和規則。這些策略可以按計畫執行或按需執行。成功執行遵從性策略後，會獲得遵從性結果，該結果提供適用資產的狀態。一致性範圍取決於各種標準，例如裝置角色、管理控制器例項等。

必要條件

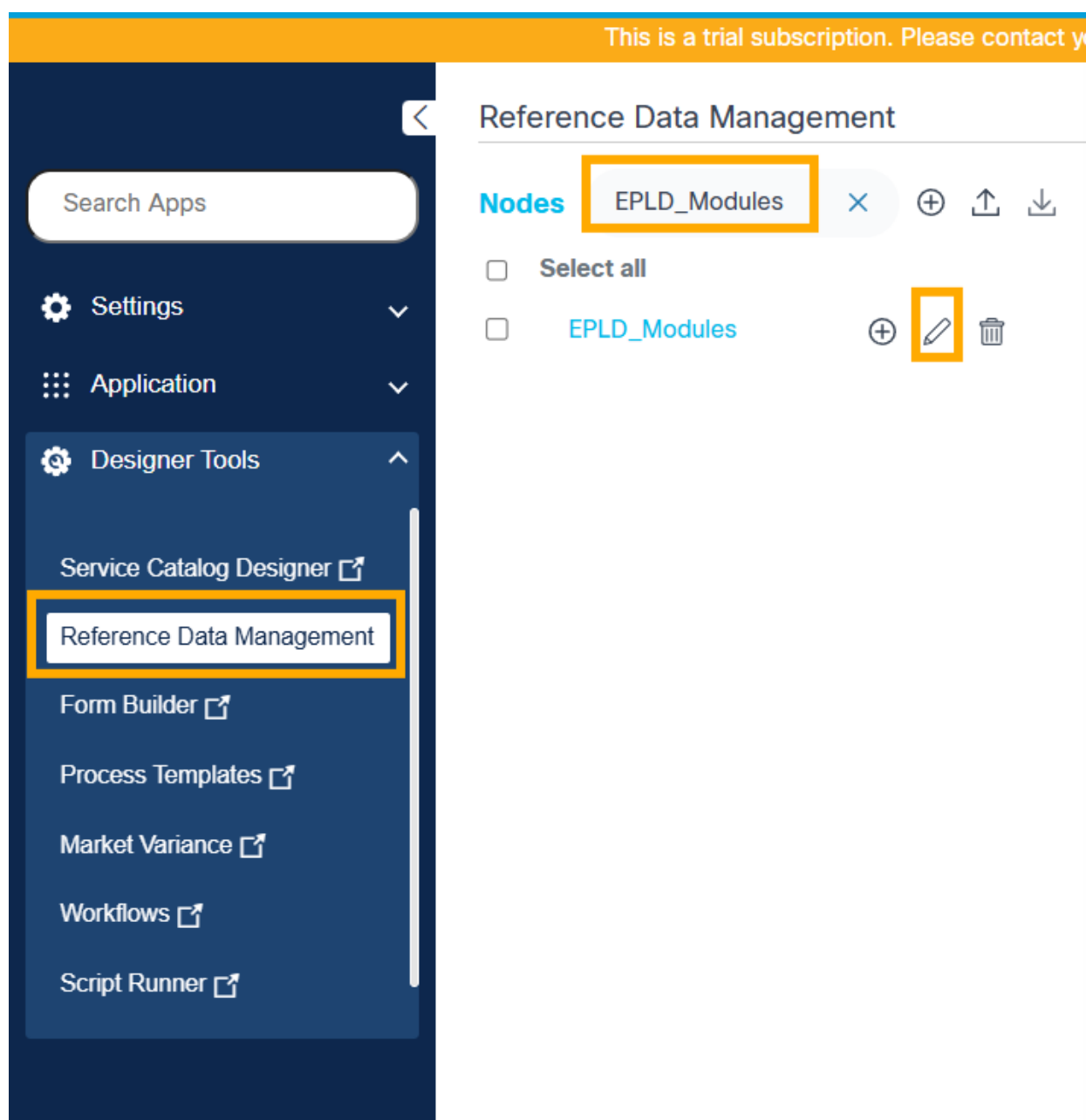
- Cisco Catalyst Center、vManage、NDFC和FMC等控制器的軟體映像必須同步。有關詳細資訊，請參閱[同步軟體映像後設資料](#)。
- 必須新增控制器（如NSO、CNC、直接到裝置和ANSIBLE）所需的軟體映像後設資料。有關詳細資訊，請參閱[新增軟體映像後設資料](#)。
- 使用者必須有權訪問RefD應用程式以管理EPLD模組資料。
- 所需版本的EPLD模組資訊應預填充到RefD應用程式中

- 如果EPLD模組資訊不可用OOB，使用者必須在RefD應用程式中手動新增

在引用資料管理應用程式中建立EPLD模組資料

建立一致性策略之前，請在RefD應用程式中建立EPLD模組引用資料。RefD應用程式套件括Nexus軟體版本v10.2(8)和v10.4(5)的EPLD模組資訊。對於其他裝置版本，必須在RefD應用程式中手動新增EPLD型號資訊。

完成以下步驟，將其他版本新增到EPLD模組後設資料中：



參考資料管理

1. 導航到Reference Data Management應用程式，然後搜尋「EPLD_Modules」。

2. 選擇「EPLD_Modules」檔案並選擇編輯圖示。

Edit Node

Name* EPLD_Modules Data Source* Internal Data Type* JSON ☐ Protected data

```
1 {
2   "N9K-C92348GC-X": {
3     "10.5(2)": [
4       {
5         "Module": "IOFPGA",
6         "Version": "0x15"
7       }
8     ],
9     "10.5(1)": [
10      {
11        "Module": "IOFPGA",
12        "Version": "0x15"
13      }
14    ]
15  },
16  "N9K-C93108TC-EX": {
17    "10.5(2)": [
18      {
19        "Module": "IOFPGA",
20        "Version": "0x15"
21      }
22    ]
23  }
24 }
```

EPLD_Modules.json × Cancel Save Upload Download

編輯節點

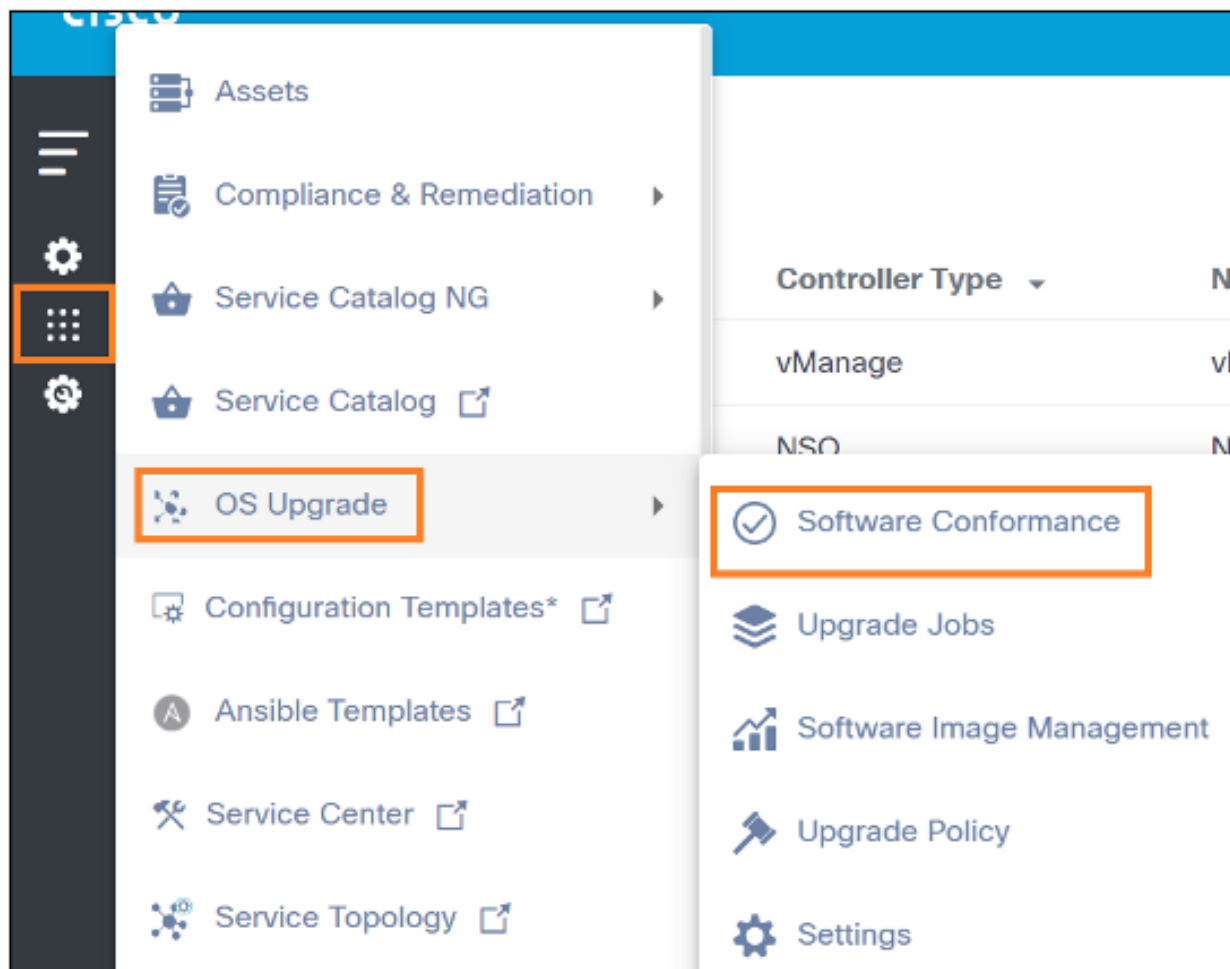
3. 通過新增具有以下結構的新條目來新增新的發行版EPLD模組後設資料：

```
structure:
  "N9K-C92348GC-X": {
    "10.5(2)": [
      {
        "Module": "IOFPGA",
        "Version": "0x15"
      }
    ]
  }
}
```

4. 按一下Save並驗證可在一致性策略中選擇的新EPLD模組後設資料。預填充受支援版本的EPLD資料。

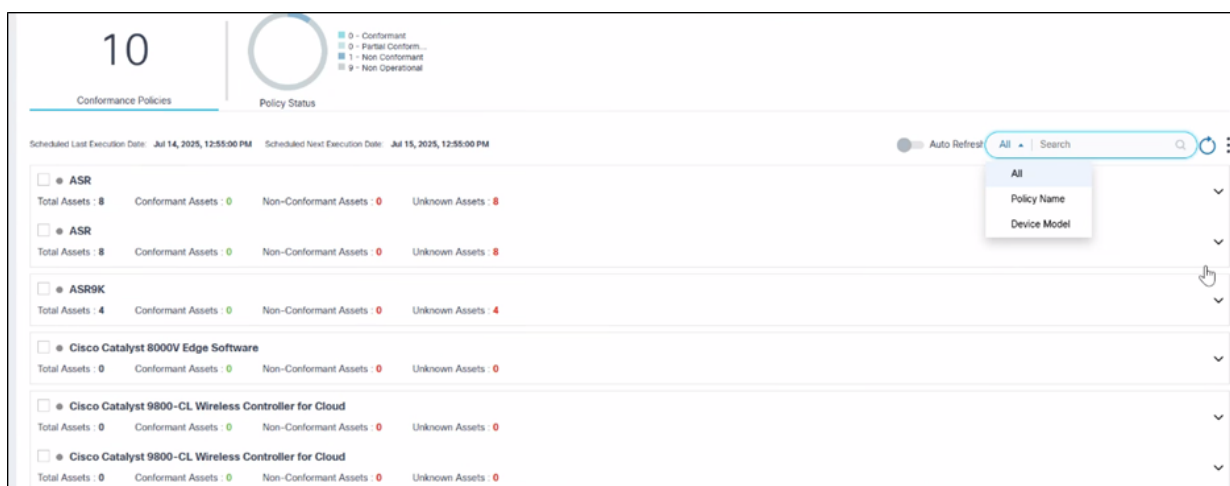
檢視和管理軟體符合性

1. 使用具有軟體一致性訪問許可權的憑據登入到BPA。



軟體符合性導覽

- 選擇OS Upgrade > Software Conformance。系統隨即會顯示「Software Conformance」頁面。



軟體符合性

Software Conformance頁包含以下內容：

- 頂部顯示的分析部分提供以下內容：

- 系統中存在的符合性策略的總數
- 根據以下條件進行篩選的Policy Status快速過濾器：
 - Conformant: 具有指定型號的所有BPA管理的裝置都在定義的軟體版本上
 - 部分一致性: 某些具有指定型號的BPA管理的裝置位於定義的軟體版本上；其餘裝置處於不同的軟體版本中
 - 不符合項: 與給定軟體版本相比，具有指定型號的所有BPA受管裝置都處於不同的軟體版本上
 - 非操作: 根據策略中指定的裝置型號，找不到適用的裝置
- 計畫最後執行日期和計畫下次執行日期，指明以前執行的計劃一致性檢查的日期和時間以及下一個計劃一致性檢查針對所有策略的時間
- 用於根據裝置型號、策略名稱或所有過濾策略的搜尋欄位；使用者可以選擇All以搜尋所有引數
- 啟用時，自動刷新切換允許按使用者定義的間隔自動刷新進行中一致性策略。要啟用切換：
 - 轉到OS Upgrade > Settings以更改刷新間隔
 - 使用所需值修改自動刷新間隔
 - 按一下「Save」
- 啟用「自動刷新」切換後，軟體一致性策略儀表板會以新時間間隔刷新
- 一個Refresh圖示，用於刷新頁面並清除所選篩選器
- 一個More Options圖示，提供以下選項：
 - 建立策略
 - 運行所有策略
 - 刪除多個所選策略

策略根據裝置型號進行分組，並以可擴展面板形式顯示，從而提供不同控制器管理的裝置型號的單一檢視。

Cisco Catalyst 9500 Switch			
Total Assets : 2	Conformant Assets : 2	Non-Conformant Assets : 0	Unknown Assets : 0

合規性策略的摺疊檢視

在摺疊檢視中，面板顯示裝置模型和快速統計資訊，如Total Assets、Conformant Assets、Non-Conformant Assets和Unknown Assets。

Cisco Catalyst 9500 Switch								
Total Assets : 2		Conformant Assets : 2		Non-Conformant Assets : 0		Unknown Assets : 0		
Name	Region	Device Role	Target Version	Created By	Created On	Executed On	State	Action
Cat 9500	Global	All	17.06.04	admin	May 8, 2023, 5:19 PM	May 8, 2023, 5:41 PM	enabled	⋮
							1	Items per page 10

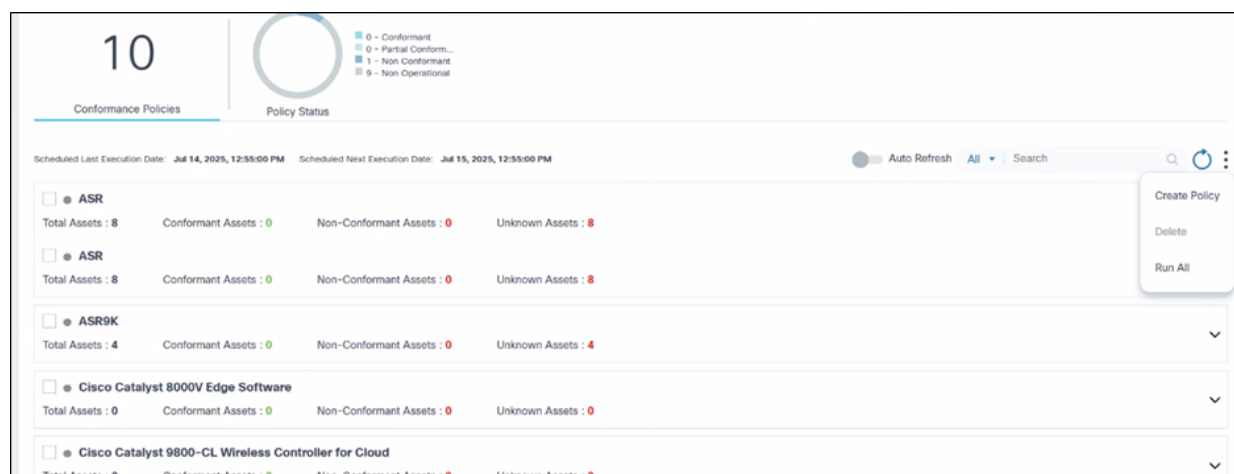
合規策略的擴展檢視

在展開檢視中，將顯示與裝置型號相關的所有策略。對於每個策略，可以通過從Action列中選擇

More Options圖示來執行其他操作，包括Run、Edit Policy、View Results等。

建立軟體一致性策略

1. 使用具有軟體一致性管理訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Software Conformance。系統隨即會顯示「Software Conformance」頁面。



建立策略

3. 選擇More Options圖示> Create Policy。

The screenshot shows the 'Create Policy' form. It includes the following fields and options:

- Policy Name*: Test-Policy
- Device Model*: NSK-C9364C-GX
- Target Version*: 10.2.2
- SMU(s): Select option(s)
- EPLD: n9000-epkd.10.2.2.F.img
- Region*: Global
- Device Role(s)*: Any
- Asset group(s): All
- Additional Conformance Check Template: Select option
- State: Enable (toggle)

Buttons: Cancel, Create

建立策略窗體

4. 在Policy Name、Device Model(s)、Target Version、SMU、EPLD、Device Role、Asset Groups和Additional Conformance和Additional ConformanceCheck Template欄位中輸入資訊。SMU、資產組和其他符合性檢查模板是可選欄位。



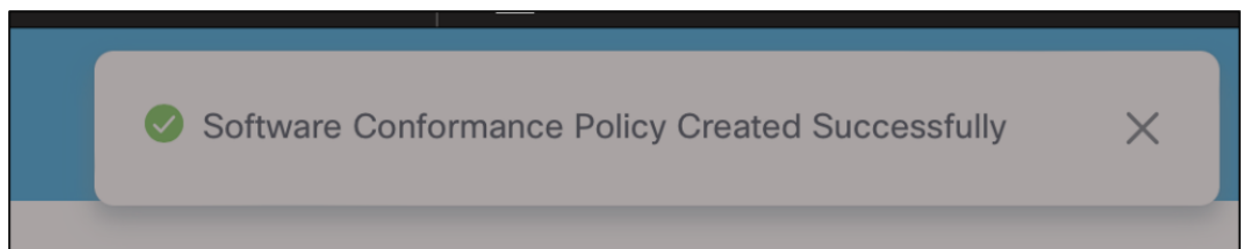
附註：使用者現在可以在「建立一致性策略」表單中選擇多個裝置型號。

 附註：軟體一致性框架可以針對管理裝置的特定模型、角色或控制器例項的裝置，對基本OS版本和SMU修補程式運行一致性檢查。如果需要任何其他自定義檢查，則可以使用所需的命令和驗證規則建立流程模板，這些命令和驗證規則可以對映到Additional Conformance Check Template欄位。

5. 按一下「Create」。系統會顯示確認。

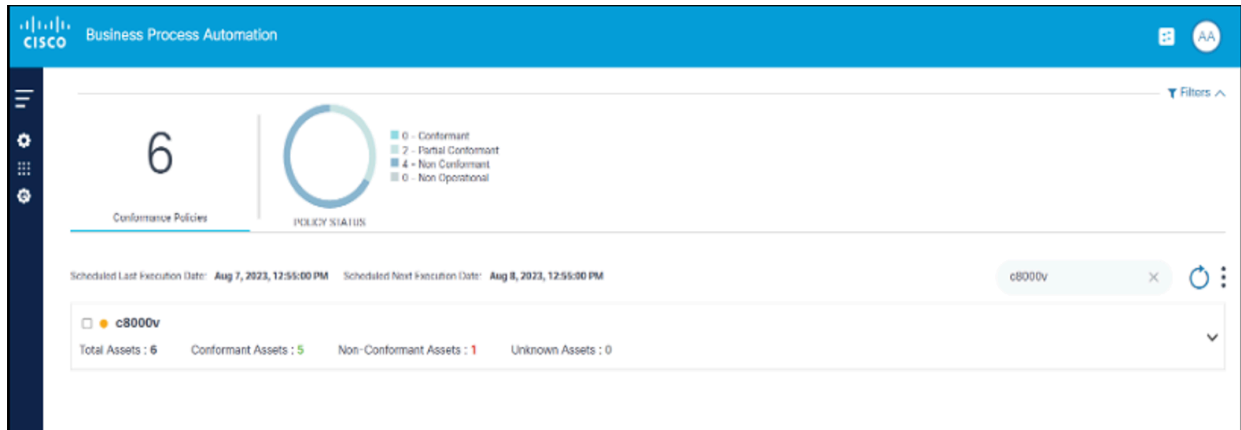
 附註：應註明以下清單。

- 用例管理員可以為所選裝置型號靈活地建立具有不同裝置角色的多個策略。可以在單個策略中選擇多個角色。
- 如果從Device Role(s)下拉選單中選擇Any，則會禁用所有其他裝置角色（例如，訪問、核心等）。如果選擇了任何其他裝置角色，則Any被禁用。
- 對於CNC、NSO、ANSIBLE和Direct-to-Device等控制器管理的裝置，可以使用Any角色(從Device Role(s)下拉選單中選擇)來執行合規性檢查，因為這些裝置沒有角色資訊。
- 如果從FMC的Device Role(s)下拉選單中選擇Any，則在所有裝置（包括獨立、控制和資料裝置）上執行軟體一致性。
- 只有CNC、NSO、ANSIBLE、FMC、直接到裝置和NDFC控制器支援SMU的一致性和升級。
- 此版本僅支援Region下拉清單中的Global
- 使用者可以從下拉選單中選擇「資產組」。預設情況下會選擇全部。使用者可以選擇一個或多個資產組。如果選擇特定資產組，則僅針對所選資產組的裝置執行策略。
- 如果未顯示Device Model、Target Version和SMU(s)欄位的預期值，請按一下Discover Images，然後重試。
- Device Model、Asset Group和Role欄位共同形成唯一策略；不允許重複策略。
- 僅當選定裝置型號和目標版本可以使用EPLD映像後設資料時，EPLD欄位才會填充值。
- Policy Name是唯一的，不允許重複的策略名稱。



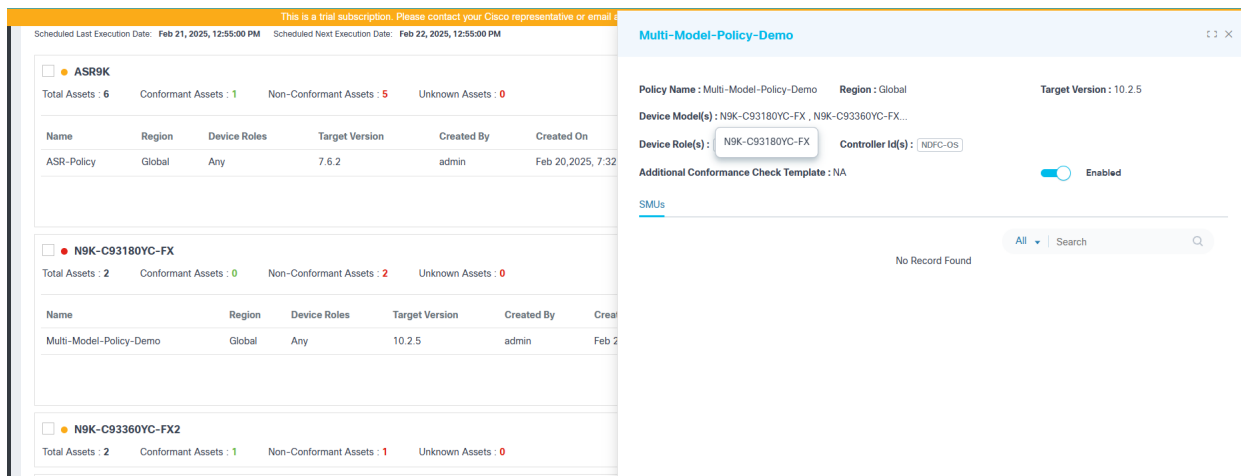
符合策略建立確認

- 標籤到OS Upgrade Next Generation（下一代）的流程模板顯示在Additional Conformance Check Template欄位中。



