

BPA用户指南OS升级v5.1

- [简介](#)
 - [主要功能](#)
 - [端到端流](#)
 - [价值理念](#)
 - [支持的控制器和设备平台](#)
 - [新功能](#)
- [先决条件](#)
- [使用操作系统升级应用程序](#)
 - [软件映像管理](#)
 - [软件映像](#)
 - [同步软件映像元数据](#)
 - [添加软件映像元数据](#)
 - [批量上传软件映像元数据](#)
 - [编辑现有软件映像元数据](#)
 - [删除软件映像元数据](#)
 - [映像分发服务器管理](#)
 - [映像分发服务器](#)
 - [添加镜像文件服务器详细信息](#)
 - [编辑镜像文件服务器详细信息](#)
 - [删除镜像文件服务器详细信息](#)
 - [软件见解](#)
 - [先决条件](#)
 - [将软件见解数据提取到BPA](#)
 - [查看和管理安全建议](#)
 - [查看和管理优先级错误](#)
 - [查看软件见解](#)
 - [查看和选择供应商建议的软件版本](#)
 - [确定需要软件升级的设备](#)
 - [软件一致性](#)
 - [先决条件](#)
 - [在引用数据管理应用程序中创建EPLD模块数据](#)
 - [查看和管理软件一致性](#)
 - [创建软件一致性策略](#)
 - [按需执行软件一致性检查](#)
 - [安排执行软件一致性检查](#)
 - [更新软件一致性策略](#)
 - [删除软件一致性策略](#)
 - [查看和下载一致性结果](#)
 - [升级策略](#)
 - [先决条件](#)
 - [查看和管理升级策略](#)
 - [创建升级策略](#)

- [网桥SMU](#)
- [编辑升级策略](#)
- [查看升级策略](#)
- [删除升级策略](#)
- [控制对升级策略的访问](#)
- [升级作业](#)
 - [先决条件](#)
 - [查看和管理升级作业](#)
 - [安排升级作业](#)
 - [编辑作业中的批处理](#)
 - [升级作业执行和进度监控](#)
 - [下载软件升级报告](#)
 - [存档作业](#)
 - [删除作业](#)
 - [删除作业中的批次](#)
 - [取消作业](#)
 - [回滚已完成的作业或升级](#)
- [设置](#)
 - [软件一致性](#)
 - [回滚](#)
- [部署配置](#)
- [访问控制](#)
 - [基于角色的访问控制](#)
 - [资源组](#)
 - [零信任标志设置](#)
- [操作系统升级问题故障排除](#)
 - [创建一致性策略时看不到目标设备型号](#)
 - [软件一致性显示非运行状态](#)
 - [某些设备的软件符合性结果状态未知](#)
 - [升级作业完成进度百分比](#)
 - [作业安排已达到，设备停滞在“等待”状态](#)

简介

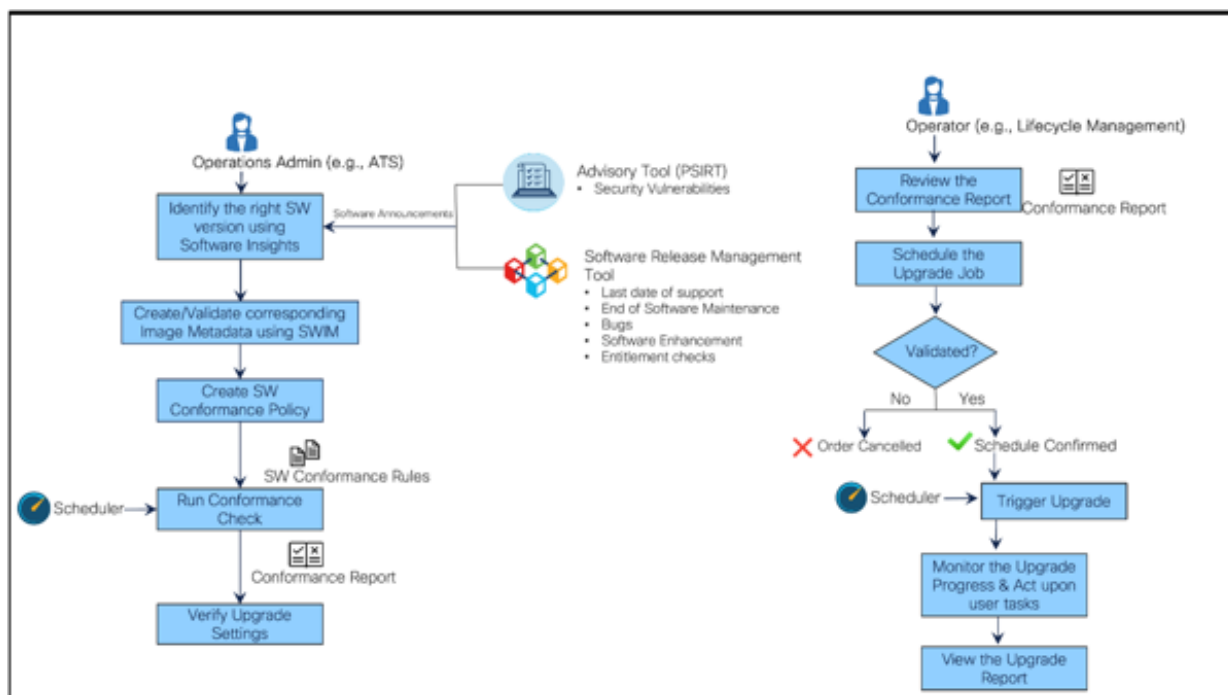
Business Process Automation(BPA)OS Upgrade应用程序提供全面的自动化解决方案，可在不同域之间执行软件一致性和网络设备升级。它支持多个域控制器并提供统一的用户体验。它支持基本操作系统(OS)升级和软件维护更新(SMU)或RPM软件包管理器(RPM)补丁更新。

主要功能

OS升级应用提供以下关键自动化功能：

- 软件映像管理:供软件升级过程使用的软件映像及其版本（来自所有供应商）的集中列表
- 软件见解:识别暴露于网络资产的软件风险和漏洞，并深入了解供应商推荐的软件版本
- 软件一致性:标识网络中必须升级其软件映像的所有资产
- 升级过程方法(MOP)定义:为每个供应商设备型号或系列预先定义升级过程以及预先检查和事后检查
- 升级作业:在跨地理区域的维护时段安排非一致性资产的升级，监控升级进度并获得详细报告

端到端流



端到端流

上图显示了两个不同用户角色的操作系统升级应用呼叫流：运营管理员和网络运营商，开箱即用 (OOB)。有关OOB角色和相应权限的详细信息，请参阅[访问控制](#)。

角色	描述	工作空间
操作管理员	发现影响网络资产的软件漏洞（例如，公告、漏洞、寿命终止公告）	BPA:操作系统升级/软件映像管理/建议
操作管理员	确定受影响的软件版本和受影响的资产，并根据供应商提供的建议确定正确的目标版本	BPA:操作系统升级/软件映像管理/见解
操作管理员	创建所需的软件映像元数据	BPA:操作系统升级/软件映像管理/软件映像
操作管理员	为受影响的设备模型创建意图，并按需或按计划执行策略时执行策略	BPA:操作系统升级/软件一致性策略
操作管理员	标识不符合项或受影响的资产	BPA:操作系统升级/软件符合性/查

角色	描述	工作空间
		看结果
操作管理员	根据升级MOP创建或修改升级策略；这包括预先定义预先检查和事后检查、分发或激活工作流程、流量转移或逆转，以及单步或多步升级的回滚	BPA:操作系统升级/升级策略
网络操作员	安排作业以升级所有不符合项设备	BPA:操作系统升级/升级作业
网络操作员	监控升级作业进度	BPA:操作系统升级/升级作业/作业详细信息
网络操作员	执行用户任务（如果有）以排查问题，并使流程能够继续下一步	BPA:操作系统升级/升级作业/作业详细信息

价值理念

操作系统升级应用提供以下附加值：

- 一种API — 首先支持从北向运营支持系统(OSS)和业务支持系统(BSS)中更轻松地使用服务的方法
- 跨由各种域控制器管理的网络快速验证网络设备的软件符合性
- 通过使用批处理、排队和调度机制，操作员可以更好地控制升级作业
- 可以提前创建升级作业供查看并在以后执行
- 一种排队机制，能够以最少到零的故障实现更快的吞吐量
- 升级前自动配置备份，可在发生故障时实现无缝恢复
- 检查前和检查后执行，确保成功升级而不中断服务
- 一种策略驱动的方法，通过预验证和验证后检查、分发或激活、流量转移或反向以及回滚流程，灵活地预先定义升级MOP，允许根据需要进行自定义

支持的控制器和设备平台

以下平台已在BPA中验证，并且受支持OOB。但是，该框架是通用的，可以扩展到新的平台。未来版本将根据优先级提供对其他平台的OOB支持。

域控制器	设备平台
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS、Cisco IOS-XE
vManage v20.12.4	- Cisco IOS、Cisco IOS-XE
	注意：设备必须是v17.9.x或更高版本，远程服务器分发

域控制器

设备平台

才能正常工作

Nexus控制面板交换矩阵控制器
(NDFC)v12.1.2e和v12.2.2

- Cisco-NXOS(N9k)

防火墙管理中心(FMC)v7.4.1

- Firepower 3140

— 思科IOSXR(NCS540、NCS560、ASR9K)

网络服务协调器(NSO)v6.3

- Cisco-NXOS(N9K)

注意：需要NX-OS NED v5.25.17或更高版本

跨网络控制器(CNC)v6.0

— 思科IOSXR(NCS540、ASR9K)

ANSIBLE v2.9.18(AWX - 17.1.0)

— 思科IOSXR(NCS540、ASR9K)

直接到设备(通过电传网络(Telnet)和安全
外壳(SSH))

— 思科IOSXR(NCS540、ASR9K)

新功能

有关此版本的操作系统升级使用案例可用的增量功能，请参阅[BPA发行说明](#)。

先决条件

在使用操作系统升级应用程序之前，必须满足以下前提条件：

- 操作系统升级、备份和恢复、调度程序服务和所有必需的平台服务或控制器代理服务均已启动并正在运行
- 加载所需的工件（例如，工作流程、流程模板、默认升级策略等）
- 添加所需的控制器并成功同步设备；有关详细信息，请参阅[支持的控制器和设备平台](#)

使用操作系统升级应用程序

OS升级应用由以下组件组成：

- 软件映像管理(SWIM)
- 映像分发服务器管理
- 软件见解
- 软件一致性
- 升级策略
- 升级作业

- 设置

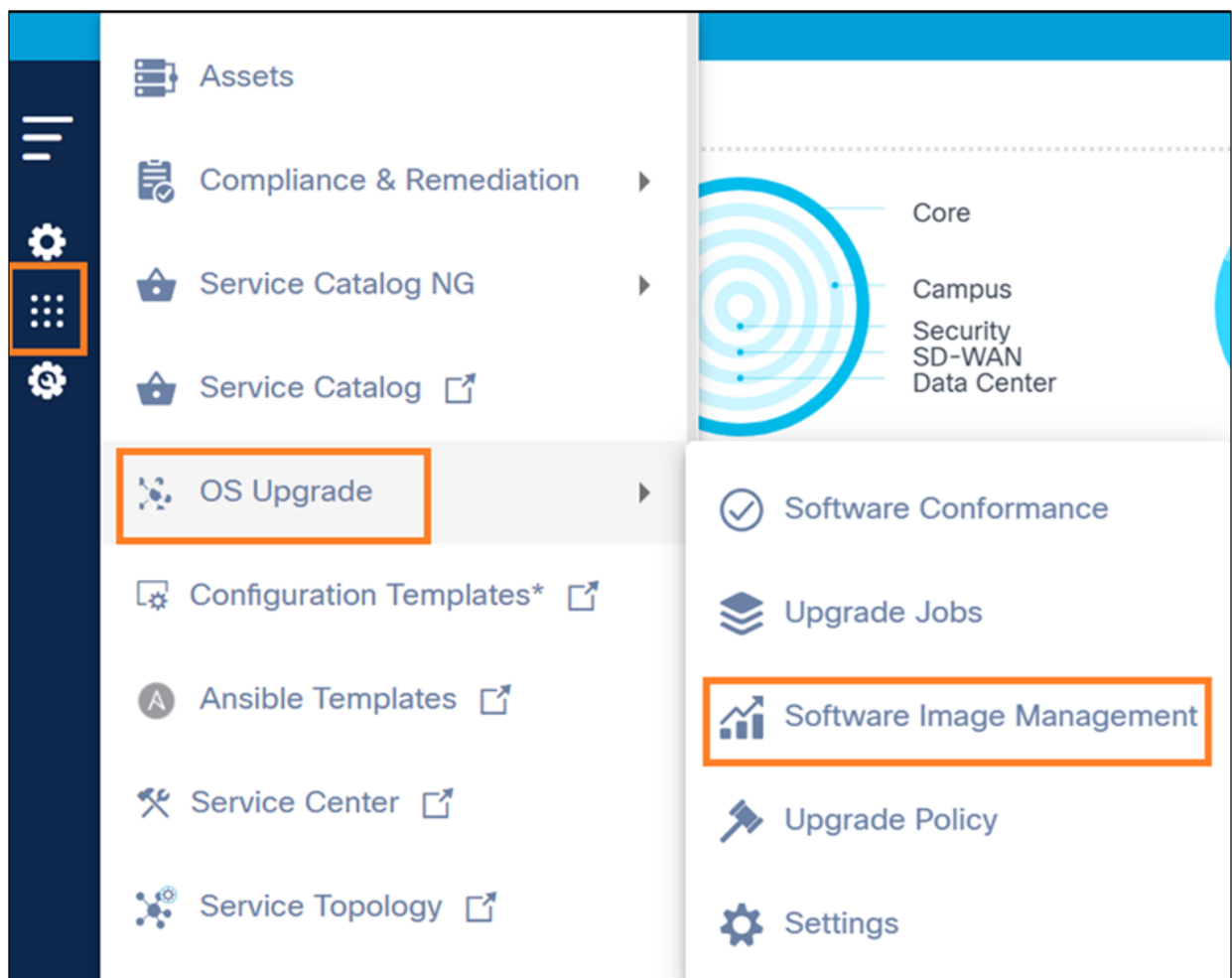
软件映像管理

SWIM组件允许Operations用户维护没有OOB映像管理支持的控制器（如NSO、ANSIBLE、CNC、FMC和直接到设备）的软件映像详细信息。它还列出了vManage、NDFC和Cisco Catalyst Center等控制器维护的软件映像详细信息，从而提供了跨所有域控制器维护的软件的集中列表。软件映像和映像分发服务器是SWIM模块中的两个主要子组件。

软件映像

要访问“软件映像”(Software Images)页面，请执行以下操作：

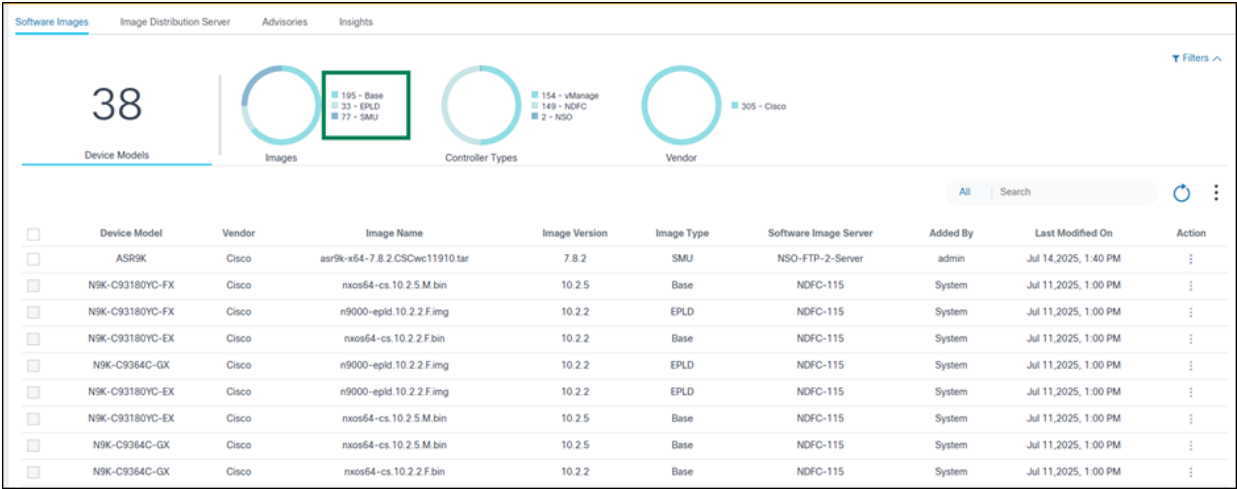
1. 使用有权访问软件映像管理的凭证登录到BPA。



软件映像管理导航

2. 选择OS Upgrade > Software Image Management。

Image Management页面显示以下选项卡：软件映像、Image Distribution Server、Advisories和Insights。



软件映像选项卡

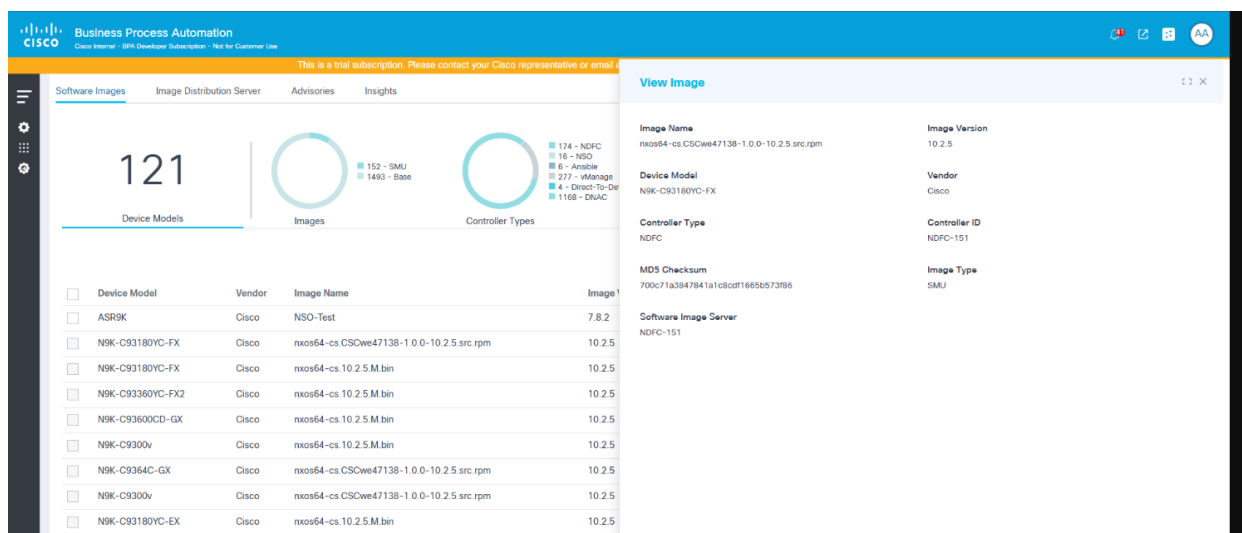
Software Images选项卡包含以下内容：

- 顶部显示的分析部分，提供以下功能：
 - 设备型号和相关软件映像的总数
 - 一种Images快速过滤器，允许根据类型（例如base、SMU）过滤图像；该数字表示与相应图像类型相关联的图像总数
 - Controller Types快速过滤器，允许根据托管图像的控制器类型（例如Cisco Catalyst Center、vManage、NSO或NDFC、直接到设备、CNC、ANSIBLE、FMC）过滤图像；该数字表示与相应控制器类型相关联的映像总数
 - Vendor快速过滤器，允许根据发布软件的供应商过滤映像
- More选项图标提供以下功能：
 - 添加映像详细信息:添加新映像元数据
 - 批量上传:以.csv格式批量上传图像元数据
 - 同步映像:同步来自控制器（例如Cisco Catalyst Center、vManage、NDFC和FMC）的映像元数据
 - 全部删除:批量删除选定的映像

 注意：仅允许NSO、ANSIBLE、CNC和直接到设备控制器添加、删除和批量上传图像详细信息。

- Search过滤器可用于搜索图像，包括以下独占搜索过滤器：
 - 全部:跨所有字段搜索
 - 镜像名称:搜索具有特定图像名称的图像
 - 设备型号:搜索具有指定模型的图像

- 映像版本:搜索具有特定软件版本的映像
- 软件映像服务器:搜索与特定镜像文件服务器相关联的镜像
- Refresh图标用于刷新页面并清除所选过滤器。
- 现有图像显示在包含以下列的网格表中：
 - 设备型号：映像详细信息适用的设备型号
 - 供应商:发布软件映像的供应商
 - 镜像名称:映像的文件名
 - 映像版本:映像的软件版本
 - 映像类型:确定图像类型(例如，基础、SMU、电子可编程逻辑设备(EPLD))
 - 软件映像服务器:当前映像所在的镜像文件服务器
 - 添加者:添加图像元数据的用户
 - 上次修改时间:上次映像详细信息更新的时间戳
 - 操作：提供更多选项图标，可从中选择行特定的操作（例如，编辑、删除）
- 通过点击相应的列标题对图像排序



查看图像

- 单击某一行将打开“查看图像”窗口

同步软件映像元数据

要执行软件映像的按需同步，请执行以下操作：



同步映像

1. 选择More Options图标> Sync Images。vManage、Cisco Catalyst Center、NDFC和FMC中的映像元数据详细信息在BPA中发现并保留。



注意：对于FMC控制器，每次执行同步时都会保留现有数据。仅附加新图像。

2. 如果FMC控制器中的映像名称包含单词“FTD”或“Firepower Threat_Defense”，则该映像的deviceModel将映射为FTD。

或者

如果FMC控制器的映像名称包含单词“FMC”、“FW_Mgmt_Center”或“Firewall_Management_Center”，则该映像的deviceModel将映射为FMC。

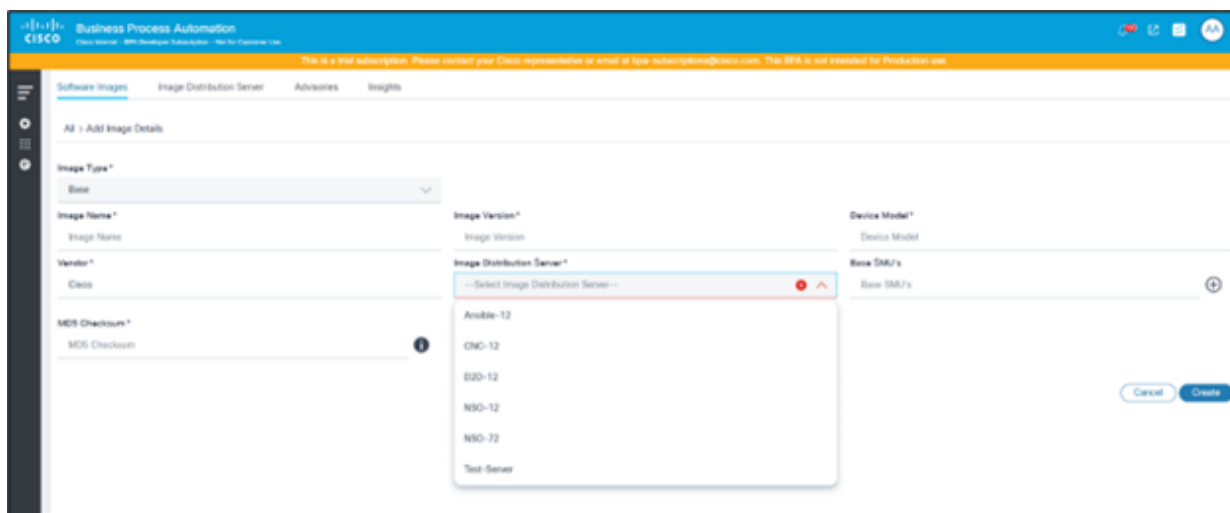


注意：FMC不会将模型信息与映像元数据相关联。同步完成后，编辑相应的映像元数据并根据需要更新模型。如果没有型号更新，FMC升级过程将无法按预期工作。

3. vManage远程服务器中的映像在同步操作后，首先在Version列中映射通用唯一标识符(UUID)。操作员必须手动编辑所需的远程服务器元数据，并使用适当的映像版本更新这些元数据。如果未完成此映射，则其他OS升级组件（例如，软件一致性、升级策略、升级作业等）无法按预期工作。
4. 要定期安排自动SWIM元数据同步，请参阅[部署配置](#)。

添加软件映像元数据

1. 选择更多选项图标> 添加图像详细信息。系统将显示Add Image Details页面。



添加映像详细信息

2. 在以下字段中输入信息：

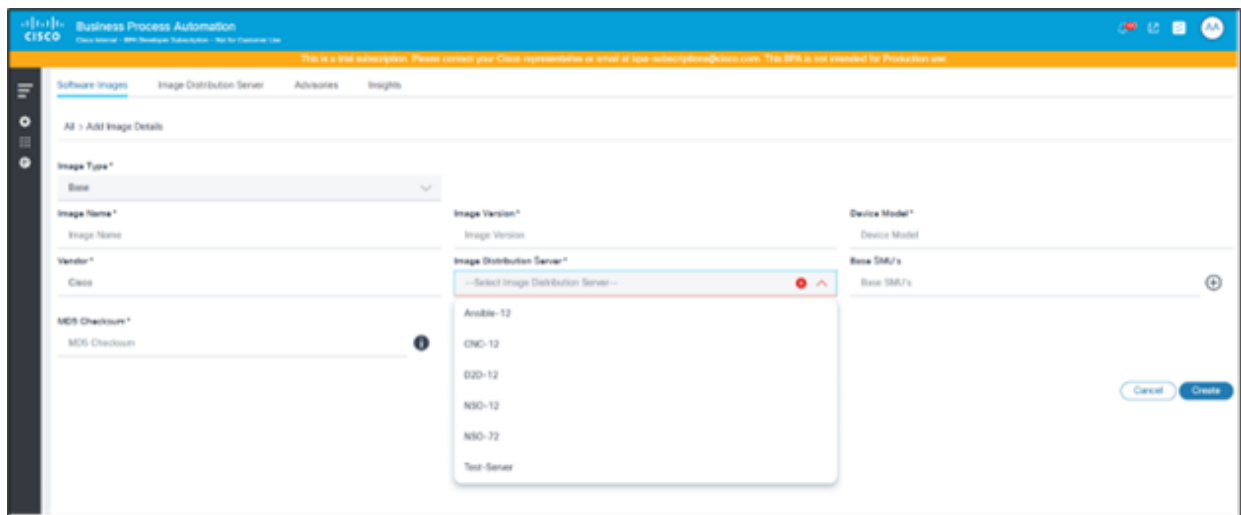
- 映像类型:映像类型（例如，base、SMU、EPLD）
- 镜像名称:映像文件的名称；用户可以在“名称”字段中输入图像的相对或绝对路径。如果用户提供了绝对路径，则直接从该路径获取图像；如果用户提供相对路径，则系统会通过其在分发过程中添加存储库服务器中定义的基本路径解析完整路径
- 映像版本:映像的软件版本
- 设备型号:为其标记图像的设备型号

 **注意：**设备型号应与适用设备的CNC、NSO、Direct-To-Device或ANSIBLE控制器提供的型号信息匹配。

- 供应商:发布映像的供应商或提供商；默认值为Cisco，但可以根据需要进行更改
- Image Distribution服务器:选择承载映像名称字段中指示的软件文件的映像分发服务器。在选择图像分发服务器时，为与图像分发服务器中定义的指定控制器类型相关联的所有控制器ID生成图像。如果用户在映像分发服务器下添加或删除控制器实例，则将为这些控制器实例添加或删除相应的软件映像。
- 基本SMU:SMU出现在基层的黄金图像中；此选项仅在图像类型为Base时适用
- MD5校验和:用于验证的映像MD5校验和