符合性策略的搜尋結果

6. 通過在Search欄位中輸入裝置型號來查詢建立的策略。

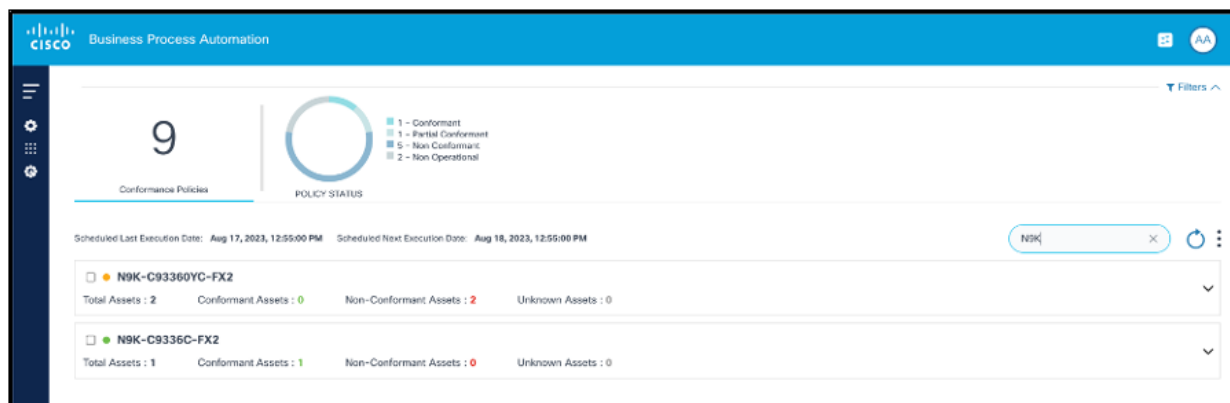


檢視符合性策略

7. 按一下Policy以檢視策略的詳細資訊檢視。

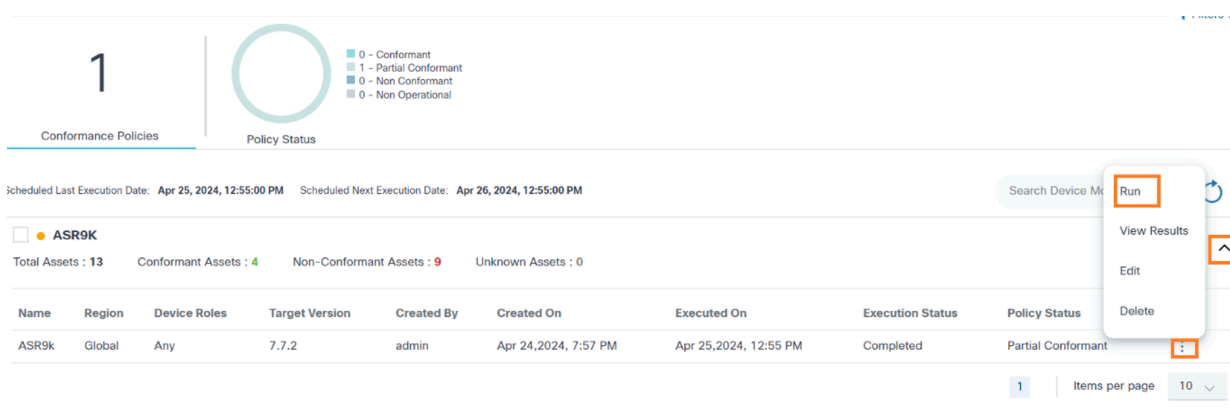
按需執行軟體一致性檢查

1. 使用具有執行訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Software Conformance。系統隨即會顯示「Software Conformance」頁面。



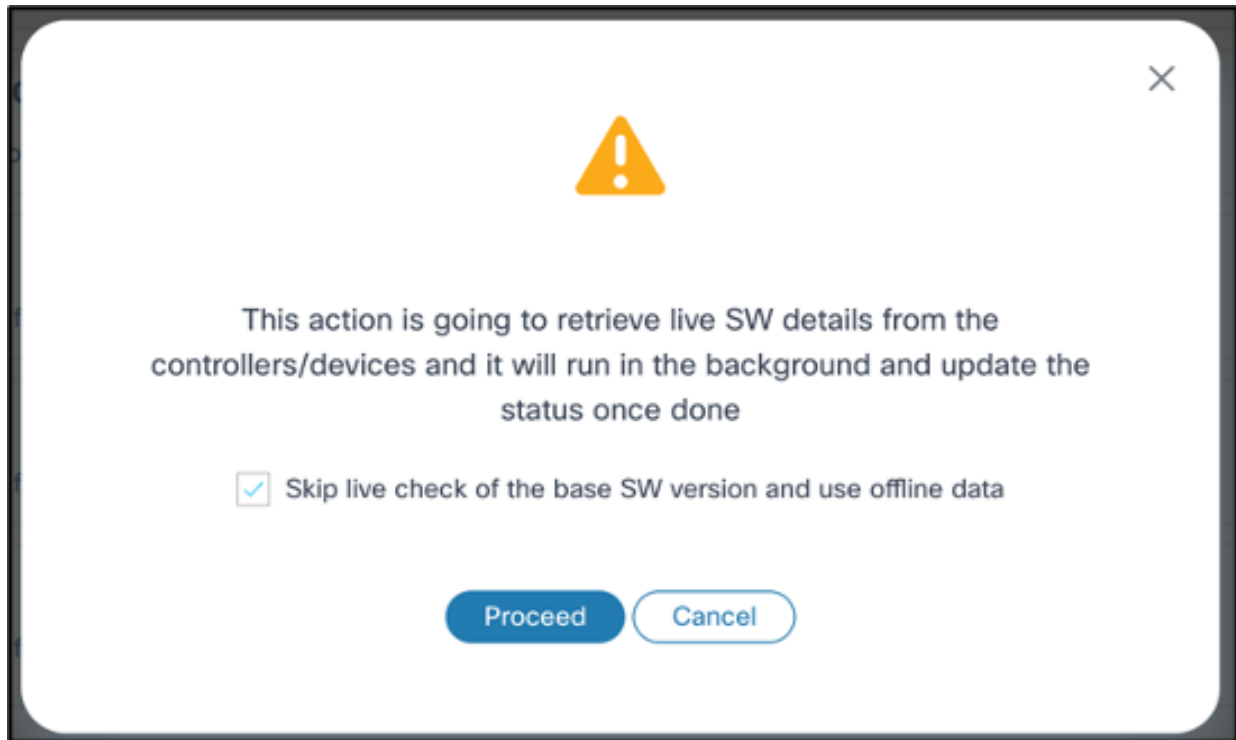
策略搜尋

3. 使用Search欄位查詢要按需執行的策略。



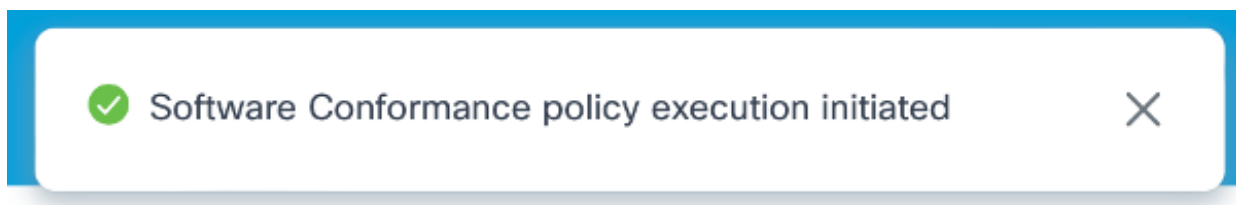
運行

4. 在策略的Action列中，選擇More Options > Run。系統將顯示確認資訊，以驗證是否應對裝置執行即時清點檢查。



運行合規性策略的確認

5. 如果在運行一致性檢查之前需要即時清單同步，請清除Skip Live Check of the Base SW Version and use offline data覈取方塊，然後單擊Proceed。在這種情況下，一致性檢查只在同步後執行。通知將顯示在右上角。



合規策略執行通知

 附註：應註明以下清單。

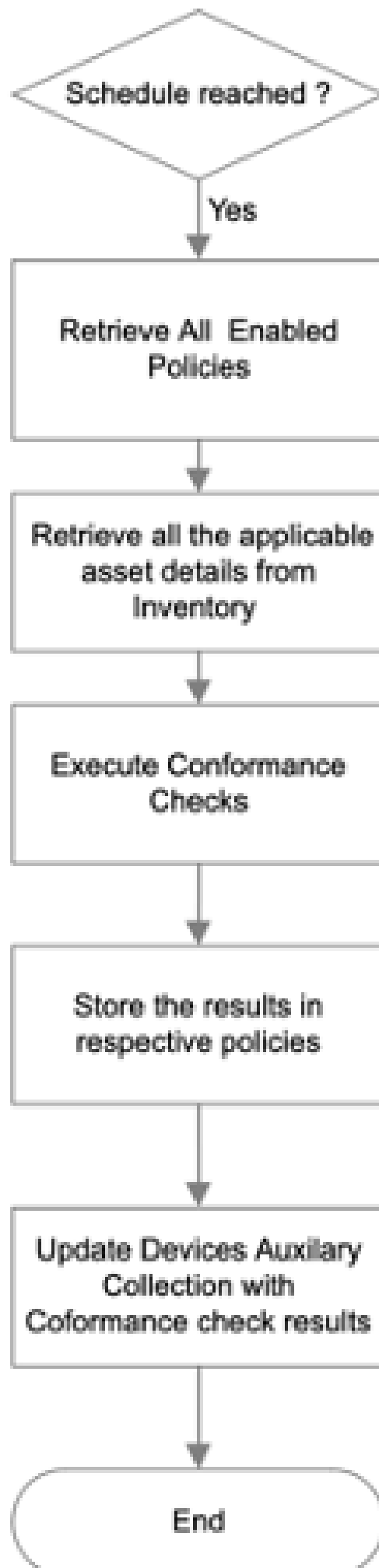
- 預設情況下使用資產庫存資料執行一致性檢查。
- 在此過程中，如果清單或裝置同步失敗，則相應的策略裝置將標籤為Unknown，並跳過SMU檢查。
- 對於SMU，在執行符合性檢查之前從裝置檢索即時資料，以檢查是否選中了「Skip Live Check of the Base SW Version and use offline data」覈取方塊。
- 當策略包括多個裝置模型時，針對裝置模型執行該策略將啟動所有關聯策略的執行。

安排執行軟體一致性檢查

可使用計畫程式服務定期自動執行軟體一致性檢查。可以將計畫的一致性檢查配置為運行：

- 每日
- 一天兩次
- 每週
- 一次

一旦達到計畫，處於「已啟用」狀態的所有策略將自動執行，一致性結果將儲存在各自的策略中。

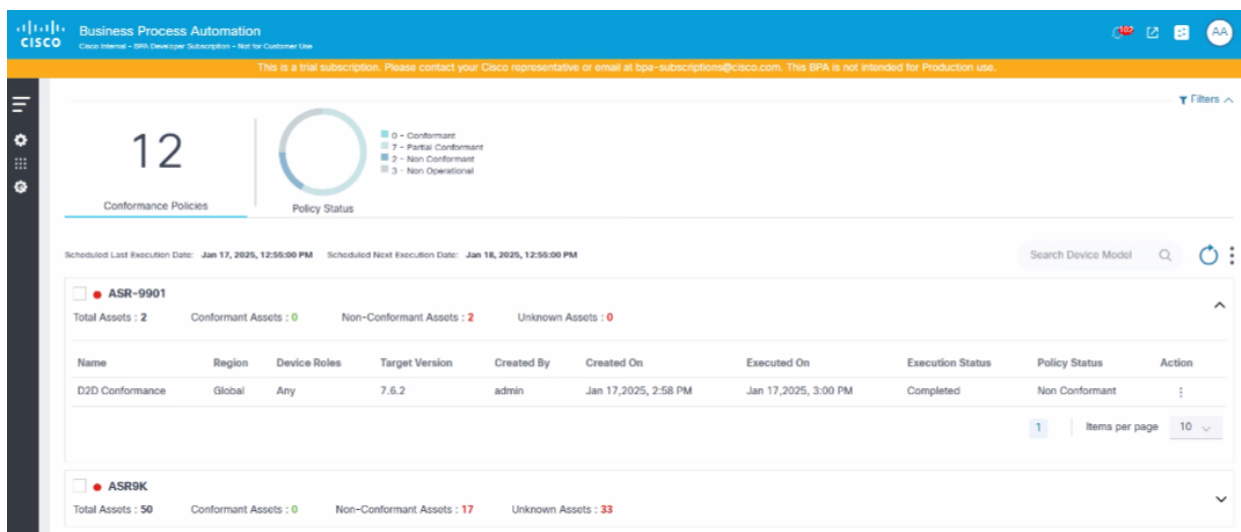


軟體一致性檢查呼叫的計畫執行

有關詳細資訊，請參閱[軟體一致性](#)。

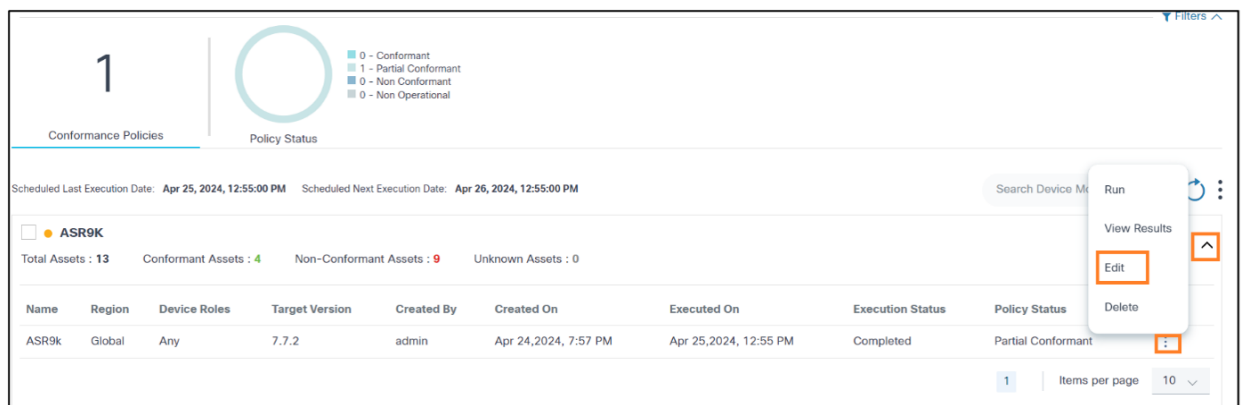
更新軟體一致性策略

1. 使用具有軟體一致性管理訪問許可權的憑據登入到BPA
2. 選擇OS Upgrade > Software Conformance。系統隨即會顯示「Software Conformance」頁面。



軟體符合性

3. 使用Search欄位查詢所需的策略。



編輯

4. 在策略的Action列中，選擇More Options圖示> Edit。

All > N9K-C93180YC-FX > Multi-Model-Policy-Demo Sync Images

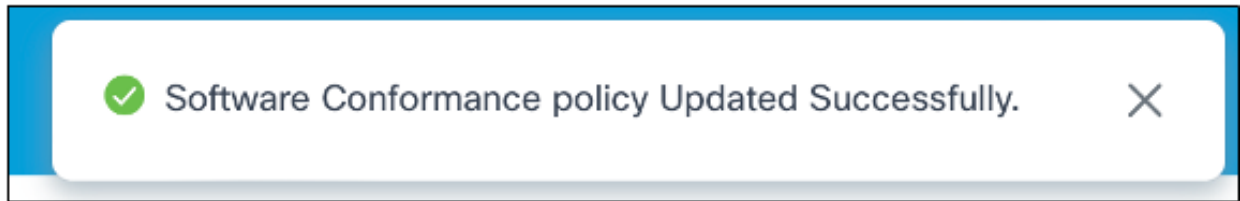
Policy Name*	Device Model*	Target Version*	SMU(s)
Multi-Model-Policy-Demo	N9K-C93180YC-FX, N9K-C93360YC-FX2	10.2.5	Select option(s)
Region*	Device Role(s)*	Controller ID(s)	Additional Conformance Check Template
Global	Any	NDFC-OS	Select option

State
☒ Enable

Cancel Save

編輯已填寫詳細資訊的符合性策略

5. 根據需要編輯目標版本、SMU、裝置角色、控制器ID、策略狀態和其他一致性檢查模板欄位。
6. 按一下「Save」。系統會顯示確認。



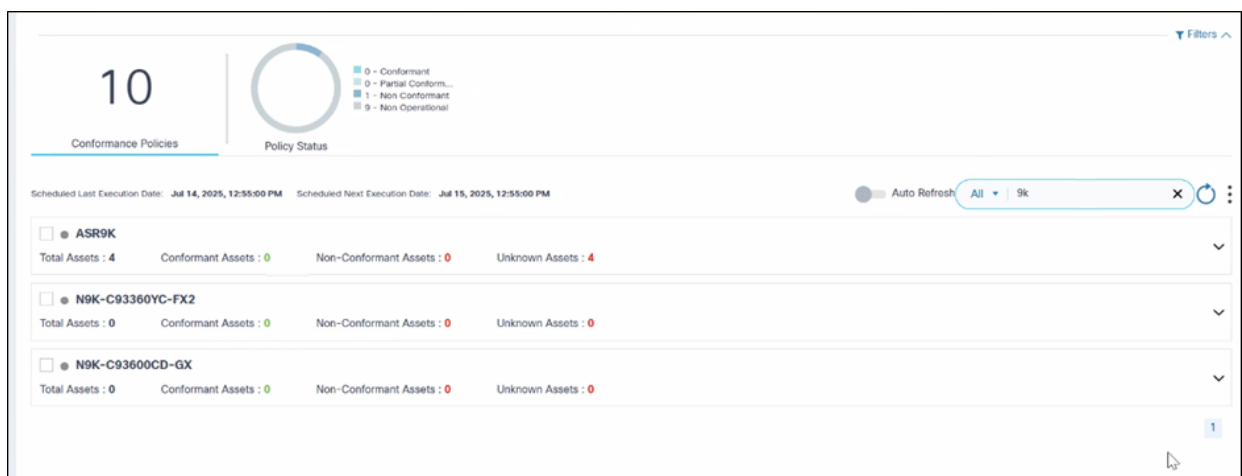
確認更新成功



附註：當軟體一致性策略用於正在進行的升級作業時，無法編輯該策略。

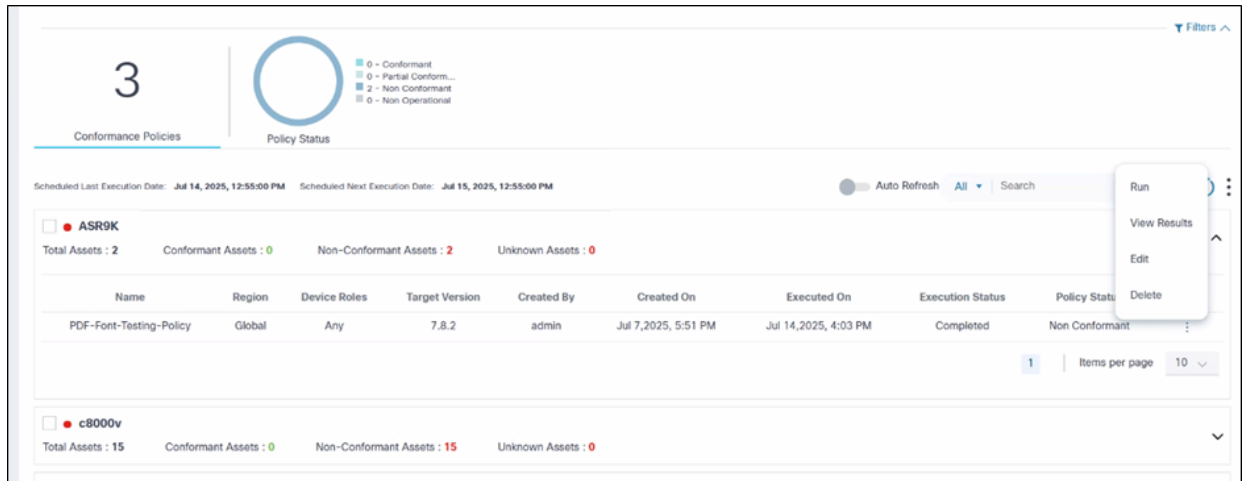
刪除軟體一致性策略

1. 使用具有管理訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Software Conformance。系統隨即會顯示「Software Conformance」頁面。