3. Click Create.系统随即会显示Progress通知，并显示一条确认消息。

 **注意：**在升级策略中使用网桥SMU之前，必须添加其映像元数据。要添加网桥SMU，请从映像类型下拉列表中选择SMU。



添加网桥SMU映像元数据

批量上传软件映像元数据

	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

包含图像信息的CSV文件示例

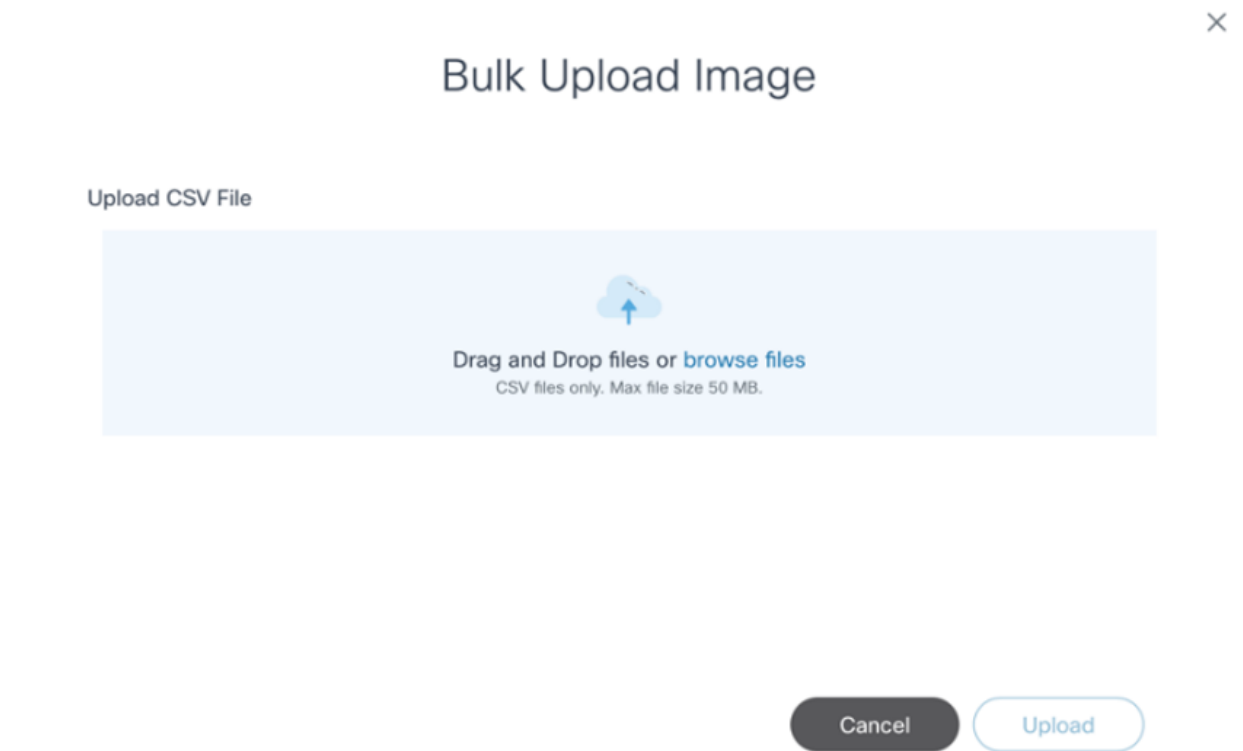
1. 准备包含所需映像详细信息和以下列名的.csv文件：

- 镜像名称
- version
- 设备型号
- 供应商
- 图像类型

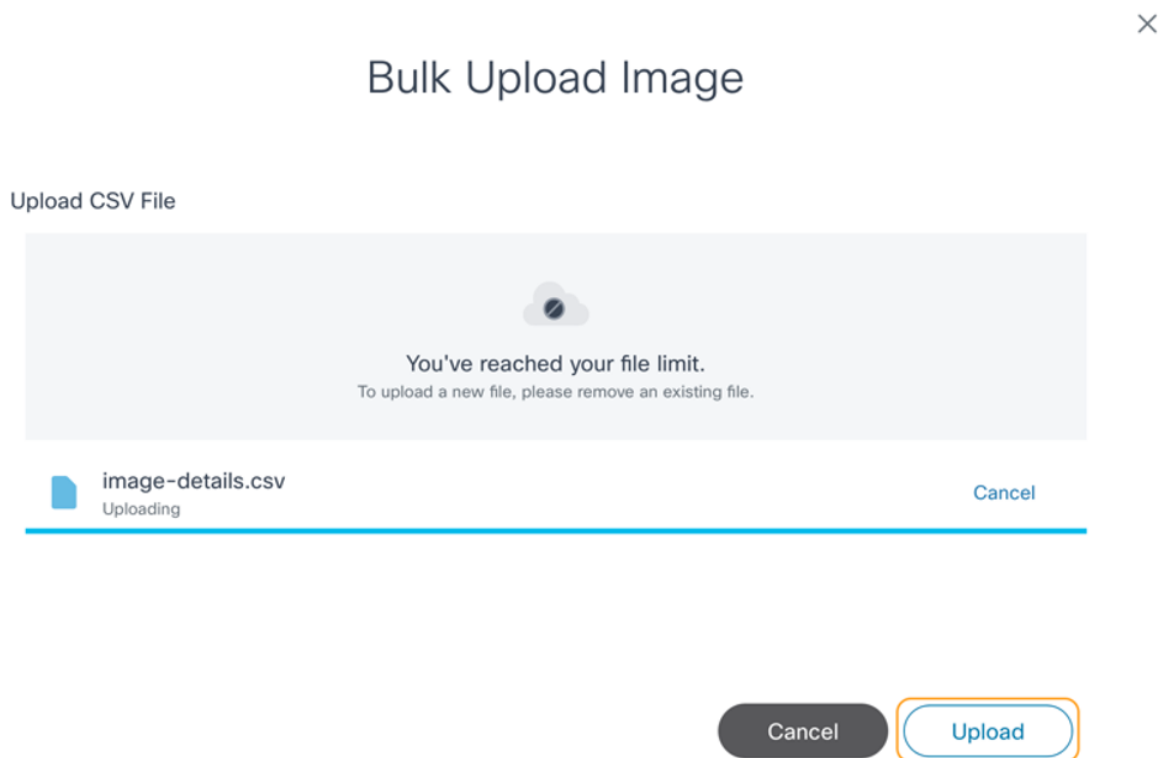
 注意：仅支持Base、SMU和EPLD值。

- 映像分发服务器
- MD5校验和

2. 选择更多选项图标> 批量上传。Bulk Upload Image窗口打开。



批量上传图像



批量上传映像 — CSV上传

3. 选择准备的.csv文件，然后单击Upload。验证并处理来自.csv的映像详细信息。文件上传后，将显示最终批量上传状态。



Bulk Upload Image

Upload CSV File

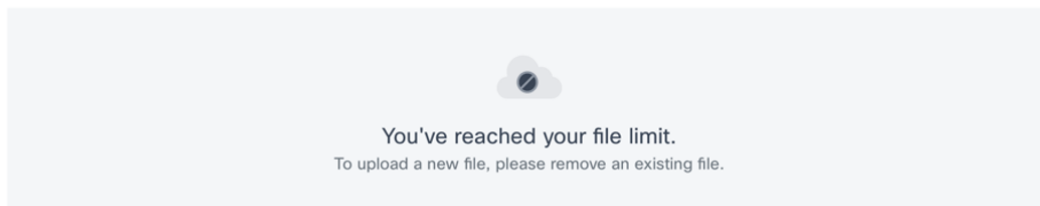


image-details.csv
Uploading

Cancel

Total upload status: Success: 2, Failed: 0

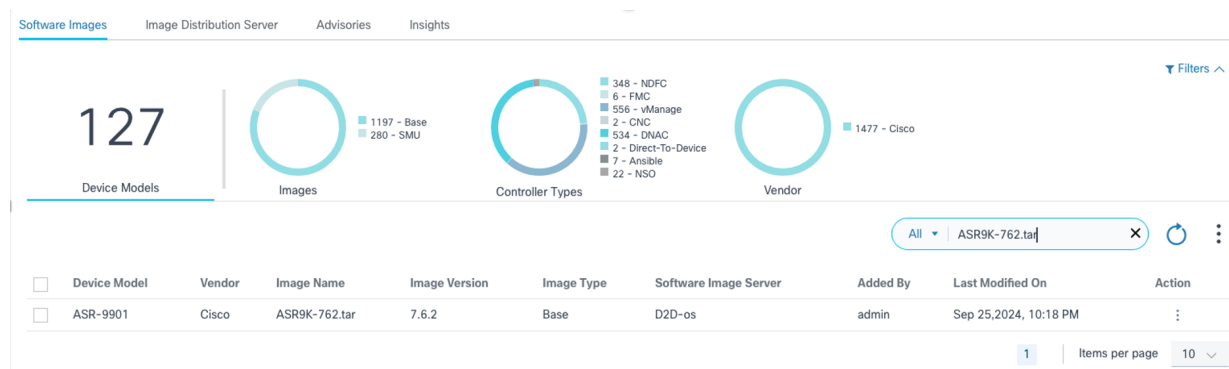
Cancel

Upload

成功批量映像上传状态

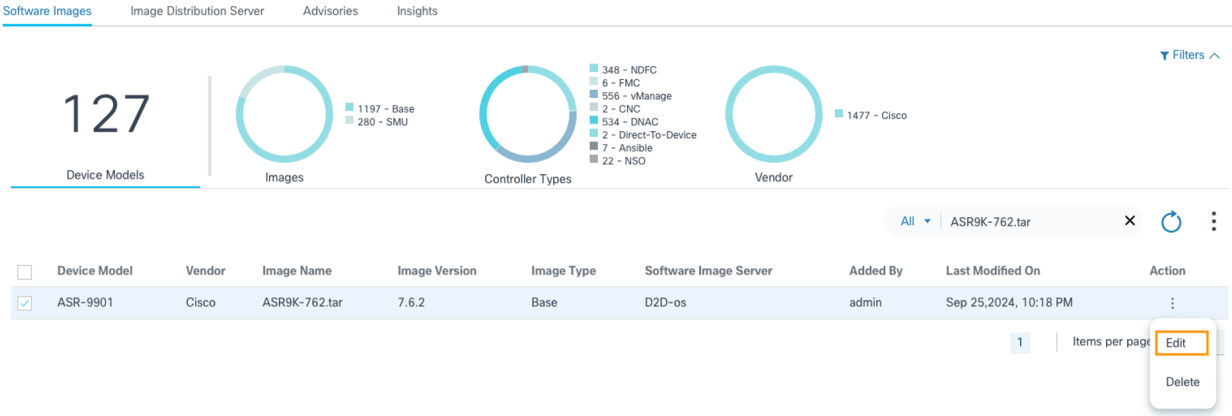
 注意：如果出现数据验证错误（例如，重复记录或无效参数），错误消息将以网格形式显示在“批量上传图像”(Bulk Upload Image)窗口中。用户可以更正.csv文件中的值并重新上传。

编辑现有软件映像元数据



在软件映像元数据中搜索

1. 使用Search (搜索) 过滤器找到需要更新的图像。



编辑

2. 从所需图像的Action列中，选择More Options图标> Edit。

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

编辑软件映像

3. 更新所需参数，然后单击Save保存更改，或单击Cancel放弃更改。系统随即会显示进度通知，然后会显示映像更新的确认消息。



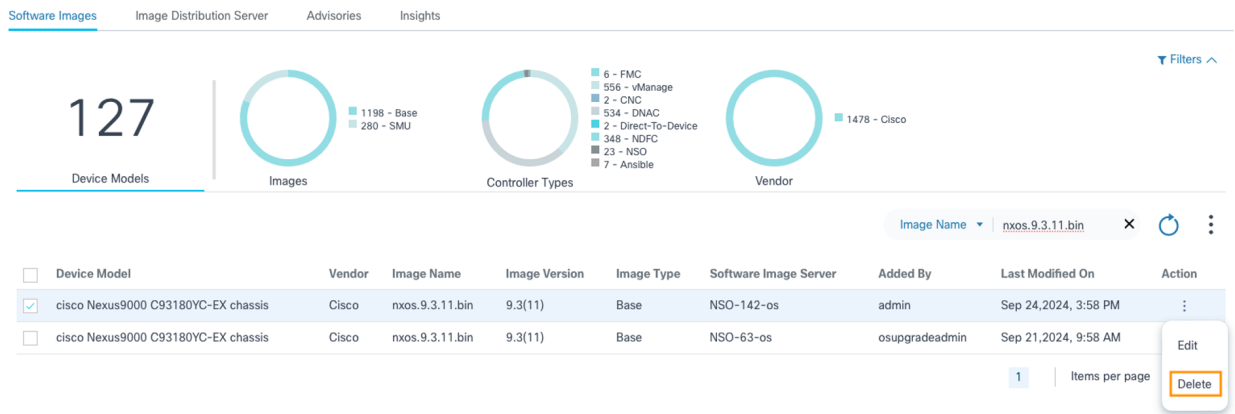
注意：下面列出了一些注意事项。

- CNC、NSO、D2D、ANSIBLE、FMC和vManage控制器均可进行编辑（仅适用于远程服务器映像元数据）
- 仅vManage远程服务器映像支持更新设备模型
- 只能为vManage远程服务器映像元数据更新软件版本字段
- 对于vManage映像，用户可以查看软件映像服务器来代替控制器实例

删除软件映像元数据

在软件映像元数据中搜索

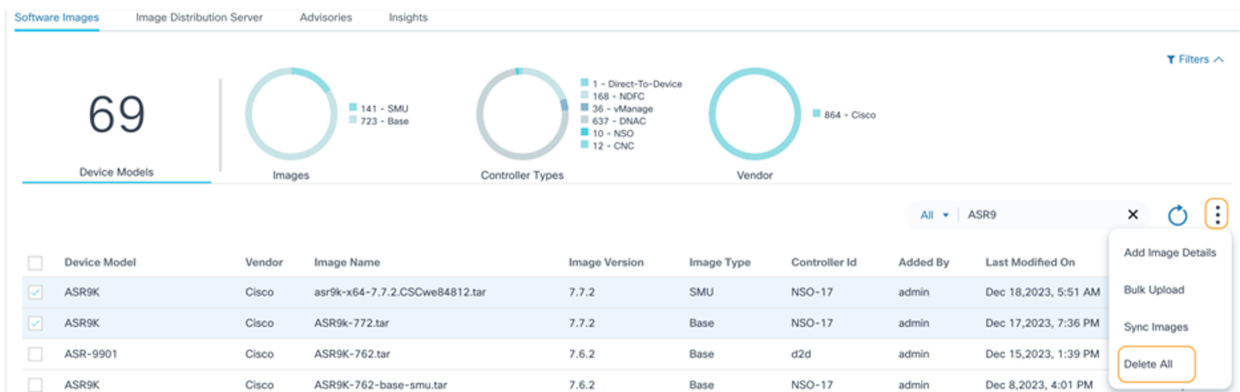
1. 使用Search字段查找所需图像。



DELETE

2. 从所需图像的操作列中，选择更多选项图标> 删除以删除图像。

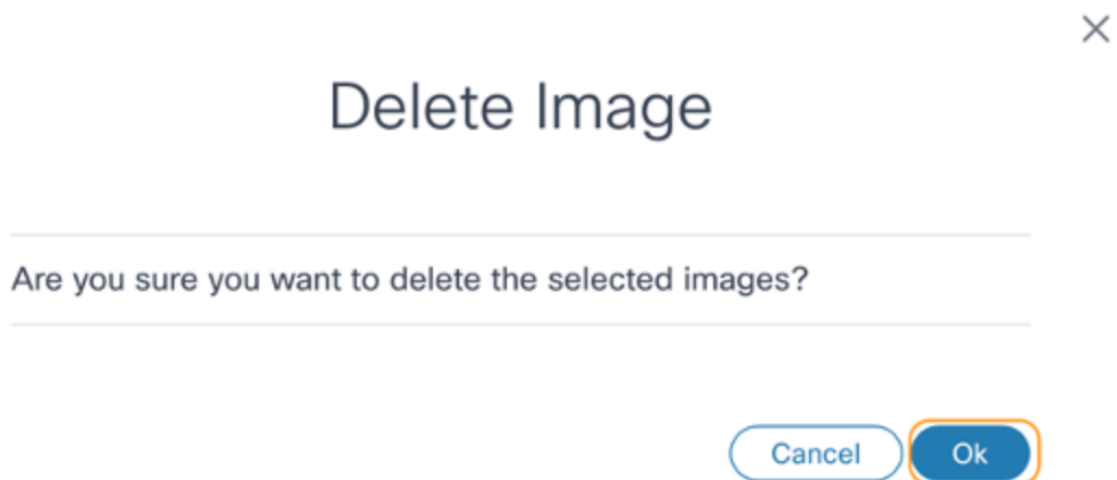
或者



全部删除

选择所需图像，然后选择更多选项图标> 全部删除以删除多个图像。

系统随即会显示确认。



确认

3. Click OK.系统随即会显示进度通知，然后会显示确认消息。



注意：下面列出了一些注意事项。

- 只能为NSO、ANSIBLE、Direct-to-Device和CNC控制器添加图像元数据。对于所有其他企业控制器，利用内置SWIM功能，并从各自的控制器中发现映像
- NSO、ANSIBLE、Direct-to-Device和CNC控制器的映像服务器不支持映像发现功能。
- 默认情况下，vManage remote server image metadata包含UUID for version parameter post-sync。用户必须编辑元数据并使用相应版本更新UUID。相应的映像版本可以通过vManage控制器或登录映像存在的设备来识别。

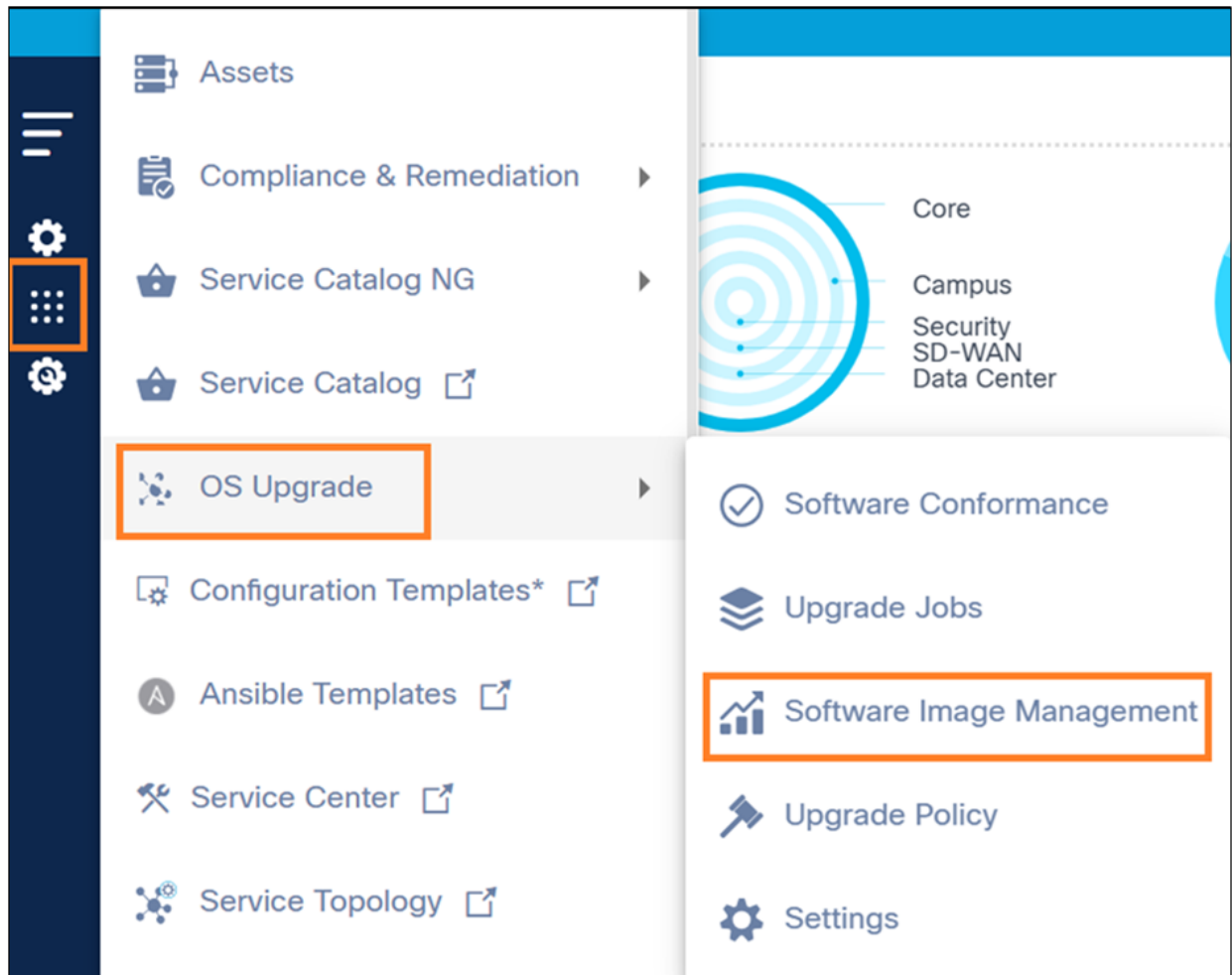
映像分发服务器管理

映像分发服务器

该组件允许Operations用户维护没有OOB映像存储库管理支持的CNC、NSO、ANSIBLE、FMC和直接到设备控制器的映像存储库服务器详细信息。

要访问Image Distribution Server页：

1. 使用对映像分发服务器具有管理访问权限的凭据登录到BPA。



软件映像管理

2. 选择OS Upgrade > Software Image Management。

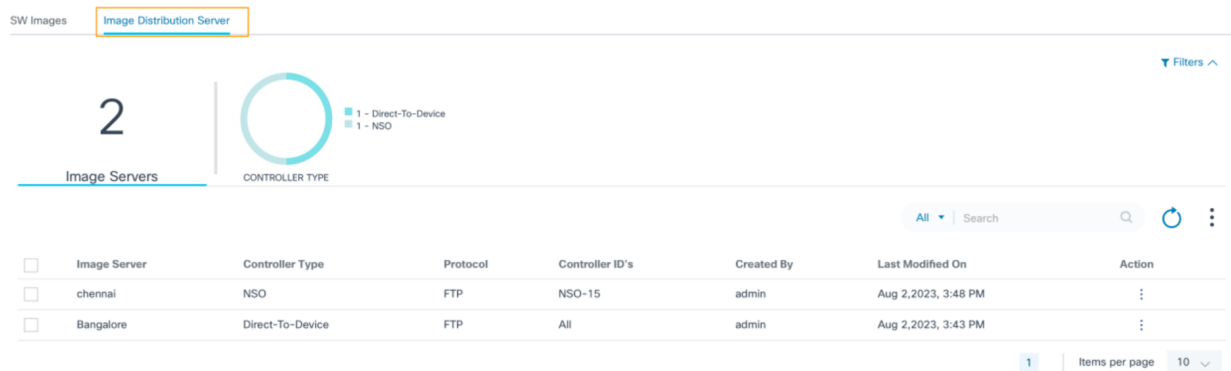


Image Distribution Server选项卡

3. 单击Image Distribution Server选项卡。

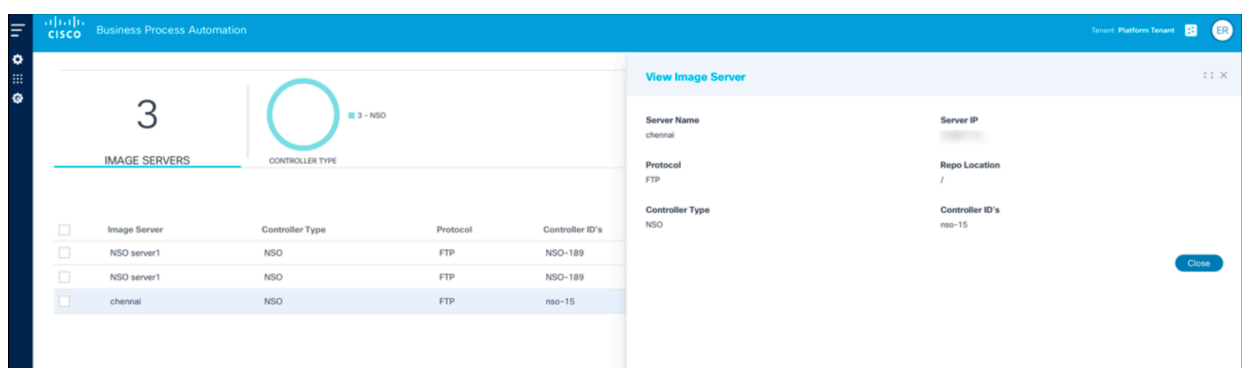
Image Distribution Server选项卡包含以下内容：

- 顶部显示的分析部分，提供以下功能：

- 此BPA实例上已登录的镜像文件服务器总数
- Controller Type快速过滤器，允许基于控制器类型（例如NSO、Direct-to-Device、CNC、ANSIBLE、FMC）过滤图像服务器；该数字表示与该控制器类型关联的映像分发服务器总数
- 提供以下功能的更多选项图标：
 - 添加映像服务器:添加新映像分发服务器
 - 全部删除:批量删除选定的分发服务器
- 可用于搜索分发服务器并包含以下独占搜索过滤器的Search过滤器：
 - 全部:跨所有字段搜索
 - 映像服务器:搜索具有特定服务器名称的服务器
 - 控制器ID:搜索与特定控制器ID关联的服务器
- 可用于刷新页面和清除所选过滤器的刷新图标
- 现有分发服务器显示在具有以下列的网格表中：
- 映像服务器:存储库服务器的唯一名称
 - 控制器类型:此映像服务器适用的控制器类型
 - 协议:存储库服务器支持的复制协议

 注意：仅支持FTP、SCP和安全文件传输协议(SFTP)

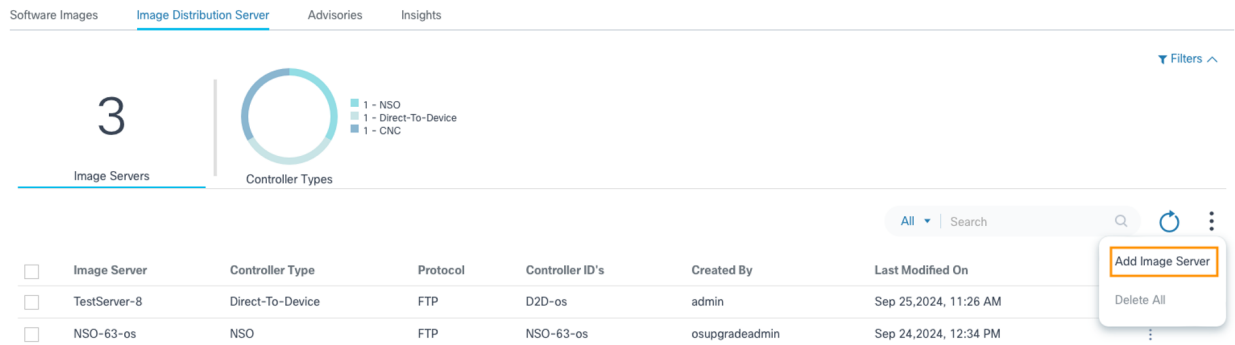
- 控制器ID:当前存储库服务器可用或适用的控制器实例；控制器实例是指通过该控制器管理的设备
- 创建者：登录存储库服务器的用户
- 上次修改日期:上次更新服务器详细信息的时间戳
- 操作：提供行特定的操作，例如Edit和Delete