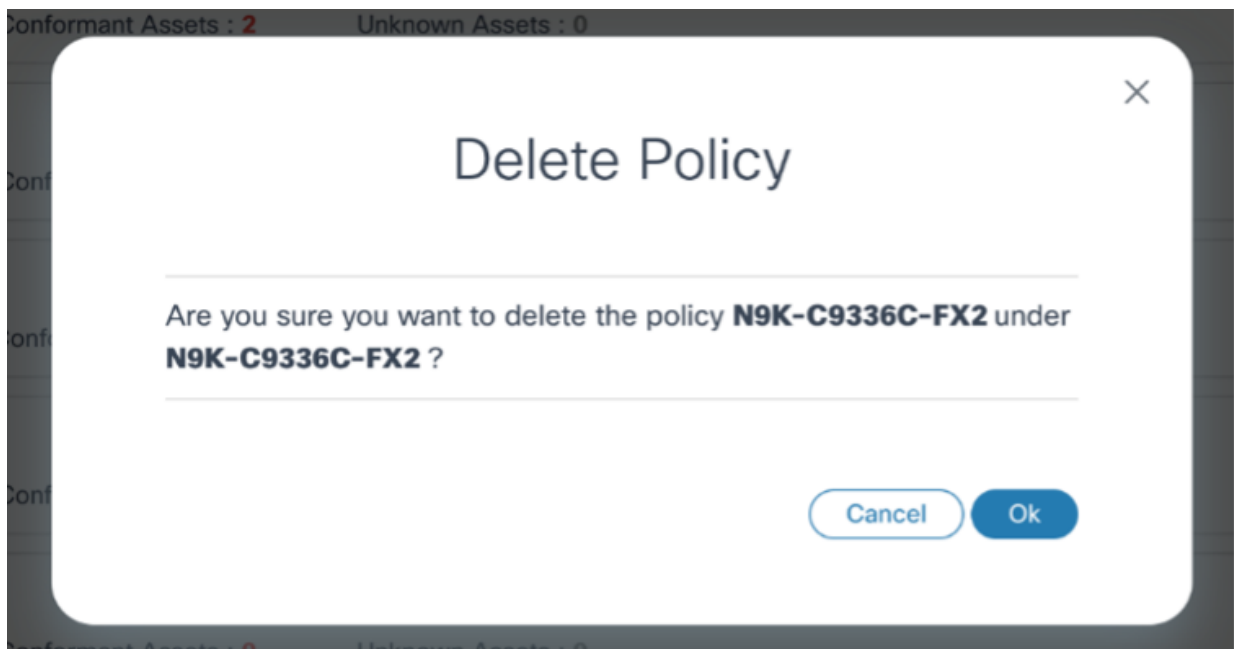
符合性策略的搜尋結果

3. 使用Search欄位查詢所需的策略。

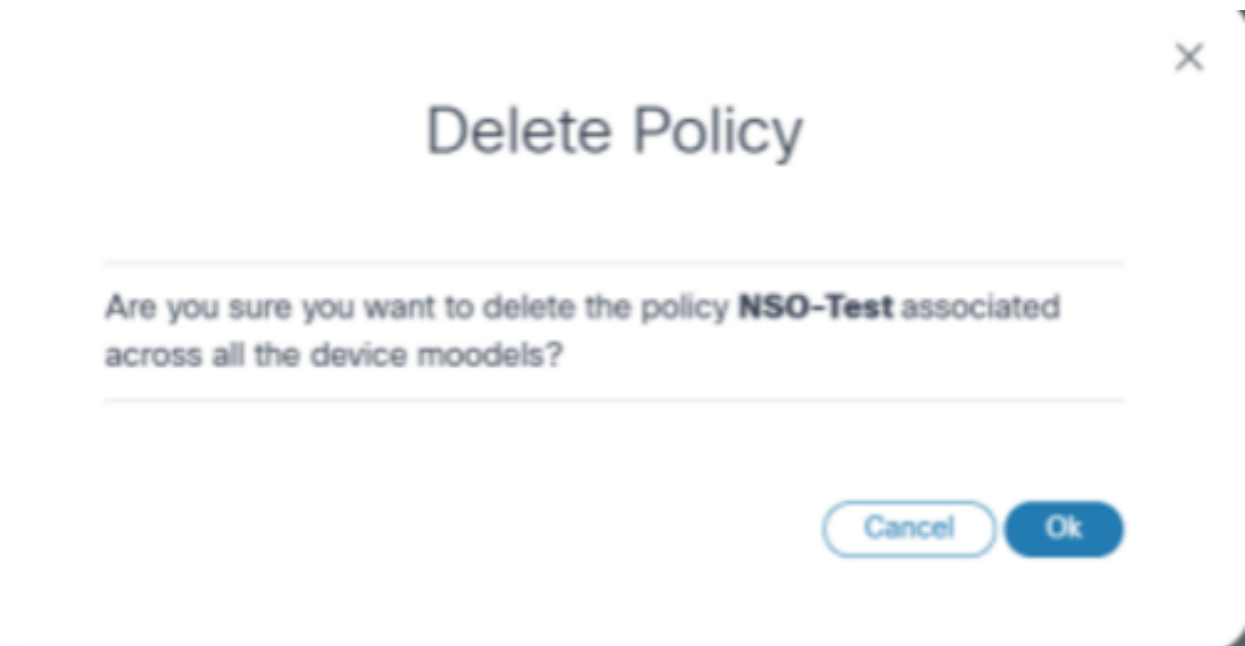


刪除

4. 從策略的Action列中，選擇More Options圖示> Delete。此時將開啟確認視窗。



刪除策略確認



刪除策略確認（如果策略與多個模型關聯）

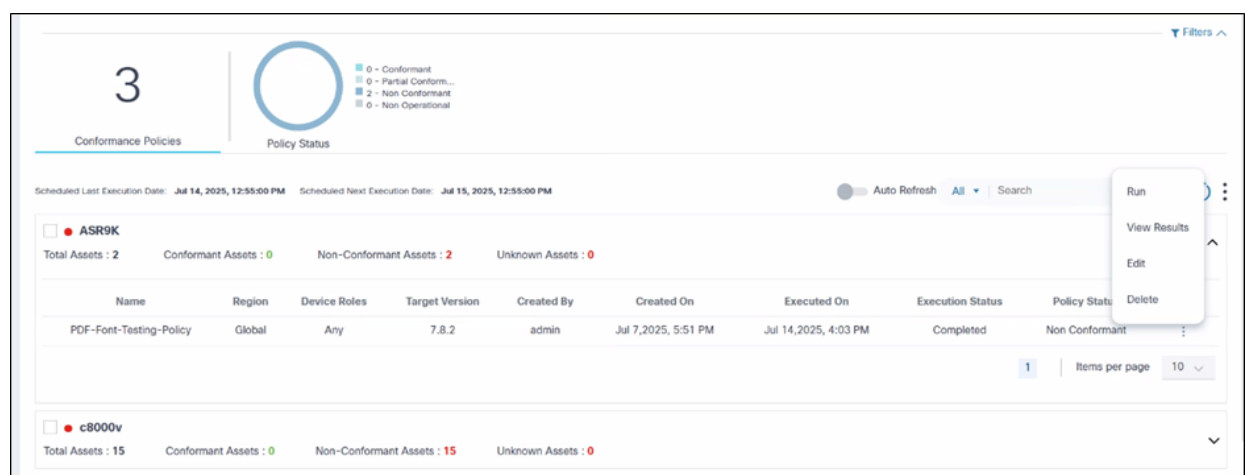
5. 按一下「OK」（確定）。策略即被刪除。

 附註：應註明以下清單。

- 如果策略與多個裝置模型關聯，則刪除策略將刪除每個關聯模型的所有相關策略。
- 當軟體一致性策略用於正在進行的升級作業時，無法刪除該策略。

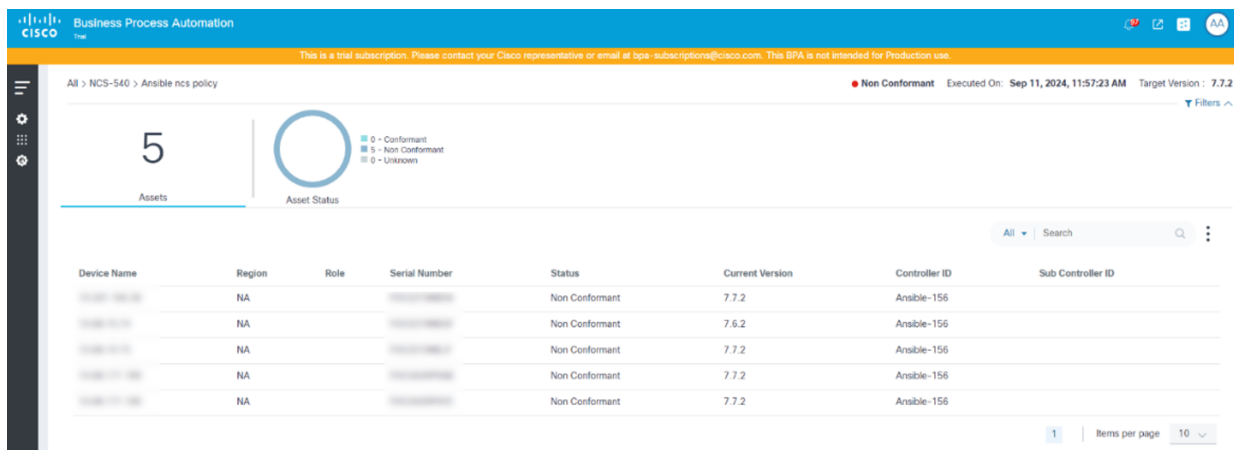
檢視和下載符合性結果

一旦策略被執行：

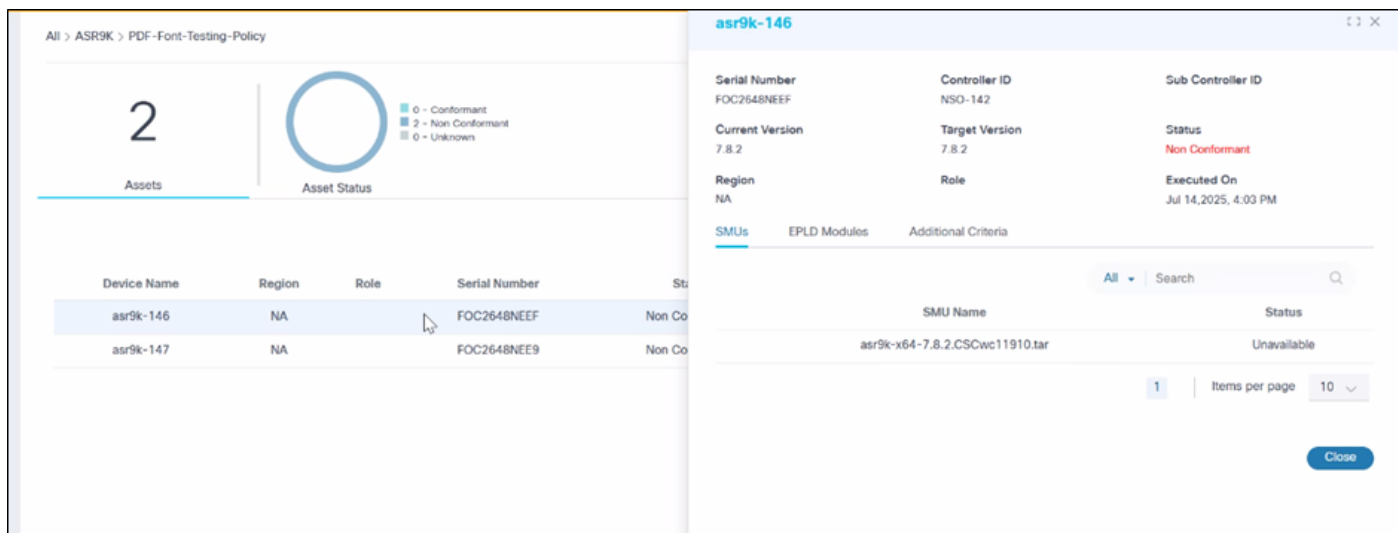


檢視結果選項

1. 在「Software Conformance」頁面上，選擇「More Options」圖示>「View Results」。Results頁面顯示了使用者可在其中檢視裝置的一致性狀態。



檢視結果



Command Output:

Label : 7.7.2

Node 0/RP0/CPU0 [RP]

Boot Partition: xr_lv32

Active Packages: 11

```

ncs540-xr-7.7.2 version=7.7.2 [Boot image]
ncs540-lictrl-1.0.0.0-r772
ncs540-mpls-1.0.0.0-r772
ncs540-li-1.0.0.0-r772
ncs540-mgbl-1.0.0.0-r772
ncs540-isis-1.0.0.0-r772
ncs540-ospf-1.0.0.0-r772
ncs540-k9sec-1.0.0.0-r772
ncs540-mcast-1.0.0.0-r772
ncs540-mpls-te-rsvp-1.0.0.0-r772
ncs540-eigrp-1.0.0.0-r772

```

Node 0/0/CPU0 [LC]

Boot Partition: xr_lcp_lv32

Active Packages: 11

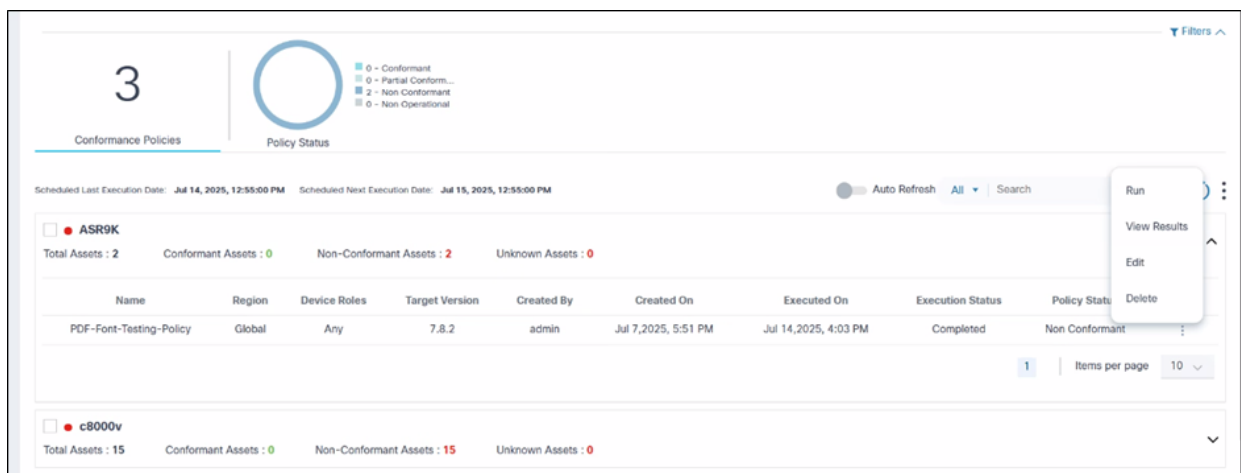
```

ncs540-xr-7.7.2 version=7.7.2 [Boot image]
ncs540-lictrl-1.0.0.0-r772
ncs540-mpls-1.0.0.0-r772
ncs540-li-1.0.0.0-r772
ncs540-mgbl-1.0.0.0-r772

```

2. 選擇一行以顯示特定資產詳細資訊以及SMU狀態和其他條件。

 附註：SMU詳細資訊僅顯示NSO、CNC、ANSIBLE、直接到裝置和NDFC控制器資產。僅顯示NDFC控制器的EPLD模組。



The screenshot displays a web-based interface for managing network policies. At the top, there's a summary section with a large number '3' and a circular progress indicator. Below this, the 'Conformance Policies' section is active, showing a table of policies. The first policy listed is 'PDF-Font-Testing-Policy' with a status of 'Non Conformant'. A context menu is open over this policy, showing options like 'Run', 'View Results', 'Edit', and 'Delete'. The second policy, 'c8000v', is partially visible below.

Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status
PDF-Font-Testing-Policy	Global	Any	7.8.2	admin	Jul 7, 2025, 5:51 PM	Jul 14, 2025, 4:03 PM	Completed	Non Conformant

檢視結果

3. 從裝置的「操作」列中，選擇更多選項圖示> 檢視結果。

13

Assets

Asset Status

4 - Conformant

9 - Non Conformant

0 - Unknown

All

Search

Download

Device Name	Region	Role	Serial Number	Status	Current Version	Controller ID	Sub Controller ID
10.201.156.156	NA		10.201.156.156	Non Conformant	7.6.2	ANSIBLE-156	
10.201.156.156	NA		10.201.156.156	Conformant	7.7.2	ANSIBLE-156	
10.201.156.156	NA		10.201.156.156	Conformant	7.7.2	ANSIBLE-156	
10.201.156.156	NA		10.201.156.156	Non Conformant	7.6.2	ANSIBLE-156	
10.201.156.156	NA		10.201.156.156	Non Conformant	7.6.2	ANSIBLE-156	
10.201.156.156	NA		10.201.156.156	Non Conformant	7.6.2	NSO-183	

下載

4. 選擇More Options圖示> Download,以.csv格式下載結果並顯示SMU可用性狀態。

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Device Na	Serial Num	Controller	Sub Contr	Region	Device Rol	Current Ve	Target Ver	Device Sta	Execution	ncs540-7	Complianc	Complianc	Remarks				
2	10.201.156.156	10.201.156.156	Ansible-156		NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	Success	Device conformance check completed along with Process Template				
3	10.201.156.156	10.201.156.156	Ansible-156		NA		7.6.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	NA	Device conformance check completed				
4	10.201.156.156	10.201.156.156	Ansible-156		NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	Success	Device conformance check completed along with Process Template				
5	10.201.156.156	10.201.156.156	Ansible-156		NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	Success	Device conformance check completed along with Process Template				
6	10.201.156.156	10.201.156.156	Ansible-156		NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	Success	Device conformance check completed along with Process Template				
7																		

Excel工作表檢視

附註：「檢視結果」僅顯示最近執行的符合性檢查的結果。使用者只能檢視他們有權訪問的資產。對於非操作策略，將禁用檢視結果。

可能的裝置狀態：

- Conformant:指示裝置符合定義的策略
- 不符合項:表示裝置在滿足以下條件時不符合要求：

目標版本	SMU	合規性檢查	狀態
不符合項	不適用	不適用	不符合項
符合者	不可用	規則失敗	不符合項
符合者	可使用	規則失敗	不符合項
符合者	不可用	規則成功	不符合項

- 未知:表示由於裝置沒有當前軟體版本資訊，無法執行裝置軟體一致性檢查。

Unknown狀態的條件包括：

目標版本	SMU	EPLD	合規性檢查	狀態
不符合項	不適用	不適用	不適用	不符合項
符合者	不可用	不符合項	規則失敗	不符合項
符合者	不可用	符合者	規則失敗	不符合項
符合者	可使用：	符合者	規則失敗	不符合項
符合者	可使用：	不符合項	規則失敗	不符合項
符合者	不可用	符合者	規則成功	不符合項
符合者	不可用	符合者	規則成功	不符合項

可能的SMU狀態：

- 可使用:指示SMU存在於裝置中，並且處於活動狀態
- 不可用:表示SMU可能不存在或確實存在但處於「非活動」狀態

可能的EPLD模組狀態：

- Conformant:指示裝置中存在具有預期目標版本的EPLD模組
- 不符合項:指示裝置中存在預期目標版本不匹配的EPLD模組
- 缺少模組:表示裝置中未配置或訂閱EPLD模組

可能的合規性檢查模板狀態：

- 成功:指示裝置使用有效命令和規則成功執行流程模板
- 失敗:指示裝置無法執行流程模板（例如，命令不正確時）
- 不適用:表示裝置不符合執行過程模板的條件（例如，當裝置不符合定義的目標版本時）



附註：應註明以下清單。

-
- 軟體一致性檢查僅適用於屬於預設租戶的裝置
 - 軟體一致性檢查依賴於資產清單作為裝置當前軟體版本的真實來源。如果資產清單資料已過時，則軟體一致性檢查結果已過時。要避免陳舊的資料問題，請在開始執行合規性策略時使用即時清點檢查功能
 - 可以在OS Upgrade > Settings > Software Conformance中更改預設計畫
 - 升級到BPA 5.1後，所有預先存在的策略都將移至禁用狀態；使用者必須編輯每個策略，選擇

適當的值，啟用它，然後儲存更改以供將來使用

升級策略

升級策略元件支援兩種型別的策略：

- 單步策略：
 - Any-Any
 - <特定源版本(7.7.1)> - <特定目標版本(7.7.2)>
- 多步驟策略：
 - 7.7.1版 — 7.7.2版
 - v7.7.2 - 7.7.8
- 多步驟升級可包括網橋SMU，如下例所示：
 - v7.7.1 - v7.7.1[網橋SMU]
 - V7.7.1[網橋SMU] - 7.7.8

升級策略元件提供預定義以下平台特定對象的靈活性：

- 升級路徑
- 驗證前後的模板或工作流程
- 分發工作流
- 啟用工作流
- 備份工作流
- 超時值
- 回滾工作流
- 有效的前差異和後差異
- 流量轉移工作流或流量逆轉工作流

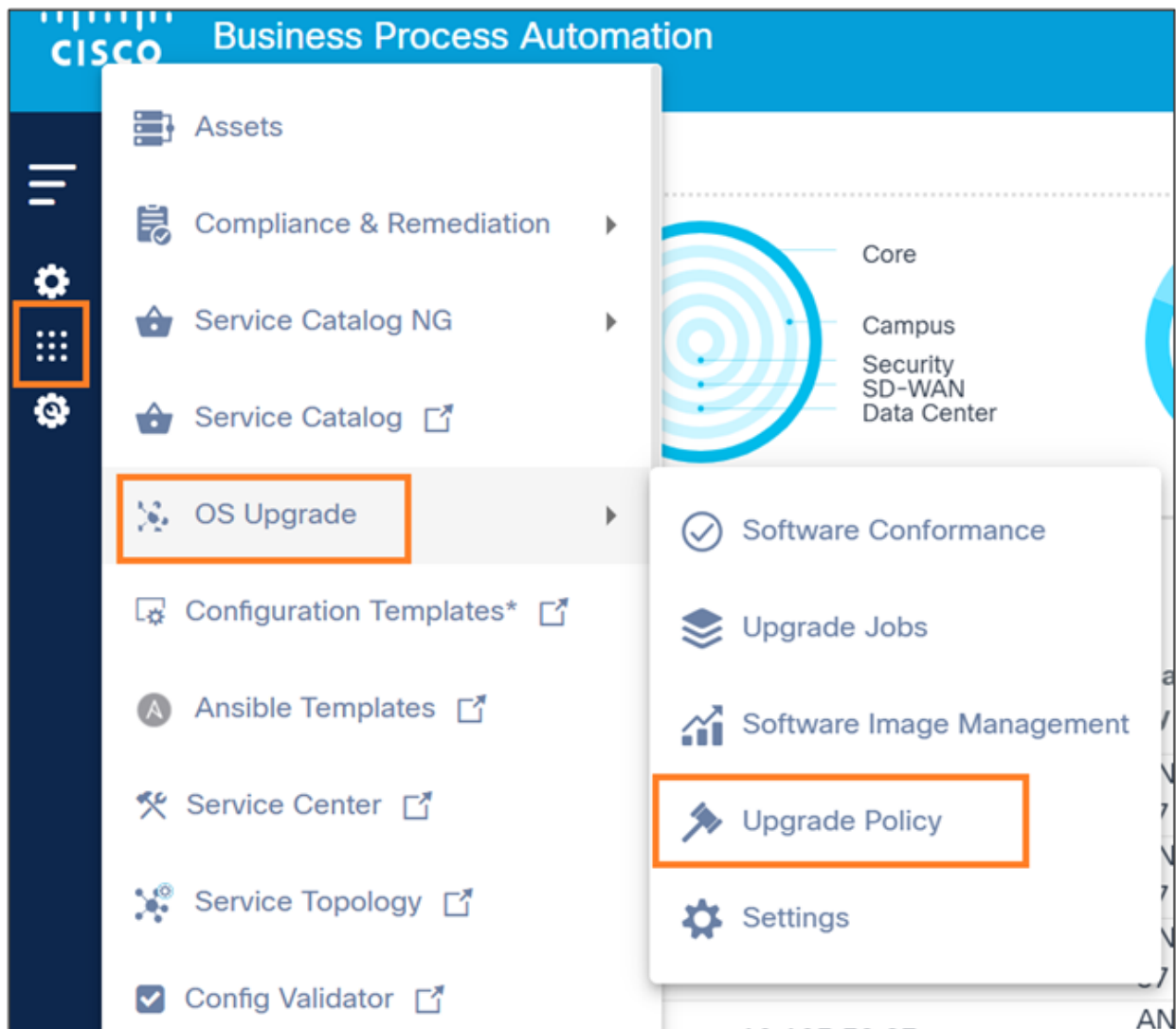
必要條件

- 必需的驗證前和驗證後流程模板或工作流程
- 所需的備份、分發、啟用和回滾工作流程
- 所需的映像後設資料

檢視和管理升級策略

要訪問「升級策略」(Upgrade Policy)頁面，請執行以下操作：

1. 使用對升級策略具有足夠訪問許可權的憑據登入到BPA。



升級策略導航

2. 選擇OS Upgrade > Upgrade Policy。系統隨即會顯示Upgrade Policy頁面。

The screenshot displays the 'Upgrade Policy' page. At the top left, there is a large number '8' representing the total number of policies. Below it, a donut chart shows the distribution of controller types. The legend for the donut chart is as follows:

- 1 - CNC
- 1 - DNAC
- 1 - Direct-To-Device
- 1 - FMC
- 1 - NDFC
- 1 - vManage
- 1 - Ansible
- 1 - NSO

Below the chart, there is a table with the following columns: Device Model, Controller Type, Name, Created By, Last Modified On, and Action. The table contains one row of data:

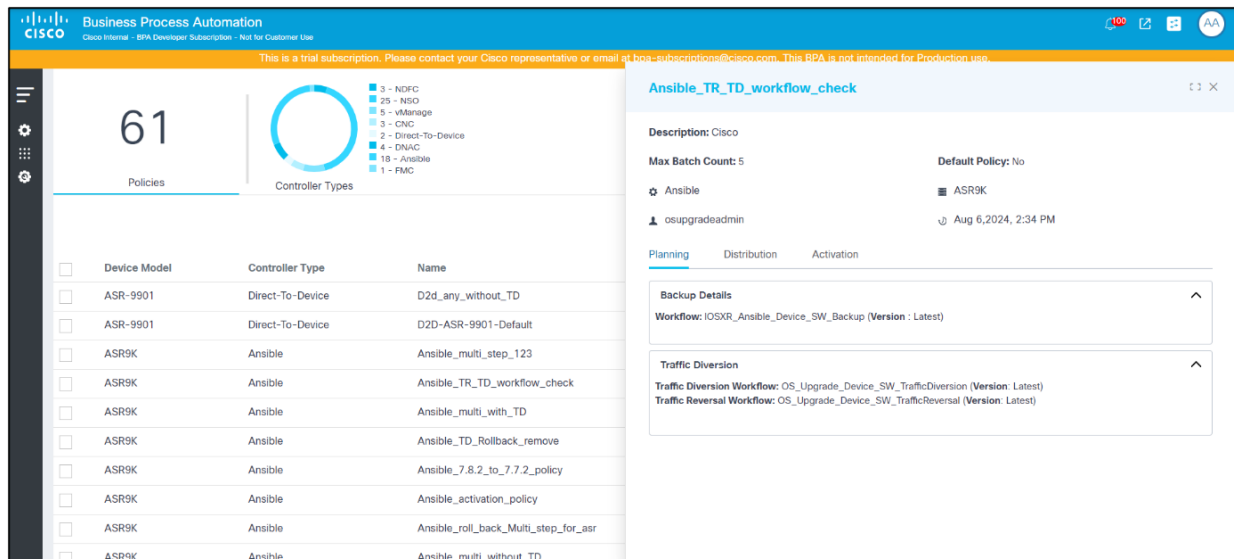
Device Model	Controller Type	Name	Created By	Last Modified On	Action
ASR-9901	Direct-To-Device	D2D-ASR-9901-Default	System	Mar 22, 2024, 11:14 AM	