查看镜像文件服务器面板

- 单击某一行将打开“查看镜像文件服务器”窗口

添加镜像文件服务器详细信息



添加镜像文件服务器

4. 选择更多选项图标> 添加镜像文件服务器。系统随即会显示Add Image Server页面。

Software Images **Image Distribution Server** Advisories Insights

All > Add Image Server

Server Name *

Server Name

Root Location *

Root Location

User Name *

Username

Server IP *

Server IP

Controller Type *

Select option ▾

Password *

Protocol *

Select option ▾

Controller Instances *

Cancel

Create

添加镜像文件服务器详细信息

Software Images **Image Distribution Server** Advisories Insights

All > Add Image Server

Server Name *

Demo-server ✓

Root Location *

/ ✓

User Name *

calo ✓

Server IP *

1.2.3.4 ✓

Controller Type *

NSO ✓ ▾

Password *

Protocol *

FTP ✓ ▾

Controller Instances *

NSO-142-OS ▾

Cancel

Create

添加包含示例详细信息的镜像文件服务器

5. 在以下字段中输入信息：

- 服务器名：映像存储库服务器的唯一名称
- 服务器 IP:存储库服务器的IPv4地址

注意：在添加之前，请确保此IP可从网络设备访问。

- 协议:映像副本受映像存储库服务器支持

注意：仅支持FTP、SCP和SFTP协议。

- 回购地点：存储库服务器中映像文件的基本路径

 注意：如果镜像文件存在于镜像文件服务器资料档案库文件夹的根目录下，则“/”作为值工作。

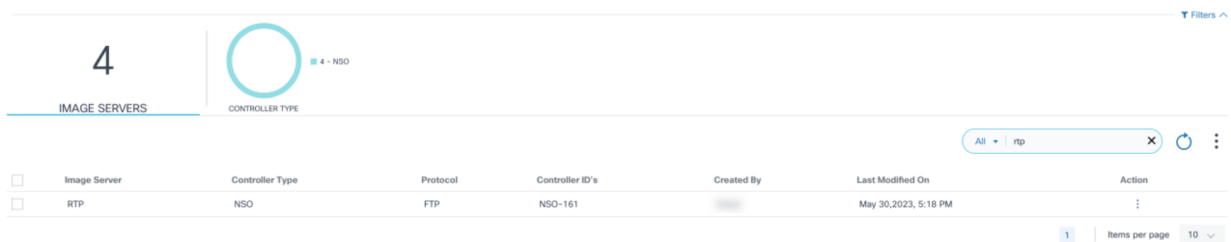
- 控制器类型:当前镜像文件服务器适用的控制器类型

 注意：仅支持NSO、直接到设备、CNC和ANSIBLE。

- 控制器实例:一个或多个适用的控制器实例，基于它们管理的设备，应使用给定的映像存储库服务器来复制映像
- 用户名：用于访问存储库中的映像文件的自定义凭据

6. Click Create.系统随即会显示进度通知，然后会显示确认消息。

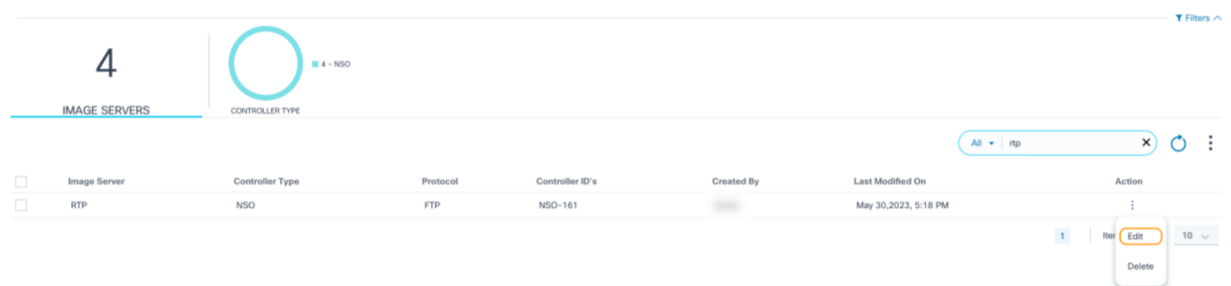
编辑镜像文件服务器详细信息



☐	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	⋮

镜像文件服务器搜索

7. 使用Search字段找到需要更新的分发服务器。



☐	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 Delete

编辑镜像文件服务器

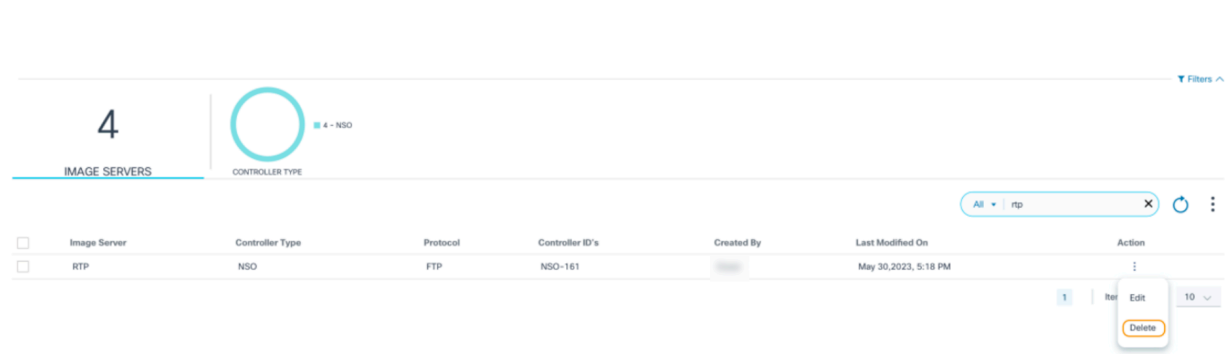
8. 从操作列中，选择更多选项图标> 编辑。

9. 更新所需的参数。

10. Click Save.系统随即会显示进度通知，然后会显示确认消息。

删除镜像文件服务器详细信息

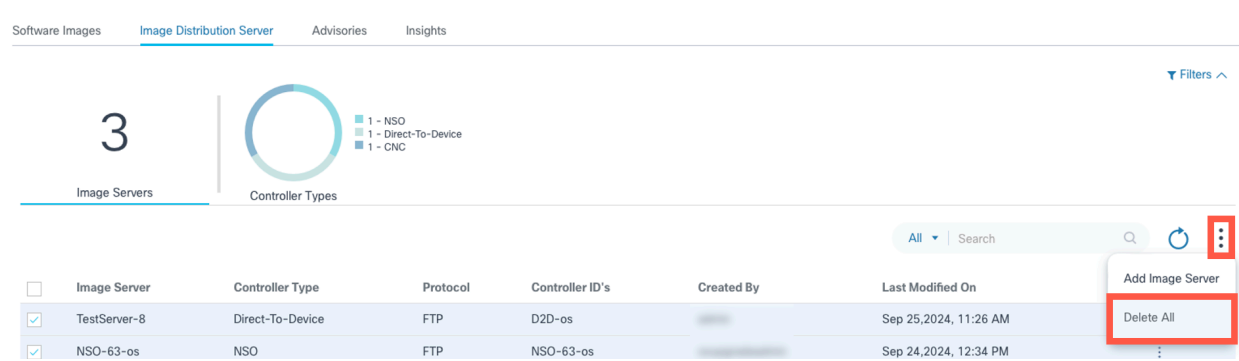
1. 使用Search过滤器找到所需的服务器。



删除镜像文件服务器

2. 从操作列中，选择更多选项图标> 删除以删除单个分发服务器。

或者



删除多个镜像文件服务器

选择所需的服务器，然后选择更多选项图标> 全部删除以删除多个分发服务器。

系统随即会显示确认。



Delete Image Server

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

Cancel

Ok

删除确认

3. Click OK.系统随即会显示进度通知，然后会显示确认消息。

软件见解

Software Insights可发现所有安全漏洞，如网络资产暴露的安全公告、漏洞和软件寿命终止等。它还为由Cisco Catalyst Center和NDFC控制器管理的设备型号提供软件建议。它允许管理员用户为网络资产选择建议的软件版本，并在建议可用时为设备型号创建一致性策略。

先决条件

- 启用适配器以获得见解。Cisco insights服务器的适配器，名为“Cisco-Insights-Adapter”，提供OOB。要与某些外部第三方Insights服务器集成，需要构建相应的适配器。有关详细信息，请参阅[BPA开发人员指南](#)中的配置Insights适配器。
- BPA系统需要互联网连接才能连接到思科云。
- 在继续同步操作之前，验证client_id和client_secret是否处于适配器配置中。
- 如果需要，可以按照以下步骤配置互联网代理。
- 对于IOS-XR OS类型，可根据需要在Reference Data Management(RefD)中完成自定义设备系列到型号的映射。有关自定义系列到型号映射的详细信息，请参阅[BPA开发人员指南](#)。
- BPA Kubernetes Pod需要访问互联网才能从思科收集建议、漏洞和寿命终止详细信息。如果BPA网络没有直接互联网访问，但可通过代理访问，请使用以下步骤使Kubernetes Pod使用互联网代理。

1. 使用实际代理地址更新脚本，代替<<http://proxy-domain.com:port>>。
2. 根据部署YAML或舵图中的每个Pod配置环境参数。
3. 通过在NO_PROXY或no_proxy配置中添加所有部署名称，在Kubernetes节点中执行以下脚本。
。

```
#!/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}')

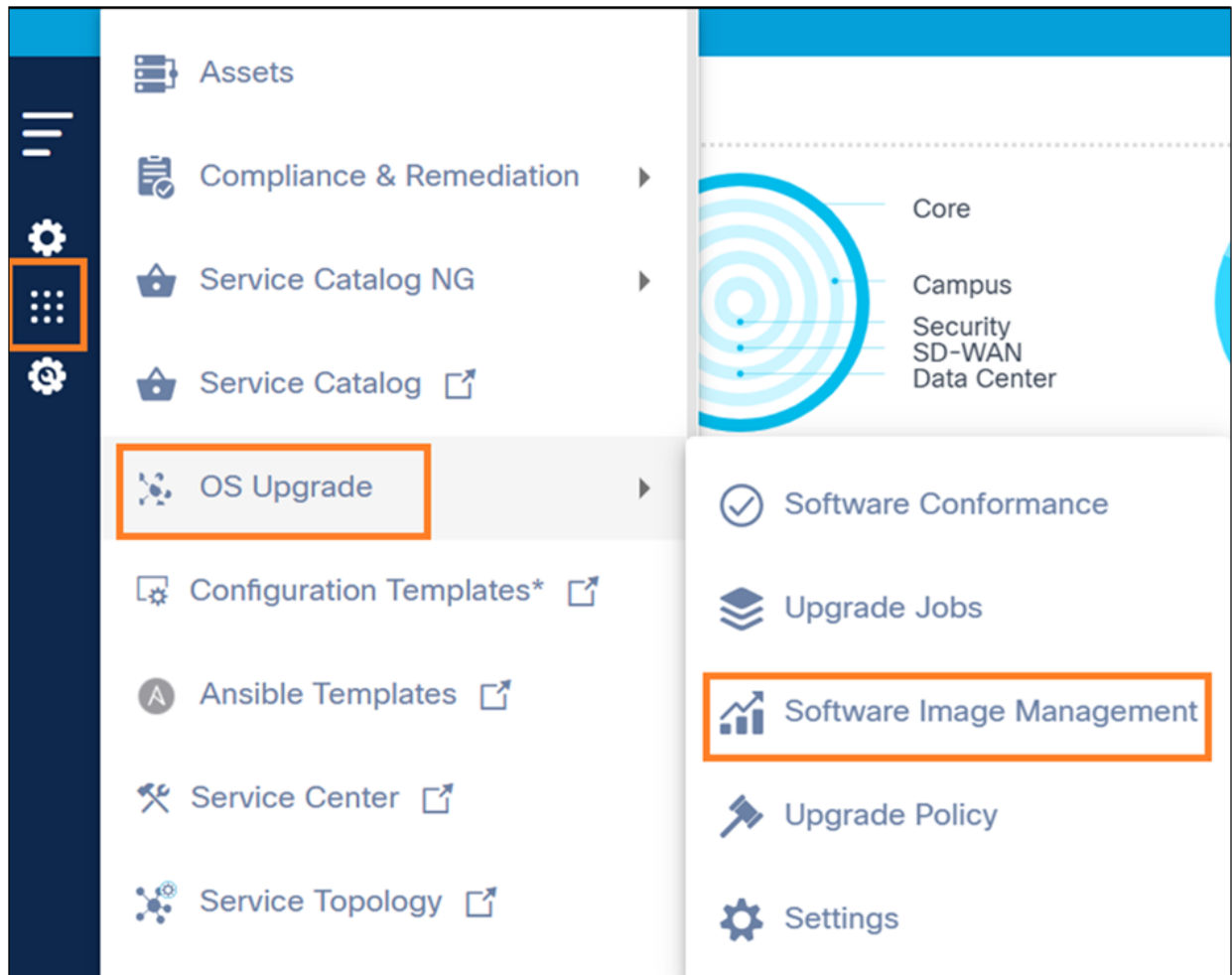
# Loop through each deployment and set the environment variables
for dp in $deployments;do
    kubectl set env deployment/$dp\
        HTTP_PROXY=$HTTP_PROXY \
        HTTPS_PROXY=$HTTPS_PROXY \
        http_proxy=$http_proxy \
        https_proxy=$https_proxy \
        NO_PROXY=$NO_PROXY \
        no_proxy=$no_proxy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

 **注意：**通过如上所述设置代理，insights适配器可访问思科网络并将所需的软件分析数据下载到BPA。要在不使用代理的情况下直接连接到任何其他外部Insights服务器，请确保将其添加到no_proxy变量。

将软件见解数据提取到BPA

要将软件见解数据同步到BPA，请执行以下操作：

1. 使用有权访问同步软件见解数据的凭据登录BPA。



软件映像管理导航

2. 从侧面板中选择OS Upgrade > Software Image Management。



“建议”选项卡

3. 单击Advisories选项卡。

同步以将软件见解提取到BPA



同步以将软件见解提取到BPA

4. 单击Sync。

这将发现与资产相关的所有安全建议、优先级错误、寿命终止公告和软件建议。安全建议和软件生

命周期终止日期取决于操作系统类型和软件版本。根据产品ID和软件版本确定优先级错误和软件建议。

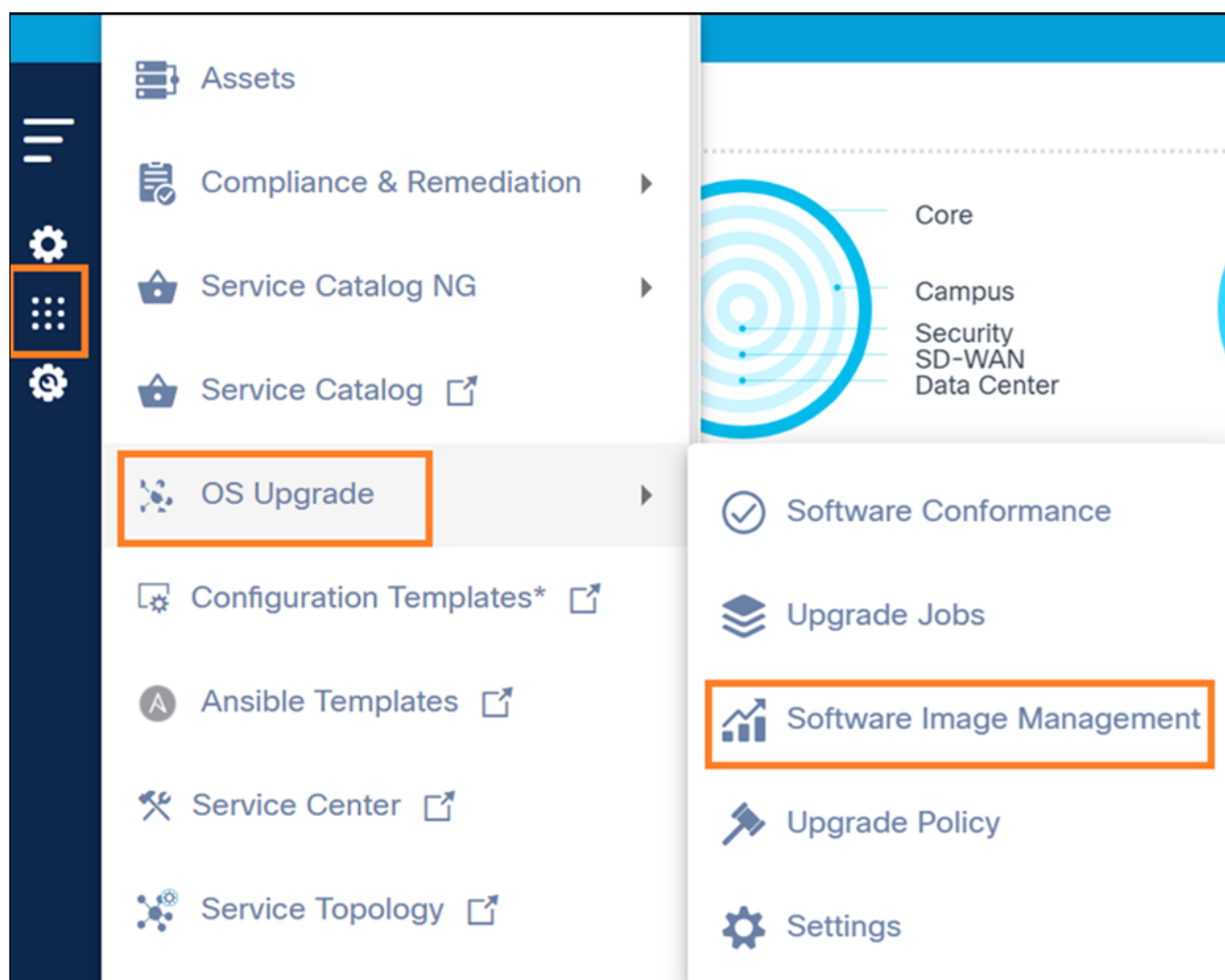
上次更新时间显示见解数据上次同步的日期和时间，Sync Status字段显示上次同步状态。

 注意：所有适用的建议、漏洞、版本注释和建议均通过“Cisco-Insights-Adapter”文件从思科云获取。

查看和管理安全建议

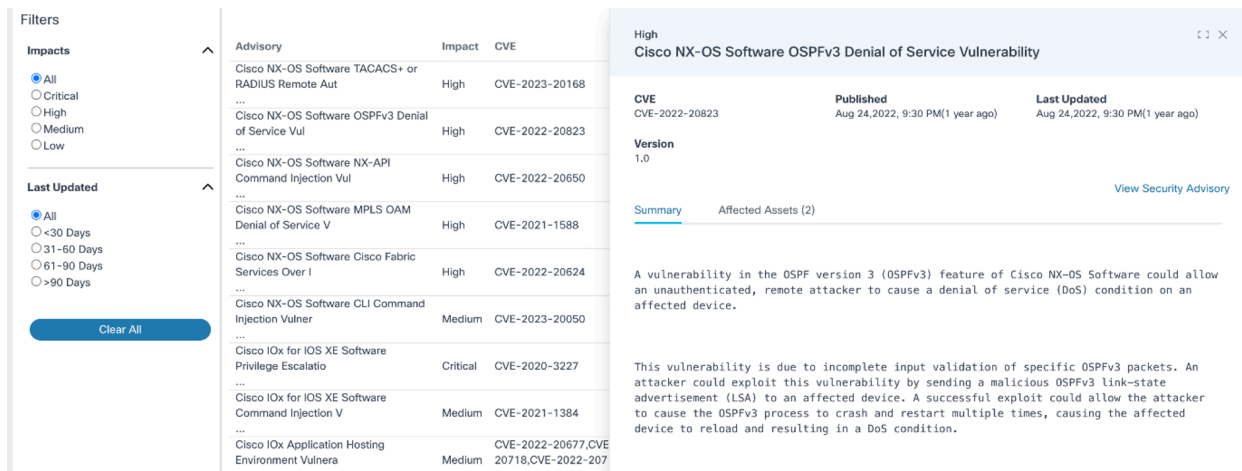
要访问“建议”(Advisories)页面：

1. 使用具有管理咨询访问权限的凭证登录到BPA。



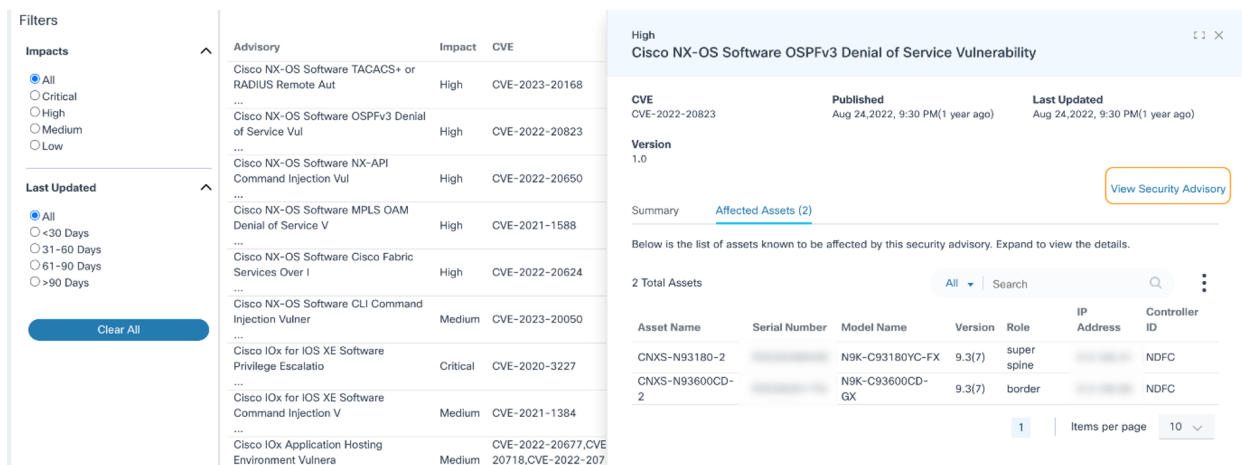
软件映像管理导航

2. 选择OS Upgrade > Software Image Management。



咨询详细信息视图

- 选择顾问行将打开顾问的详细信息视图，其中包括以下选项卡：
 - 摘要:显示所选顾问的摘要；默认显示
 - 受影响的资产：显示可能受影响的资产详细信息，如资产名称、序列号、型号、软件版本、IP地址和控制器ID;可以在此选项卡中对资产进行排序和搜索



查看安全建议

- 查看安全建议链接：导航到官方的“建议”页面

查看和管理优先级错误



选择优先级错误

按上一节所述打开Advisories页后，点击Priority Bugs选项卡。系统随即会显示Priority Bugs页面。

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 are determined by matching the product Id and SW version of the devices

Last Updated : Dec 20, 2023, 1:17:06 PM Sync Status : Completed Sync

Priority Bugs 73 Total

All Search

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 QSFP 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

1 2 3 ... 8 Next Items per page 10

优先级错误

Priority Bugs页上提供了以下选项：

- Severity过滤器，允许根据漏洞严重性进行过滤；默认情况下会选择全部
- Search过滤器可用于搜索Bug，包括以下独占搜索过滤器：
 - 全部：跨所有字段搜索
 - Bug ID:搜索具有指定漏洞ID的漏洞
 - 摘要:搜索摘要中存在特定关键字的错误
 - 产品版本：搜索与特定产品ID或软件版本相关的漏洞
- Refresh图标可用于刷新页面和清除所选过滤器
- 优先级错误显示在具有以下列的表中：
 - Bug ID
 - 严重级别:Bug严重性
 - 摘要:Bug的摘要详细信息
 - 产品版本:产品ID和软件版本受到影响
 - 可能受影响的资产：可能受Bug影响的资产数量
- 可通过点击除“可能受影响的资产”之外的任何列标题来执行排序

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 are determined by matching the product Id and SW version of the devices

Last Updated : Dec 20, 2023, 1:17:06 PM Sync Status : Completed Sync

Priority Bugs 73 Total

All Search

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 QSFP 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

1 2 3 ... 8 Next Items per page 10

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:	

Bug详细信息视图

- 点击Bug可打开该Bug的详细视图，其中包括：
 - “摘要”选项卡：显示Bug Severity、Description和Workcomediation详细信息

The screenshot displays the 'Bug Details View' for a specific security advisory. The left sidebar contains navigation tabs: 'Security Advisories', 'Priority Bugs', and 'Filters'. The 'Priority Bugs' tab is active, showing a list of bugs with columns for 'Bug ID', 'Severity', and 'Summary'. The main content area shows the details for 'Sev 6' (CSCwh39932), including a description of the issue: 'N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device'. Below this, the 'Affected Assets' tab is selected, showing a table of assets affected by the advisory. The table has columns for 'Asset Name', 'Serial Number', 'Model Name', 'Version', 'Role', 'IP Address', and 'Controller ID'. Two assets are listed: 'CNXS-N93360YC-2' and 'CNXS-N93360YC-1', both with model 'N9K-C93360YC-FX2' and version '10.2(5)'. The 'Role' is 'border' and the 'Controller ID' is 'NDFC-151'.

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-2019-11461
CSCwi43066	3	DOC: Update N9K SFlow documentation for 9.4.1
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 QSFP inter
CSCwi23447	2	Nexus 9504 unable to upgrade correctly fr
CSCwi26553	6	Web UI on 17.9.4 performance/response is
CSCwh99413	4	Console Logging for some XPATH Isco-IO
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset At

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

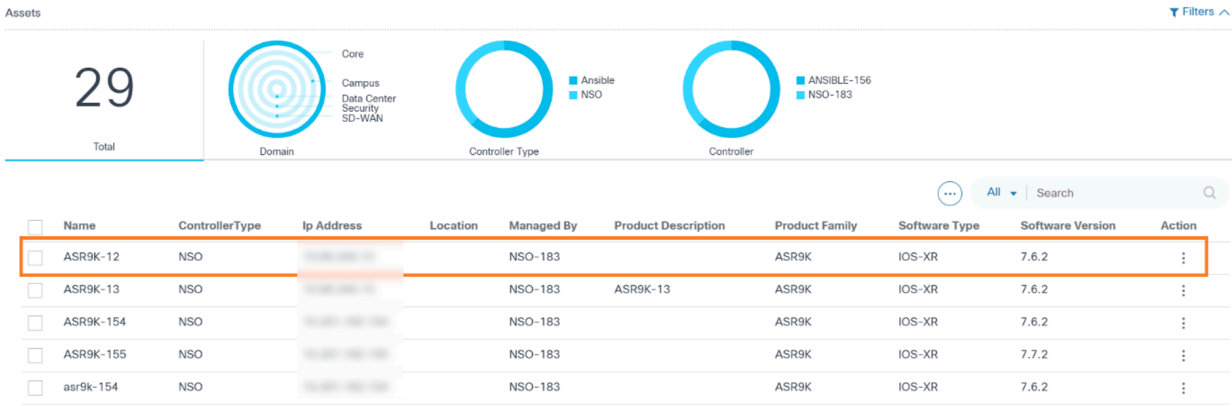
受影响的资产选项卡

- 受影响的资产选项卡：显示所有可能受影响的资产详细信息，例如资产名称、序列号、型号、软件版本、IP地址和控制器ID;可以在此选项卡中对资产进行排序和搜索

This screenshot is identical to the one above, showing the 'Bug Details View' for 'Sev 6' (CSCwh39932). It highlights the 'Affected Assets' tab, which lists two assets: 'CNXS-N93360YC-2' and 'CNXS-N93360YC-1'. Both assets are N9K-C93360YC-FX2 models running version 10.2(5), with a role of 'border' and controller ID 'NDFC-151'.

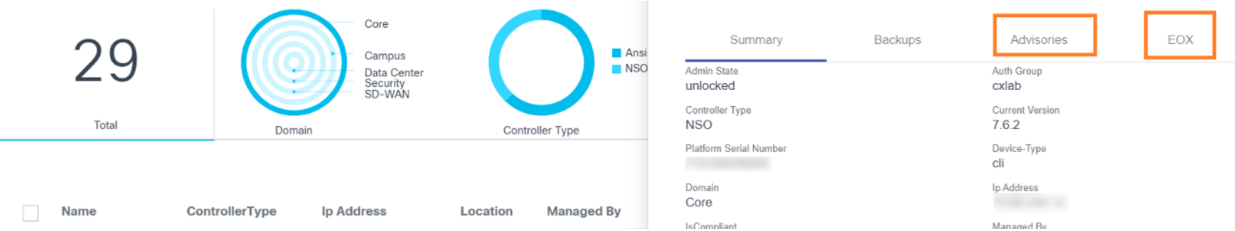
查看优先级错误

- 查看优先级错误(View Priority Bugs)链接：导航至正式的漏洞搜索工具



资产

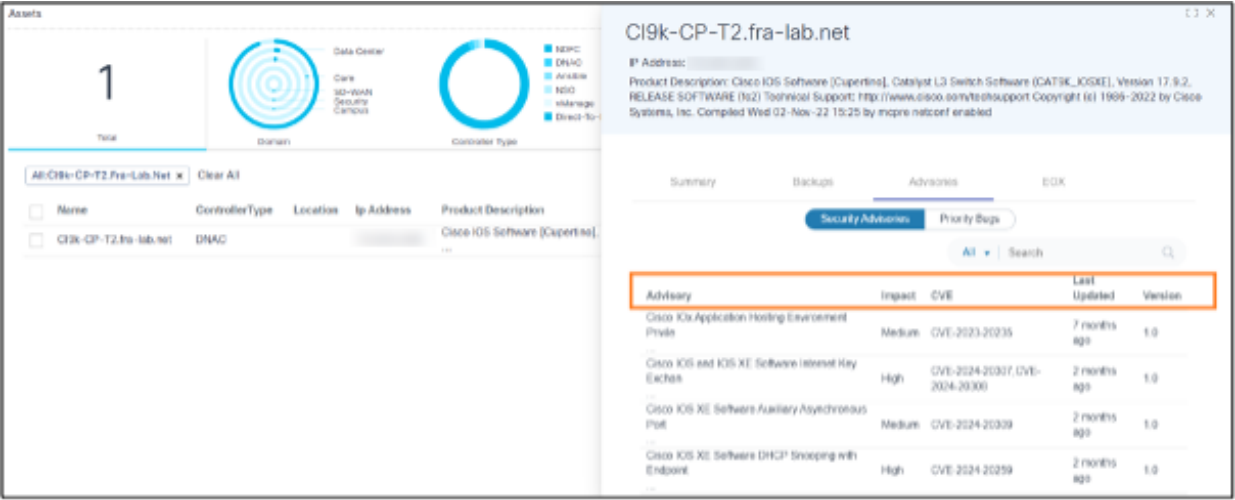
在Asset Manager中，用户可以查看所有资产的列表。选择任何资产时，面板会显示资产级别信息，其中包括按两个选项卡组织的资产软件漏洞详细信息：建议和EOX。



建议和EOX

Advisories选项卡包含两个子选项卡：Security Advisories和Priority Bugs。有关这些选项卡的更多详细信息在下面的部分中提供。

Security Advisories



所选资产的安全建议

在Security Advisories子选项卡上，用户可以查看影响所选资产的所有安全建议。安全建议表中的列包括Advisories、Impact、CVE、Last Updated和Version。

Assets

1

Total

Domain

Controller Type

All: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:

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

安全建议搜索

Assets

1

Total

Domain

Controller Type

All: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:

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

安全建议搜索 — 影响选项

用户可根据Advisories、Impact、CVE、Last Updated和Version列中的值搜索建议。分页允许用户在页面之间导航。

优先级错误

Assets

1

Total

Domain

Controller Type

All: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:

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

影响选定资产的优先级漏洞

在Priority Bugs子选项卡上，用户可以访问影响给定资产的所有优先级漏洞。此选项卡中的列包括Bug ID、Severity和Summary。

Assets

1

Total

Domain

Data Center

Core

SD-WAN

Security Campus

Controller Type

NDPC

DNAC

Ansible

NSO

vManage

Direct-To

All: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:

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

9800

x

Bug ID	Severity	Summary
CSCwe10941	6	9800: add SNMP OIDs
CSCwe10951	6	9800: align certain IOS-XE OIDs with the same OID

1

Items per page

10

按摘要搜索优先级错误

Assets

1

Total

Domain

Data Center

Core

SD-WAN

Security Campus

Controller Type

NDPC

DNAC

Ansible

NSO

vManage

Direct-To

All: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:

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

Severity

6

x

Bug ID	Severity	Summary
CSCwe36940	6	ENR: ability to advertise /32 and /31 routes for
CSCwe10941	6	9800: add SNMP OIDs
CSCwe10951	6	9800: align certain IOS-XE OIDs with the same OID

1

Items per page

10

按严重性搜索优先级错误

用户可根据Bug ID、Severity和Summary列中的值搜索优先级漏洞。分页便于在页面之间轻松导航。

EOX

CI9k-CP-T1.fra-lab.net

IP Address:

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选项卡

EOX选项卡显示特定于资产的软件寿命终止数据，包括三个重要日期：

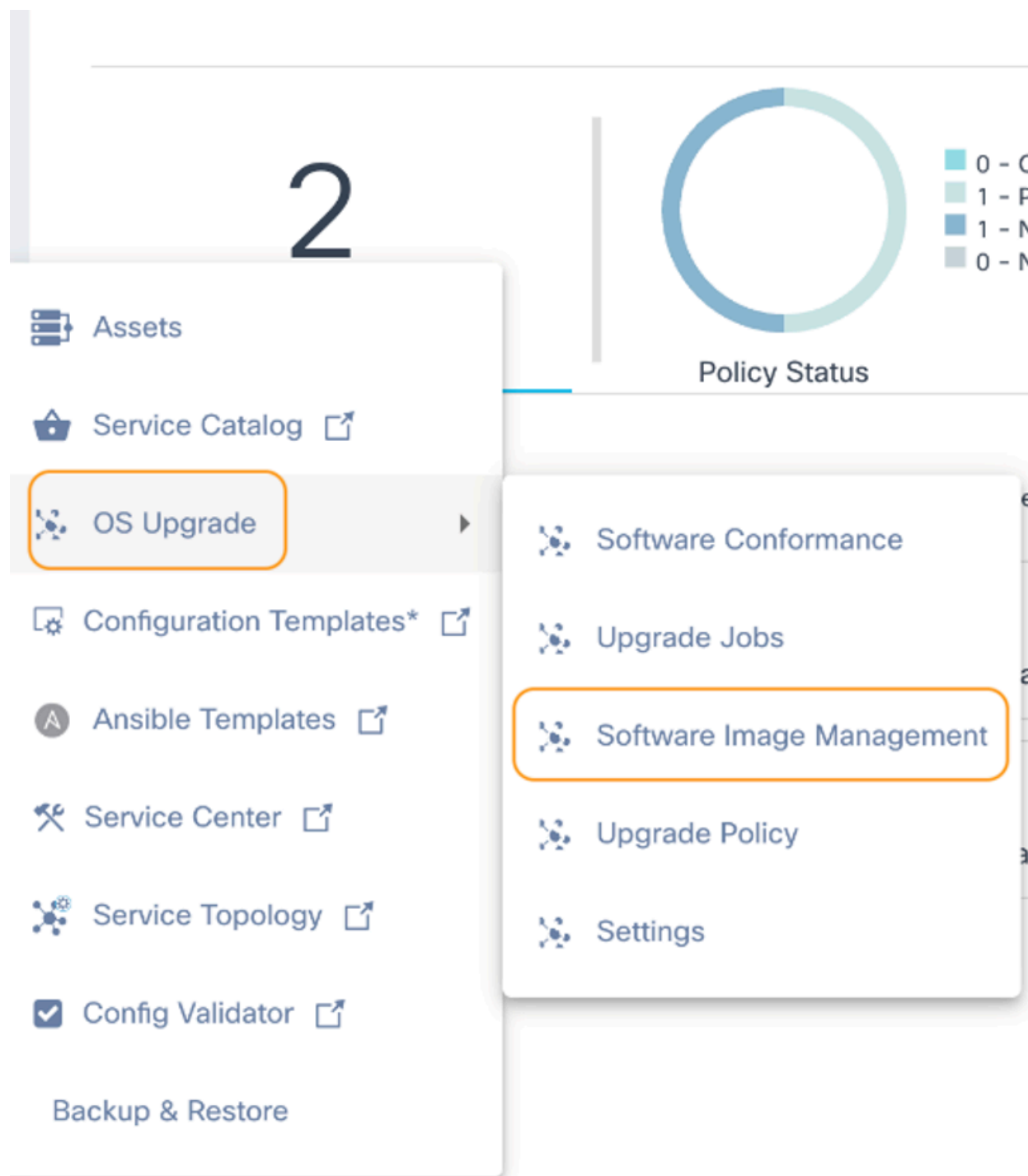
- 软件维护结束
- 安全支持终止
- 最后支持日期

查看软件见解

Software Insights为Cisco Catalyst Center和NDFC控制器管理的设备型号提供软件建议，允许管理员用户为设备型号创建一致性策略（如果建议可用）。

要访问Software Insights:

1. 使用具有对Insights管理访问权限的凭证登录到BPA。



软件映像管理

2. 从侧面板中选择OS Upgrade > Software Image Management。

Software Images

Image Distribution Server

Advisories

Insights

Filters

Suggestions

All

No

Yes

Clear All

24 Total Device Models

All

Search