升級策略

Upgrade Policy頁包含以下內容：

- 頂部顯示的分析部分提供以下內容：

- 系統中的升級策略總數
- Controller Types快速過濾器，提供按控制器型別進行過濾的功能
- 一個更多選項圖示，提供用於建立策略和批次處理操作(如刪除所有選定策略)的選項
- 用於搜尋策略的搜尋篩選器，可按如下方式篩選：
 - All:在所有欄位中進行搜尋
 - 裝置型號:搜尋具有指定模型的策略
 - 名稱:搜尋具有指定策略名稱的策略
 - 建立者:搜尋具有指定使用者的策略
- 通過按一下相應的列名或表欄位對策略進行排序



策略詳細資訊檢視

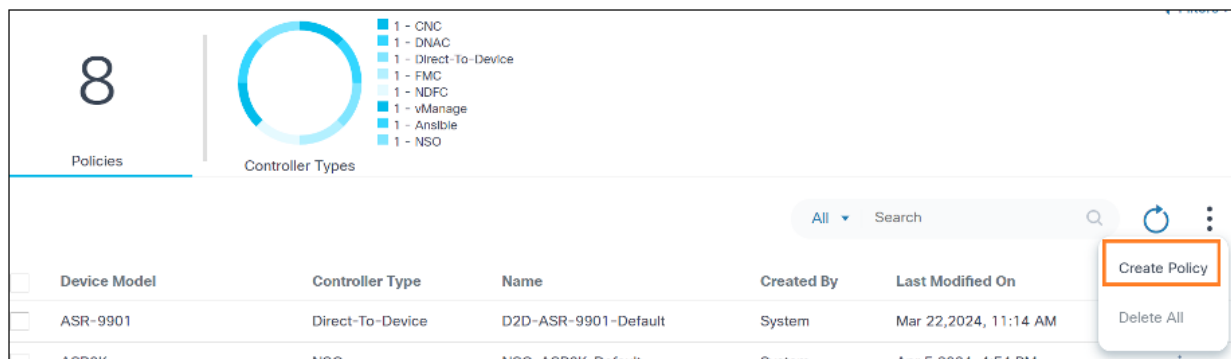
- 按一下特定策略或排列策略的詳細資訊檢視



附註：如果策略名稱唯一，則相同的裝置型號和控制器型別可以具有任意數量的策略。

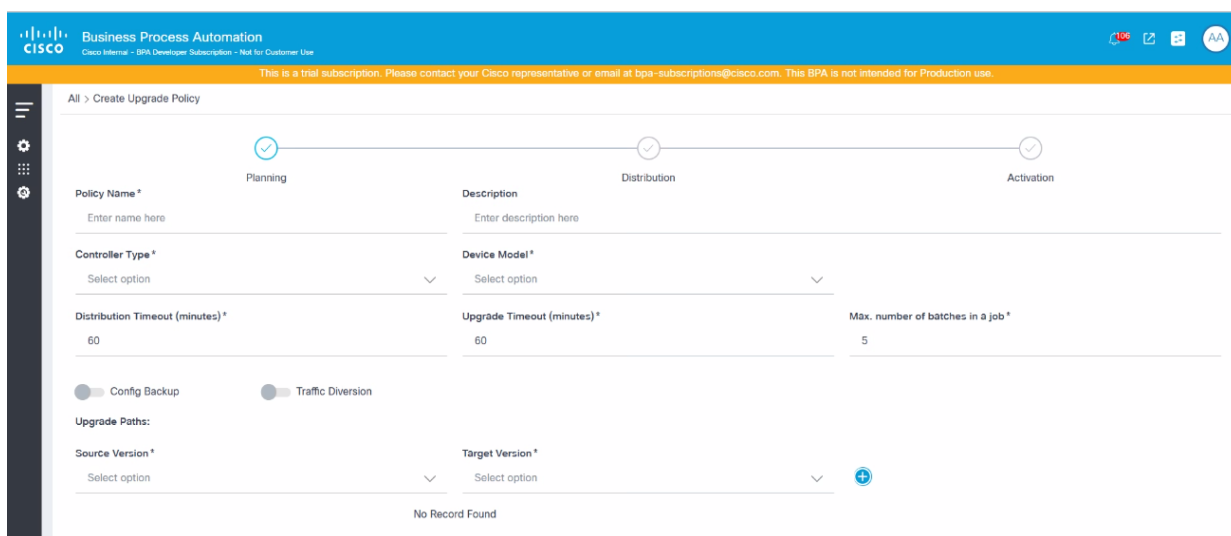
建立升級策略

1. 使用具有升級策略管理訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Policy。系統隨即會顯示Upgrade Policy頁面。



建立策略

3. 選擇More Options > Create Policy。系統隨即會顯示Create Upgrade Policy頁面。



建立升級策略

規劃

1. 配置與整體策略相關的引數。下表對每個欄位進行了簡要說明。

欄位	說明
策略名稱	策略的名稱
說明	策略的簡要說明
控制器型別	用於執行作業系統升級的相應控制器
裝置型號	用於執行作業系統升級的裝置型號
分發超時 (分鐘)	映像分發活動的最長等待時間 (分鐘)
升級超時 (分鐘)	映像啟用活動的最長等待時間 (分鐘)
作業中的最大批數	可以新增到作業中的批數；允許的最大批數為20
配置備份切換	如果需要備份，啟用此切換並完成vManage和Direct-to-Device控制器視窗中的以下欄位：

- Workflow Name:適用的備份工作流

附註：如果找不到工作流，請確保工作流已正確標籤有 OS Upgrade NextGen標籤

— 使用最新工作流:如果選中，則使用所選工作流的最新版本

- Workflow Version:定製工作流程版本；只有在未選擇「使用最新工作流」時才能選擇。

對於NDFC、NSO、CNC和Cisco Catalyst中心控制器，備份通過備份和還原服務進行。因此，必須在「備份詳細資訊」視窗中選擇備份和還原策略。

附註：使用者必須為控制器型別選擇適當的策略。有關備份和還原策略的詳細資訊，請參閱[備份和還原](#)部分。

要為Nexus裝置啟用備份，目標裝置上必須存在功能scp-server配置。

如果需要流量轉移，請啟用此切換，並在流量轉移視窗中填寫以下欄位：

- Traffic Distribution Workflow:適用的流量轉移工作流。

附註：如果找不到工作流，請確保工作流已正確標籤了 OS Upgrade NextGen標籤

流量分流切換

- Traffic Reversal Workflow:適用的流量沖銷工作流。

附註：如果找不到工作流，請確保工作流已正確標籤了 OS Upgrade NextGen標籤

— 使用最新工作流:以上所選工作流程的最新版本

- Workflow Version:定製工作流程版本；只有在未選擇「使用最新工作流」時才能選擇

升級路徑定義適用的步驟升級路徑；可以在以下欄位中新增多個源版本和目標版本，以滿足不同的需求

升級路徑

- Source Version:升級路徑的開始版本

-目標版本:升級路徑的結束版本

- Source Version(Any)to Target Version(Any):這是通過為Source Version和Target Version欄位選擇Any (這是所有裝置型號的預設值) 來實現的；在此案例中，Distribution和Activation頁面提供統一的升級過程

- 源版本 (特定版本) 到目標版本 (特定版本) :這可以通過選擇裝置型號可用的特定映像版本來實現；可以新增多個源版本和目標版本；分發和啟用升級過程輸入的數量與新增的源版本和目標版本的數量相匹配，並且每個均顯示為帶有相應源版本和目標版本標籤的可摺疊部分。升級路徑要求將強制的SMU作為網橋SMU新增到各自的升級路徑，然後再升級到目標版本。有關網橋SMU的詳細資訊，請參閱下一節。

橋接SMU

橋接式SMU (也稱為強制升級或降級SMU) 是前提條件，必須在升級或降級到同一平台或型號的另一個軟體版本之前安裝。

在升級路徑中新增網橋SMU

Policy Name*
Enter name here

Description
Enter description here

Controller Type*
NSO

Device Model*
ASR9K

Distribution Timeout (minutes)*
60

Upgrade Timeout (minutes)*
60

Max. number of batches in a job*
5

☐ Config Backup ☐ Traffic Diversion

Upgrade Paths:

Source Version
Select option

Target Version
Select option

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2		7.7.2	⋮

1 | Delete Path Add Bridge SMUs

Cancel Next

升級路徑選項

1. 新增升級路徑後，選擇更多選項圖示。將顯示Delete Path和Add Bridge SMUs選項。

Policy Name* Enter name here ✓

Controller Type* NSO ✓

Distribution Timeout (minutes)* 60

Upgrade Paths:

Source Version Select option ✓

Target Version Select option ✓

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2		7.7.2	⋮

1 | Delete Path Add Bridge SMUs

Cancel Next

新增網橋SMU

- 選擇Add Bridge SMUs。Add Bridge SMUs視窗開啟。將顯示指定升級路徑的所有可用網橋SMU。

Add Bridge SMUs

Select option(s)

☒ asr9k-x64-7.6.2.CSCwf77420.tar

☐ asr9k-x64-7.6.2.CSCwc41614.tar

新增網橋SMU

- 在Add Bridge SMUs視窗中，選中要新增網橋SMU的相應覈取方塊，或清除覈取方塊以刪除它們。新增網橋SMU後，升級路徑將使用選定的網橋SMU詳細資訊進行更新。

Policy Name* ASR9kPolicy ✓

Controller Type* NSO ✓

Distribution Timeout (minutes)* 60

Upgrade Paths:

Source Version Select option ✓

Target Version Select option ✓

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2	asr9k-x64-7.6.2.CSCwf77420.tar	7.7.2	⋮

使用橋接器SMU的升級路徑

 附註：在升級過程中，包括網橋SMU的每個升級路徑都被視為兩步升級。對於上圖所示的升級路徑，最終升級路徑為：

- 7.6.2 - 7.6.2 [網橋SMU]

此路徑表示使用網橋SMU更新7.6.2版上運行的裝置。

- 7.6.2 [網橋SMU] - 7.7.2

此路徑表示將裝置從v7.6.2升級到v7.7.2。在這種情況下，裝置的源版本為7.6.2，包括應用於它的網橋SMU。

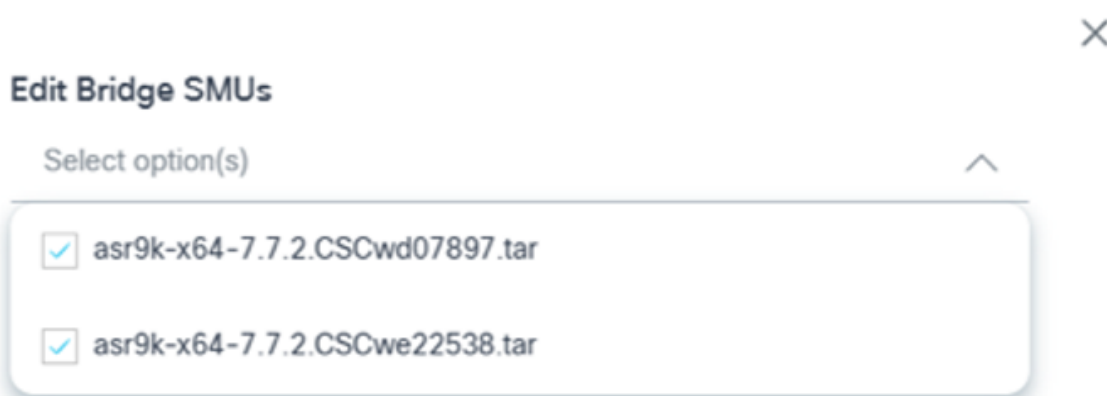
編輯網橋SMU

Source Version		Target Version	
Select option		Select option	
Source Version	Bridge SMU(S)	Target Version	Action
7.7.2	asr9k-x64-7.7.2.CSCwe22538.tar,asr9k-x64-7.7.2.CSCwd07897.tar	7.8.2	1 Items per page Delete Path Edit Bridge SMUs

CancelNext

使用橋接器SMU的升級路徑

1. 在升級路徑部分，選擇更多選項圖示> 編輯Bridge SMU。Edit Bridge SMUs視窗開啟。



編輯網橋SMU

2. 選中或清除相應的覈取方塊以更新網橋SMU。
3. 按一下「OK」（確定）。系統將顯示變更摘要。

Policy Name * ASR9K bridge 772

Controller Type * NSO

Distribution Timeout (minutes) * 60

Upgrade Paths:

Source Version Select option

Target Version Select option

Source Version	Bridge SMU(S)	Target Version	Action
7.7.2	asr9k-x64-7.7.2.CSCwd07897.tar, asr9k-x64-7.7.2.CSCwe22538.tar	7.8.2	:

1 | Items per page 25

Cancel Next

更改摘要

- 驗證更改摘要，然後按一下下一步。

刪除網橋SMU

Source Version Select option

Target Version Select option

Source Version	Bridge SMU(S)	Target Version	Action
7.7.2	asr9k-x64-7.7.2.CSCwe22538.tar, asr9k-x64-7.7.2.CSCwd07897.tar	7.8.2	:

1 | Items per page

Delete Path

Edit Bridge SMUs

Cancel Next

編輯網橋SMU

- 在升級路徑部分，選擇更多選項圖示> 編輯Bridge SMU。Edit Bridge SMUs視窗開啟。

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

編輯網橋SMU

- 清除相應的覈取方塊以刪除Bridge SMU。
- 按一下「OK」（確定）。系統將顯示變更摘要。

Planning

Description

Distribution

Activation

Policy Name *

ASR9K bridge 772

Controller Type *

NSO

Distribution Timeout (minutes) *

60

Device Model *

ASR9K

Upgrade Timeout (minutes) *

60

Max. number of batches in a job *

5

Config Backup

Traffic Diversion

Upgrade Paths:

Source Version

Target Version

Source Version

7.7.2

Target Version

7.8.2

Action

:

1

Items per page

25

Cancel

Next

更改摘要

分佈

分佈採用與影象分佈相關的輸入引數（即影象複製）。以下映像是每個升級路徑型別所需的輸入引數。

Planning

Distribution

Activation

Workflow Name *

ASR9K_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Pre Check Templates

Post Check Templates

Select option(s)

asr9k_distribution_precheck

asr9k_distribution_postcheck

Pre/Post Workflow

Previous

Next

Image Distribution部分 — 單步升級

Planning

Distribution

Activation

Workflow Name *

ASR9K_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Pre Check Templates

Post Check Templates

Select option(s)

Select option(s)

Select option(s)

Pre/Post Workflow

Pre check Workflow *

Post check Workflow *

OS_Upgrade_Precheck_PostCheckExample

OS_Upgrade_Precheck_PostCheckExample

Use latest workflow

Use latest workflow

Workflow Version *

Workflow Version *

Select option

Select option

Previous

Next

Image Distribution Section — 啟用pre/post工作流程的單步升級

Planning

Distribution

Activation

7.6.2 to 7.7.2

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asrk_distribution_precheck

Post Check Templates

asrk_distribution_postcheck

Pre/Post Workflow

Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asrk_distribution_precheck

Post Check Templates

asrk_distribution_postcheck

Pre/Post Workflow

Previous

Next

配送部分 — 多步驟升級

Planning

Distribution

Activation

7.6.2 to 7.7.2

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

Select option(s)

Post Check Templates

Select option(s)

Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

Use latest workflow

Workflow Version *

Select option

Post check Workflow *

Select option

Workflow Version *

Select option

Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

Select option(s)

Post Check Templates

Select option(s)

Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

Use latest workflow

Workflow Version *

Select option

配送部分 — 多步驟升級

Planning

Distribution

Activation

7.6.2 to 7.7.2

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asrk_distribution_precheck

Post Check Templates

asrk_distribution_postcheck

Pre/Post Workflow

Use the same properties for all the below upgrade paths

7.7.2 to 7.7.2[Bridge SMUs]

Workflow Name *

ASRK_Device_SW_Distribution

Use latest workflow

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asrk_distribution_precheck

Post Check Templates

asrk_distribution_postcheck

Pre/Post Workflow

7.7.2[Bridge SMUs] to 7.8.2

Previous

Next

分佈部分 — 網橋SMU升級

1. 配置與影象分發相關的引數。
2. 下表提供了每個欄位的簡要說明。

欄位	說明
workflow 名稱	適用的分發 workflow
使用最新 workflow	選擇所選 workflow 的最新版本
workflow 版本	定製 workflow 版本；僅當未選中「使用最新 workflow」復選框時，才能選擇此選項
	在兩個階段（即預檢查和後檢查）中執行的流程模板
前/後通用模板	附註：檢查僅特定於分佈里程碑。
	有關詳細資訊，請參閱 流程模板
前/後 workflow 切換	允許使用者選擇在分發里程碑內執行檢查前或檢查後 workflow。開啟切換時，只能配置檢查前或檢查後 workflow。包括在預檢查階段單獨執行的命令。
預檢 workflow	附註：這些檢查特定於分佈里程碑。
	後檢查 workflow 包括在後檢查階段唯一執行的命令。
後檢查 workflow	附註：這些檢查特定於分佈里程碑。
	包含排他性預檢查命令的流程模板；模板僅在檢查前階段執行。
預檢模板	附註：檢查僅特定於分佈里程碑。
	包含排他性檢查後命令的流程模板；模板僅在檢查後階段執行。
檢查後模板	附註：檢查僅特定於分佈里程碑。
	在多選升級中，所有升級路徑均應用一致的屬性。
對下列所有升級路徑使用相同的屬性	附註：如果選中該選項，則在多選升級中，相同屬性將應用於所有升級路徑。



附註： workflow 或流程模板必須正確標籤有 OS Upgrade Next-Gen 標籤。

3. 按一下下一步以繼續進入啟用部分。

啟用

欄位	說明
工作流名稱	適用的啟用工作流
使用最新工作流	選擇所選工作流的最新版本
工作流版本	定製工作流程版本；僅當未選中「使用最新工作流」覈取方塊時才能選擇在兩個階段（即預檢查和後檢查）中執行的流程模板。
前/後通用模板	附註：檢查僅特定於啟用里程碑。 有關詳細資訊，請參閱 流程模板 包含排他性預檢查命令的流程模板；模板僅在檢查前階段執行。
預檢模板	附註：檢查僅特定於啟用里程碑。 包含排他性檢查後命令的流程模板；模板僅在檢查後階段執行。
過帳檢查模板	附註：檢查僅特定於啟用里程碑。
有效的事前/事後差異	選擇忽略差異的流程模板。 附註：檢查僅特定於啟用里程碑。 適用的回滾工作流。
回滾工作流	附註：如果在多選升級中選擇了具有回滾工作流的升級路徑之一，則預設情況下會選擇具有回滾工作流的其它所有升級步驟。 此自定義預檢查工作流程包含特定命令，可以選擇和檢視這些命令的執行結果。
預檢工作流程	。只在預檢查階段進行。 附註：這些檢查特定於啟用里程碑。 此自定義檢查後工作流程包含特定命令，可以選擇和檢視這些命令的執行結果。
後檢查工作流	。僅在檢查後階段執行。 附註：這些檢查特定於啟用里程碑。
對下列所有升級路徑使用相同的屬性	在多選升級中，所有升級路徑均應用一致的屬性。 附註：如果選中該選項，則在多選升級中，相同屬性將應用於所有升級路徑。

 附註：應該注意以下幾點：

- 必須在NSO中配置Nexus裝置所需的公鑰演算法。
- 配置bgp、bfd和hsrp的功能以在Nexus裝置中執行檢查前和檢查後模板。

3. 按一下「Create」。將顯示欄位的摘要。

Summary

Name: Single step upgrade

Description: This upgrade policy for ansible

Max Batch Count: 5

Default Policy: No

Ansible

NCS-540

Planning Distribution Activation

Backup Details

Submit

摘要 — 單步升級策略

Summary

Name: Multi step upgrade

Description: This upgrade policy for ansible

Max Batch Count: 5

Default Policy: No

Ansible

NCS-540

Planning Distribution Activation

Backup Details

Upgrade Paths

Submit

摘要 — 多步驟升級策略

- 驗證欄位的摘要並點選Submit。系統將顯示進度通知，然後顯示確認消息。成功建立策略後，該頁面上將顯示策略。

可以根據需要為其他裝置型號建立其他升級策略。

編輯升級策略

7 Policies

CONTROLLER TYPES

- 2 - DNAC
- 1 - NSO
- 1 - Direct-To-Device
- 1 - vManage
- 2 - NDFC

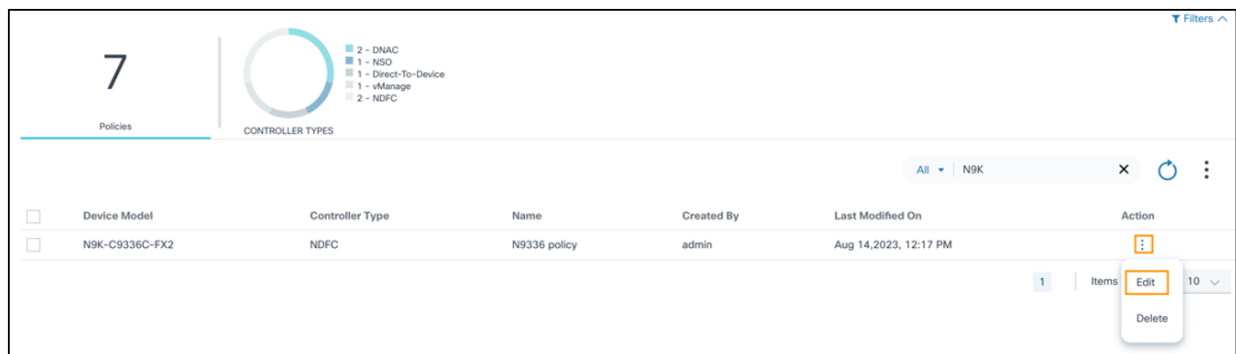
All N9K

Device Model	Controller Type	Name	Created By	Last Modified On	Action
N9K-C9336C-FX2	NDFC	N9336 policy	admin	Aug 14, 2023, 12:17 PM	

1 Items per page 10

升級策略的搜尋結果

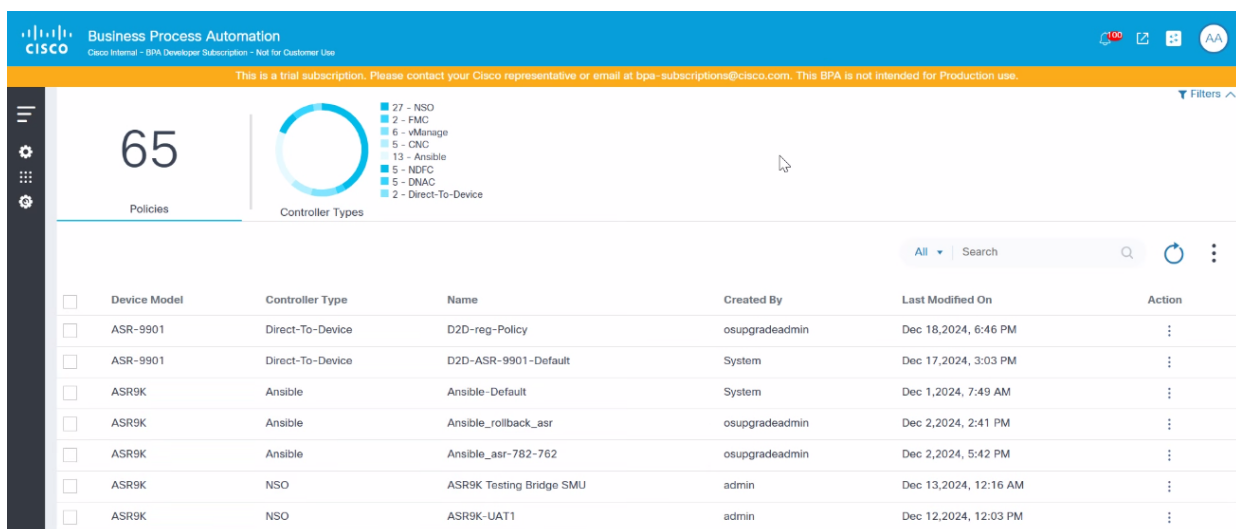
- 在Upgrade Policy頁面中，使用Search欄位找到所需的策略。



編輯升級策略

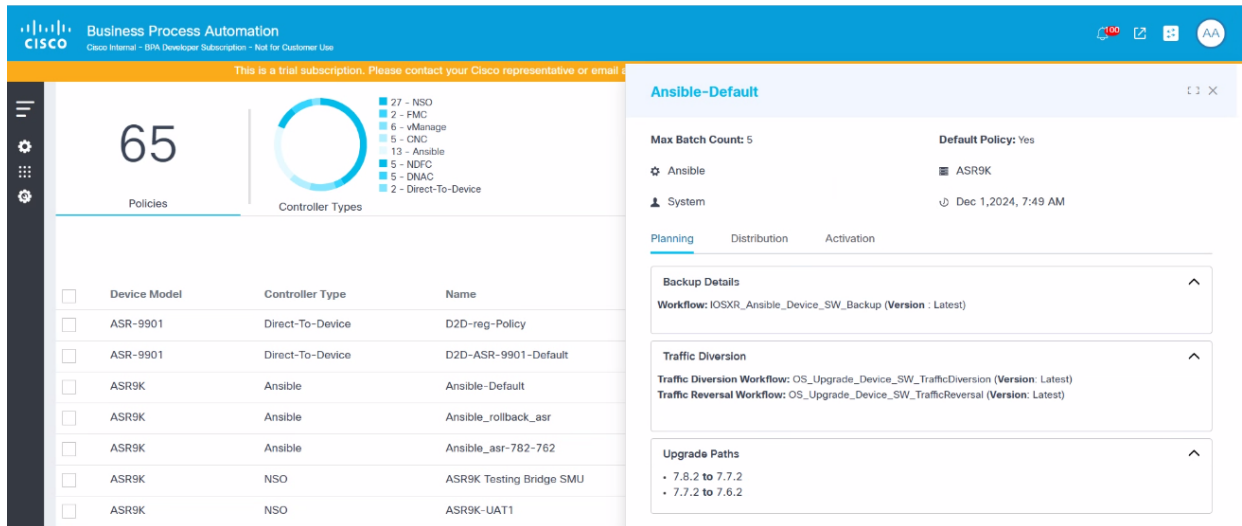
2. 在策略的Action列中，選擇More Options圖示> Edit。
3. 更新相關欄位，然後點選更新。系統將顯示變更摘要。
4. 驗證更改摘要並點選提交。系統隨即會顯示進度通知，然後是一條確認消息。

檢視升級策略



升級策略

1. 在Upgrade Policy頁面中，選擇所需的升級策略行。此時將開啟策略的詳細資訊檢視。

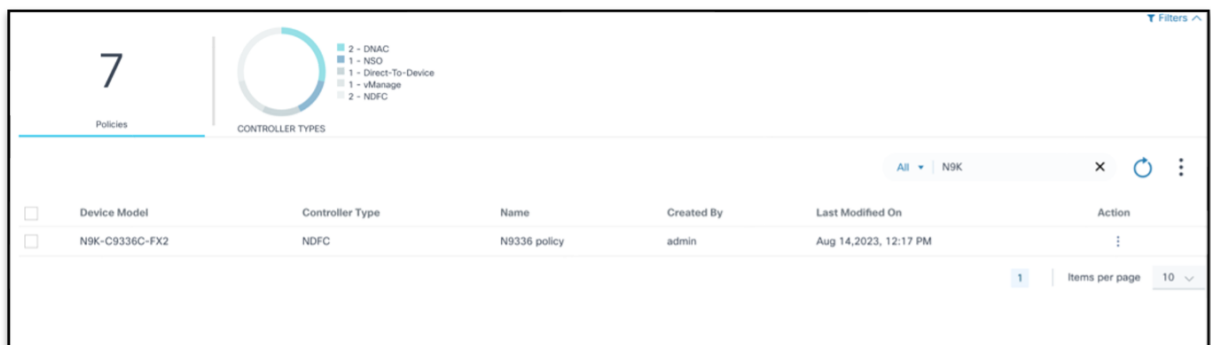


升級策略詳細資訊檢視

刪除升級策略

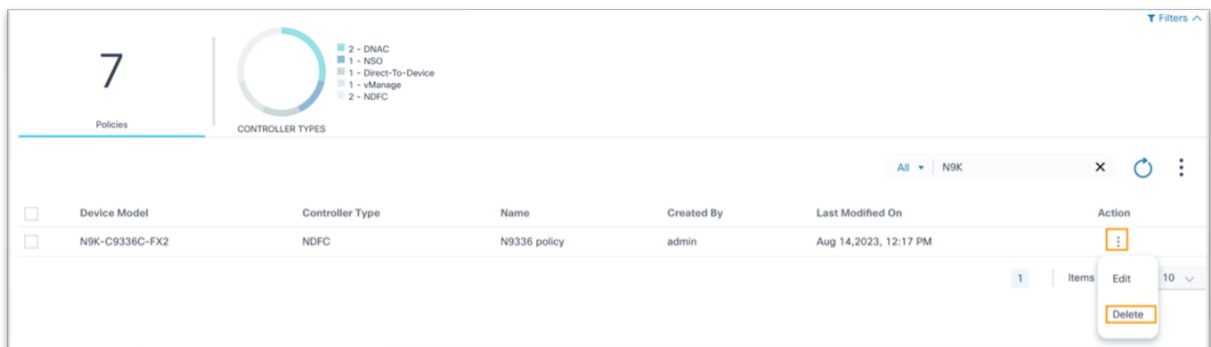


附註：無法刪除預設策略，但使用者可以編輯流程模板和工作流。



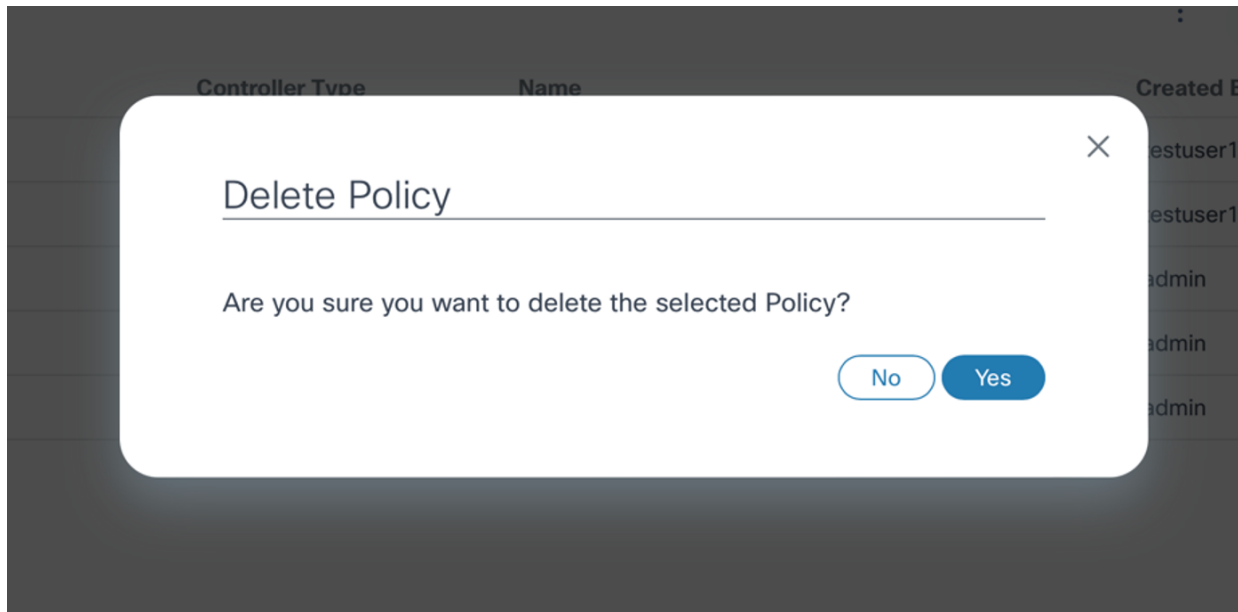
升級策略

1. 在Upgrade Policies頁面中，使用Search欄位找到所需的策**。



刪除升級策略

2. 在策略的Action列中，選擇More Options > Delete。此時將開啟確認視窗



刪除策略確認

3. 按一下「Yes」。

控制對升級策略的訪問

此功能為升級策略提供訪問控制，限制未經授權的使用者更新作業系統升級應用程式中定義的策略。管理員可以通過定義具有可訪問策略的資源組來限制訪問。

要建立資源組，請執行以下操作：

1. 導覽至Settings > Resource Groups。
2. 使用非管理員使用者可以訪問的策略建立資源組。現在，屬於此使用者組的非管理員使用者只能訪問此資源組中可用的策略。
3. 建立訪問策略以將資源組與使用者組相關聯，

如需詳細資訊，請參閱[存取控制](#)。



附註：應該注意以下幾點。

- 使用者可能會選擇不正確的工作流程進行分發和啟用，從而導致意外行為。使用者負責正確對映工作流程並驗證重要事件（如分發、啟用、回滾和裝置模型）的適用性。
- 工作流和流程模板必須與OS Upgrade Next-Gen標籤進行對映，以便它們在建立或更新策略時可供選擇。

- 無法刪除系統使用者建立的預設OOB策略，但使用者可以編輯流程模板和工作流。

升級作業

使用升級作業應用程式管理軟體升級，該應用程式由一個或多個批次組成，每個批次具有一個或多個網路裝置。可在草稿模式下建立作業並儲存多次。升級只能在提交作業後開始，允許操作員提前計畫更改。

必要條件

- 預留的升級維護視窗
- 升級變更請求的預批准
- Config Backup and Restore服務必須已啟動並正在運行
- 計畫程式服務必須已啟動並正在運行
- 適用於外部系統（如票證系統）的BPA介面卡（如果有）必須裝入

檢視和管理升級作業

- 使用有權訪問升級作業的憑據登入到BPA。
- 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。



升級作業

Upgrade Job頁包含以下內容：



附註：預設情況下，將顯示10個作業。頁碼可用於導航到其他作業頁。

- Active Jobs和Archived Jobs切換，可用於在活動作業和歸檔作業之間切換
- 頂部顯示的分析部分提供以下內容：
 - 與作業關聯的作業和資產合計
 - 使用以下篩選器的階段圖表：
 - 草稿:作業處於草稿階段，尚未提交
 - Commit:作業已提交到所有必要的裝置、批次或計畫，直到達到計畫
 - 部署:已啟動一個或多個批的升級活動
 - 完成:屬於所有批的所有裝置的升級活動已完成
 - 控制器型別圖表：允許通過Cisco Catalyst Center、vManage、NSO、NDFC、直接到裝置、CNC、ANSIBLE和FMC控制器型別進行作業過濾
 - 具有以下篩選條件的「作業型別」圖表：
 - 分發:將映像從控制器暫存或複製到裝置的作業
 - 啟用:執行裝置軟體的啟用或升級的作業
 - 分發和啟用:同時執行裝置軟體的暫存、複製和啟用或升級的作業
- Search欄位，可用於跨所有後設資料執行常規搜尋，或按Job Name和Created By欄位執行
- Refresh圖示，可用於刷新作業摘要和清除Search欄位中的圖表篩選器或任何自定義搜尋
- 更多選項圖示，提供用於建立新升級作業和存檔或Delete選定作業的選項；使用者可以選擇或取消選擇全部
- 作業顯示為面板，提供以下資訊的快速檢視：
 - 如果有可用的任何使用者任務，則會顯示使用者任務圖示以及使用者任務數
 - 建立作業的使用者
 - 作業建立日期
 - 批和資產的數量
 - 控制器型別（例如Cisco Catalyst Center、vManage、NDFC、直接到裝置、CNC、ANSIBLE或FMC）
 - 目標版本
 - 適用的裝置型號
 - 作業階段（即草稿、提交、部署和完成）的里程碑檢視，每個里程碑都有一個顏色圖例：
 - 灰色:里程碑尚未開始
 - 藍色:里程碑正在進行
 - 紅色:里程碑問題
 - 綠色:里程碑已完成
 - 里程碑末尾顯示作業狀態的顏色圖例：
 - 綠色:作業已完成
 - 紅色:作業存在問題
 - 藍色:作業正在進行

要建立作業，請執行以下操作：



建立升級作業選項

1. 在升級作業頁面中，選擇更多選項圖示> 建立作業。將顯示Create Upgrade Job頁。

建立升級作業

2. 在名稱欄位中輸入作業名稱。
3. 選擇Controller Type (例如Cisco Catalyst Center、vManage、NDFC、直接到裝置、CNC、FMC、ANSIBLE或NSO)。
4. 選擇具有非一致性裝置的符合性策略。

 附註：只有至少執行一次且具有至少一個非一致性裝置的符合策略才可以從清單中獲得，從而自動標識在選擇策略後將要使用的適用的升級策略。

在「作業摘要」下的「建立作業」窗體的左側將顯示以下詳細資訊：

- 受影響的裝置型號

 附註：當所選一致性策略有多個關聯的裝置型號時，將顯示多個裝置型號。

- 目標版本

- 現有發行版本及其相應計數的聚合
- 允許的最大批數
- 不符合項資產總數

 附註：如果選定的一致性策略與多個裝置模型關聯，則它會顯示所有關聯模型的非一致性資產聚合。

- 用於新增批的選項

5. 選擇以下升級作業型別之一：

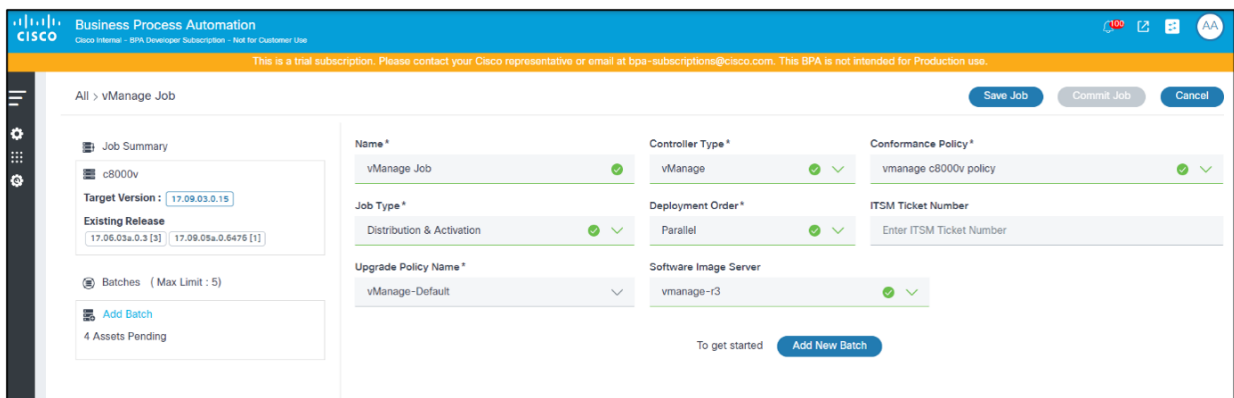
- 分發:當實際啟用之前暫存軟體映像時，僅分發作業很有用
- 啟用:僅啟用作業對於執行裝置升級很有幫助，因為裝置已通過僅分發作業完成分發
- 分發和啟用:在同一作業中同時進行映像分發或暫存和啟用，這在具有充足的維護視窗以涵蓋將映像複製到裝置和升級兩種情況的情形中很有用

6. 選擇升級順序。多個裝置在並行模式下同時處理，而裝置在順序模式下逐個處理。

 附註：可在並行模式下處理的最大裝置數取決於部署配置。所選升級順序適用於整個作業，但可以根據需要在特定批內覆蓋。

7. 在IT服務管理(ITSM)票證編號欄位中添加變更請求編號。
8. 選擇Upgrade Policy Name。根據控制器型別和符合策略裝置型號，僅顯示適用的升級策略；使用者可以選擇一個升級策略。如果軟體一致性策略有多個關聯的模型，則會顯示與每個模型關聯的所有相關升級策略。使用者應仔細選擇適用於所有型號的升級策略。
9. 選擇Software Image Server以指定使用哪個vManage映像儲存庫（例如，本地或遠端）。

 附註：此輸入僅適用於vManage控制器型別。



建立已填寫詳細資訊的升級作業（一致性策略具有一個模型）

建立已填寫詳細資訊的升級作業（一致性策略有多個模型）

10. 按一下儲存作業以儲存草稿，直到準備提交作業為止。

新增批處理並新增新批處理

11. 要新增批處理，請按一下新增批處理連結或新增新批處理。將打開「批創建」視窗。

批處理建立

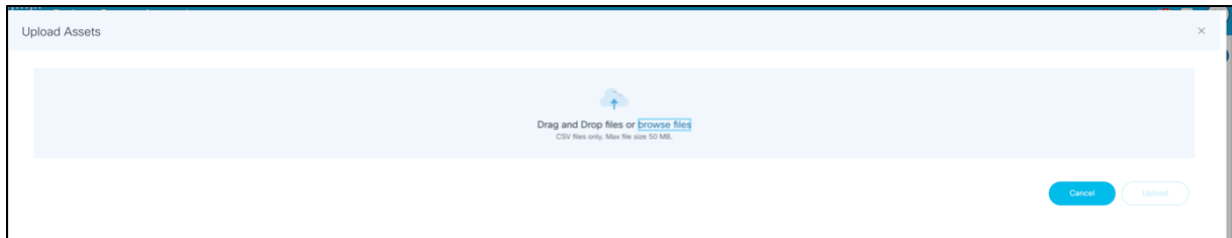
12. 輸入相關批名並選擇部署訂單。

附註：此處選擇的升級型別優先於「作業建立」頁面上所選的型別

13. 選擇Software Image Server以指定使用哪個vManage資源庫（例如，本地或遠端）。

 附註：此欄位僅適用於vManage控制器型別。此處選擇的軟體映像服務器優先於在「作業建立」頁面上選擇的軟件映像伺服器

14. 將資產新增到批中。可以通過兩種方式將資產新增到批中：



上傳資產

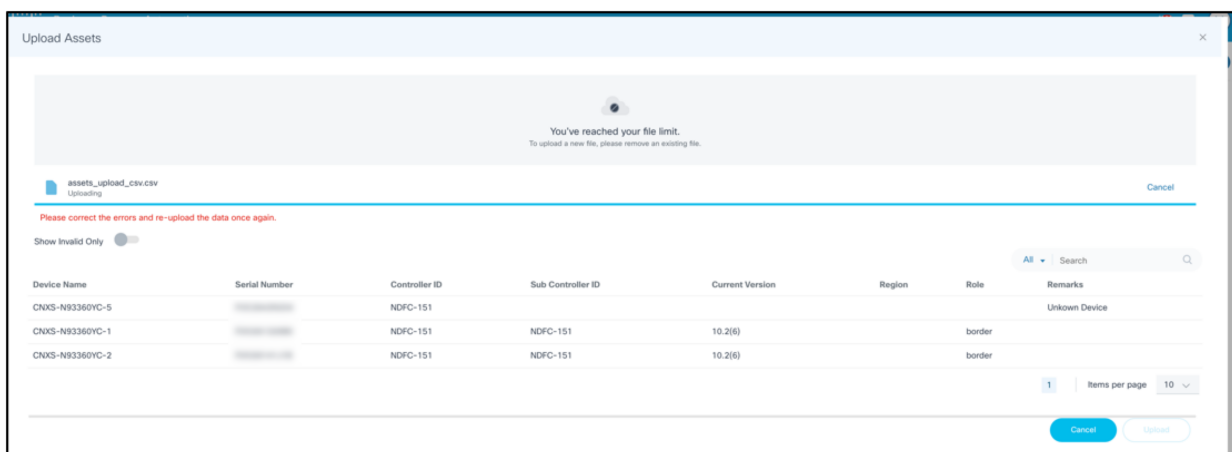
選項 1:

- 按一下「Upload Assets」。Upload Assets視窗開啟。
- 選擇要上傳的.csv檔案。

 附註：.csv檔案必須具有以下詳細資訊：

- 裝置名稱：裝置或資產的名稱
- 序列號：裝置的序列號
- 控制器ID:管理裝置的控制器名稱
- 子控制器ID:管理裝置的子控制器ID的名稱

- 按一下「Upload」。將驗證.csv檔案資料並顯示有效資料和無效資料。Show Invalid Only切換可用於從上載的資產詳細資訊中篩選無效裝置。



通過CSV檔案上載的示例資產

- d. 如果上傳的檔案中存在錯誤，請更正錯誤並重新上傳。



附註：只有所有上傳的裝置都有效時，使用者才能繼續選擇資產。

新增批 — 所選資產

選項 2:

- a. 按一下「Add Assets」。將開啟資產選擇視窗。



附註：上傳資產 和Add Assets不能同時使用。

- b. 僅對於FMC控制器型別，請選擇用於執行升級的控制節點或獨立節點。



附註：不允許資料裝置在升級作業中，因為資料節點的升級由其控制節點處理。

裝置選擇

c. 選擇要與當前批次一起包含的相應裝置。

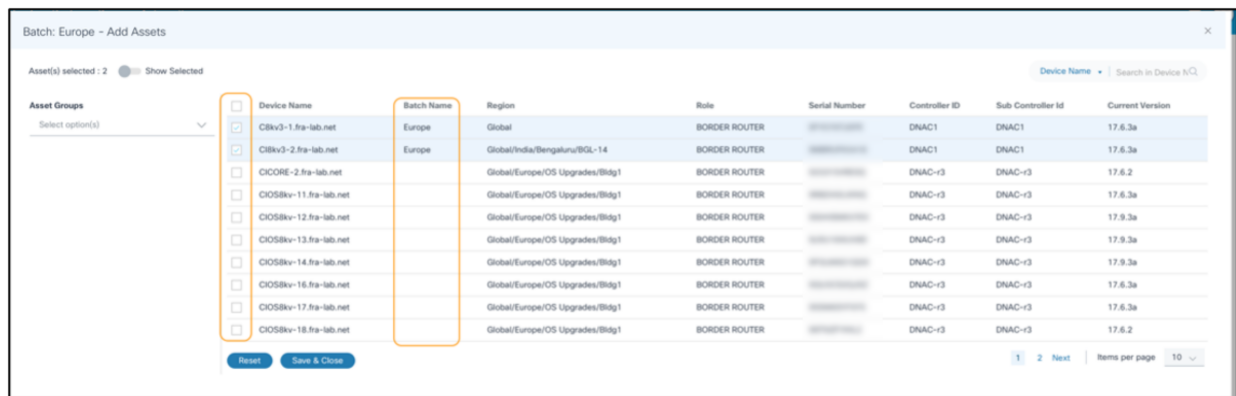
Search篩選器可用於根據不同的屬性篩選裝置，並且可以通過選中Device Name列標題中的覈取方塊來批次選擇符合篩選條件的所有裝置。使用者還可以選擇按資產組進行篩選。

可以啟用Show Selected切換以僅檢視所選資產。

 附註：啟用Show Selected切換後，將禁用Asset Groups篩選器。

d. 按一下「Save and Close」。

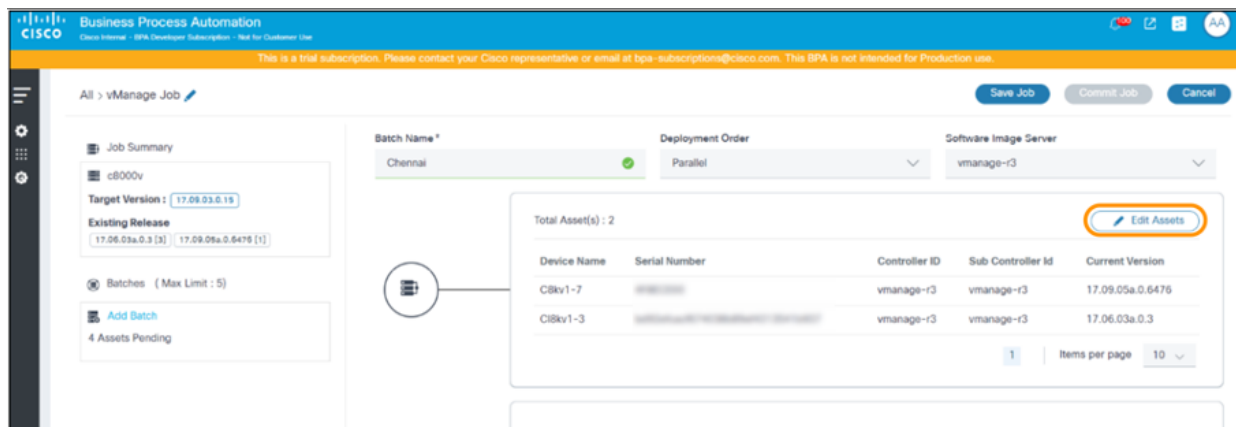
按一下重置將放棄選擇並保留資產選擇的原始狀態。



Device Name	Batch Name	Region	Role	Serial Number	Controller ID	Sub Controller ID	Current Version
CBkv3-1.fra-lab.net	Europe	Global	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
CBkv3-2.fra-lab.net	Europe	Global/India/Bengaluru/SGU-14	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
OCORE-2.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.2
OIOSBkr-11.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
OIOSBkr-12.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
OIOSBkr-13.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
OIOSBkr-14.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
OIOSBkr-16.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
OIOSBkr-17.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
OIOSBkr-18.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.2