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选项卡

3. 单击Insights选项卡。

Insights选项卡包含以下内容：

- 一种过滤器，允许用户根据建议过滤数据。默认情况下会选择所有。
 - 是过滤设备型号的数据并提供建议
 - 没有过滤设备型号的数据，无建议

Software Images

Image Distribution Server

Advisories

Insights

Filters

Suggestions

☒ All

☐ No

☐ Yes

Clear All

29 Total Device Models

All

Search

Device Model

Product Family

Software Type

Current Releases

Selected Release

Assets

Suggest

Export to CSV

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

导出至CSV

- More Options图标提供Export to CSV选项以导出页面中显示的数据
 - Refresh图标用于刷新页面并清除所选过滤器
 - Search过滤器用于搜索数据，包括以下独占搜索过滤器：
 - 全部:在所有列中进行搜索(例如Device Model、Product Family和Software Type)
 - 设备型号:搜索具有特定设备型号名称的数据
 - 产品系列搜索具有特定产品系列名称的数据
 - 软件类型:搜索具有特定软件类型名称的数据
- 现有设备型号显示如下：
 - 设备型号:设备型号的名称
 - 产品系列：设备型号所属的产品系列的名称
 - 软件类型:设备型号所属的软件类型的名称

- 当前版本:设备型号资产中当前存在的唯一软件版本的列表
- 所选版本:建议版本已根据思科提供的建议选择为可选版本
- 资产:设备型号的资产管理器中存在的资产数量
- 建议:对于设备型号可用的任何建议，显示Yes或No

Software ImagesImage Distribution ServerAdvisoriesInsights

Filters

Suggestions

- All
- No
- Yes

Clear All

24 Total Device Models

AllSearch

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	⋮

Prev123NextItems per page10

查看建议导航

- 操作：通过More Options图标(例如View Suggestions和View Assets)提供特定于行的操作



注意：如果设备型号没有任何建议，则禁用“查看建议”。

查看和选择供应商建议的软件版本

Software ImagesImage Distribution ServerAdvisoriesInsights

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

SuggestionsAffected Assets (1)

② Select one of the Cisco suggested software releases as the standard or policy while taking into consideration known issues and any workaroundLast 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 sev1 0 sev2 1 sev3 4 sev4 1 sev5 0 sev6 1	Future Exposure : 7 sev1 0 sev2 1 sev3 4 sev4 1 sev5 0 sev6 1
Security Advisories	Current Exposure : 0 Critical 0 High 0 Informational 0 Low 0 Medium 0	Future Exposure : 0 Critical 0 High 0 Informational 0 Low 0 Medium 0
EoX	End of SW Maintenance Nov 30, 2023 End of Security Support Feb 28, 2025 Last date of Support Aug 31, 2025	End of SW Maintenance Nov 30, 2023 End of Security Support Feb 28, 2025 Last date of Support Aug 31, 2025

“建议”选项卡

从操作列中选择更多选项图标> 查看建议，会打开一个侧面板，其中包含所有深入分析详细信息。Suggestions选项卡包含所选设备型号的当前版本和建议的版本详细信息；设备型号可能包含多个建议。以下数据可用：

- 版本和日期:如果思科云中提供了当前版本和建议版本的版本、日期和注释详细信息；如果资产属于多个版本，则所有适用版本在当前列中显示为逗号分隔值
- 创建一致性策略:允许管理员为设备角色为Any的特定版本创建一致性策略

 注意：只有NDFC控制器设备型号才支持创建一致性策略

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

删除策略选项

 注意：如果设备型号已存在任何策略，则会显示错误。如果不存在任何策略，则会在Enabled状态下创建策略。如果策略是通过Insights创建的，则用户可以选择删除策略。

- 错误:显示每个版本的整合漏洞计数
- 安全性建议:显示每个版本的整合建议计数
- EoX:显示每个版本的软件维护终止、安全支持终止以及支持终止日期

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

受影响的资产选项卡

从操作列中选择更多选项图标> 查看资产将打开一个侧面板，默认情况下会显示受影响的资产选项卡。“受影响的资产”选项卡在“资产名称”、“序列号”、“型号名称”、“软件版本”、“IP地址”和“控制器ID”等列中显示潜在受影响的资产详细信息。可以在此选项卡中对资源进行排序和搜索。

确定需要软件升级的设备

有关详细信息，请参阅[软件一致性](#)。

软件一致性

软件一致性帮助确定网络中不符合目标软件版本的资产。验证基于用于定义软件合规意图的策略和规则。这些策略可以按计划或按需执行。成功执行一致性策略后，即会获得一致性结果，该结果提供适用资产的状态。一致性范围取决于各种标准，例如设备角色、管理控制器实例等。

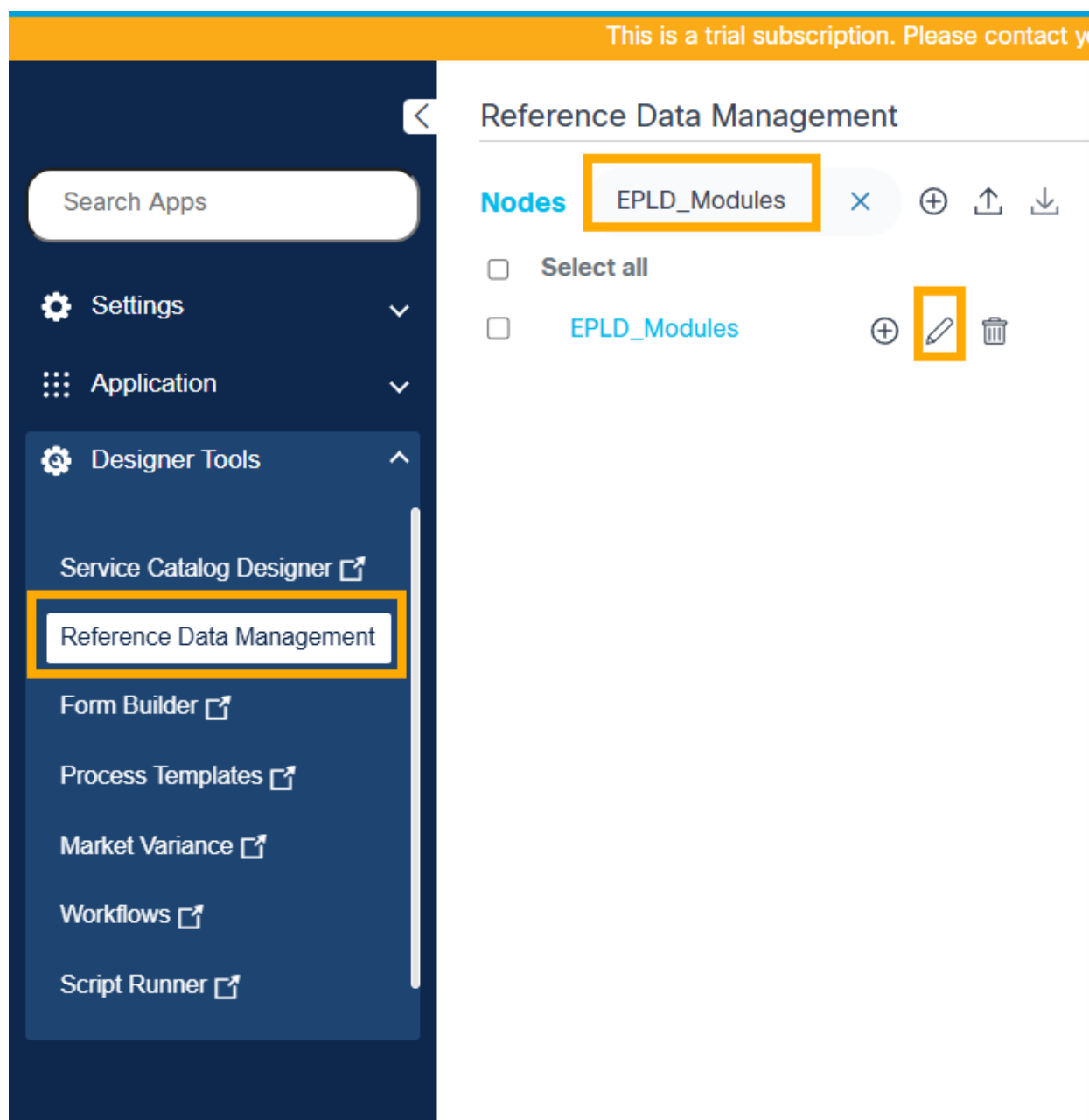
先决条件

- Cisco Catalyst Center、vManage、NDFC和FMC等控制器的软件映像必须同步。有关详细信息，请参阅[同步软件映像元数据](#)。
- 必须添加NSO、CNC、Direct-to-Device和ANSIBLE等控制器的必需软件映像元数据。有关详细信息，请参阅[添加软件映像元数据](#)。
- 用户必须有权访问RefD应用程序以管理EPLD模块数据。
- 所需版本的EPLD模块信息应预填充到RefD应用程序中
- 如果EPLD模块信息不可用OOB，用户必须在RefD应用程序中手动添加

在引用数据管理应用程序中创建EPLD模块数据

创建一致性策略之前，请在RefD应用程序中创建EPLD模块参考数据。RefD应用包括Nexus软件版本v10.2(8)和v10.4(5)的EPLD模块信息。对于其他设备版本，必须在RefD应用中手动添加EPLD型号信息。

完成以下步骤，将其他版本添加到EPLD模块元数据中：



参考数据管理

1. 导航到Reference Data Management应用程序并搜索“EPLD_Modules”。
2. 选择“EPLD_Modules”文件并选择Edit图标。

编辑节点

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 x Cancel Save Upload Download

编辑节点

3. 通过附加具有以下结构的新条目来添加新的发行版EPLD模块元数据：

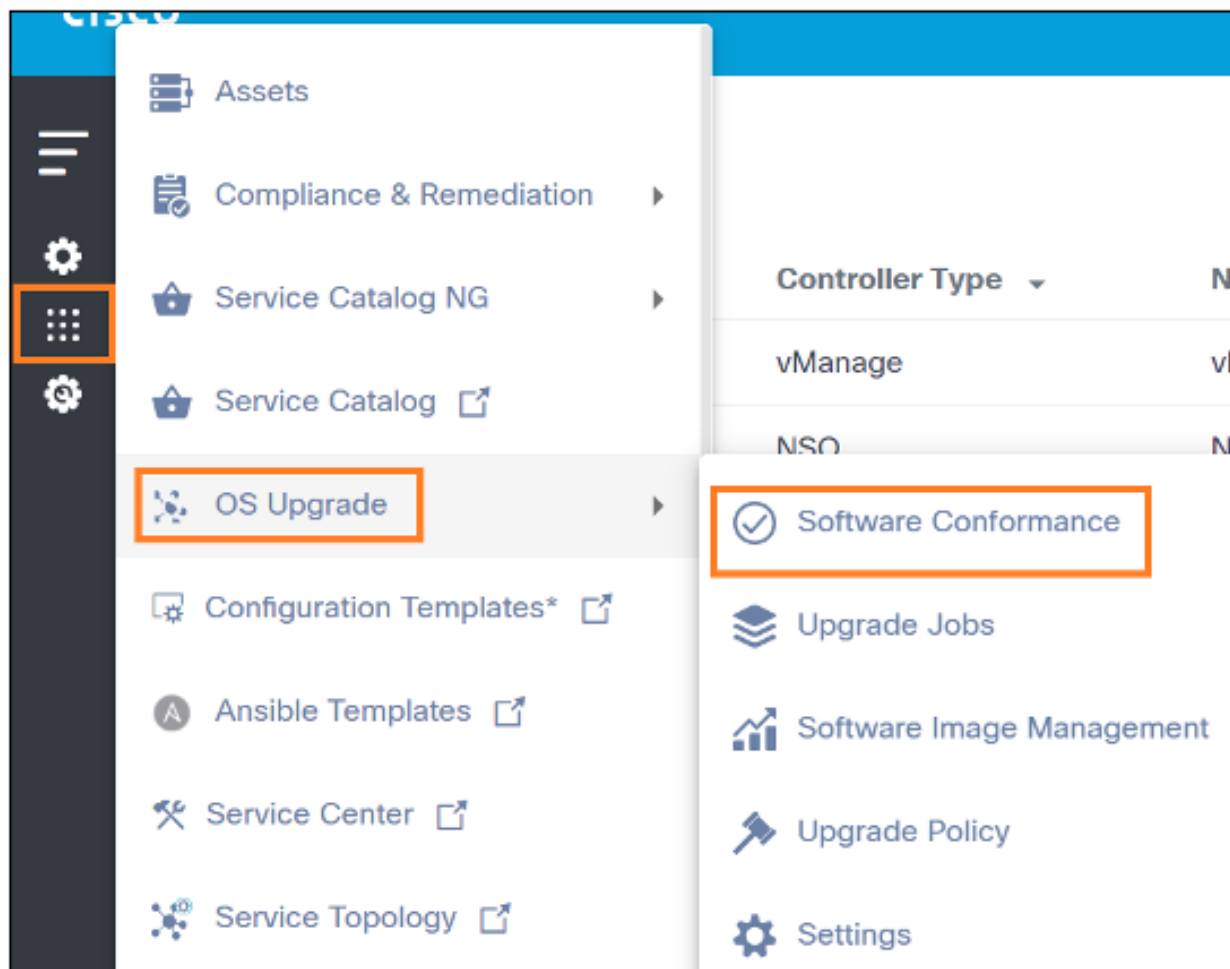
structure:

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

4. 单击Save并验证可在一致性策略中选择的新EPLD模块元数据。预填充受支持版本的EPLD数据。

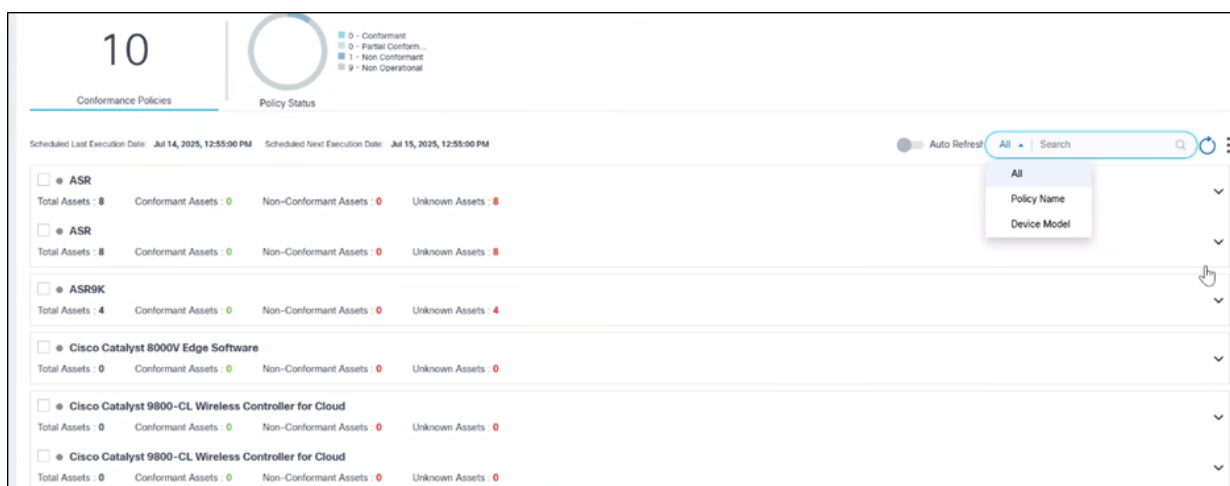
查看和管理软件一致性

1. 使用有权访问软件一致性的凭据登录到BPA。



软件一致性导航

2. 选择OS Upgrade > Software Conformance。系统随即会显示Software Conformance页面。



软件一致性

Software Conformance页包含以下内容：

- 顶部显示的分析部分，提供以下功能：

- 系统中存在的符合性策略的总数
- 根据以下条件过滤的Policy Status快速过滤器：
 - 一致性:具有指定型号的所有BPA管理的设备都在定义的软件版本上
 - 部分一致性:具有指定型号的一些BPA管理的设备位于定义的软件版本上；其余设备处于不同的软件版本
 - 不符合项:与给定软件版本相比，具有指定型号的所有BPA受管设备都处于不同的软件版本上
 - 非操作:根据策略中指定的设备型号，找不到适用的设备
- Scheduled Last Execution Date和Scheduled Next Execution Date，指明之前执行的计划一致性检查的日期和时间以及下一个计划一致性检查用于所有策略的时间
- Search字段，用于根据设备型号、策略名称或所有内容过滤策略；用户可以选择All以跨所有参数搜索
- Auto Refresh切换允许在启用时按用户定义的间隔自动刷新正在进行的一致性策略。要启用切换，请执行以下操作：
 - 转到OS Upgrade > Settings以更改刷新闻隔
 - 使用所需值修改自动刷新闻隔
 - 点击保存
- 启用Auto Refresh切换时，软件一致性策略控制面板会以新的间隔刷新
- 刷新图标可刷新页面并清除所选过滤器
- 提供以下选项的More选项图标：
 - 创建策略
 - 运行所有策略
 - 删除多个所选策略

策略根据设备型号进行分组，并以可扩展面板形式显示，以便在由不同控制器管理的设备型号之间提供单一视图。



合规性策略的折叠视图

在折叠视图中，面板显示设备模型和快速统计信息，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

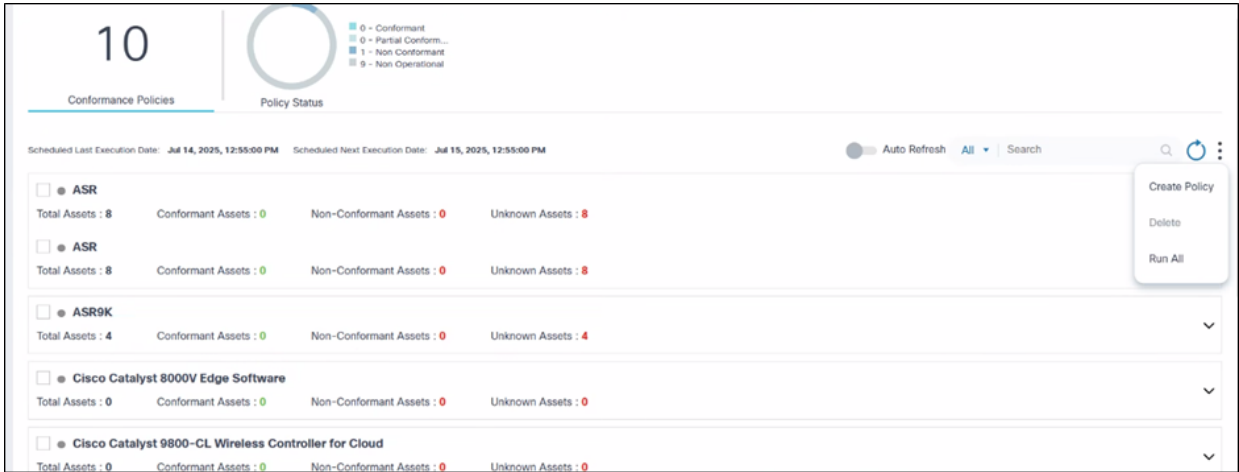
合规策略的扩展视图

在展开视图中，将显示与设备型号相关的所有策略。对于每个策略，可以通过从Action列中选择

More Options图标执行其他操作，包括Run、Edit Policy、View Results等。

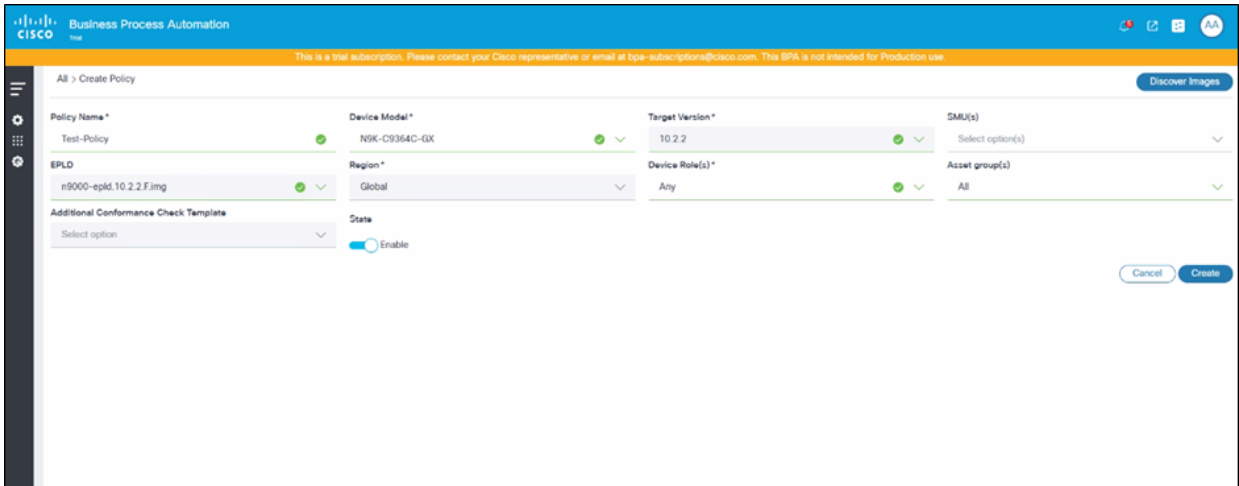
创建软件一致性策略

- 1. 使用具有软件一致性管理访问权限的凭证登录到BPA。
- 2. 选择OS Upgrade > Software Conformance。系统随即会显示Software Conformance页面。



创建策略

- 3. 选择More Options图标> Create Policy。



创建策略表单

- 4. 在Policy Name、Device Model(s)、Target Version、SMU、EPLD、Device Role、Asset Groups和Additional Conformance Check Template字段中输入信息。SMU、资产组和其他一致性检查模板是可选字段。

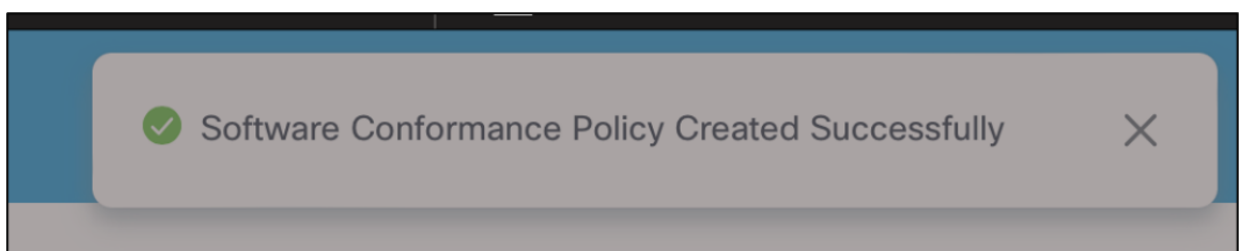
注意：现在，用户可以在“创建合规性策略”表单中选择多个设备型号。

 注意：软件一致性框架可以根据管理设备的特定模型、角色或控制器实例对基本OS版本和SMU补丁运行一致性检查。如果需要任何其他自定义检查，可以使用所需的命令和验证规则创建流程模板，这些命令和验证规则可以映射到其他一致性检查模板字段。

5. Click Create.系统随即会显示确认。

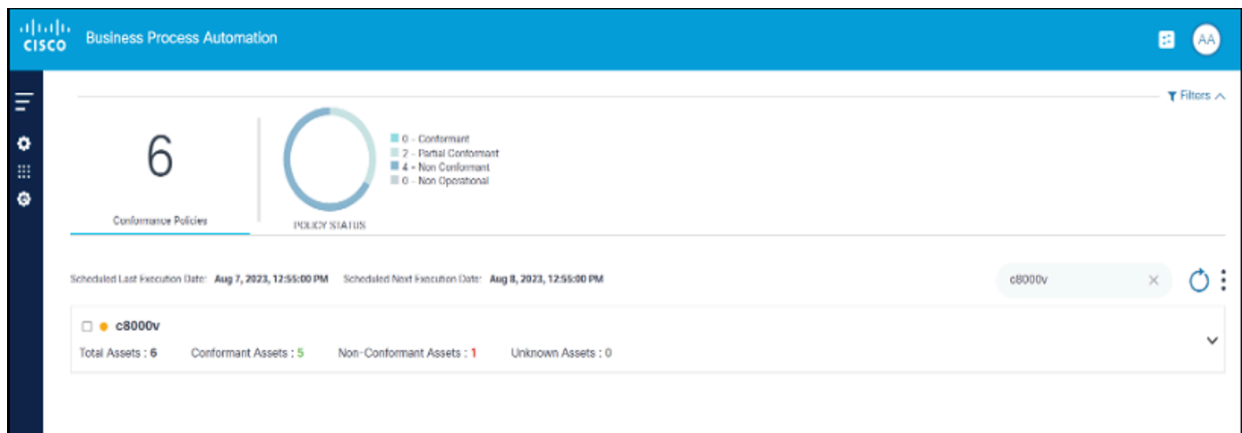
 注意：下面列出了一些注意事项。

- 使用案例：管理员可以为所选设备型号灵活地创建具有不同设备角色的多个策略。可以在单个策略中选择多个角色。
- 如果从Device Role(s)下拉列表中选择了Any，则所有其他设备角色（例如，Access、Core等）都将被禁用。如果选择了任何其他设备角色，则禁用Any。
- 对于由CNC、NSO、ANSIBLE和直接到设备等控制器管理的设备，Any角色(从Device Role(s)下拉列表中选择)可用于执行合规性检查，因为这些设备没有角色信息。
- 如果从FMC的设备角色下拉列表中选择了Any，则软件一致性在所有设备上执行，包括独立设备、控制设备和数据设备。
- 只有CNC、NSO、ANSIBLE、FMC、直接到设备和NDFC控制器支持SMU一致性和升级。
- 此版本仅支持Region下拉列表中的Global
- 用户可以从下拉列表中选择“资产组”。默认情况下会选择所有。用户可以选择一个或多个资产组。如果选择了特定资产组，则仅针对所选资产组的设备执行策略。
- 如果未显示Device Model、Target Version和SMU(s)字段的预期值，请单击Discover Images，然后重试。
- Device Model、Asset Group(s)和Role字段共同形成唯一策略；不允许重复策略。
- 只有当EPLD映像元数据可用于所选设备型号和目标版本时，EPLD字段才会填充值。
- Policy Name是唯一的，不允许重复的策略名称。



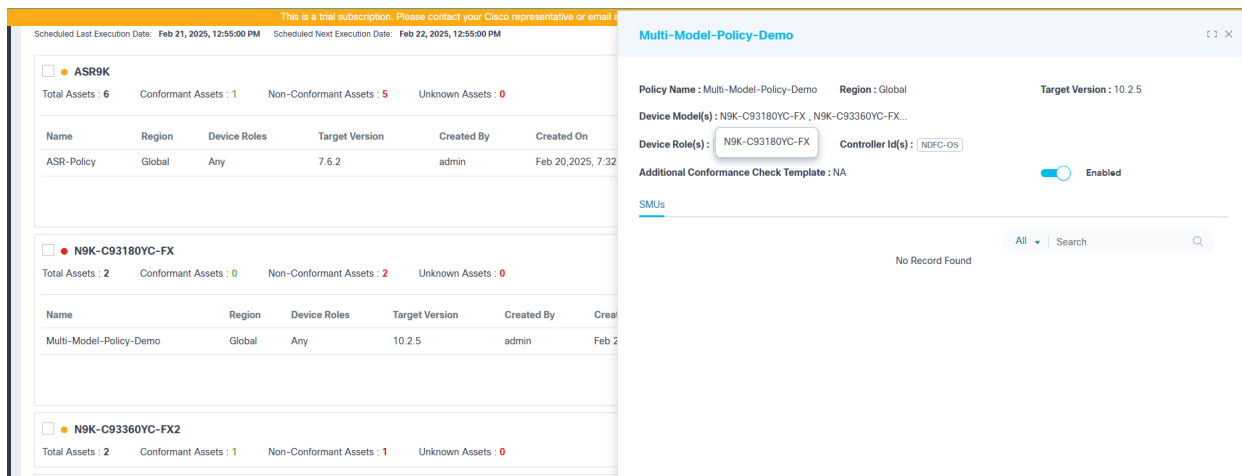
一致性策略创建确认

- 标记为OS Upgrade Next Generation（下一代）的流程模板显示在Additional Conformance Check Template字段中。



符合性策略的搜索结果

6. 通过在Search字段中输入设备型号找到创建的策略。

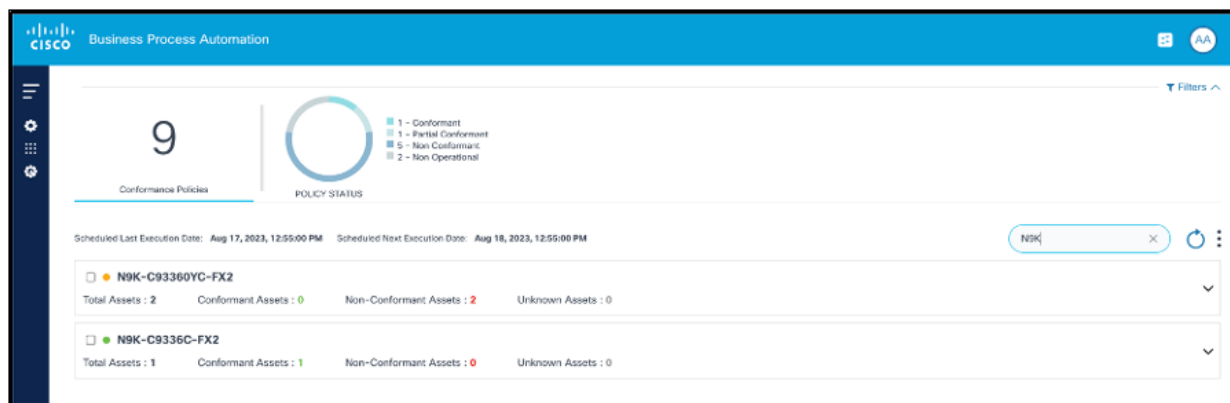


查看合规性策略

7. 单击Policy查看策略的详细信息视图。

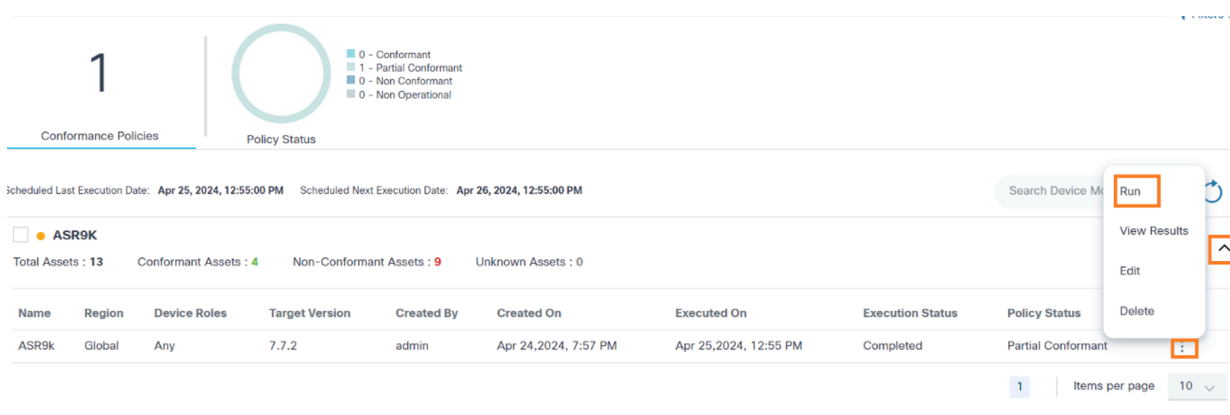
按需执行软件一致性检查

1. 使用具有执行访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Software Conformance。系统随即会显示Software Conformance页面。



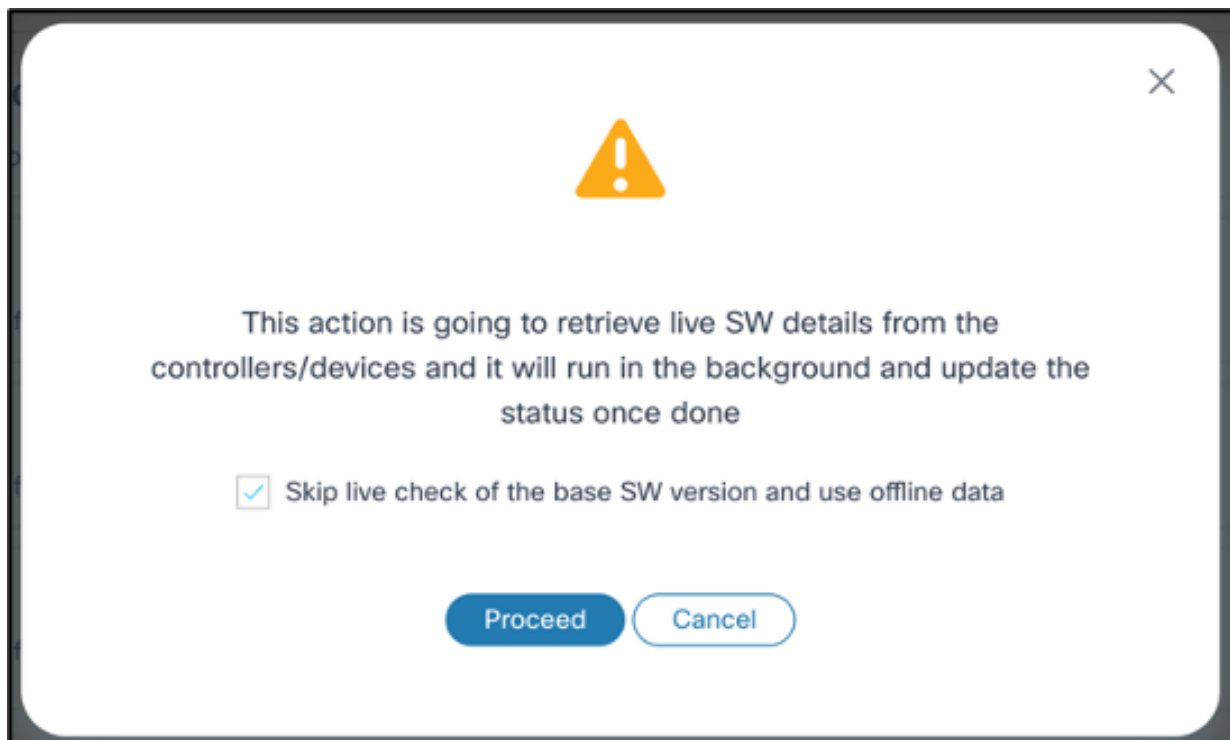
策略搜索

3. 使用Search字段找到要按需执行的策略。



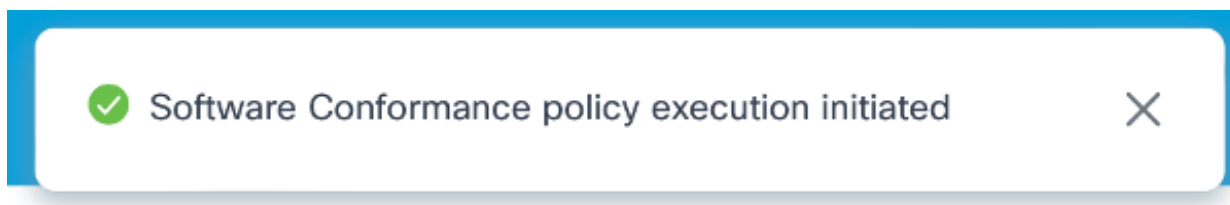
运行

4. 从策略的Action列中，选择More Options > Run。系统会显示确认消息，以验证是否应对设备执行实时资产检查。



运行合规性策略的确认

5. 如果在运行一致性检查之前需要实时资产同步，请清除Skip Live Check of the Base SW Version and use offline data复选框，然后单击Proceed。在这种情况下，一致性检查仅在同步后执行。通知将显示在右上角。



一致性策略执行通知



注意：下面列出了一些注意事项。

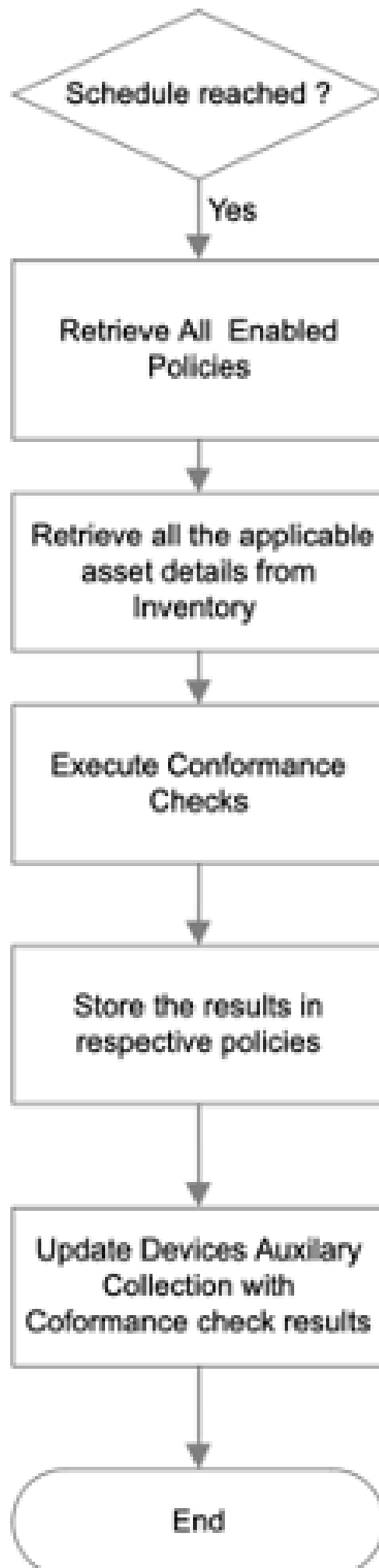
- 默认情况下，使用资产库存数据执行一致性检查。
- 在此过程中，如果清单或设备同步失败，相应的策略设备将标记为未知，并跳过SMU检查。
- 对于SMU，在执行一致性检查之前从设备检索实时数据，以检查是否选中了Skip Live Check of the Base SW Version and use offline data复选框。
- 当策略包括多个设备模型时，针对设备模型执行该策略会启动所有关联策略的执行。

安排执行软件一致性检查

可使用调度程序服务定期自动执行软件一致性检查。可以将计划的一致性检查配置为运行：

- 每天
- 一天两次
- 每周
- 一次

一旦达到计划，处于“已启用”状态的所有策略将自动执行，并且一致性结果将存储在各自的策略中。