重設

e. 如果資產選擇需要修改，請按一下編輯資產。



Device Name	Serial Number	Controller ID	Sub Controller ID	Current Version
CBkv1-7		vmanage-r3	vmanage-r3	17.09.05a.0.6476
CBkv1-3		vmanage-r3	vmanage-r3	17.06.03a.0.3

批次編輯資產

f. 選擇或清除資產以進行必要的更改，然後按一下儲存並關閉。在編輯批資產時，可以使用複選標籤和「批名」列中顯示的批名標識當前作為不同任務和批的一部分的所選資產。

升級作業計畫程式

- 從日期選取器中選擇日期，並從時間選取器中選擇時間，以計畫觸發為當前批選擇的升級型別的時間。

附註：所選作業型別會更改可用計畫的型別。

可能的方案如下：

作業型別	立即分發切換	計畫日期和時間	分發詳細資訊
分佈	預設情況下禁用	Active (作用中)	在指定的計畫日期和時間分發
分佈	已啟用	已停用	作業提交後進行分發
啟用	不適用	Active (作用中)	啟用在指定的日期和時間進行
發佈與啟用	預設情況下禁用	Active (作用中)	在指定的日期和時間進行分發和啟用
發佈與啟用	已啟用	Active (作用中)	分發將在指定的計畫日期和時間執行作業提交和啟用後觸發

CISCO Business Process Automation

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > vManage Upgrade

Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.06.02.0.2788

Existing Release: 17.06.02a.0.2 [3] 17.09.03.0.15 [2] 17.09.05a.0.64/6 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name* Enter Batch Name

Deployment Order Parallel

Software Image Server Select option

Select Assets Upload Assets Add Asset

Distribute Now

September 2024

Start Time: Image Distribution

Create Batch

分配作業型別計畫選項

CISCO Business Process Automation

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > vManage Upgrade

Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.06.02.0.2788

Existing Release: 17.06.02a.0.2 [3] 17.09.03.0.15 [2] 17.09.05a.0.64/6 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name* Enter Batch Name

Deployment Order Parallel

Software Image Server Select option

Select Assets Upload Assets Add Asset

Distribute Now

September 2024

Start Time: Image Activation

Create Batch

啟用作業型別計畫選項

Distribute Now & Activate Later

August 2023

Start Time: 13:10

Create Batch

分發和啟用作業型別計畫選項

Business Process Automation

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > vManage Upgrade

Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.06.02.0.2786

Existing Release: 17.06.03a.0.3 [2] 17.09.03.0.15 [2] 17.09.05a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name*

Enter Batch Name

Deployment Order: Parallel

Software Image Server: Select option

Select Assets

Upload Assets Add Asset

Distribute Now & Activate Later

September 2024

Start Time: Image Activation

Create Batch

啟用立即分發和稍後啟用切換的分發和啟用作業型別計畫選項

附註：應註明以下清單。

- 當計畫多個批次時，在兩個批次之間提供時間間隔，以便避免系統過載。如果多個批重疊，請考慮將其新增到單個批中。
- 啟用Distribute Now和Activate Later切換後，在作業提交時間和啟用計畫之間提供時間間隔。如果不是，啟用工作流可能會建立需要手動干預的使用者任務（即，使用者必須等到分發完成後再重試）。

16. 按一下Create Batch。可以在頁面左側檢視批處理。

Business Process Automation

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > vManage Job

Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.09.03.0.15

Existing Release: 17.06.03a.0.3 [3] 17.09.05a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

4 Assets Pending

Batch Name*

Chennai

Deployment Order: Parallel

Software Image Server: vmanage-r3

Total Asset(s): 2

Edit Assets

Device Name	Serial Number	Controller ID	Sub Controller Id	Current Version
C8kv1-7		vmanage-r3	vmanage-r3	17.09.05a.0.6476
C8kv1-3		vmanage-r3	vmanage-r3	17.06.03a.0.3

1 Items per page 10

Distribute Now & Activate Later

August 2024

建立作業 — 提交作業

根據需要建立多個批次。作業可以處於「草稿」狀態，直到所有必需資訊都可用為止。

 附註：按一下儲存作業以儲存草稿，從而避免丟失作業資料。

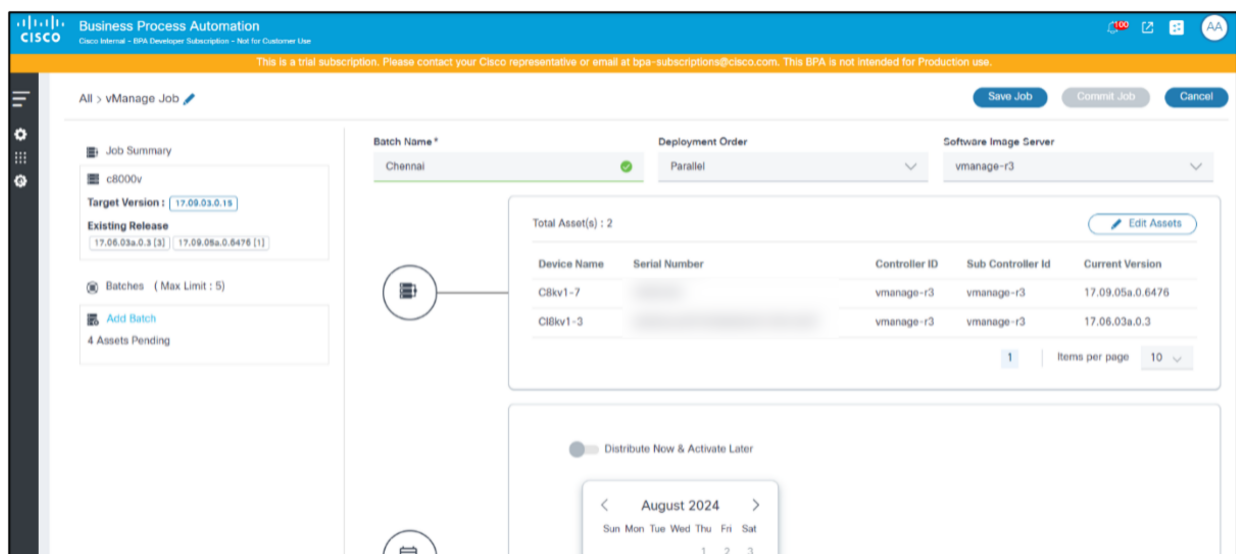
17. 按一下Commit Job以完成作業建立。當為任何批處理觸發排程時，作業將轉換為「部署」狀態。

 附註：可在「升級策略」頁面上擴展或更新最大批數的閾值。

編輯作業中的批處理

 附註：僅當作業處於「草稿」階段時，才能更新批處理。

1. 從左側面板中選擇所需的批處理。



編輯資產

2. 按一下Edit Assets。
3. 通過選擇或清除新增資產或載入資產中的資產，或通過更改日期或開始時間修改批計畫，進行必要的更改。
4. 按一下Update Batch。

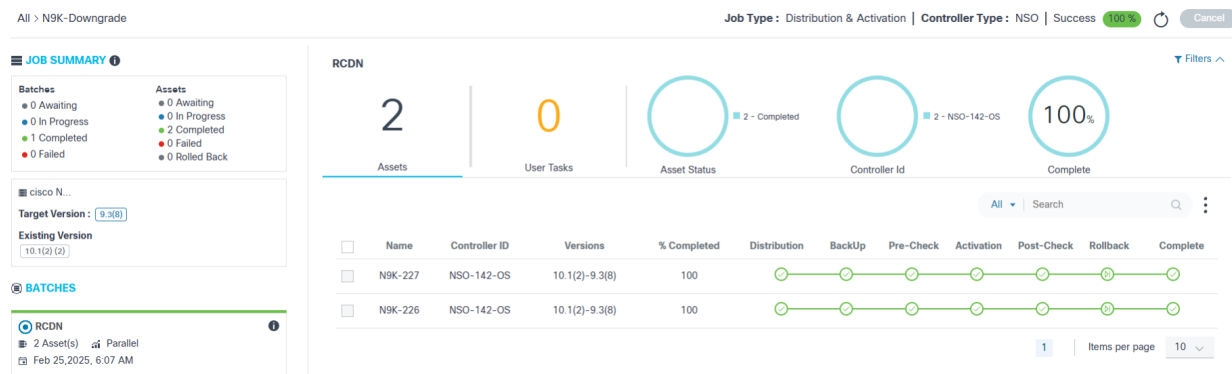
升級作業執行和進度監控

1. 使用有權訪問升級作業的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。

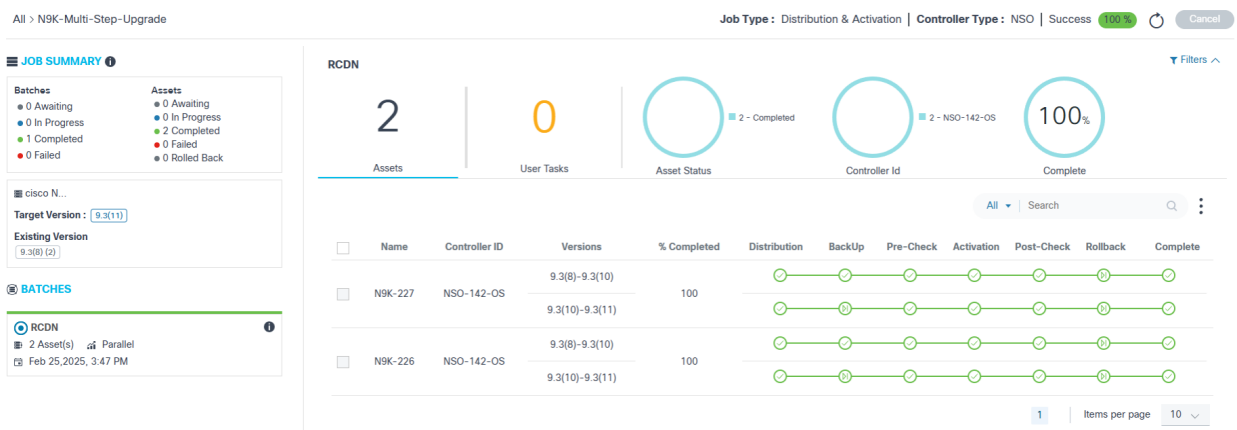


升級作業

3. 將Search篩選器與可用的圖表篩選器結合使用，可快速篩選作業。
4. 按一下所需的作業。將顯示作業摘要頁。



一步升級



多步驟升級

左側面板提供以下資訊：

All > N9K-Multi-Step-Upgrade

☰ JOB SUMMARY ⓘ

Batches

- 0 Awaiting
- 0 In Progress
- 1 Completed
- 0 Failed

Assets

- 0 Awaiting
- 0 In Progress
- 2 Completed
- 0 Failed
- 0 Rolled Back

作業摘要

- 批次和相應資產的快速彙總

☰ c8000v

Target Version : 17.09.01a.0.240

Existing Version

17.09.03.0.15 (1)

符合性策略詳細資訊 (如果策略有一個模型)



 N9K-C93...,N9K-C93...

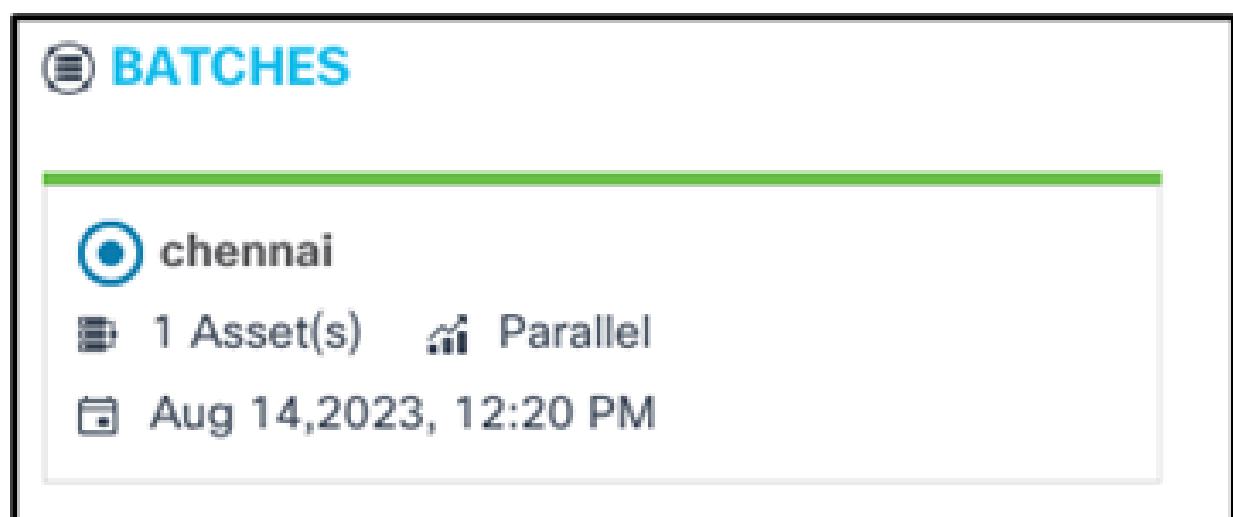
Target Version : 10.2.5

Existing Release

9.3(7) [4]

符合性策略詳細資訊 (如果策略有多個模型)

- 作業的受影響裝置型號、目標軟體版本和現有版本版本
- 作為此作業一部分的批處理清單



 **BATCHES**

 **chennai**

 1 Asset(s)  Parallel

 Aug 14,2023, 12:20 PM

批次詳細資訊

- 批次詳細資訊：
 - 灰色頂部邊框表示批處理正在等待計畫
 - 藍色頂部邊框表示批處理部署正在進行中
 - 綠色頂部邊框表示批處理部署已完成

「作業摘要」頁面的頂部顯示以下信息：

All > vmanage_1_2_e2e Job Type : Distribution & Activation | Controller Type : vManage | Success 100 %  

作業頂部摘要

- 當前作業的breadcrumb導航 (例如 , All > vmanage_1_2_e2e) 。 All選項切換到「作業」控

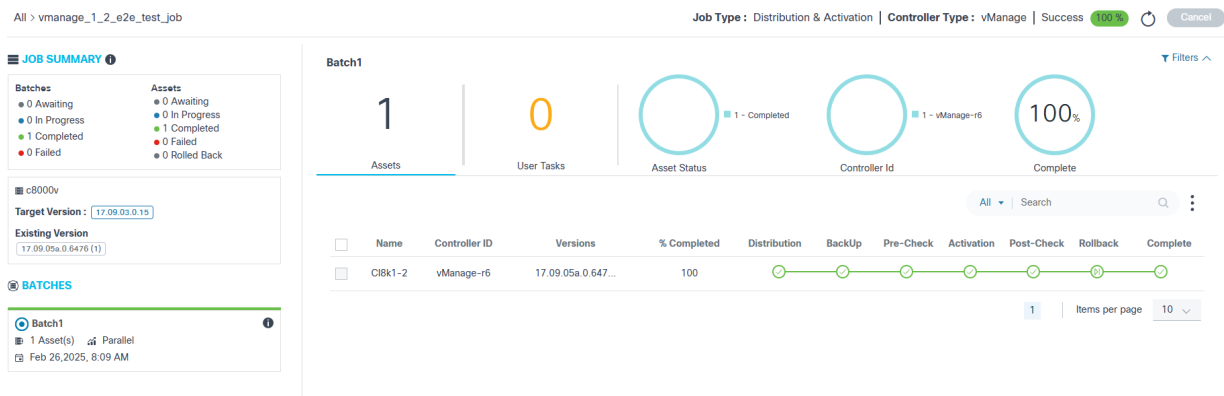
制面板

- 作業型別
- 控制器型別
- 完成百分比的作業狀態：
 - 成功:升級作業成功
 - 失敗:升級作業由於某種原因失敗
 - 進行中:升級作業正在進行



附註：即使達到一個批的計畫，作業狀態也移至進行中

- 等待:作業已提交，但正在等待達到一個或多個批處理計畫



作業摘要

Job Summary頁上提供了以下選項：

- Refresh圖示允許使用者按需檢索更新
- 「取消」用於取消「草稿」和「提交」階段中的作業，除非達到任何批的計畫
- 啟用會在「草稿」狀態下使用與以前完成的作業相同的批次和資產建立新的啟用作業
 - 僅當作業型別為「分配」且已成功完成時，才能啟用
 - 如果已建立啟用作業並按一下Activate，則會顯示一條消息，顯示先前建立的作業的狀態，並提供重定向已建立的作業的選項；在新建立的作業中，使用者可以選擇編輯或刪除批處理或資產，但作業型別、控制器型別和一致性策略不可編輯。
- 分析部分下方顯示分頁顯示的資產清單
- Search欄位允許對欄位進行一般性和特定欄位搜尋，例如：
 - 裝置名稱
 - 控制器ID
 - 序列號

Name	Controller ID	Sub Controller ID	Serial Number	Distribution	BackUp	Pre-Check	Activation	Post-Check	Download
NCS540-75	CNC-211			✓	✓	✓	✓	✓	
NCS540-36	CNC-211			✓	✓	✓	✓	✓	

下載批處理報告

- 通過選擇更多選項圖示> 下載來下載批處理級報告的選項；此報告包含批級別詳細資訊以及裝置詳細資訊

	Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
☐	CNXS-N93360YC-1...	NDFC	10.2(5)-10.3.5	100	✓	✓	✓	✓	✓	✓	✓

排序 — 單步升級

	Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
☐	N9K-227	NSO-142-OS	9.3(8)-9.3(10)	100	✓	✓	✓	✓	✓	✓	✓
☐			9.3(10)-9.3(11)		✓	✓	✓	✓	✓	✓	✓

排序 — 多步驟升級

JOB SUMMARY

1

Batches

● 0 Awaiting

● 0 In Progress

● 1 Completed

● 0 Failed

Assets

● 0 Awaiting

● 0 In Progress

● 1 Completed

● 0 Failed

● 0 Rolled Back

ASR9K

Target Version : 7.7.2

Existing Version

7.6.2 (1)

BATCHES

chennai

1 Asset(s) Parallel

Feb 19, 2025, 4:48 PM

chennai

1

Assets

0

User Tasks

1 - Completed

Asset Status

1 - NSO-142

Controller Id

Complete

All

Search

	Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
☐			7.6.2-7.6.2[Bri...		✓	⏸	✓	✓	✓	✓	✓
☐	ASR9K-79	NSO-142	7.6.2[Bridge SM...	100	✓	⏸	✓	✓	✓	✓	✓

7.6.2[Bridge SMUs] - 7.7.2

1

Items per page

10

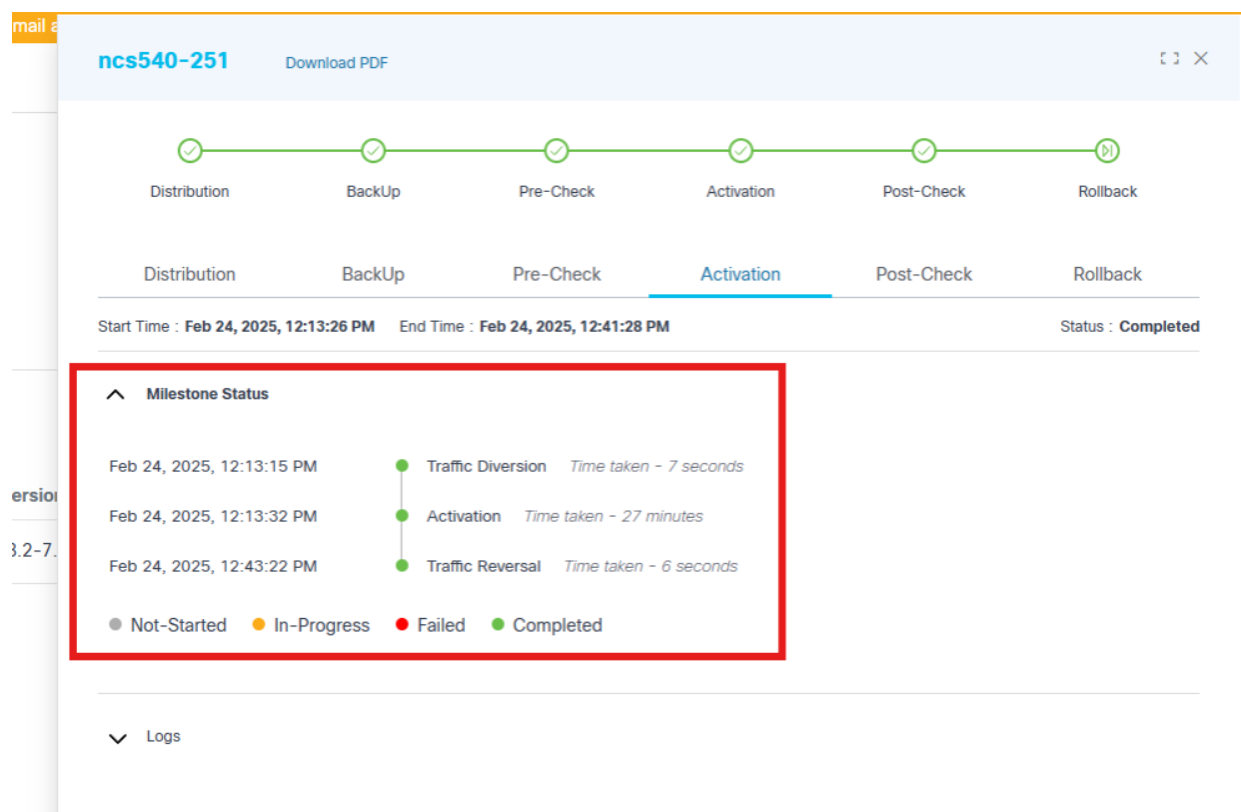
排序 — 網橋SMU升級

- 可通過按一下列名稱來進行排序
- 每台裝置顯示以下升級里程碑以及名稱、控制器ID、版本和% Completed:
 - 分佈
 - 備份
 - 預檢查

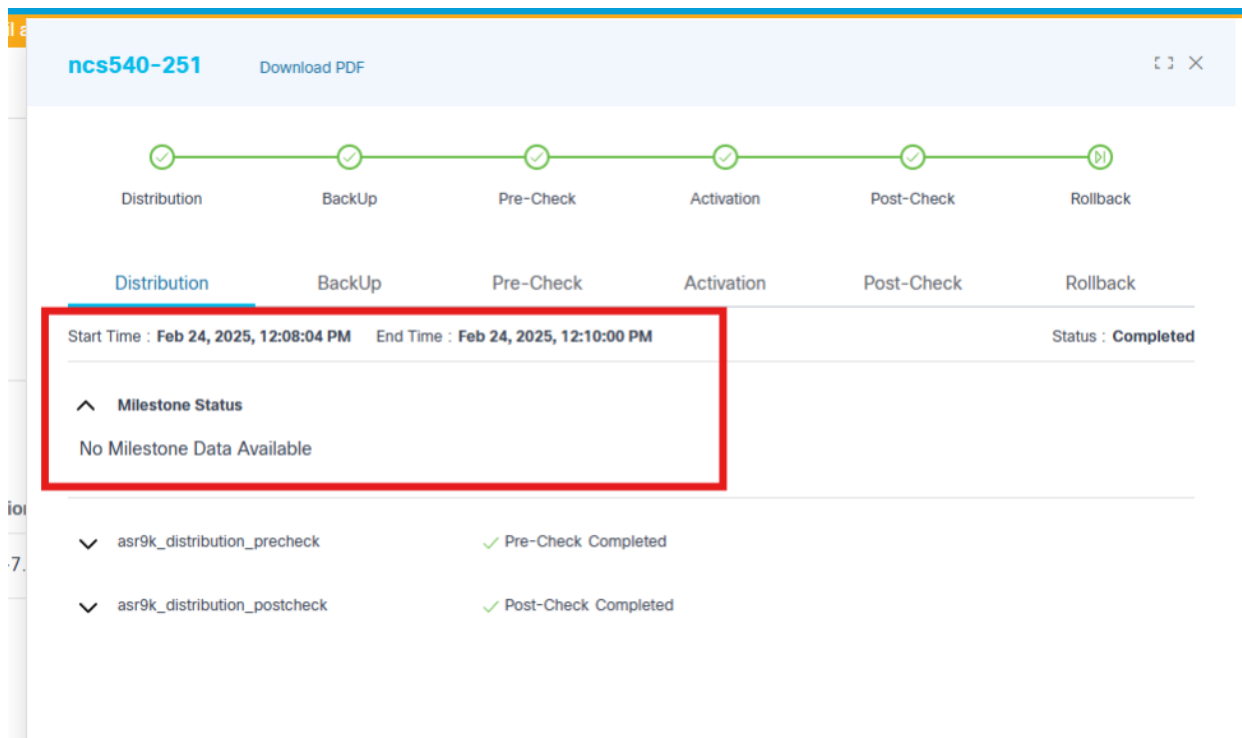
- Traffic-Distribution
- 啟用
- 後檢查
- Traffic-Reversal
- 回滾
- 完成