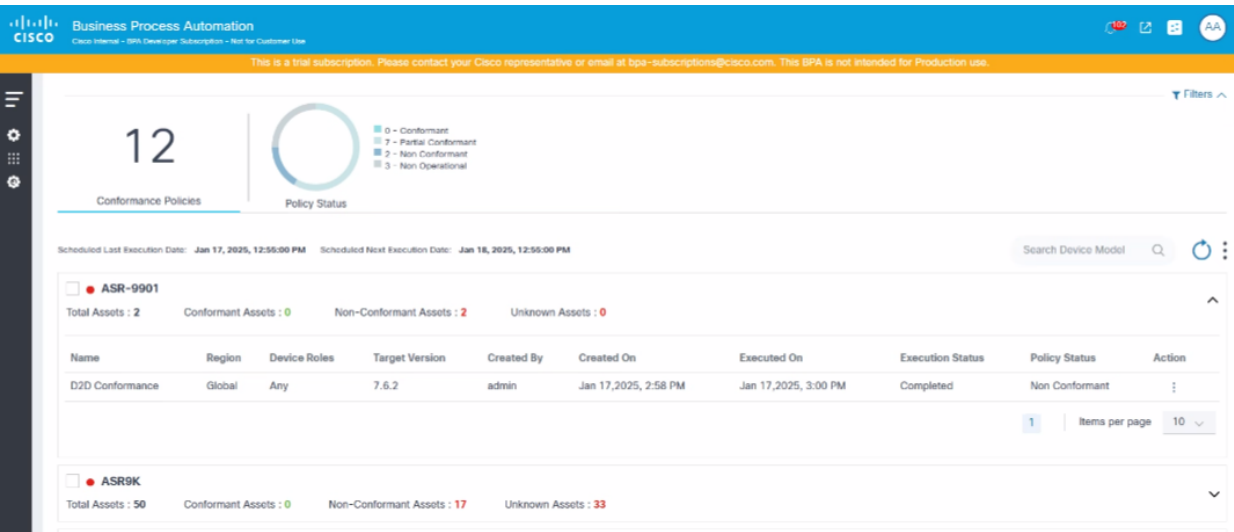


软件一致性检查调用流的计划执行

有关详细信息，请参阅[软件一致性](#)。

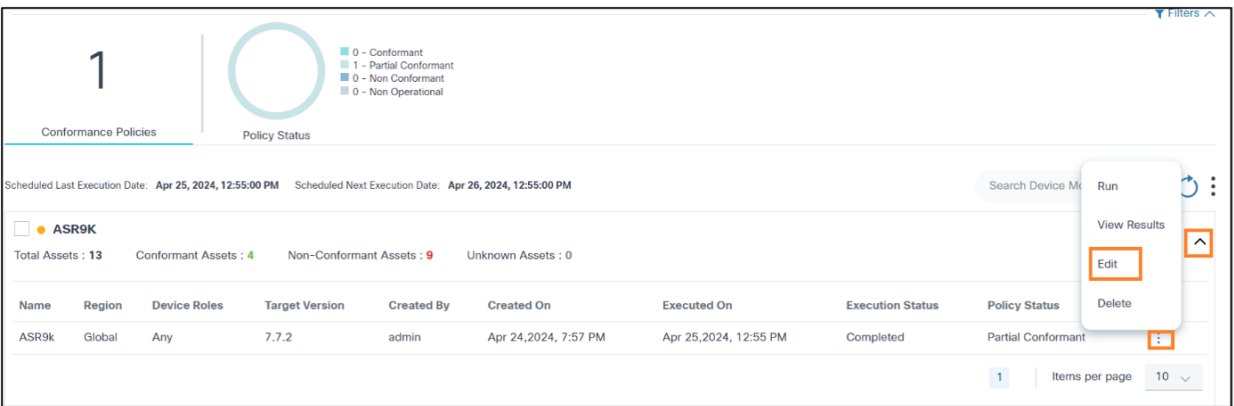
更新软件一致性策略

- 1. 使用具有软件一致性管理访问权限的凭证登录到BPA
- 2. 选择OS Upgrade > Software Conformance。系统随即会显示Software Conformance页面。



软件一致性

- 3. 使用Search字段查找所需的策略。



编辑

- 4. 从策略的Action列中，选择More Options图标> Edit。

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

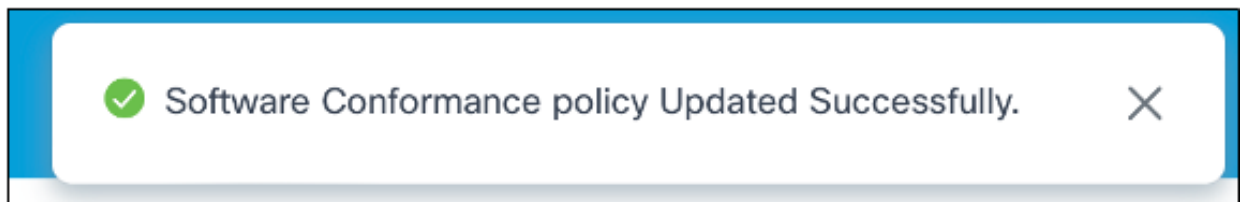
Policy Name*	Device Model*	Target Version*	SMU(s)
Multi-Model-Policy-Demo	N9K-C93180YC-FX, N9K-C93360YC-FX2	10.2.5	Select option(s)
Region*	Device Role(s)*	Controller ID(s)	Additional Conformance Check Template
Global	Any	NDFC-OS	Select option

State
☒ Enable

Cancel Save

编辑已填写详细信息的符合性策略

5. 根据需要编辑目标版本、SMU、设备角色、控制器ID、策略状态和其他一致性检查模板字段。
6. Click Save.系统随即会显示确认。



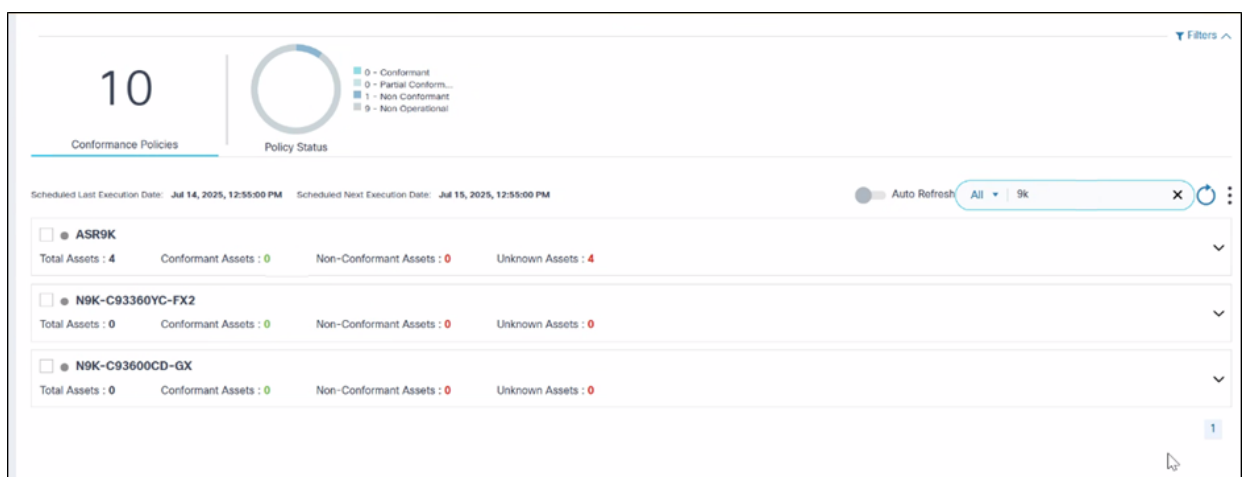
确认更新成功



注意：当软件一致性策略用于正在进行的升级作业时，无法编辑该策略。

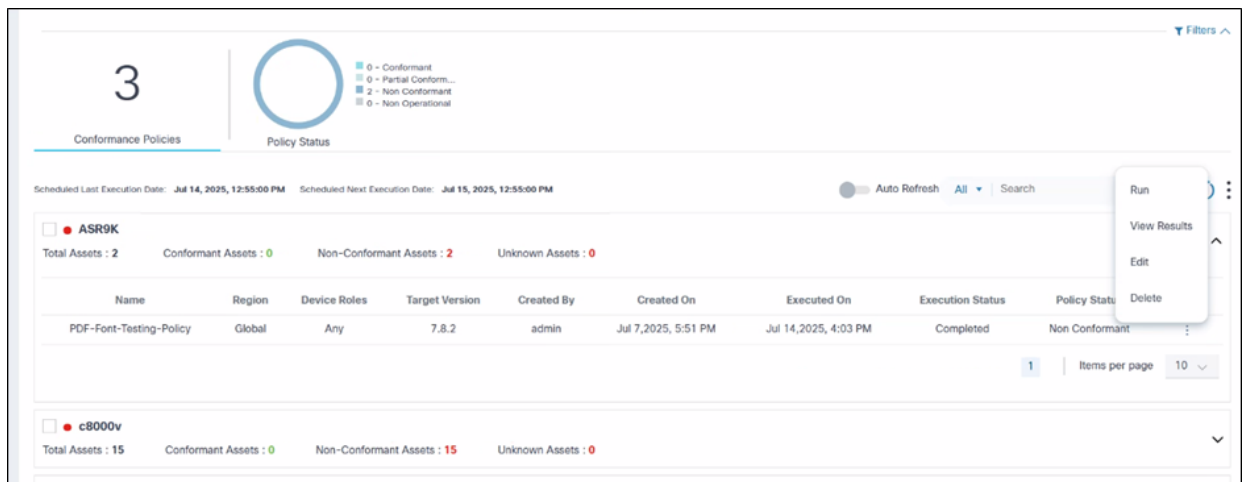
删除软件一致性策略

1. 使用具有管理访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Software Conformance。系统将显示Software Conformance页面。



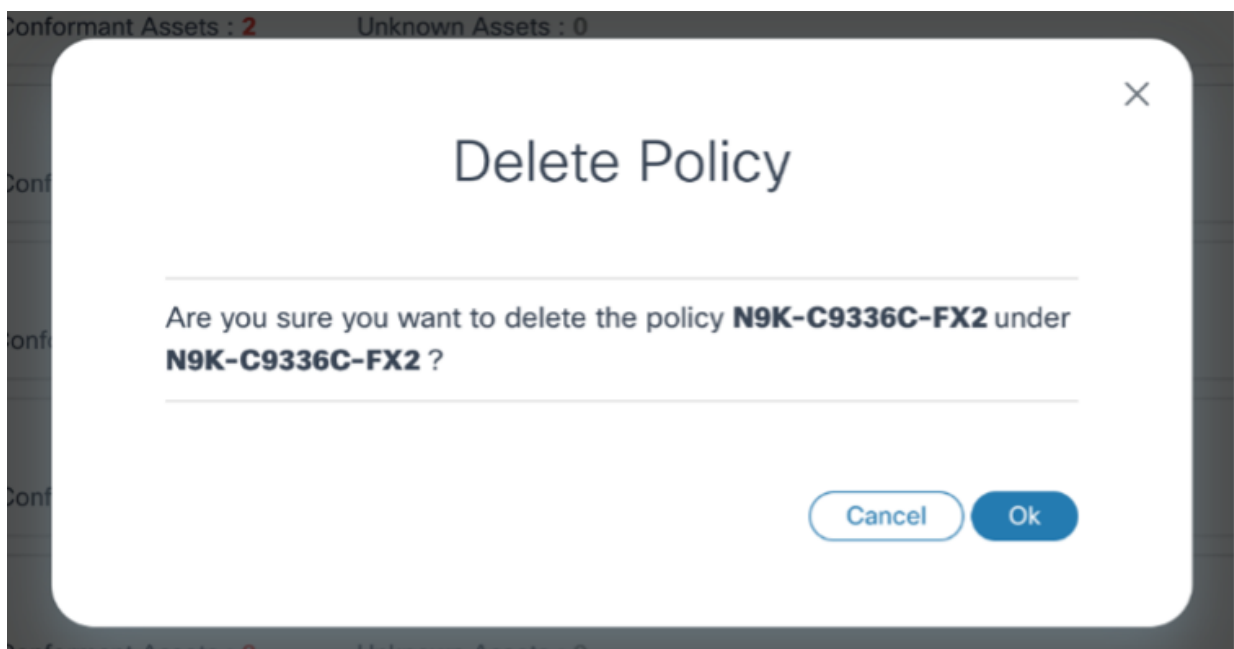
符合性策略的搜索结果

3. 使用Search字段查找所需的策略。

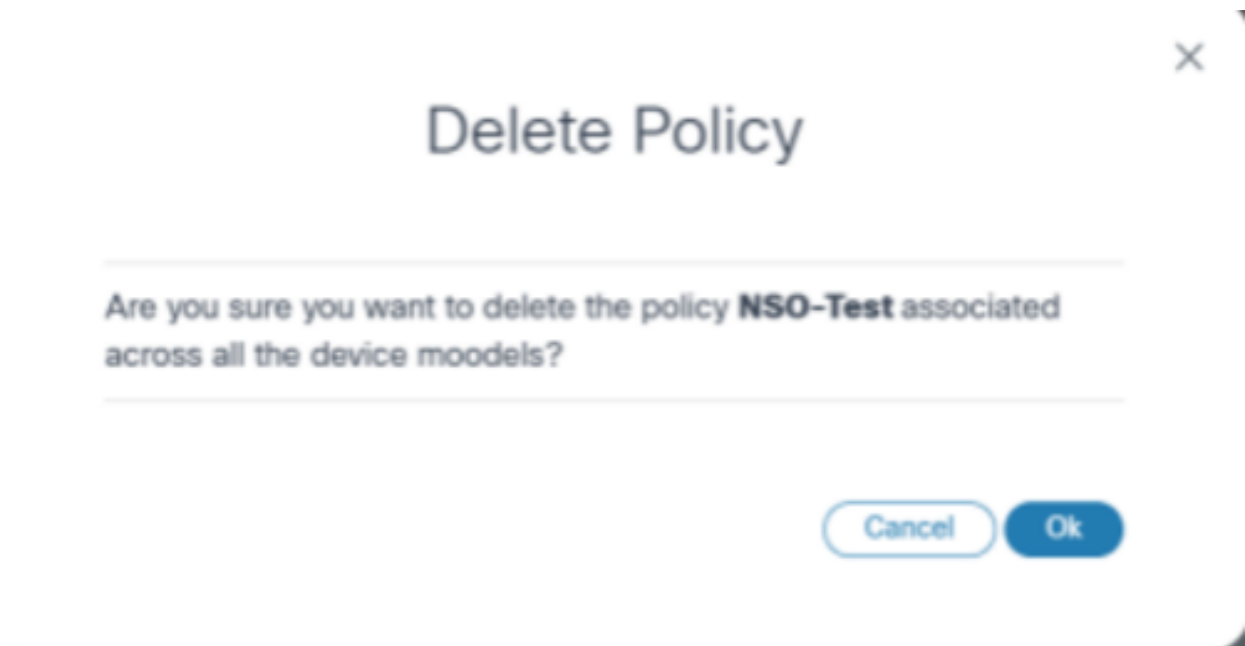


DELETE

4. 从策略的Action列中，选择More Options图标> Delete。确认窗口即会打开。



删除策略确认



删除策略确认 (如果策略与多个型号关联)

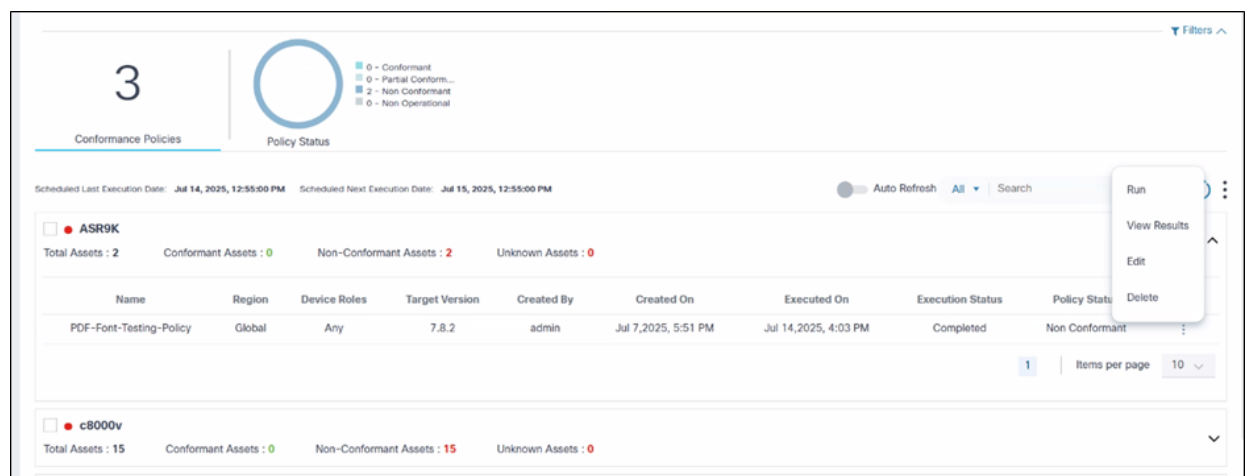
5. Click OK.策略即被删除。

 注意：下面列出了一些注意事项。

- 如果策略与多个设备型号关联，则删除策略会删除每个关联型号的所有相关策略。
- 当软件一致性策略用于正在进行的升级作业时，无法删除该策略。

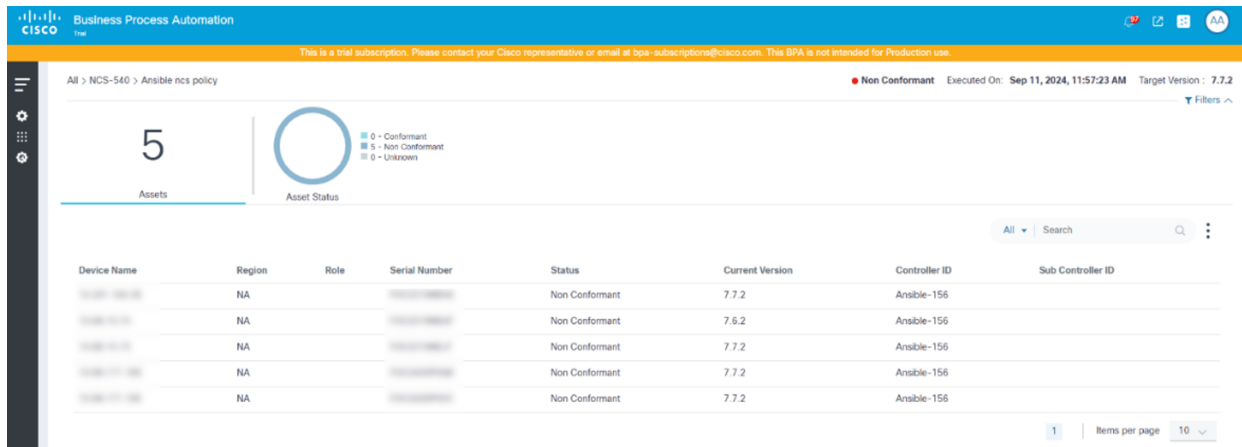
查看和下载一致性结果

策略执行后：

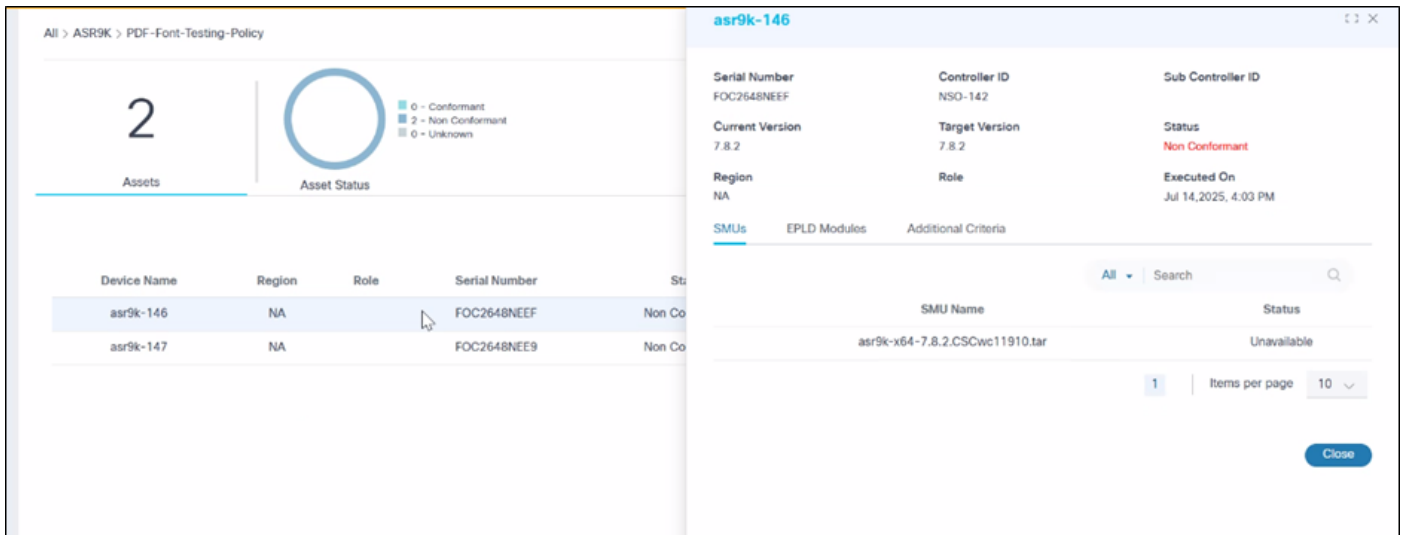


查看结果选项

1. 在Software Conformance页面上，选择More Options图标>View Results。显示Results页面，用户可以在其中查看设备的一致性状态。



查看结果



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. 选择一行以显示特定资产详细信息以及SMU状态和其他条件。



注意：SMU详细信息仅显示NSO、CNC、ANSIBLE、直接到设备和NDFC控制器资产。EPLD模块仅适用于NDFC控制器。

The screenshot displays the 'Conformance Policies' section of a management console. It features a summary card for 'ASR9K' with 2 total assets, 0 conformant, 2 non-conformant, and 0 unknown. Below this is a table listing policies, with the first row highlighted. A context menu is open over the first row, showing options: Run, View Results, Edit, and Delete.

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

Below the table, another policy 'c8000v' is partially visible, showing 15 total assets, 0 conformant, 15 non-conformant, and 0 unknown.

查看结果

3. 从设备的Action列中，选择More Options图标> View Results。

13

Assets

4 - Conformant

9 - Non Conformant

0 - Unknown

Asset Status

All

Search

Download

下载

4. 选择More Options图标> Download,以.csv格式下载结果并显示SMU可用性状态。

	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	10.200.156.156		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	10.200.156.156		Ansible-156		NA		7.6.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst	NA	Device conformance check completed					
4	10.200.156.156		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	10.200.156.156		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	10.200.156.156		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工作表视图

 注意：“查看结果”仅显示最近执行的一致性检查的结果。用户只能查看他们有权访问的资产。对于非操作策略，View Results被禁用。

可能的设备状态：

- 一致性:表示设备符合定义的策略
- 不符合项:表示设备在满足以下条件时不符合要求：

目标版本	SMU	合规性检查	状态
不符合项	不适用	不适用	不符合项
符合者	不可用	规则失败	不符合项
符合者	线上	规则失败	不符合项
符合者	不可用	规则成功	不符合项

- 未知:表示由于设备当前没有软件版本信息，无法执行设备软件一致性检查。

“未知”状态的条件包括：

目标版本	SMU	EPLD	合规性检查	状态
不符合项	不适用	不适用	不适用	不符合项
符合者	不可用	不符合项	规则失败	不符合项
符合者	不可用	符合者	规则失败	不符合项
符合者	线上	符合者	规则失败	不符合项
符合者	线上	不符合项	规则失败	不符合项
符合者	不可用	符合者	规则成功	不符合项
符合者	不可用	符合者	规则成功	不符合项

可能的SMU状态：

- 线上:表示SMU存在于设备中，并且处于活动状态
- 不可用:表示SMU可能不存在或存在，但处于“非活动”状态

可能的EPLD模块状态：

- 一致性:表示EPLD模块存在于具有预期目标版本的设备中
- 不符合项:表示设备中存在预期目标版本不匹配的EPLD模块
- 缺少模块:表示未在设备中配置或订用EPLD模块

可能的合规性检查模板状态：

- 成功:表示设备使用有效命令和规则成功执行了过程模板
- 失败:表示设备无法执行流程模板（例如，命令不正确时）
- 不适用:表示设备不符合执行流程模板的条件（例如，当设备不符合所定义的目标版本时）

 注意：下面列出了一些注意事项。

- 软件一致性检查仅适用于属于默认租户的设备
- 软件一致性检查依靠资产清单作为设备当前软件版本的真实来源。如果资产清单数据过时，则软件一致性检查结果过时。要避免陈旧数据问题，请在开始执行一致性策略时使用实时资产检查功能
- 可以在OS Upgrade > Settings > Software Conformance中更改默认计划
- 升级到BPA 5.1后，所有预先存在的策略都将移至禁用状态；用户必须编辑每个策略，选择适

当的值，将其启用，然后保存更改以供将来使用

升级策略

升级策略组件支持两种类型的策略：

- 单步策略：
 - 任意
 - <特定源版本(7.7.1)> - <特定目标版本(7.7.2)>
- 多步骤策略：
 - v7.7.1 - 7.7.2
 - v7.7.2 - 7.7.8
- 多步骤升级可包括网桥SMU，如下例所示：
 - v7.7.1 - v7.7.1[网桥SMU]
 - V7.7.1[网桥SMU] - 7.7.8

升级策略组件可灵活地预定义以下平台特定对象：

- 升级路径
- 验证前后的模板或工作流程
- 分发工作流程
- 激活工作流程
- 备份工作流程
- 超时值
- 回滚工作流
- 有效的前差异和后差异
- 流量转移工作流或流量逆转工作流

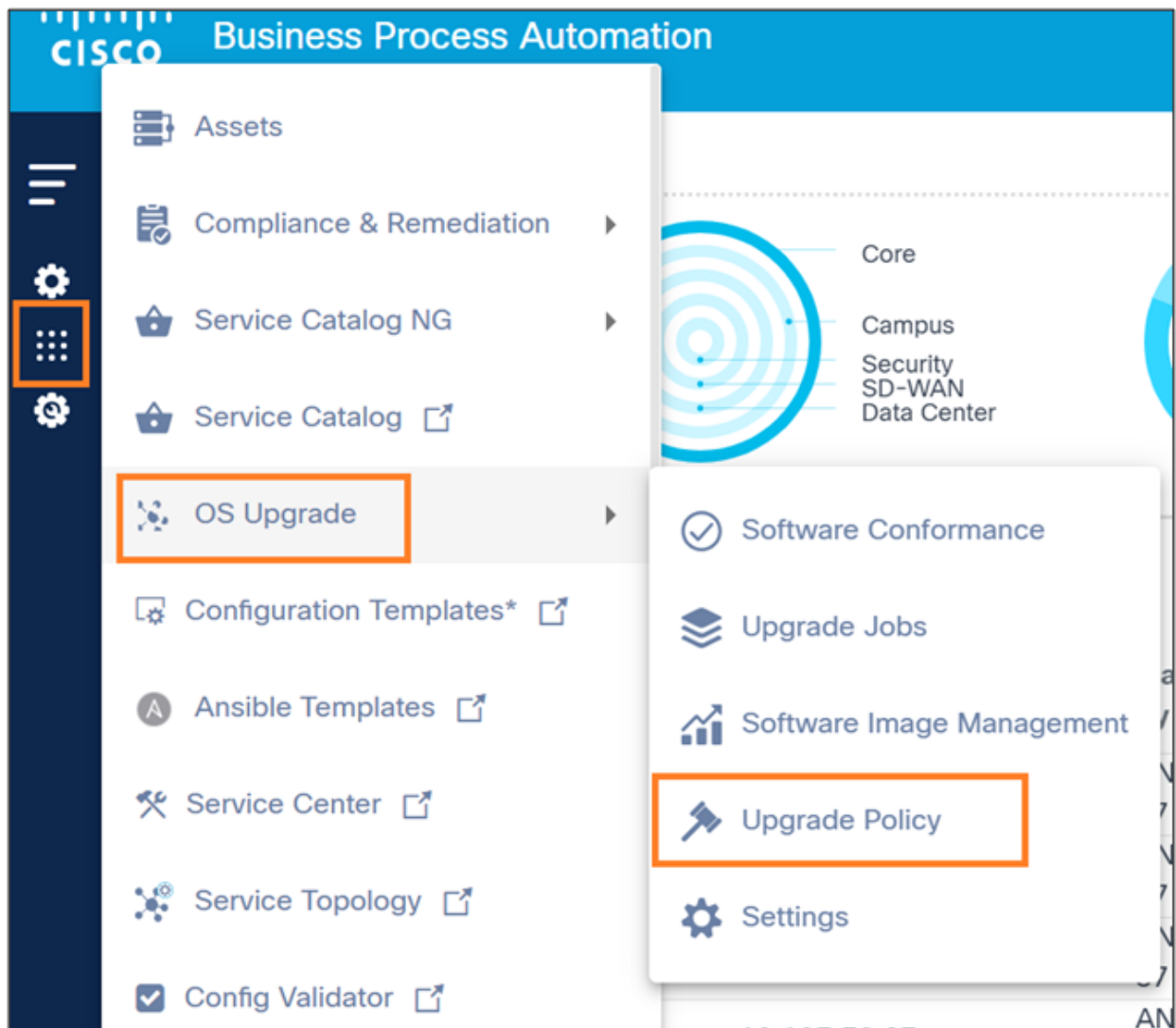
先决条件

- 必需的验证前和验证后流程模板或工作流程
- 所需的备份、分发、激活和回滚工作流程
- 所需的映像元数据

查看和管理升级策略

要访问“升级策略”(Upgrade Policy)页面：

1. 使用对升级策略具有足够访问权限的凭证登录到BPA。



升级策略导航

2. 选择OS Upgrade > Upgrade Policy。系统将显示Upgrade Policy页面。

The screenshot shows 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 displays the distribution of Controller Types. The chart is divided into segments for CNC, DNAC, Direct-To-Device, FMC, NDFC, vManage, Ansible, and NSO, each with a count of 1. Below the chart, a table lists the policies. The table has columns for Device Model, Controller Type, Name, Created By, Last Modified On, and Action. The first row shows a policy for ASR-9901, Direct-To-Device, with the name D2D-ASR-9901-Default, created by System, and last modified on Mar 22, 2024, at 11:14 AM.

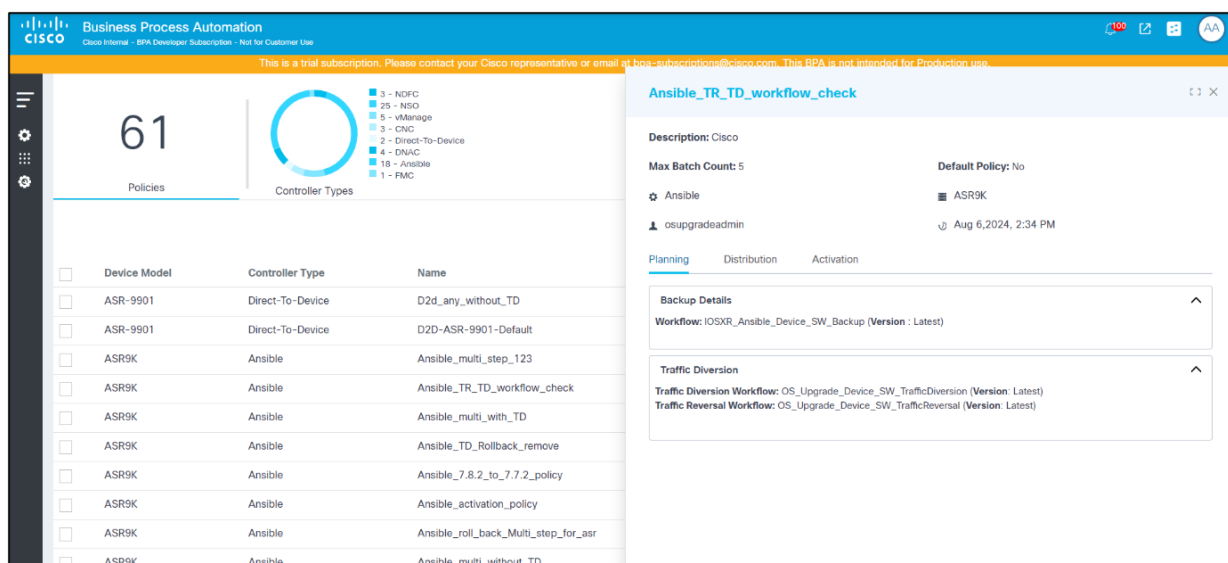
Device Model	Controller Type	Name	Created By	Last Modified On	Action
ASR-9901	Direct-To-Device	D2D-ASR-9901-Default	System	Mar 22, 2024, 11:14 AM	

升级策略

Upgrade Policy页面包含以下内容：

- 顶部显示的分析部分，提供以下功能：

- 系统中的升级策略总数
- Controller Types快速过滤器，提供按控制器类型过滤的能力
- 一个More Options图标，该图标提供Create Policy和Delete All selected policies等批量处理操作的选项选项
- 用于搜索策略的Search过滤器，可按如下方式过滤：
 - 全部:在所有字段中搜索
 - 设备型号:搜索具有指定模型的策略
 - 名称：搜索具有指定策略名称的策略
 - 创建者：搜索具有指定用户的策略
- 通过点击相应的列名称或表字段对策略进行排序



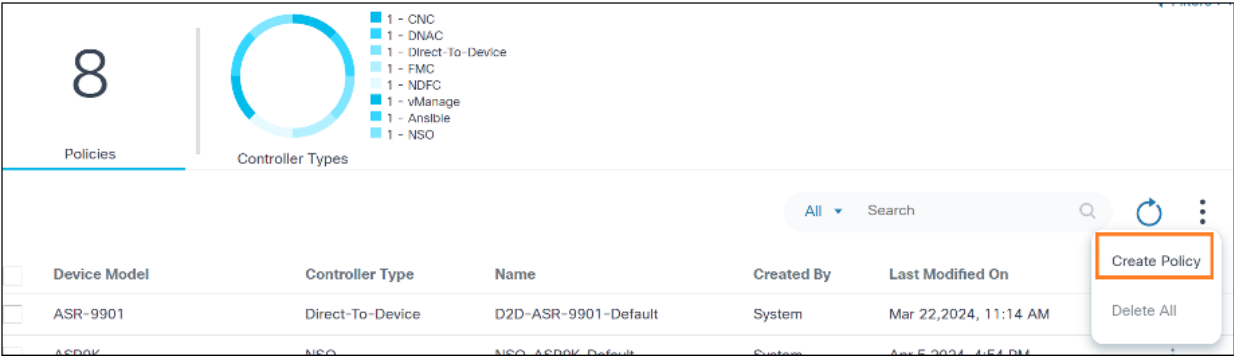
策略详细信息视图

- 点击特定策略或排列策略的详细视图

 **注意：**如果策略名称是唯一的，则相同的设备型号和控制器类型可以具有任意数量的策略。

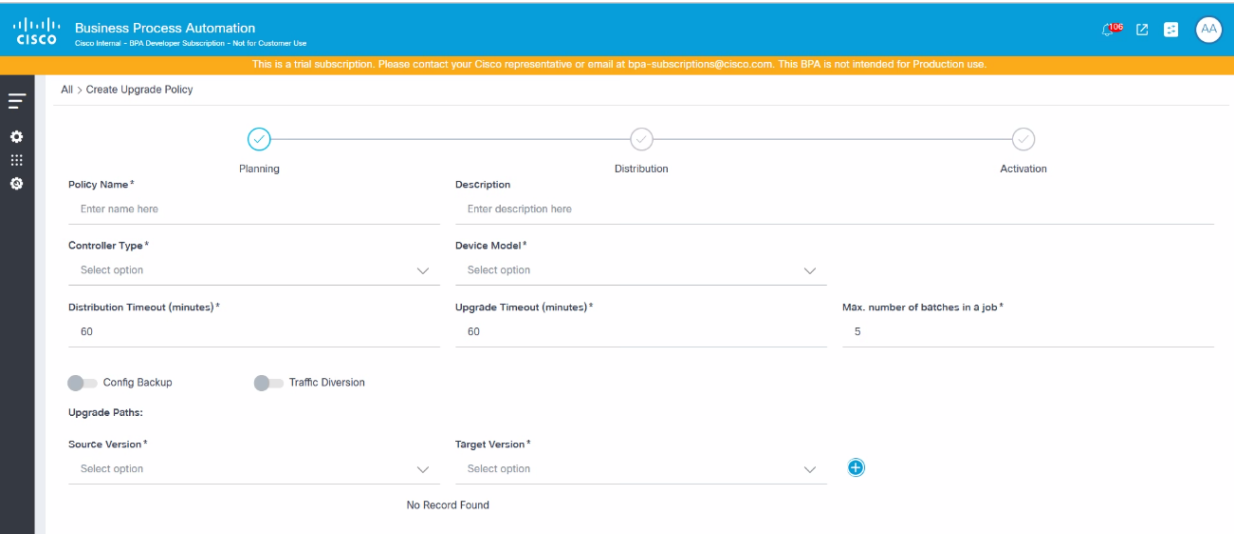
创建升级策略

1. 使用具有升级策略管理访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Upgrade Policy。系统将显示Upgrade Policy页面。



创建策略

3. 选择More Options > Create Policy。系统随即会显示Create Upgrade Policy页面。



创建升级策略

规划

1. 配置与整体策略相关的参数。下表对每个字段进行了简要说明。

字段	描述
策略名称	策略的名称
描述	策略简要说明
控制器类型	用于执行操作系统升级的适当控制器
设备型号	用于执行操作系统升级的设备型号
分发超时（分钟）	映像分发活动的最长等待时间（以分钟为单位）
升级超时（分钟）	映像激活活动的最长等待时间（以分钟为单位）
作业中的最大批数	可以添加到作业中的批数；允许的最大批数为20
配置备份切换	如果需要备份，请启用此切换，并在vManage和Direct-to-Device控制器的窗口中填写以下字段：

字段

描述

— workflow名称:适用的备份workflow

注意：如果找不到workflow，请确保workflow已正确标记了OS Upgrade NextGen标记

— 使用最新workflow:如果选中，则使用所选workflow的最新版本

— workflow版本:定制workflow版本；只有在未选择使用最新工作流时，才能选择此选项。

对于NDFC、NSO、CNC和Cisco Catalyst Center控制器，备份通过备份和还原服务进行。因此，必须在“备份详细信息”窗口中选择备份和恢复策略。

注意：用户必须为控制器类型选择适当的策略。有关备份和还原策略的详细信息，请参阅[备份和还原](#)部分。

要为Nexus设备启用备份，目标设备上必须存在功能scp-server配置。

如果需要流量转移，请启用此切换，并在流量转移窗口中填写以下字段：

-流量分流workflow:适用的流量转移工作流。

注意：如果找不到workflow，请确保workflow已正确标记了OS Upgrade NextGen标记

— 流量逆转workflow:适用的流量逆转workflow。

注意：如果找不到workflow，请确保workflow已正确标记了OS Upgrade NextGen标记

— 使用最新workflow:以上所选workflow的最新版本

— workflow版本:定制workflow版本；只有在未选择使用最新工作流时，才能选择

升级路径定义适用的步骤升级路径；可以在以下字段中添加多个源版本和目标版本，以满足不同的需求

-源版本:升级路径的开始版本

流量分流切换

升级路径

字段	描述
	— 目标版本:升级路径的结束版本 -源版本(Any)到目标版本(Any):这可以通过为Source Version和Target Version字段选择Any来实现，这是所有设备型号的默认值；在此场景中，Distribution和Activation页面提供统一的升级过程 -源版本（特定版本）到目标版本（特定版本）:这可以通过选择设备型号可用的特定映像版本来实现；可以添加多个源版本和目标版本；分发和激活升级过程输入的数量与添加的源版本和目标版本的数量匹配，并且每个版本都显示为带有相应源版本和目标版本标记的可折叠部分。升级路径要求先在源版本上应用强制SMU，然后再通过将这些SMU作为网桥SMU添加到相应的升级路径来升级到目标版本。有关网桥SMU的详细信息，请参阅下一节。

网桥SMU

网桥SMU（也称为强制升级或降级SMU）是前提条件，在升级或降级到同一平台或型号的另一个软件版本之前必须安装。

在升级路径中添加网桥SMU

✓

Planning

✓

Distribution

✓

Activation

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

7.6.2

Bridge SMU(S)

Target Version

7.7.2

Action

⋮

1

Delete Path

Add Bridge SMUs

Cancel

Next

升级路径选项

1. 添加升级路径后，选择更多选项图标。将显示Delete Path和Add Bridge SMUs选项。

✓

Planning

✓

Distribution

✓

Activation

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

添加网桥SMU

2. 选择Add Bridge SMUs。Add Bridge SMUs窗口打开。将显示指定升级路径的所有可用网桥SMU。

×

Add Bridge SMUs

Select option(s)

☒ asr9k-x64-7.6.2.CSCwf77420.tar

☐ asr9k-x64-7.6.2.CSCwc41614.tar

添加网桥SMU

3. 在Add Bridge SMUs窗口中，选择适当的复选框以添加网桥SMU，或清除复选框以将其删除。添加网桥SMU后，升级路径会使用选定的网桥SMU详细信息进行更新。

✓

Planning

✓

Distribution

✓

Activation

Policy Name *
ASR9kPolicy

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

asr9k-x64-7.6.2.CSCwf77420.tar

7.7.2

:

使用网桥SMU的升级路径

 注意：包括网桥SMU的每个升级路径在升级过程中都被视为两步升级。对于上图所示的升级路径，最终升级路径为：

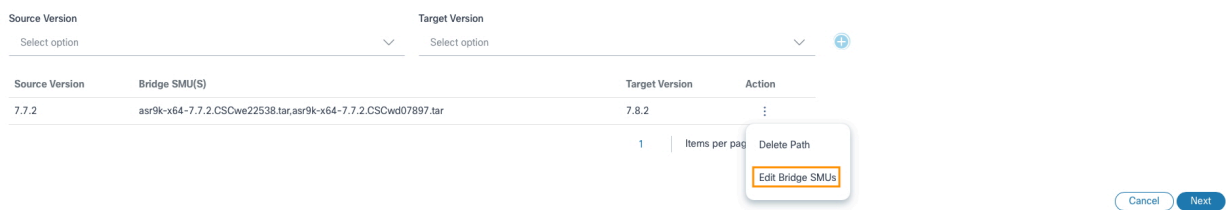
- 7.6.2 - 7.6.2 [网桥SMU]

此路径表示使用网桥SMU更新在v7.6.2上运行的设备。

- 7.6.2 [网桥SMU] - 7.7.2

此路径代表将设备从v7.6.2升级到v7.7.2。在这种情况下，设备的源版本为7.6.2，包括应用于它的网桥SMU。

编辑网桥SMU



使用网桥SMU的升级路径

1. 在升级路径部分中，选择更多选项图标> 编辑网桥SMU。Edit Bridge SMUs窗口打开。



编辑网桥SMU

2. 选中或清除相应的复选框以更新网桥SMU。
3. Click OK.系统随即会显示更改摘要。

Planning

Policy Name *
ASR9K bridge 772

Controller Type *
NSO

Distribution Timeout (minutes) *
60

☒ Config Backup

☒ Traffic Diversion

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

Distribution

Description
Enter description here

Device Model *
ASR9K

Upgrade Timeout (minutes) *
60

Max. number of batches in a job *
5

Activation

Cancel

Next

更改摘要

4. 验证更改摘要并点击下一步。

删除网桥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

编辑网桥SMU

1. 在升级路径部分中，选择更多选项图标> 编辑网桥SMU。Edit Bridge SMUs窗口打开。

×

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

编辑网桥SMU

- 清除相应的复选框以删除网桥SMU。
- Click OK.系统随即会显示更改摘要。

Planning

Description

Distribution

Activation

Policy Name *

ASR9K bridge 772

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

Target Version

Select option

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

分布

分布获取与图像分布相关的输入参数（即图像复制）。以下映像是每种升级路径类型所需的输入参数。

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 — 单步升级

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 *

Workflow Version *

OS_Upgrade_Precheck_PostCheckExample

Use latest workflow

Select option

Post check Workflow *

Workflow Version *

OS_Upgrade_Precheck_PostCheckExample

Use latest workflow

Select option

Previous

Next

Image Distribution部分 — 单步升级，启用前/后工作流程

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 — 多步骤升级

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

Post check Workflow *

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 — 多步骤升级

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

分发部分 — 网桥SMU升级

- 配置与图像分发相关的参数。
- 下表提供了每个字段的简要说明。

字段	描述
工作流程名称	适用的分发工作流程
使用最新工作流	选择所选工作流程的最新版本
工作流程版本	定制工作流程版本；仅当未选中使用最新工作流程复选框时，才能选择此选项
前/后通用模板	在两个阶段（即预检查和后检查）中执行的流程模板
前/后工作流程切换	注意：检查仅适用于分布里程碑。 有关详细信息，请参阅流程模板 允许用户选择执行分布里程碑中的检查前或检查后工作流程。打开切换时，只能配置检查前或检查后工作流程。 包括仅在预检查阶段执行的命令。
预检工作流程	注意：这些检查特定于分销里程碑。 后检查工作流程包括在后检查阶段唯一执行的命令。
检查后工作流程	注意：这些检查特定于分销里程碑。 包含排他性预检查命令的流程模板；模板仅在预检查阶段执行。
预检查模板	注意：检查仅适用于分布里程碑。 包含专用的检查后命令的流程模板；模板仅在检查后阶段执行。
检查后模板	注意：检查仅适用于分布里程碑。 在多选升级中，所有升级路径都应用了一致的属性。
为以下所有升级路径使用相同的属性	注意：如果选中，则相同的属性将应用于多选升级中的所有升级路径。



注意：工作流程或流程模板必须正确标记有OS Upgrade Next-Gen标记。

3. 单击Next继续到Activation部分。

激活

✓

Planning

✓

Distribution

✓

Activation

Workflow Name *

ASR9K_Device_SW_Activation

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

asr9k_activation_check2, asr9k_activation_check1

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

Valid Pre/Post Differences

asr9k_activation_check2, asr9k_activation_check1

▼

Rollback Workflow

Select option

▼

●

Pre/Post Workflow

Previous

Update

激活部分 — 单步升级

✓

Planning

✓

Distribution

✓

Activation

^ 7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Activation

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

asr9k_activation_check2, asr9k_activation_check1

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

Valid Pre/Post Differences

asr9k_activation_check1, asr9k_activation_check2

▼

Rollback Workflow

Select option

▼

●

Pre/Post Workflow

☐ Use the same properties for all the below upgrade paths

^ 7.7.2 to 7.8.2

Previous

Update

激活部分 — 多步骤升级

✓

Planning

✓

Distribution

✓

Activation

^ 7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Activation

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

asr9k_activation_check2, asr9k_activation_check1

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

Valid Pre/Post Differences

asr9k_activation_check1, asr9k_activation_check2

▼

Rollback Workflow

ASR9K_Device_SW_Rollback

▼

●

Pre/Post Workflow

☐ Use the same properties for all the below upgrade paths

^ 7.7.2 to 7.7.2[Bridge SMUs]

Workflow Name *

ASR9K_Device_SW_Activation

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

asr9k_activation_check2, asr9k_activation_check1

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

Valid Pre/Post Differences

asr9k_activation_check1, asr9k_activation_check2

▼

Rollback Workflow

ASR9K_Device_SW_Rollback

▼

●

Pre/Post Workflow

^ 7.7.2[Bridge SMUs] to 7.8.2

激活部分 — 网桥SMU升级

1. 配置与映像激活相关的参数。
2. 下表对每个字段进行了简要说明。

字段	描述
工作流程名称	适用的激活工作流程
使用最新工作流	选择所选工作流程的最新版本
工作流程版本	定制工作流程版本；仅当未选中Use latest workflow复选框时才能选择在两个阶段（即预检查和后检查）中执行的流程模板。
前/后通用模板	注意：检查仅适用于激活里程碑。 有关详细信息，请参阅 流程模板 包含排他性预检查命令的流程模板；模板仅在预检查阶段执行。
预检查模板	注意：检查仅适用于激活里程碑。 包含专用的检查后命令的流程模板；模板仅在检查后阶段执行。
后检查模板	注意：检查仅适用于激活里程碑。
有效的事前/事后差异	选择忽略差异的流程模板。 注意：检查仅适用于激活里程碑。 适用的回滚工作流程。
回滚工作流	注意：如果在多选升级中选择了具有回滚工作流的升级路径之一，则默认情况下会选择具有回滚工作流的其它所有升级步骤。 此自定义预检查工作流程包含可以选择和查看其执行结果的特定命令。它仅在预检查阶段执行。
预检工作流程	注意：这些检查特定于激活里程碑。 此自定义检查后工作流程包含可以选择和查看其执行结果的特定命令。它仅在后检查阶段执行。
检查后工作流程	注意：这些检查特定于激活里程碑。
为以下所有升级路径使用相同的属性	在多选升级中，所有升级路径都应用了一致的属性。 注意：如果选中，则相同的属性将应用于多选升级中的所有升级路径。

 注意：应该注意以下几点：

- 必须在NSO中配置Nexus设备所需的公钥算法。
- 配置bgp、bfd和hsrp的功能以在Nexus设备中执行检查前和检查后模板。

3. Click Create.系统随即会显示字段摘要。

Summary

Name: Single step upgrade

Description: This upgrade policy for ansible

Max Batch Count: 5

Ansible

Default Policy: No

NCS-540

Planning Distribution Activation

Backup Details

Submit

摘要 — 一步升级策略

Summary

Name: Multi step upgrade

Description: This upgrade policy for ansible

Max Batch Count: 5

Ansible

Default Policy: No

NCS-540

Planning Distribution Activation

Backup Details

Upgrade Paths

Submit

摘要 — 多步骤升级策略

- 验证字段摘要并点击Submit。系统随即会显示进度通知，然后会显示确认消息。策略在成功创建后在页面上可见。

可以根据需要为其他设备型号创建其他升级策略。

编辑升级策略

7 Policies

CONTROLLER TYPES

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

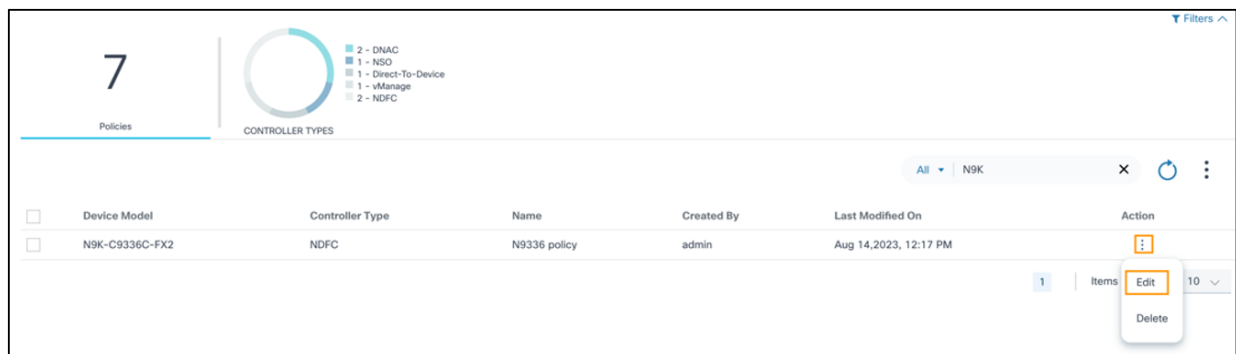
All N9K

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

升级策略的搜索结果

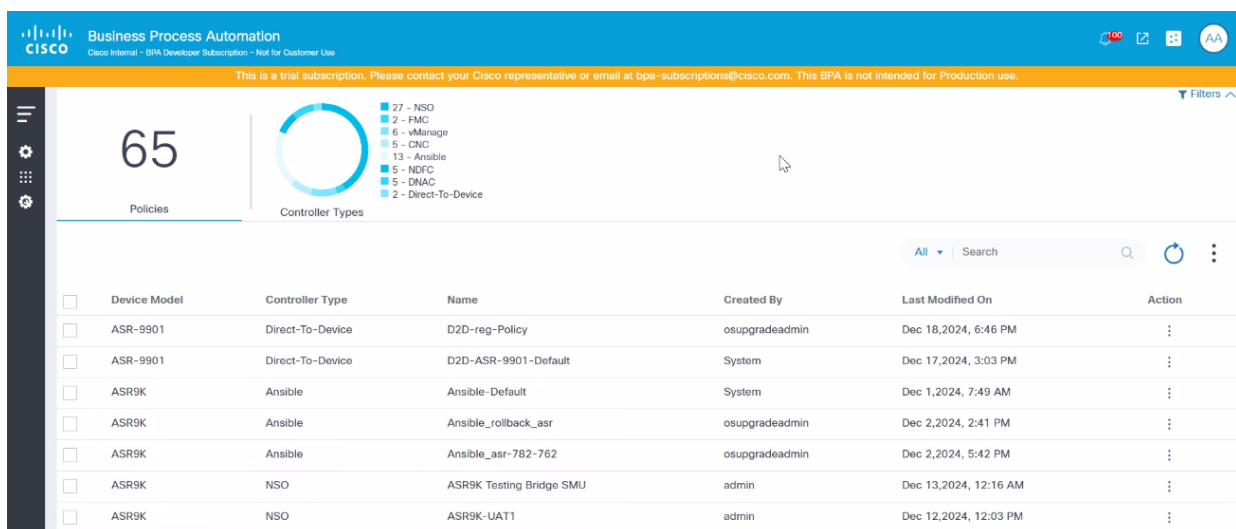
- 从升级策略页面，使用搜索字段找到所需的策略。



编辑升级策略

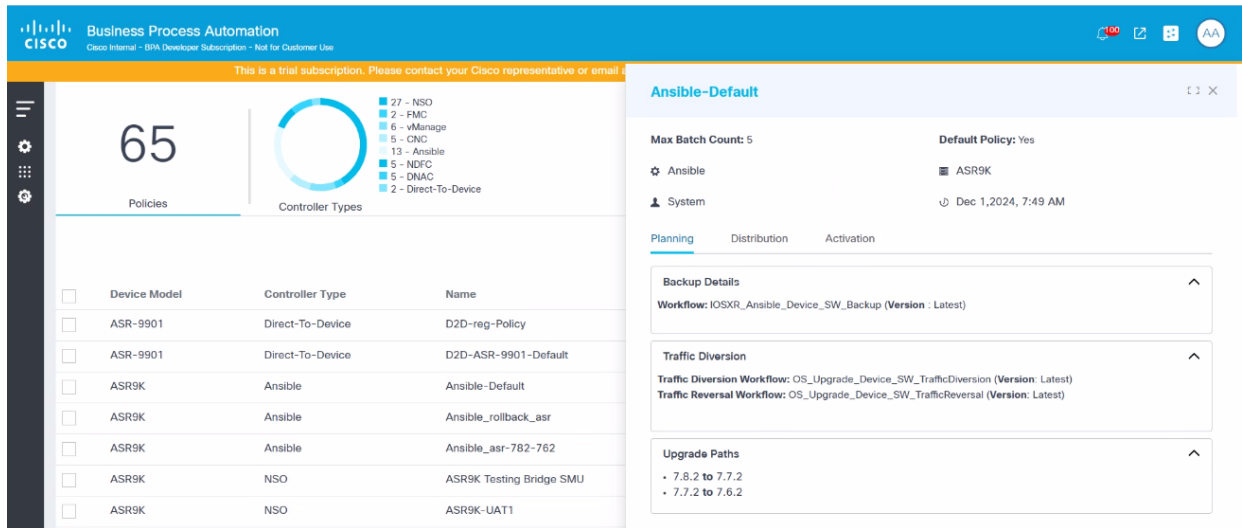
2. 从策略的Action列中，选择More Options图标> Edit。
3. 更新相关字段并点击更新。系统随即会显示更改摘要。
4. 验证更改摘要并点击提交。系统随即会显示进度通知，然后会显示确认消息。

查看升级策略



升级策略

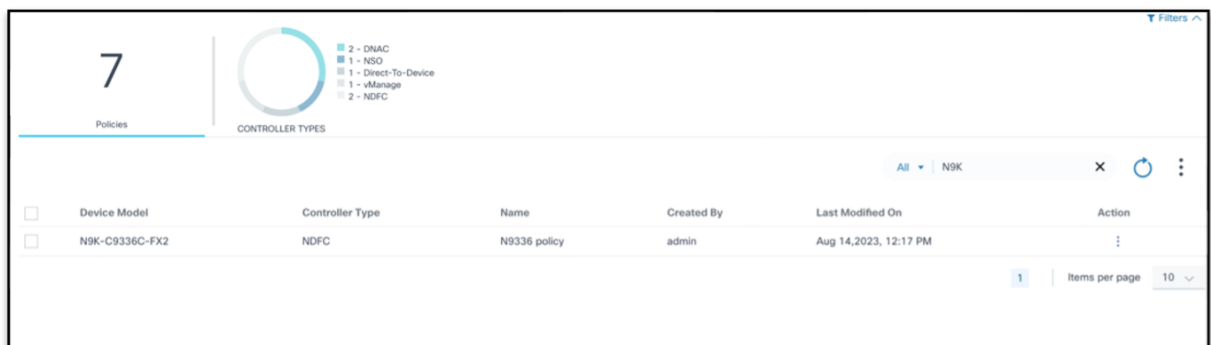
1. 从升级策略页面中，选择所需升级策略的行。系统将打开策略的详细信息视图。



升级策略详细信息视图

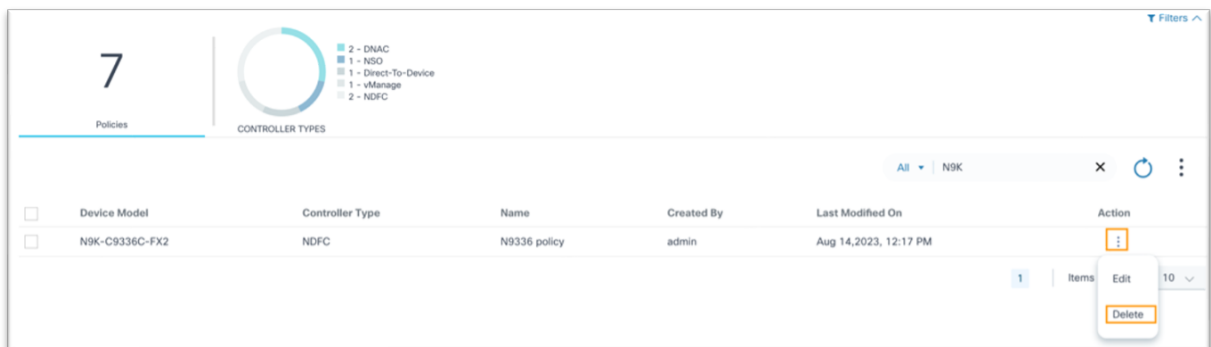
删除升级策略

 注意：无法删除默认策略，但用户可以编辑流程模板和 workflows。



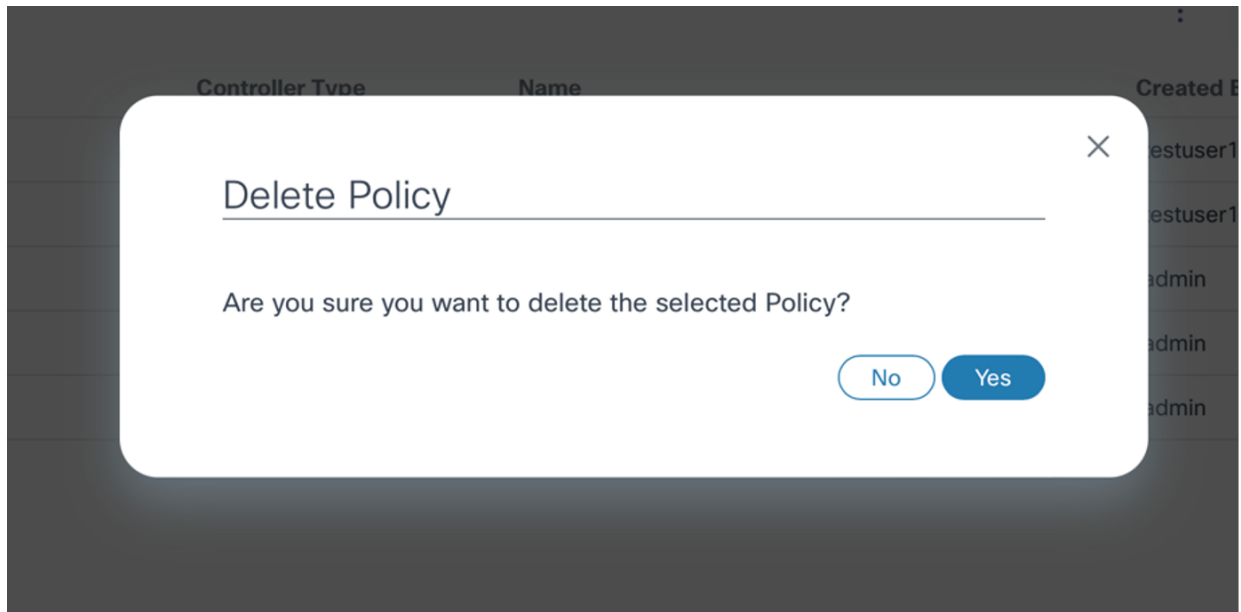
升级策略

1. 从升级策略页面，使用搜索字段找到所需的策略**。



删除升级策略

2. 从策略的Action列中，选择More Options > Delete。确认窗口打开



删除策略确认

3. 单击 Yes。

控制对升级策略的访问

此功能提供对升级策略的访问控制，限制未经授权的用户更新操作系统升级应用中定义的策略。管理员可以通过定义具有可访问策略的资源组来限制访问。

要创建资源组，请执行以下操作：

1. 导航到设置 > 资源组。