 附註：已完成百分比：根據裝置完成的里程碑數量顯示進度。系統會合計批中的所有裝置層完成百分比，以計算批完成百分比。然後，彙總所有批完成百分比以計算任務層完成百分比。

子里程碑（也稱為定製里程碑）是在新增時在標準里程碑下執行和檢視的中間重要步驟。有關新增自定義里程碑的詳細資訊，請參閱[BPA開發人員指南](#)。



子里程碑檢視（如果在標準里程碑名稱下新增子里程碑）



子里程碑檢視（如果未在標準里程碑名稱下新增子里程碑）



附註：里程碑因所選作業型別而異。TrafficReversal里程碑不可用於分發作業。

流量轉接和流量反轉將在啟用里程碑下移動。

• 里程碑顏色圖例，由以下內容組成：

- 灰色檢查:待定
- 藍色勾選:進行中
- 綠色標誌:已跳過
- 綠色勾選:Completed
- 橙色檢查:使用者任務
- Red Check:失敗

All > nso_multi_step_base

JOB SUMMARY

Batches	Assets
0 Awaiting	0 Awaiting
0 In Progress	0 In Progress
1 Completed	1 Completed
0 Failed	0 Failed
	0 Rolled Back

ASR9K

Target Version : 7.8.2

Existing Version : 7.8.2 (1)

BATCHES

Batch1	1 Asset(s)	Parallel	Feb 22, 2025, 7:56 AM
--------	------------	----------	-----------------------

Batch1

1

0

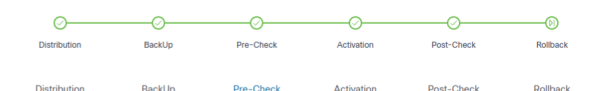
Assets

User Tasks

Name	Controller ID	Version
ASR9K-75	NSO-142-0s	7.7.2-7.8

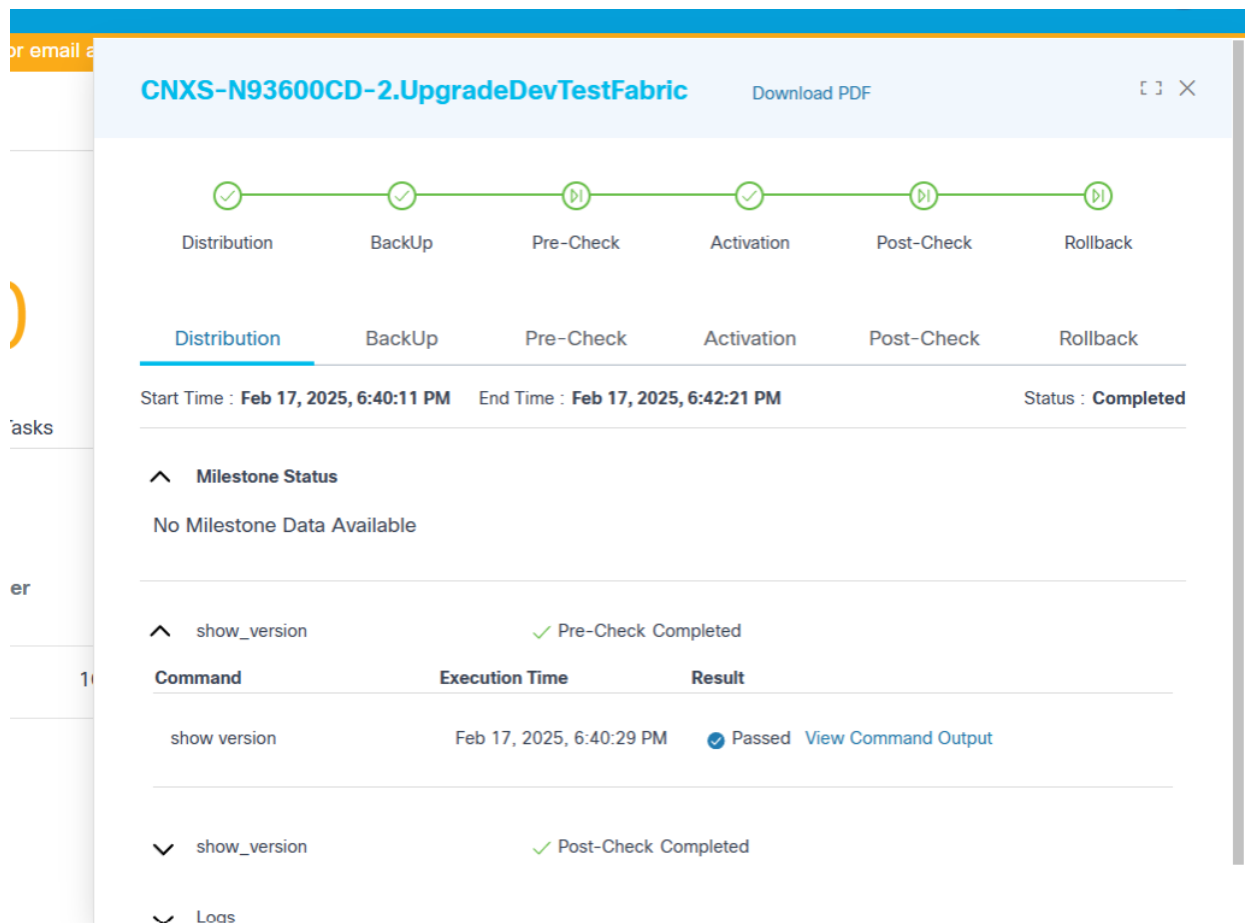
ASR9K-75

Download PDF



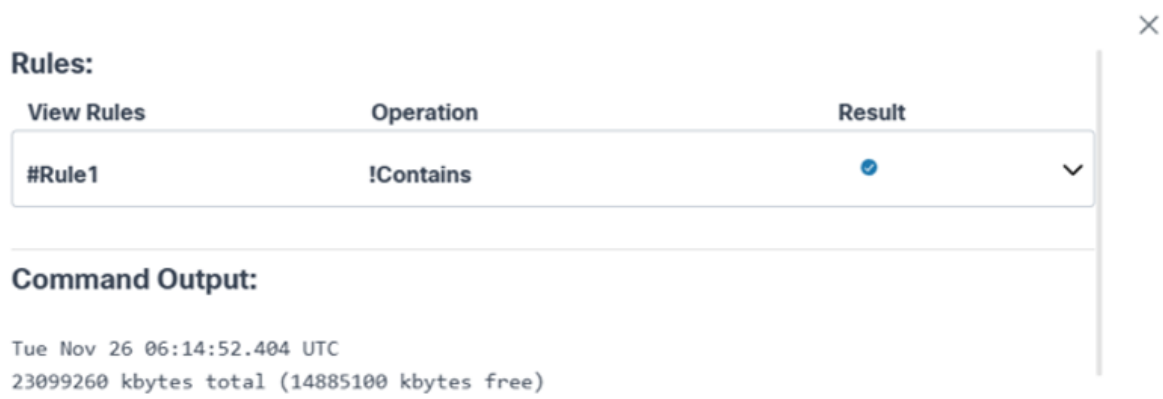
檢查前和檢查後里程碑檢視

對於執行檢查前或檢查後執行的里程碑，使用者可以檢視完整命令輸出以及各個流程模板中配置的所有命令的驗證規則及其狀態。



帶有預檢查命令輸出的分佈里程碑檢視

- 1. 要檢視命令輸出以及與檢查前和檢查後命令關聯的規則，請按一下檢視命令輸出連結。



檢查前和檢查後命令輸出及相關規則

- 2. 選擇Expand (展開) 圖示以檢視每個規則的完整詳細資訊。

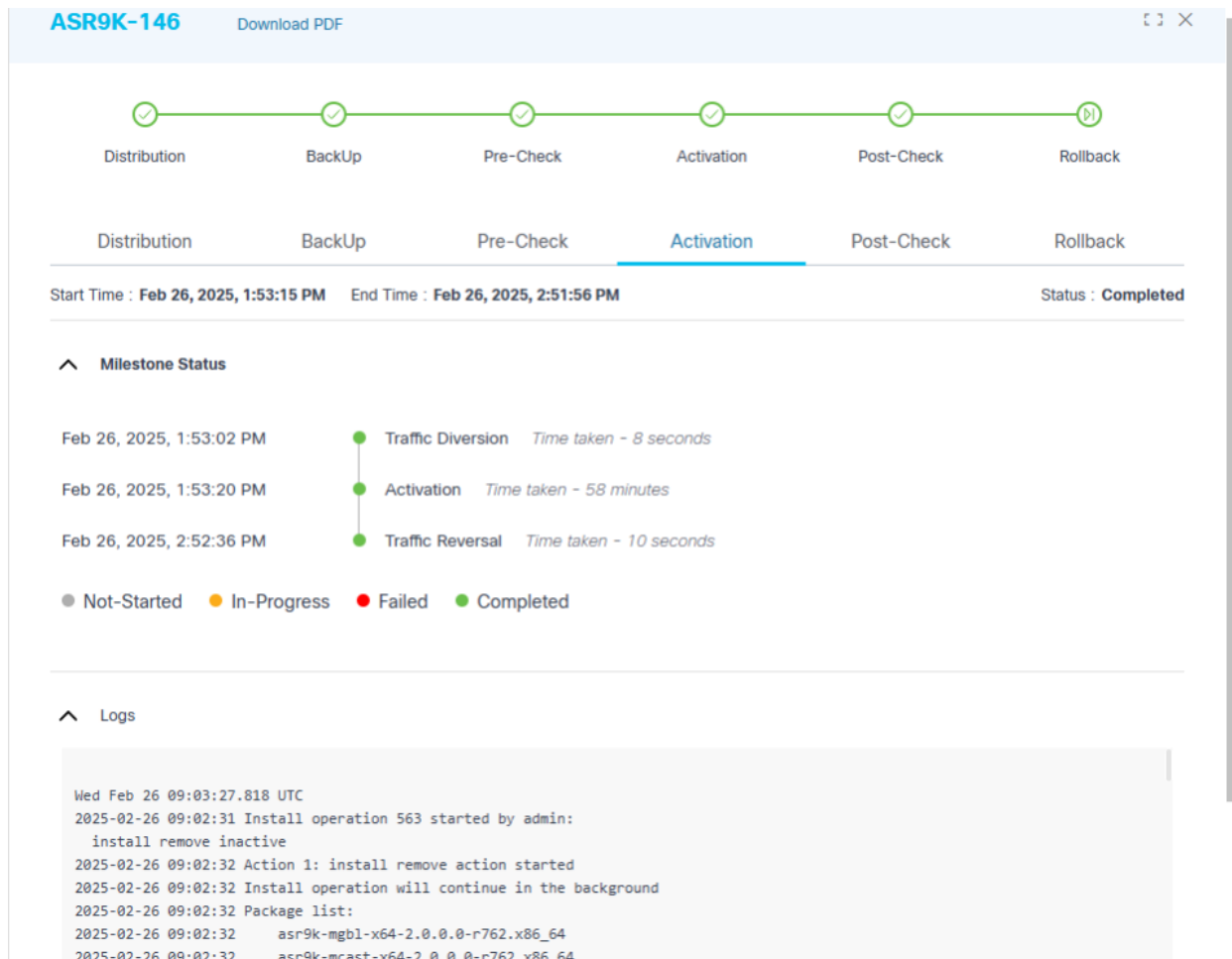
Rules:

View Rules	Operation	Result
#Rule1	!Contains	 ^
Rule:	Invalid input detected	

Command Output:

```
Tue Dec  3 20:19:26.594 UTC
disk_status_config minor 80
disk_status_config severe 90
disk_status_config critical 95
aaa admin-accounting enable false
aaa authentication users user admin
  uid      9000
  gid      100
  password
ssh_keydir /var/confd/homes/admin/.ssh
homedir    /var/confd/homes/admin
!
aaa authentication groups group aaa-r
  gid  100
  users %%__system_user__%%
!
```

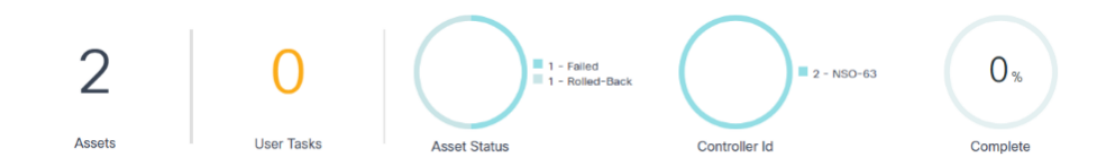
帶驗證規則的檢查前和檢查後命令輸出



使用即時日誌的啟用里程碑檢視

上圖提供了啟用里程碑的詳細資訊，包括即時日誌，以幫助監控特定裝置的軟體啟用進度。

當里程碑開始或完成時，按一下里程碑將顯示詳細資訊。



分析部分

作業摘要頁面頂部顯示的分析部分顯示與當前所選作業相關的以下資訊：

- 批名（例如，Asia）
- 篩選器^摺疊和展開分析部分
- 以下批詳細資訊按順序顯示：
 - 資產:資產總數
 - 使用者任務:等待操作使用者或管理員輸入的使用者任務總數
 - 資產狀態:根據批處理裝置的狀態對其進行篩選。已新增Rollback篩選器以幫助識別已成

功回滾的裝置。

- 控制器ID:篩選屬於所選控制器ID的批處理裝置
- 完成:整體批處理完成百分比

要處理任何使用者任務，請按一下使用者任務計數。此時將開啟「使用者任務詳細資訊」視窗，其中包含以下內容：

User Task Details			All ▾ Search 	
User Task Name	Created	Assignee		
CIOS8kv-18.fra-lab.net (98TNZFYIHL2)   View And Claim	Dec 8, 2023, 7:36:39 PM			
CIOS8kv-20.fra-lab.net (9PLCN4P91YG)   Cross launch	Dec 8, 2023, 7:34:19 PM			
CIOS8kv-17.fra-lab.net (95SM6SYF975)    View User Task UnClaim	Dec 8, 2023, 7:34:21 PM	admin		
			1	Items per page 10 ▾

使用者任務詳細資訊

- 與需要注意的各個裝置相對應的使用者任務清單
- 使用者任務選項的下列圖示：
 - 檢視和申請:檢視使用者任務詳細資訊
 - 交叉啟動:在標準UI中檢視BPA工作流任務
 - Unclaim:刪除使用者任務分配
 - 檢視使用者任務:檢視使用者任務詳細資訊

User Task

View Trace

Expand All

Collapse All

▼

connectionErrorMessageForm

Code

1005

Message

Error while executing task Device_GetInitialData_ServiceTask

Details

Following template(s) associated components having model differences: ("with_activation_checks")
["show route summary"] | reprogram | "show route (self summary)" | reprogram | "show health (self)" | reprogram | "show instance info" | reprogram | "verify_activation_checks" ("show show-thing")

Rollback

Retry All

Retry

Continue

Cancel

Close

使用者任務

使用者任務的檢視選項

- 根據任務的上下文顯示以下選項：
 - 重試:重新執行該任務
 - 全部重試:重新執行所有預先檢查和事後檢查
 - 繼續:繼續下一任務
 - 回滾:回滾到以前的版本；如果啟用或後檢查失敗，或者發現前/後檢查之間的差異無效，則此選項可用
 - 取消:取消當前作業
 - 關閉:關閉「用戶任務」視窗。
- 執行使用者任務（如果有），然後選擇刷新圖示以刷新使用者任務總數
- 批次完成百分比合計
- 按控制器ID過濾的可點選圖表



附註：控制器ID之前的數字表示由相應控制器管理的裝置總數。

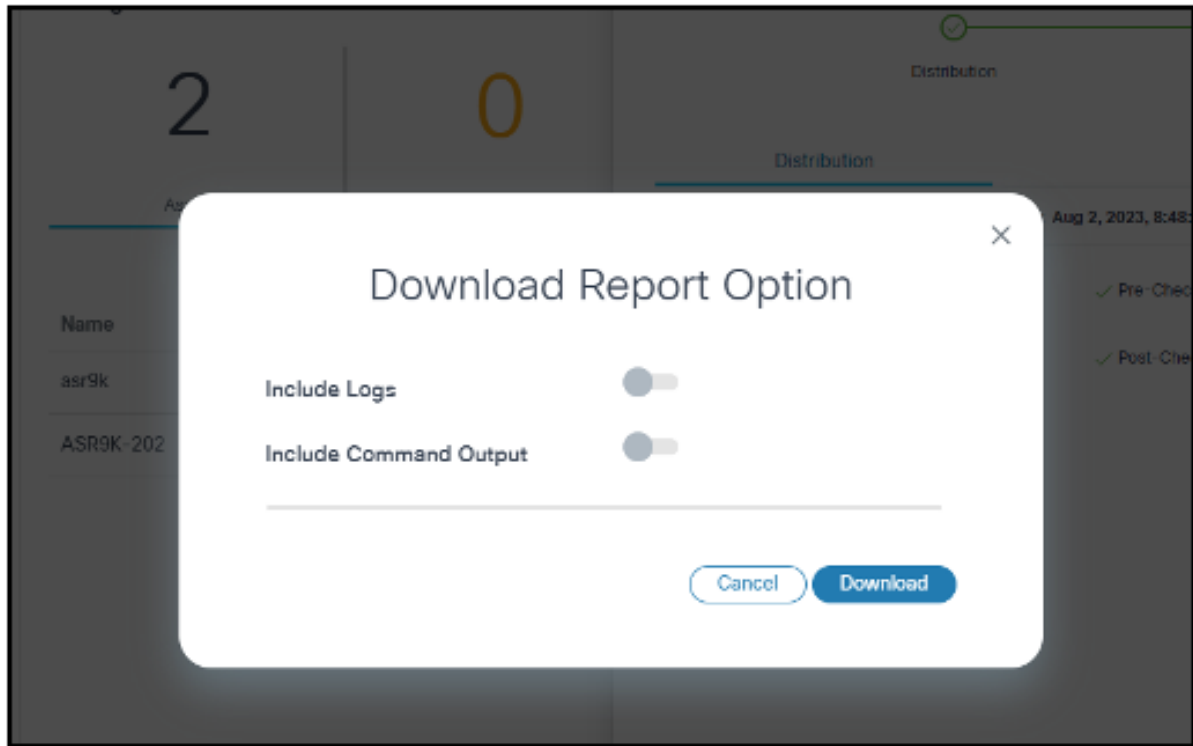
下載軟體升級報告

The screenshot displays the vmanage upgrade report interface. On the left, the 'JOB SUMMARY' section provides an overview of the upgrade process, including statistics for Batches and Assets. The right panel shows a detailed progress bar for 'Batch1', with steps: Distribution, BackUp, Pre-Check, Activation, Post-Check, and Rollback. A 'Download PDF' button is highlighted in a red box, indicating the option to download the report in PDF format.

下載PDF

裝置名稱顯示在詳細資訊檢視的標題中，後跟Download PDF。使用者可以生成並下載當前所選裝置的PDF格式的升級報告。要以PDF格式下載升級報告，請執行以下操作：

1. 按一下「Download PDF」。Download Report Option視窗開啟。



下載報告選項

2. 啟用Include Logs和Include Command Output切換。

- 包括日誌:在報告中包括即時日誌 (如果有)
- 包括命令輸出:在報告中包括預檢查和後檢查的命令輸出；在這種情況下，規則後跟命令輸出

3. 按一下「Download」。報告生成開始。

 附註：同時啟用Include Logs和Include Command Output切換功能會增加報告生成和報告大小的處理時間。僅在需要詳細報告時使用這些切換。無論命令輸出切換為On或Off，命令規則都包括在報告中。

Device Report

Device Name	asr-147
Controller ID	D2D-OSUpgrade
Serial Number	
Current Version	7.8.2
Target Version	7.7.2

Software Upgrade Version: 7.8.2 - 7.7.2

Milestone: Distribution

Milestone	Distribution
Execution Start Time	Fri, 29 Nov 2024 05:45:45 GMT
Execution End Time	Fri, 29 Nov 2024 06:24:53 GMT
Overall Status	Completed

Pre-Check

Process Template precheck_passfailrules

Command	Execution Time	Result
admin show running-config	Wed, 21 Jan 1970 01:20:59 GMT	Failed
Rules :		
Rule	View Rules	Operation Result
#Rule1	Invalid input detected	!Contains Passed
#Rule2	asdf	Contains Failed
#Rule3	qwerty	!Contains Passed

裝置報告

存檔作業

1. 使用對升級作業具有足夠訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。
3. 將Search篩選器與可用的圖表篩選器結合使用以篩選作業。
4. 選擇一個或多個作業。



存檔作業

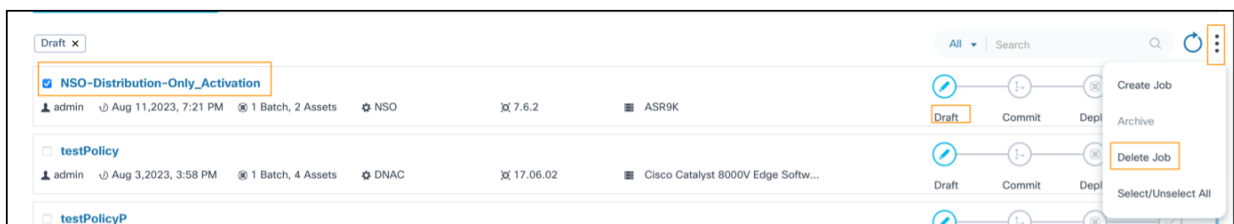
5. 選擇更多選項圖示> 存檔。



附註：只能存檔已完成的作業。

刪除作業

1. 使用對升級作業具有足夠訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。
3. 將Search篩選器與可用的圖表篩選器結合使用以篩選作業。
4. 選擇一個或多個作業。



刪除作業

5. 選擇更多選項圖示> 刪除作業。



附註：僅當作業處於「草稿」階段時，才能刪除作業。

刪除作業中的批處理

 Job Summary

 Cisco Catalyst 8000V Edge Software

Target Version : 17.06.03a

Existing Release

17.7.2 (2) 17.9.2a (11)

 Batches (Max Limit : 5)

☒ Europe 

 2 Asset(s)  Parallel

 May 20, 2023, 2:03 PM

☐ India 

 1 Asset(s)  Parallel

 May 27, 2023, 2:03 PM

 [Add Batch](#)

10 Assets Pending

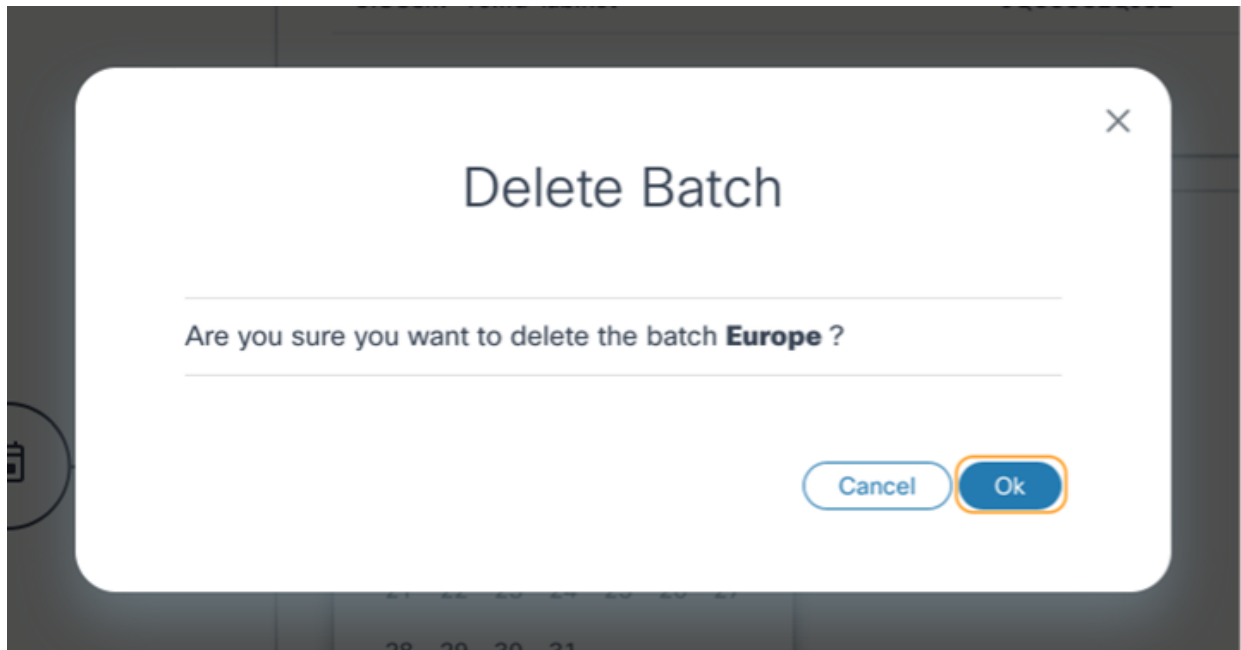
Batch Name *

Europe



刪除作業中的批處理

1. 在側面板中選擇所需批次的Delete圖示。此時將開啟確認視窗。



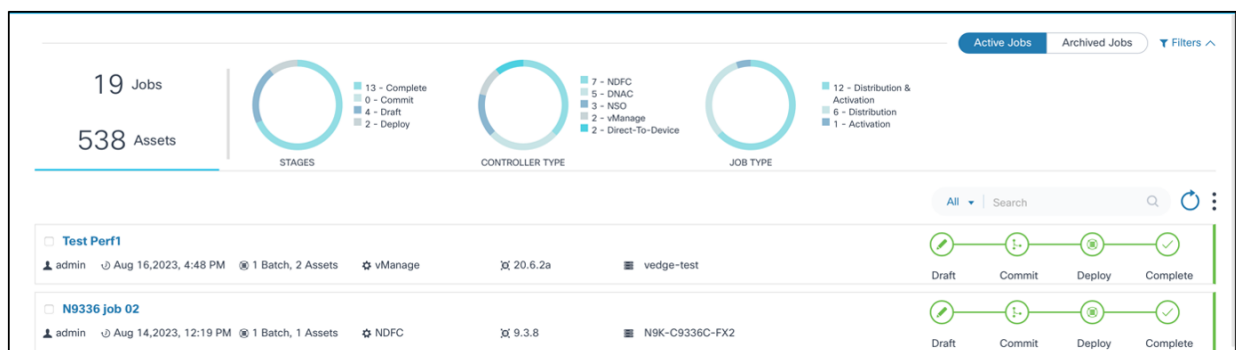
刪除批確認

2. 按一下「OK」(確定)。

與已刪除批相關聯的資產將返回到暫掛資產池，並且可在新批或現有批中進行選擇。

取消作業

1. 使用對升級作業具有足夠訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。



升級作業

3. 將Search篩選器與可用的圖表篩選器結合使用，以篩選所需的作業。
4. 按一下所需的作業。將顯示作業摘要頁。

Last Saved On : May 11,2023, 6:11 PM

Save Job

Commit Job

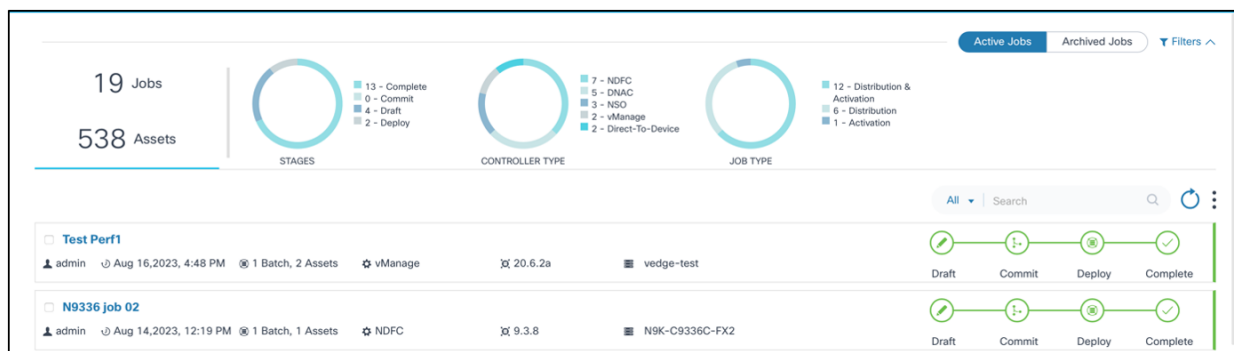
Cancel

取消

5. 按一下「Cancel」。

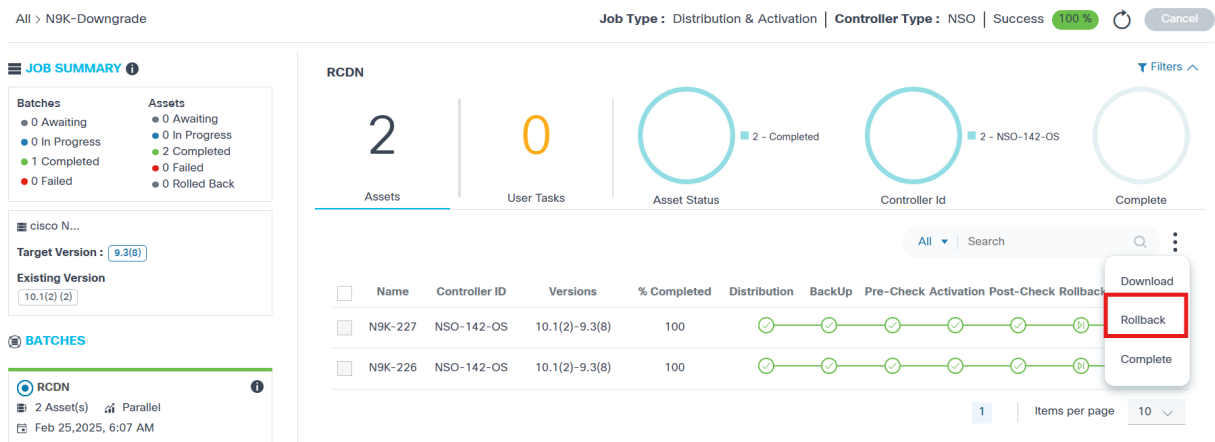
回滾已完成的作業或升級

1. 使用對升級作業具有足夠訪問許可權的憑據登入到BPA。
2. 選擇OS Upgrade > Upgrade Jobs。將顯示升級作業頁。



升級作業

3. 將Search篩選器與可用的圖表篩選器結合使用，以篩選所需的作業。
4. 按一下所需的作業。將顯示作業摘要頁。在左側窗格中選擇所需的批次，並在右側面板中選擇需要完全確認/回滾的所需裝置
5. 選擇更多選項圖示，然後根據需要按一下「回滾」或「完成」選單操作。



回滾

附註：僅當滿足以下先決條件時，才能選擇裝置：

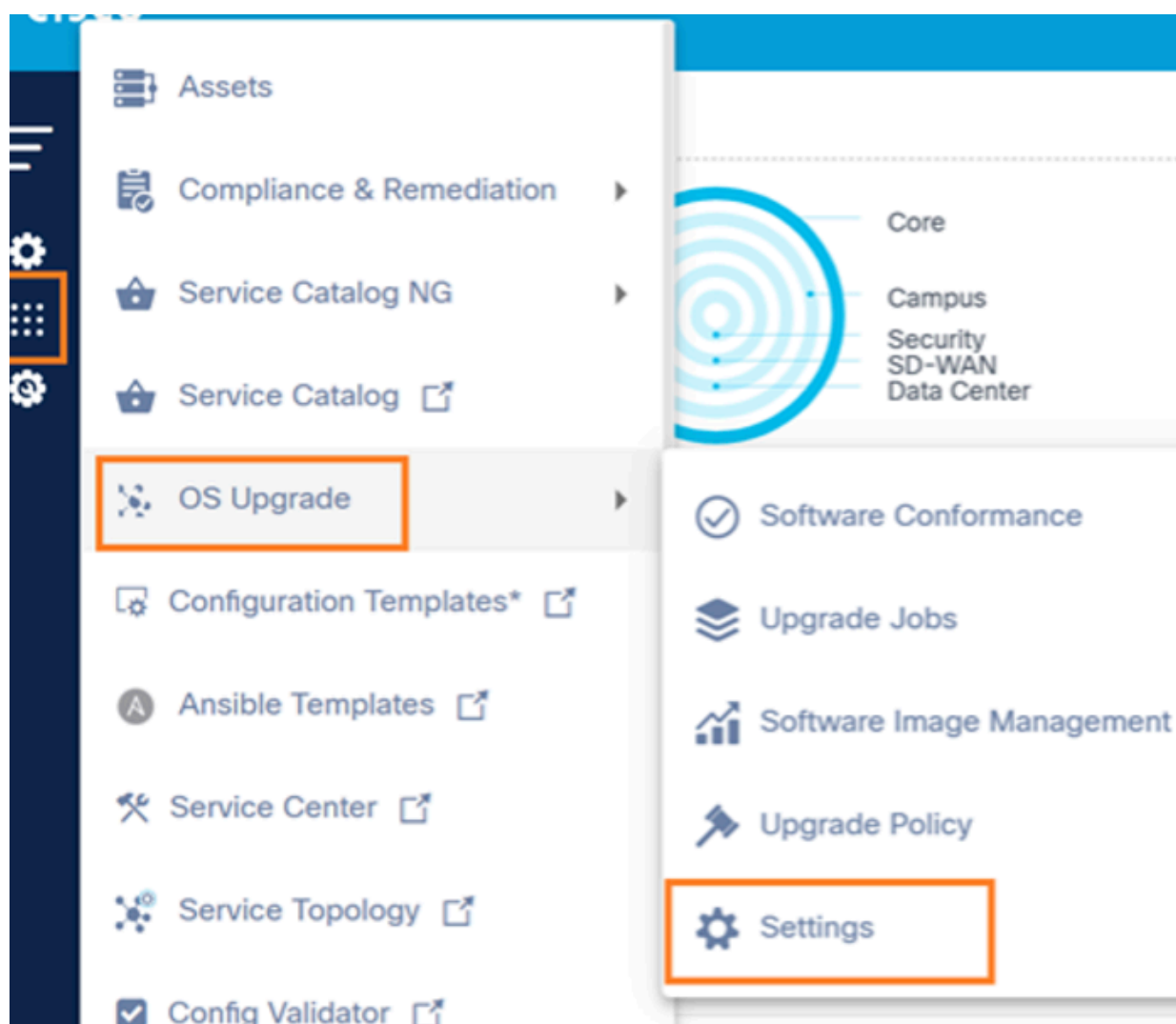
- 必須配置設定以啟用已完成升級作業的回滾選項；有關詳細資訊，請參閱[設定](#)。
- 如果在該時間內未執行任何操作，裝置將自動移至「完成」狀態
- 如果回滾之前已完成或回滾里程碑處於「等待」狀態，則裝置可用於按需回滾操作

設定

作業系統升級設定提供了一個佔位符，用於容納在作業系統升級應用程式的其他元件中使用的通用設定。

要訪問「設定」(Settings)頁面：

1. 使用對設定具有管理訪問許可權的憑據登入到BPA。



設定

2. 選擇OS Upgrade > Settings。將開啟Settings頁面。

Settings頁面包含以下兩個頁籤：

- 軟體符合性:可以在此頁籤中更新允許自動一致性執行計畫的配置
- 回滾:可以在此頁籤中更新允許回滾完整裝置升級的配置

軟體符合性

Software Conformance Rollback

Scheduled Conformance Check ☒ Enable

Start Date
07/04/2025

Cron Pattern

Minutes (0 - 59)	Hour (0 - 23)	Day (Month) (1 - 31)	Month (1 - 12)	Day (Week) (1 - 7)
25	7	*	*	*

Please click on save to check updated next execution date & time.

Auto Refresh Interval (seconds)
30

Reset Save

「軟體一致性」頁籤

Software Conformance頁籤提供以下內容：

- 計劃一致性檢查:啟用或禁用計畫
- 開始日期：選擇MM/DD/YYYY



附註：開始日期應為將來的日期。

- Cron模式：提供以下詳細資訊：
 - 分鐘(0-59)
 - 小時(0-23)
 - 天 (月) (1-31)
 - 月(1-12)
 - 天 (周) (1-7)
- 新增自動刷新間隔:預設值為30秒
- 儲存：儲存更改

回滾



「回滾」頁籤

Rollback頁籤提供以下內容：

- 使用者驗證切換:啟用或禁用使用者驗證
 - 已啟用狀態：升級作業中的裝置等待使用者確認回滾或完成升級，直到達到配置閾值時間（小時）中配置的閾值時間；到達時，裝置會自動進入Completed狀態
 - 禁用狀態：升級作業中的裝置自動完成升級，而無需等待使用者確認
- 確認閾值時間：新增閾值等待時間（以小時為單位）
- 儲存：儲存更改

部署配置

- 合規性策略檢查和SWIM後設資料的預設時間表每天配置在本地時間7:25。
- 要更改SWIM映像後設資料同步的預設計畫，請導航到BPA安裝目錄「<BPA install directory>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json」，並使用Cron表達式更新schedule.swimSchedule屬性。可以在部署後更新計畫。有關詳細資訊，請參閱[軟體一致性](#)。
- 要增加或減少不同控制器型別在並行模式下處理的最大裝置數，請執行以下操作：

1. 更新以下檔案：

- Cisco Catalyst Center檔案:"<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json"
- vManage File:"<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json"
- NDFC檔案:"<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
- FMC檔案:"<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json"

2. 導航到Update throttling > capabilities > image-activation，image-distribute以增加併發啟用或分發限制。



附註：更新這些限制之前，請參閱[支援的控制器和裝置平台](#)。

存取控制

基於角色的訪問控制

BPA支援基於角色的訪問控制(RBAC)。 在RBAC模型中，角色封裝了使用者可以執行的一組許可權（即操作）。對於訪問控制，管理員可以將預定義角色或新建立的具有許可權的角色分配給使用者組。一個使用者可屬於一個或多個使用者組，而每個使用者組可分配給一個或多個角色，這些角色賦予該組中的使用者特定的訪問許可權。

下表概述了OOB作業系統升級角色和相關許可權。

服務	群組	意圖	超級管理員	用例管理器	只讀使用者（作業系統升級使用案例只讀使用者）	操作員
OSUpgradeService	ui_app	顯示或隱藏升級作業應用程式	是	是	是	是
OSUpgradeService	ui_app	顯示或隱藏軟體一致性應用程式	是	是	是	是
OSUpgradeService	ui_app	顯示或隱藏SWIM應用程式	是	是	是	是
OSUpgradeService	ui_app	顯示或隱藏軟體升級策略應用程式	是	是	是	是
OSUpgradeService	ui_app	顯示或隱藏軟體升級設定	是	是	是	是
OSUpgradeService	升級作業	管理升級作業（例如，建立、更新、刪除和提交）	是	是	否	是
OSUpgradeService	升級作業	取消升級作業	是	是	否	是
OSUpgradeService	升級作業	按需存檔作業	是	是	否	是
OSUpgradeService	升級作業	手動批准	是	是	否	是
OSUpgradeService	Software-conformance-policy	檢視軟體一致性策略和執行結果	是	是	是	是
OSUpgradeService	Software-conformance-policy	建立、更新和刪除軟體一致性策略	是	是	否	否

服務	群組	意圖	超級管理員	用例管理器	只讀使用者 (作業系統升級使用案例只讀使用者)	操作員
OSUpgradeService	Software-conformance-policy	按需執行軟體一致性策略	是	是	否	是
OSUpgradeService	升級策略	檢視作業系統升級策略	是	是	是	是
OSUpgradeService	升級策略	管理作業系統升級策略	是	是	否	否
OSUpgradeService	Swim映像管理	建立、更新和刪除軟體映像	是	是	否	是
OSUpgradeService	Swim映像管理	觀賞游泳	是	是	是	是
OSUpgradeService	Swim映像管理	同步軟體映像	是	是	否	是
OSUpgradeService	軟體建議	同步軟體建議後設資料	是	是	否	否
OSUpgradeService	軟體建議	檢視建議或見解	是	是	是	是
OSUpgradeService	軟體建議	管理合規性策略	是	是	否	否
OSUpgradeService	軟體一致性設定	檢視軟體一致性設定	是	是	是	是
OSUpgradeService	軟體一致性設定	管理軟體一致性設定	是	是	否	否



附註：自定義角色和許可權對映可以根據要求完成。請參閱[資源組](#)。

資源組

此功能為BPA資源提供精細訪問控制，例如升級策略，限制未經授權的使用者更新作業系統升級應用程式中定義的策略。管理員可以通過定義具有可訪問策略的資源組來限制訪問。

要建立資源組，請執行以下操作：

1. 導覽至Settings > Resource Groups。

Add Resource Group

Resource Group name *
osupgrade-res-grp

Resource Type: os-upgrade-policy

Description: Enter resource group description

☐	Name	ASRSK	NSO
☐	Nso-qa1	ASRSK	NSO
☐	NSO-asr9k-policy-2	ASRSK	NSO
☒	NSO-any-to-any-policy	ASRSK	NSO

1 Items per page 10

Cancel Submit

新增資源組

2. 使用非管理員使用者可以訪問的策略建立資源組。
3. 選擇os-upgrade-policy作為Resource Type。顯示相應的資源。
4. 選擇所需的升級策略。
5. 按一下「Submit」。屬於此使用者組的非管理員使用者現在僅有權訪問所選資源組中可用的策略。

要將資源組與使用者組相關聯，請建立訪問策略。

Add Policy

Policy name *
osupgrade-access-policy

Description: Enter policy description

Resource Groups: All osupg

☐	Resource Groups
☒	osupgrade-res-grp

1 Items per page 10

Asset Groups: All Search

☐	Asset Groups	Group Type
☒	ALL-ACCESS	static
☐	ReadOnly	static
☐	replacement-nodes	static

1 Items per page 10

User Groups: All osupgrade

☐	User Groups
☒	osupgrade-user-grp

1 Items per page 10

Cancel Submit

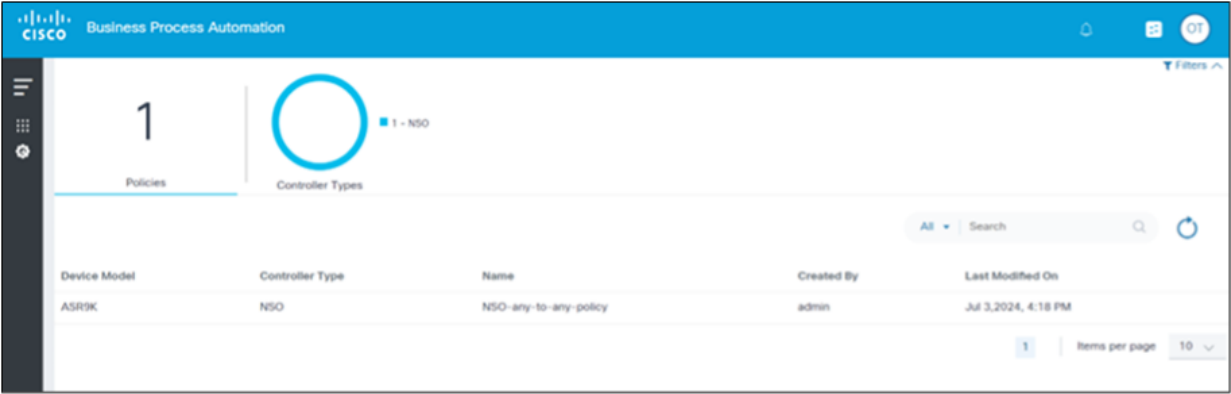
新增訪問策略

附註：建立資源組後，應通過訪問策略將其與使用者組關聯。有關以下內容的詳細資訊，請參閱[訪問控制](#)：

- 使用者
- 角色
- 使用者群組
- 訪問策略

- 資源組
- 資產組

以下是具有受限資源訪問許可權的非管理員使用者的示例：



具有資源限制的非管理員使用者

零信任標誌設定

使用者可訪問的資源可能因零信任標誌設定而異。零信任標誌可以設定為true或false。下表彙總了基於零信任標誌設定的資源訪問可能性。

使用者	使用者組	訪問策略	資源組	資源	Zero-Trust	已啟用
使用者 1	UG1	AP1	RG1	2資源	2資源	2資源
使用者 1	UG1	AP2	RG2	0資源	0資源	0資源
使用者 1	UG1	AP3	無		0資源	所有資源
使用者 1	UG1	無	無		0資源	所有資源

要啟用或禁用零信任標誌：

1. 導航到以下配置路徑：

```
cd /opt/bpa/bpa-helm-chart-
```

```
/charts/cisco-bpa-platform-mw-auth/public_conf/config.json
```

2. 修改zeroTrustPolicies值。
3. 導航到以下核心捆綁包：

```
cd /opt/bpa/bpa-helm-chart-
```

4. 運行以下命令以刪除核心掌舵：

```
helm delete bpa-rel -n bpa-ns
```

5. 運行以下命令以檢查Pod的狀態

```
kubect1 get pods -n bpa-ns
```

6. 終止所有Pod後，運行以下命令以安裝核心控制板：

```
helm install bpa-rel --create-namespace --namespace bpa-ns
```

7. 運行以下命令以驗證啟動的Pod的狀態：

```
kubect1 get pods -n bpa-ns
```

作業系統升級問題故障排除

本節提供與BPA中的OS升級應用程式所觀察到的問題相關的故障排除提示。

建立一致性策略時看不到目標裝置型號

確保相應的映像後設資料在SWIM下的軟體映像中可用。如果未找到，請執行以下任一選項：

- 同步映像以從Cisco Catalyst Center、NDFC、vManage和FMC等控制器檢索映像後設資料
- 為控制器（如NSO、CNC、直接到裝置和ANSIBLE）建立所需的影像後設資料

軟體符合性顯示非運行狀態

這可能是由於以下原因：

- 建立軟體一致性策略時，找不到具有所選模型的資產
- SWIM中的型號名稱與所有裝置的裝置清單中的符合裝置型號不匹配
- 如果選擇SMU作為軟體一致性建立的一部分，則所有裝置的SMU發現均失敗
- 為合規性檢查模板執行選擇的流程模板失敗或找不到
- 建立軟體符合性時，序列號或當前版本對於所選型號下的所有裝置均不可用

某些裝置的軟體一致性結果狀態未知

這可能是由於以下原因：

- SWIM中的型號名稱與裝置清單中的符合裝置型號不匹配
- 如果選擇SMU作為軟體一致性建立的一部分，則裝置的SMU發現失敗
- 為合規性檢查模板執行選擇的流程模板失敗或找不到
- 序列號或當前版本對於裝置不可用

升級作業完成進度百分比

如果升級作業完成進度百分比小於100（即使升級已完成），請確認在OS Upgrade > Settings > Rollback下啟用了Wait for Rollback設置，並確認User Verification已啟。如果整體完成百分比仍低於100，請選擇Rollback或Complete。

作業計畫已達到，裝置停滯在「等待」狀態

如果裝置在計畫作業啟動後停滯在「等待」狀態，請嘗試重新啟動Kafka、Camunda、Scheduler和OS Upgrade micro服務。

關於此翻譯

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