2. 使用非管理员用户可以访问的策略创建资源组。属于此用户组的非管理员用户现在仅有权访问此资源组中可用的策略。
3. 创建访问策略以将资源组与用户组相关联，

有关详细信息，请参阅[访问控制](#)。



注意：应该注意以下几点。

- 用户可能会选择不正确的工作流程进行分发和激活，从而导致意外行为。用户负责正确映射工作流程并验证重要事件（如分发、激活、回滚和设备模型）的适用性。
- 工作流和流程模板必须与OS升级下一代标记进行映射，以便在创建或更新策略时可供选择。
- 无法删除系统用户创建的默认OOB策略，但用户可以编辑流程模板和工作流程。

升级作业

使用升级作业应用程序管理软件升级，该应用程序由一个或多个批次组成，每个批次具有一个或多个网络设备。可在草稿模式下创建作业并保存多次。只有在提交作业后才能开始升级，使操作员能够预先规划更改。

先决条件

- 预留的升级维护窗口
- 升级更改请求的预审批
- Config Backup and Restore服务必须已启动并正在运行
- 计划程序服务必须已启动并正在运行
- 适用于外部系统（如订票系统）的BPA适配器（如果有）必须登录

查看和管理升级作业

1. 使用有权访问升级作业的凭据登录到BPA。
2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。



升级作业

升级作业页包含以下内容：

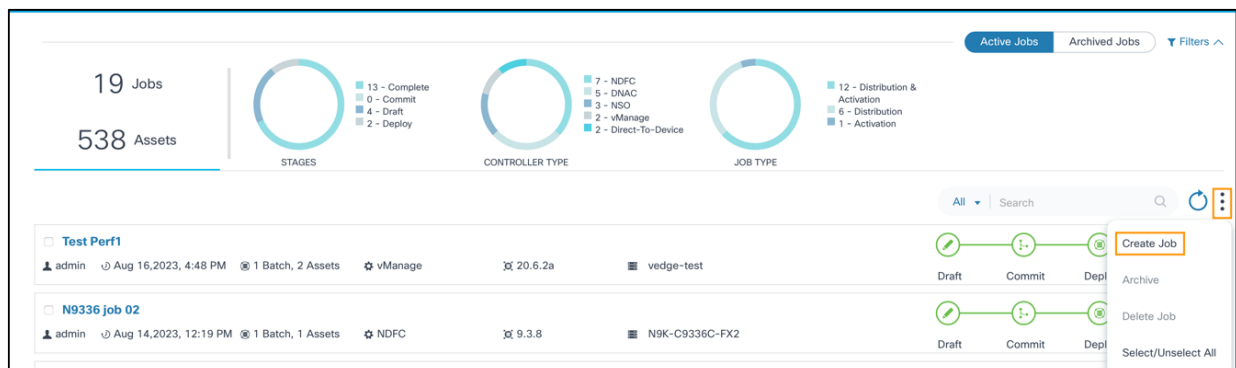
 注意：默认情况下，将显示十个作业。页码可用于导航到其他作业页。

- Active Jobs和Archived Jobs切换，可用于在活动作业和存档作业之间切换
- 顶部显示的分析部分，提供以下功能：

- 与作业关联的作业和资产总数
- 使用以下过滤器的阶段图表：
 - 草稿:作业处于草稿阶段，尚未提交
 - 提交:作业已提交到所有必要的设备、批次或计划，直到达到计划
 - 部署:已启动一个或多个批次的升级活动
 - 完成:属于所有批次的所有设备的升级活动已完成
- 控制器类型图表：允许通过Cisco Catalyst Center、vManage、NSO、NDFC、直接到设备、CNC、ANSIBLE和FMC控制器类型进行作业过滤
- “作业类型”图表具有以下筛选器：
 - 分布:从控制器向设备执行映像暂存或复制的作业
 - 激活:执行设备软件的激活或升级的作业
 - 分发和激活:同时执行设备软件的转储或复制和激活或升级的作业
- Search字段，可用于跨所有元数据执行一般搜索，或按Job Name和Created By字段执行一般搜索
- Refresh图标，可用于刷新作业摘要和清除Search字段中的图表筛选器或任何自定义搜索
- More Options图标，该图标提供Create a new upgrade job和Archive或Delete selected作业的选项；用户可以选择或取消选择全部
- 作业显示为面板，提供以下信息的快速视图：
 - 如果有可用的任何用户任务，则会显示User Task图标以及用户任务数
 - 创建作业的用户
 - 作业创建日期
 - 批和资产的数量
 - 控制器类型（例如，Cisco Catalyst Center、vManage、NDFC、直接到设备、CNC、ANSIBLE或FMC）
 - 目标版本
 - 适用的设备型号
 - 作业阶段（即草稿、提交、部署和完成）的里程碑视图，每个里程碑的颜色图例：
 - 灰色:里程碑尚未开始
 - 蓝色:里程碑正在进行
 - 红色:里程碑问题
 - 绿色:里程碑已完成
 - 里程碑末尾显示作业状态的颜色图例：
 - 绿色:作业已完成
 - 红色:作业存在问题
 - 蓝色:作业正在进行

安排升级作业

要创建作业，请执行以下操作：



创建升级作业选项

1. 从升级作业页中，选择更多选项图标> 创建作业。系统随即会显示创建升级作业页面。

创建升级作业

2. 在名称字段中输入作业名称。
3. 选择Controller Type (例如 , Cisco Catalyst Center、vManage、NDFC、直接到设备、CNC、FMC、ANSIBLE或NSO) 。
4. 选择具有非一致性设备的一致性策略。

 注意：只有至少执行一次且具有至少一个非一致性设备的符合策略才可以从列表中获得，一旦选择了策略，将自动识别要使用的适用升级策略。

以下详细信息显示在“作业摘要”(Job Summary)下的“创建作业”(Create Job)表单的左侧:

- 受影响的设备型号

 注意：当所选一致性策略有多个关联的设备型号时，会显示多个设备型号。

- 目标版本
- 现有版本及其相应计数的聚合
- 允许的最大批数
- 不符合项资产总数

 注意：如果所选一致性策略与多个设备型号关联，则它会显示所有关联型号的非一致性资产聚合。

- 用于添加批的选项

5. 选择以下升级作业类型之一：

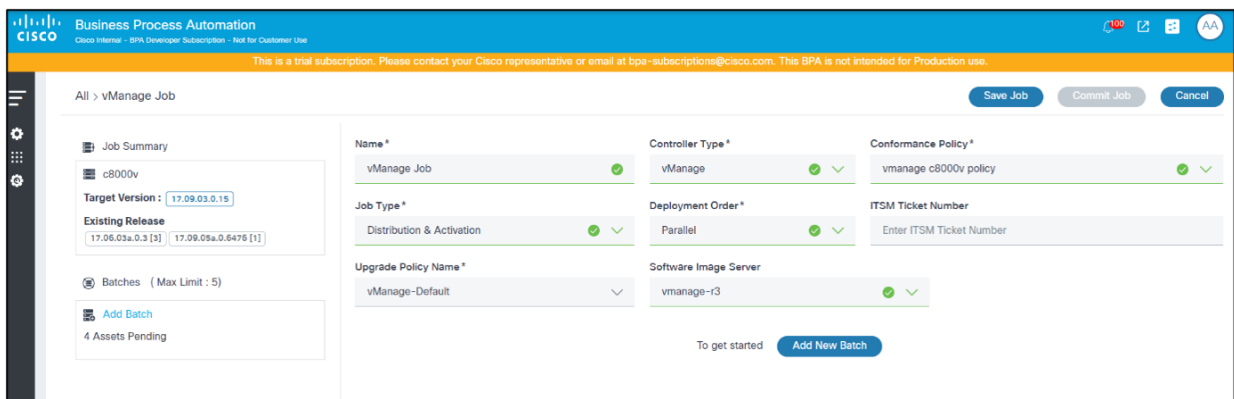
- 分布:当软件映像在实际激活之前暂存时，仅分发作业很有用
- 激活:仅激活作业对于执行设备升级很有帮助，因为设备的分发已经通过仅分发作业完成
- 分发和激活:在同一作业中同时进行映像分发或暂存和激活，这在具有充足的维护窗口以涵盖将映像复制到设备和升级的情形中很有用

6. 选择升级订单。多个设备在Parallel模式下同时处理，而设备在Sequential模式下逐个处理。

 注意：可在并行模式下处理的最大设备数取决于部署配置。所选的升级订单适用于整个作业，但可以根据需要在特定批内覆盖。

7. 在IT服务管理(ITSM)票证编号字段中添加更改请求编号。
8. 选择升级策略名称。根据控制器类型和合规策略设备型号，仅显示适用的升级策略；用户可以选择一个升级策略。如果软件一致性策略有多个关联的模型，则会显示与每个模型关联的所有相关升级策略。用户应仔细选择适用于所有型号的升级策略。
9. 选择Software Image Server以指定使用哪个vManage映像存储库（例如，本地或远程）。

 注意：此输入仅适用于vManage控制器类型。



创建已填写详细信息的升级作业（一致性策略有一个模型）

创建已填写详细信息的升级作业（一致性策略有多个模型）

10. 单击Save Job以保存草稿，直到准备提交作业为止。

添加批处理并添加新批处理

11. 要添加批处理，请点击添加批处理链接或添加新批处理。此时将打开“批创建”窗口。

批量创建

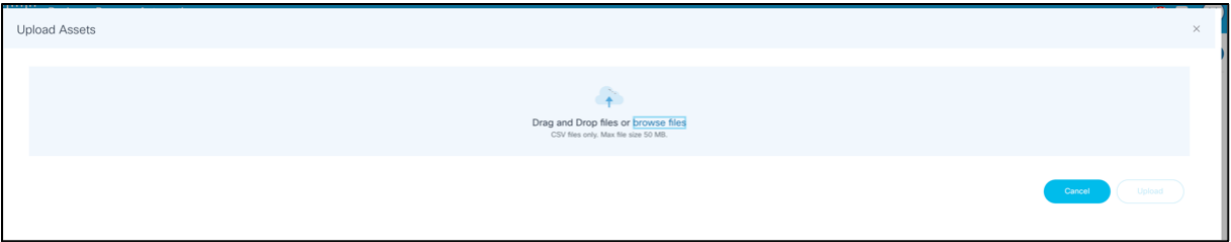
12. 输入相关批名并选择部署订单。

注意：此处选择的升级类型优先于“作业创建”页面上所选的类型

13. 选择Software Image Server以指定使用哪个vManage存储库（例如，本地或远程）。

 注意：此字段仅适用于vManage控制器类型。此处选择的软件映像服务器优先于“作业创建”页面上选择的软件服务器

14. 将资产添加到批中。可以通过两种方式将资产添加到批中：



上传资产

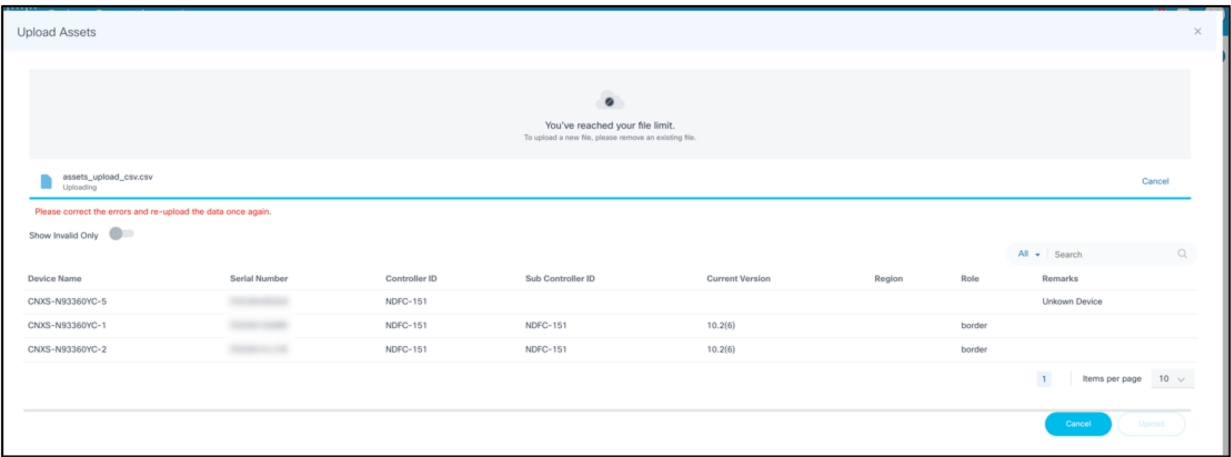
选项 1：

- a. 点击上传资产。Upload Assets窗口打开。
- b. 选择要上传的.csv文件。

 注意：.csv文件必须具有以下详细信息：

- 设备名称：设备或资产的名称
- 序列号(S):设备的序列号
- 控制器ID:管理设备的控制器的名称
- 子控制器ID:管理设备的子控制器ID的名称

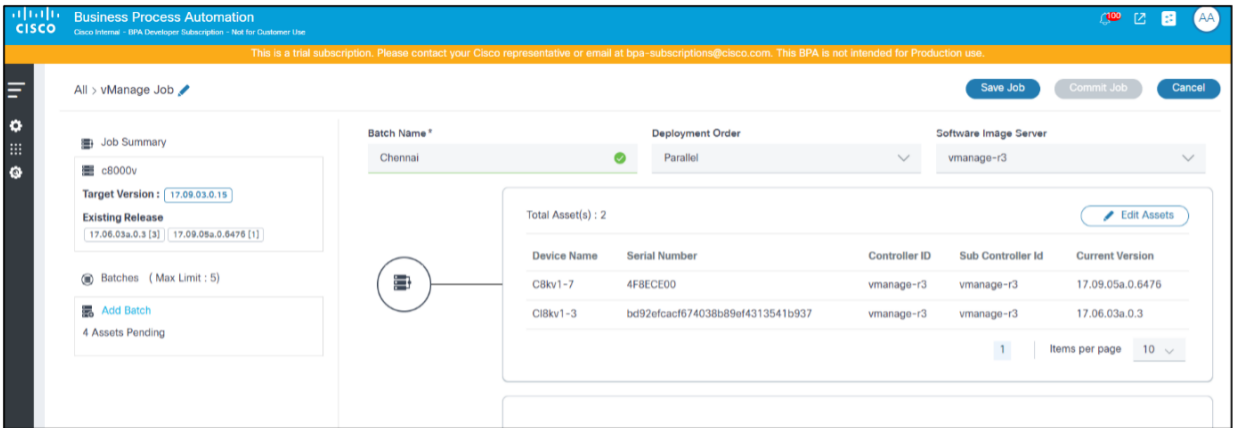
- c. 单击Upload。将验证.csv文件数据并显示有效数据和无效数据。Show Invalid Only切换可用于从上传的资产详细信息中过滤无效设备。



通过CSV文件上传的示例资产

d. 如果上传的文件中存在错误，请更正错误并重新上传。

 注意：仅当所有上传的设备都有效时，用户才能继续选择资产。



添加批 — 所选资产

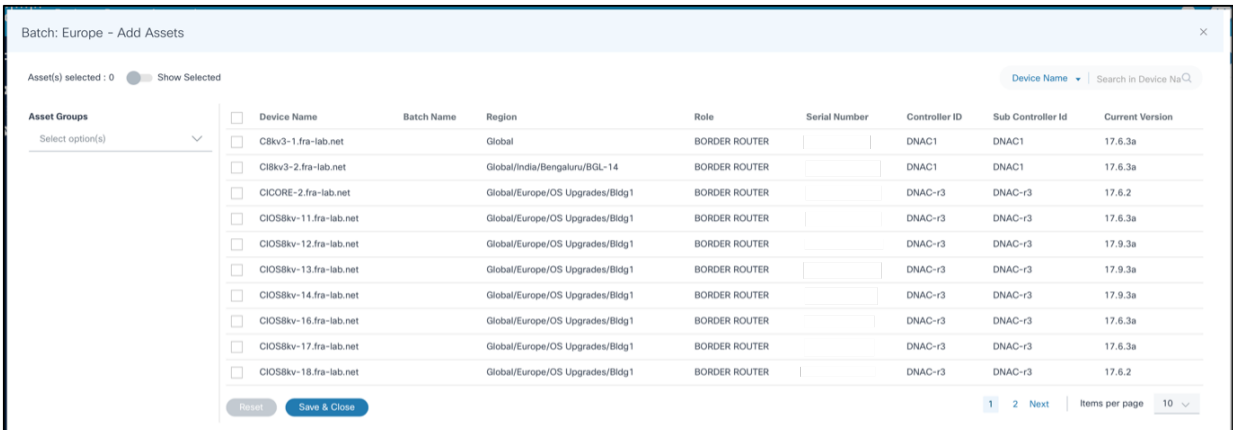
选项 2：

a. 单击Add Assets。将打开“资产选择”窗口。

 注意：上传资产 和Add Assets不能同时使用。

b. 仅对于FMC控制器类型，选择用于执行升级的控制节点或独立节点。

 注意：升级作业中不允许使用数据设备，因为数据节点的升级由其控制节点处理。



设备选择

c. 选择要与当前批一起包含的适当设备。

Search过滤器可用于根据不同的属性过滤设备，并且可通过选中Device Name列标题中的复选框来批量选择符合过滤条件的所有设备。用户还可以选择按资产组进行过滤。

可以启用Show Selected切换以仅查看所选资产。

 注意：启用Show Selected切换后，将禁用Asset Groups过滤器。

d. 单击保存并关闭。

单击Reset将放弃选择并保留资产选择的原始状态。

Batch: Europe - Add Assets

Asset(s) selected : 2 Show Selected

Asset Groups

Select option(s)

Device Name	Batch Name	Region	Role	Serial Number	Controller ID	Sub Controller Id	Current Version
☐ Cblkv3-1.fra-lab.net	Europe	Global	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☐ Cblkv3-2.fra-lab.net	Europe	Global/India/Bengaluru/BGL-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
☐ OOSBkv-11.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☐ OOSBkv-12.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☐ OOSBkv-13.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☐ OOSBkv-14.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☐ OOSBkv-16.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☐ OOSBkv-17.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☐ OOSBkv-18.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.2

Reset
Save & Close

1
2
Next
Items per page
10

Reset

e. 如果资产选择需要修改，请单击Edit Assets。

Business Process Automation
Cisco Internal - BPA Developer Subscription - Not for Customer Use

[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 : 17.09.03.0.19

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	17.09.05a.0.6476	vmanage-r3	vmanage-r3	17.09.05a.0.6476
C8kv1-3	17.06.03a.0.3	vmanage-r3	vmanage-r3	17.06.03a.0.3

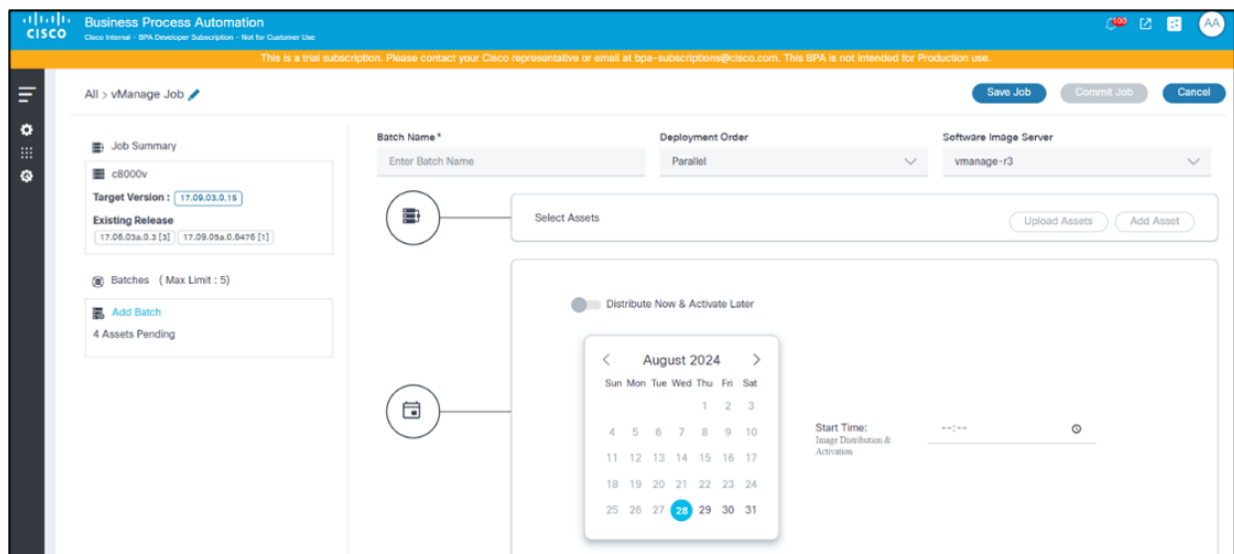
1

Items per page

10

批量编辑资产

f. 选择或清除资产进行必要的更改，然后单击保存并关闭。在编辑批资产时，可以使用复选标记和“批名”列中显示的批名标识当前作为不同任务和批的一部分的所选资产。



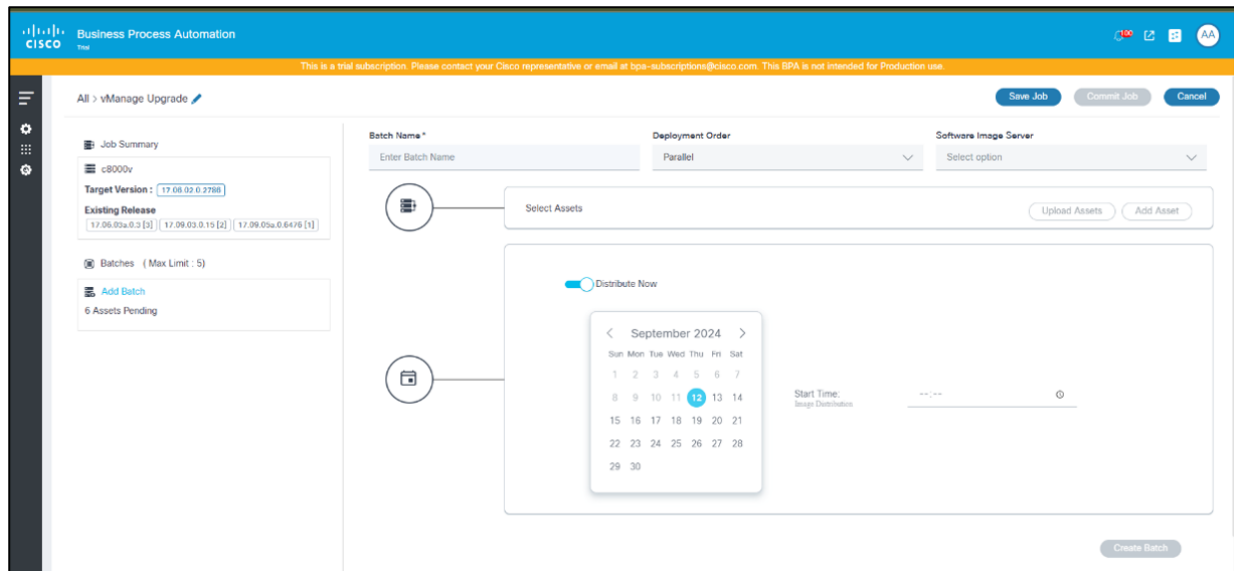
升级作业安排器

15. 从日期选择器中选择日期，从时间选择器中选择时间，以计划触发为当前批选择的升级类型的
时间。

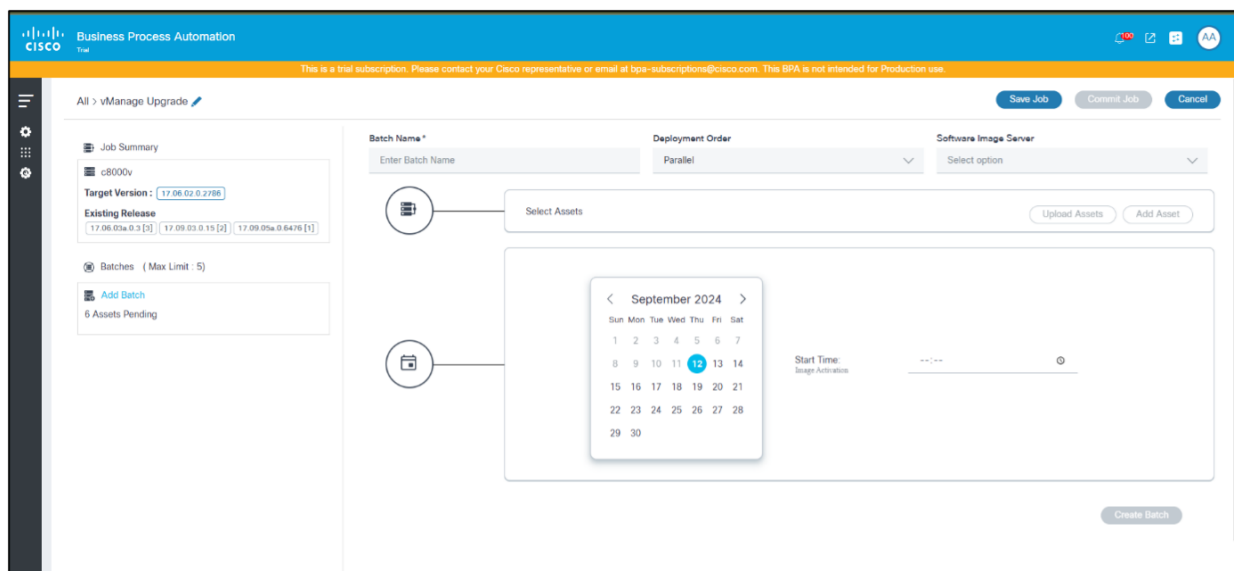
 注意：所选作业类型会更改可用计划的类型。

可能的方案如下：

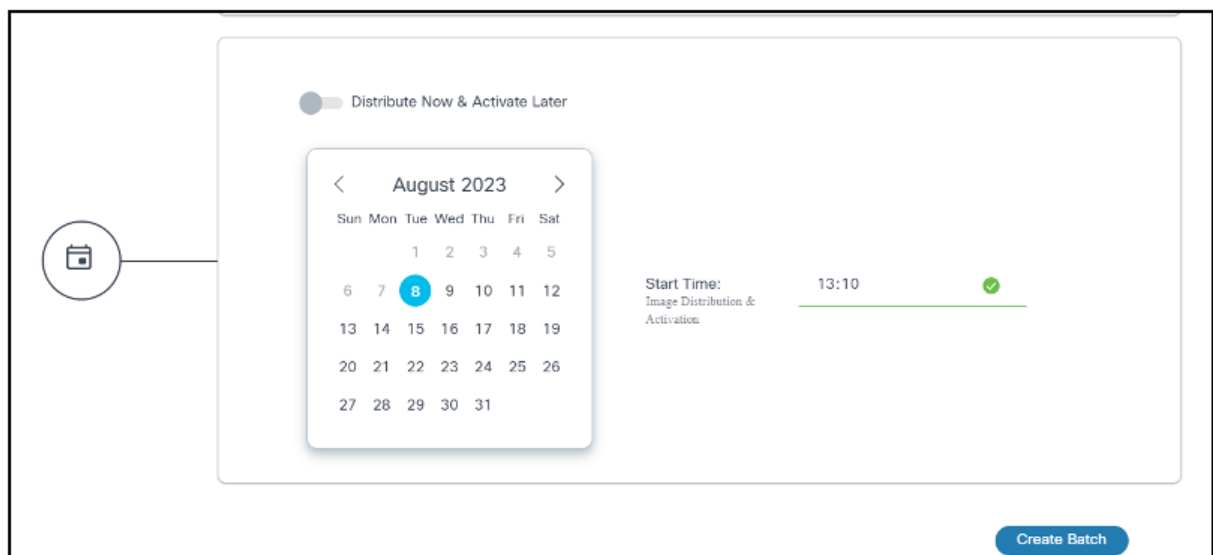
作业类型	立即分配切换	计划日期和时间	分发详细信息
分布	默认情况下禁用	主用	在指定的计划日期和时间进行分发
分布	启用	禁用	作业提交后分发
激活	不适用	主用	激活在指定的日期和时间进行
分发和激活	默认情况下禁用	主用	在指定的日期和时间进行分发和激活
分发和激活	启用	主用	分发给指定的计划日期和时间触发作业提交和激活后进行



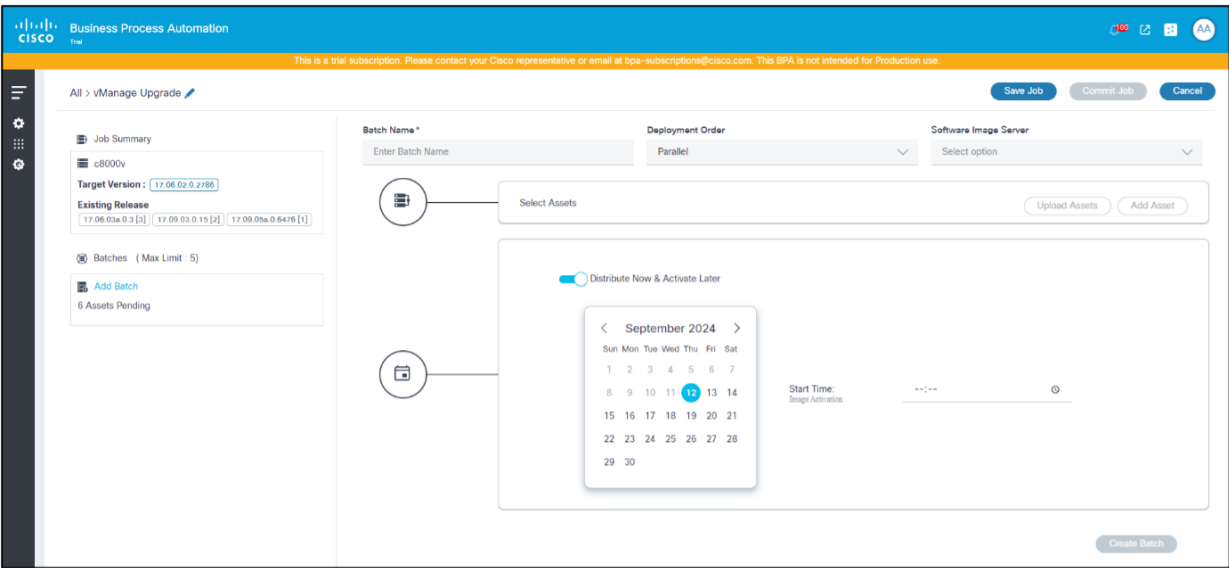
分配作业类型计划选项



激活作业类型计划选项



分发和激活作业类型计划选项



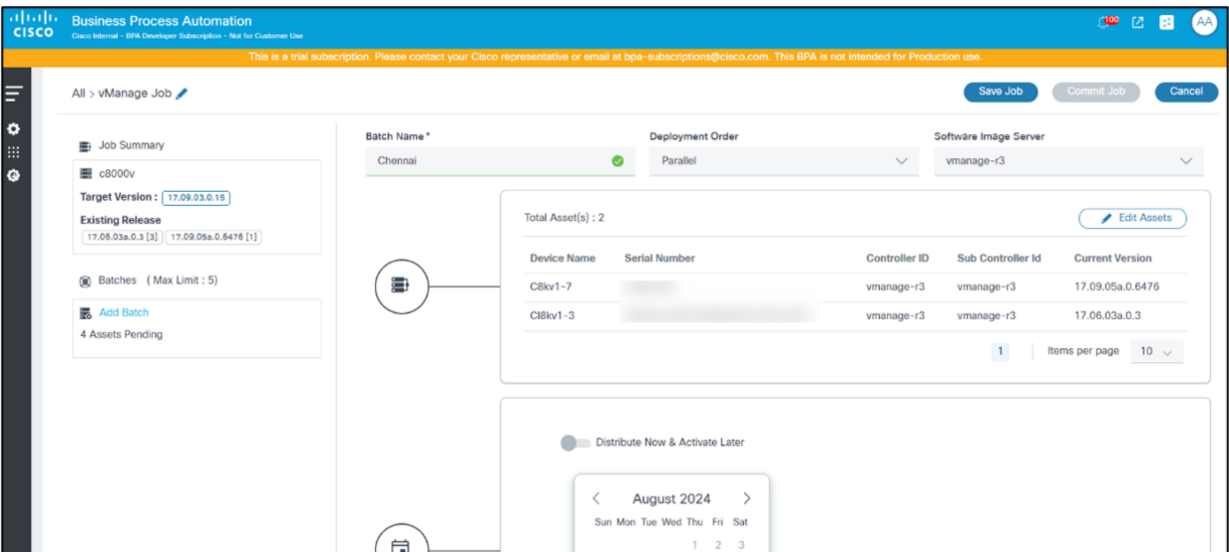
启用立即分发和稍后激活切换的分发和激活作业类型计划选项



注意：下面列出了一些注意事项。

- 当计划多个批时，在两个批之间提供时间间隔，以便避免系统过载。如果多个批重叠，请考虑将其添加到单个批中。
- 启用Distribute Now和Activate Later切换后，在作业提交时间和激活计划之间留出时间间隔。如果不是，激活工作流程可能会创建需要手动干预（即用户必须等到分发完成后再重试）的用户任务。

16. 单击Create Batch。可以在页面左侧查看批处理。



创建作业 — 提交作业

根据需要创建任意数量的批。作业可以处于“草稿”状态，直到所有必需信息都可用为止。

 注意：单击保存作业以保存草稿，从而避免丢失作业数据。

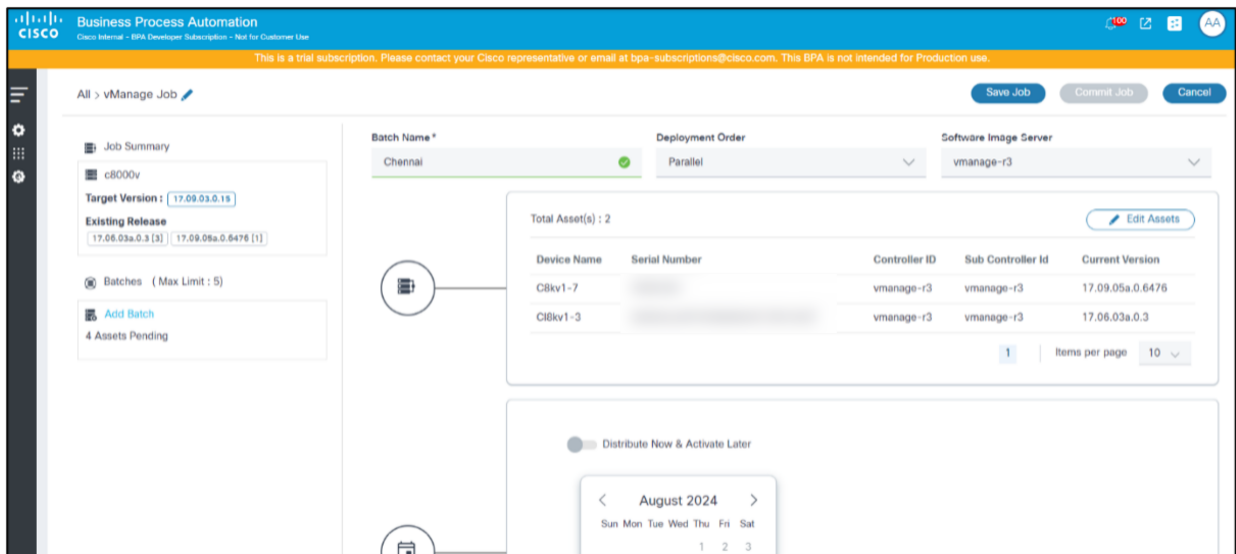
17. 单击Commit Job以完成作业创建。当为任何批处理触发计划时，作业将转换为“部署”状态。

 注意：在升级策略(Upgrade Policy)页面上可以扩展或更新最大批数的阈值。

编辑作业中的批处理

 注意：仅当作业处于“草稿”阶段时才能更新批。

1. 从左侧面板中选择所需的批处理。



编辑资产

- 2. 单击Edit Assets。
- 3. 通过选择或清除添加资产或加载资产中的资产，或者通过更改日期或开始时间修改批计划，进行必要的更改。
- 4. 单击更新批。

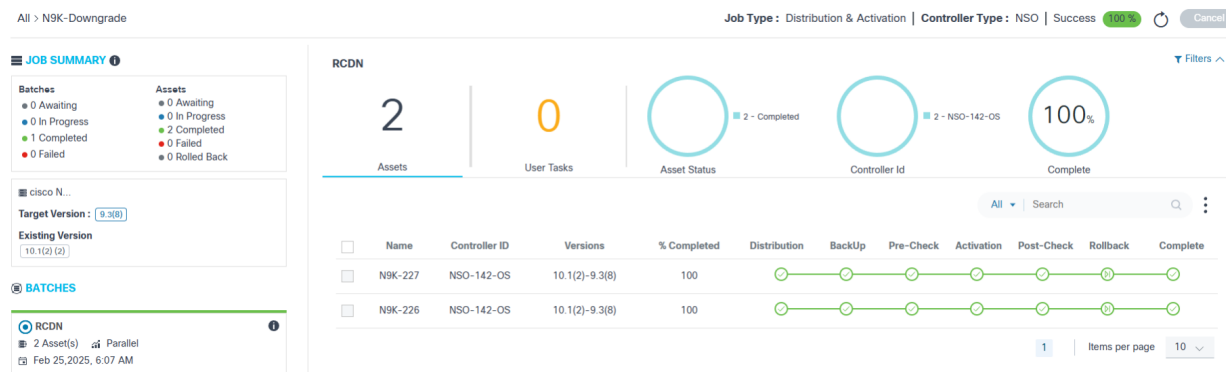
升级作业执行和进度监控

- 1. 使用有权访问升级作业的凭据登录到BPA。
- 2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。

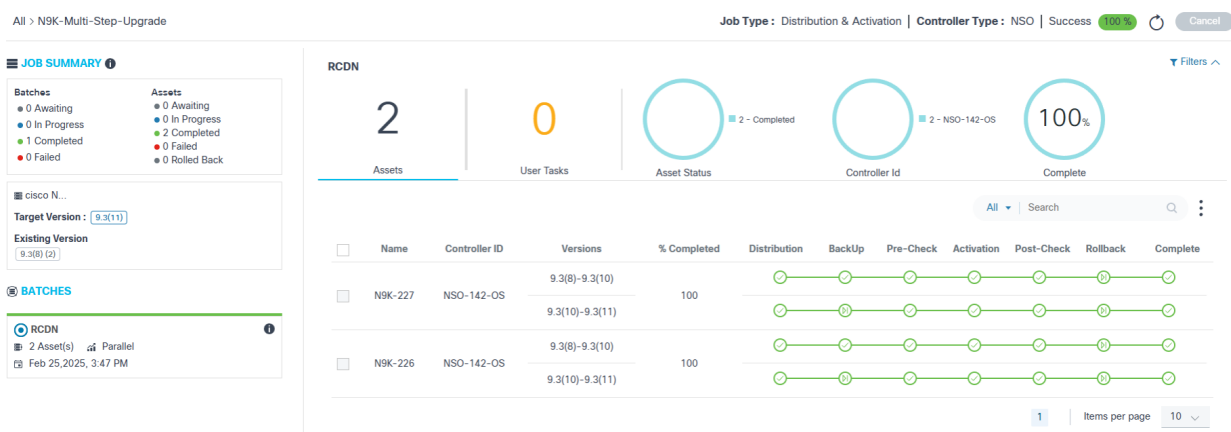


升级作业

3. 将Search过滤器与可用的图表过滤器结合使用，可快速过滤作业。
4. 单击所需的作业。系统将显示Job Summary页面。



一步升级



多步骤升级

左侧面板提供以下信息：

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

作业摘要

- 批次和相应资产的快速汇总

☰ c8000v

Target Version : 17.09.01a.0.240

Existing Version

17.09.03.0.15 (1)

合规策略详细信息（如果策略有一个模型）

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

Target Version :

10.2.5

Existing Release

9.3(7) [4]

合规策略详细信息 (如果策略有多个模型)

- 作业的受影响设备型号、目标软件版本和现有版本版本
- 作为此作业一部分的批的列表

BATCHES

chennai

1 Asset(s)

Parallel

Aug 14,2023, 12:20 PM

批次详细信息

- 批次详细信息 :
 - 灰色顶部边框表示批处理正在等待计划
 - 蓝色顶部边框表示批处理部署正在进行中
 - 绿色顶部边框表示批处理部署完成

以下信息显示在“作业摘要”(Job Summary)页面的顶部 :

All > vmanage_1_2_e2e

Job Type : Distribution & Activation | Controller Type : vManage | Success

100 %

Cancel

职位顶部摘要

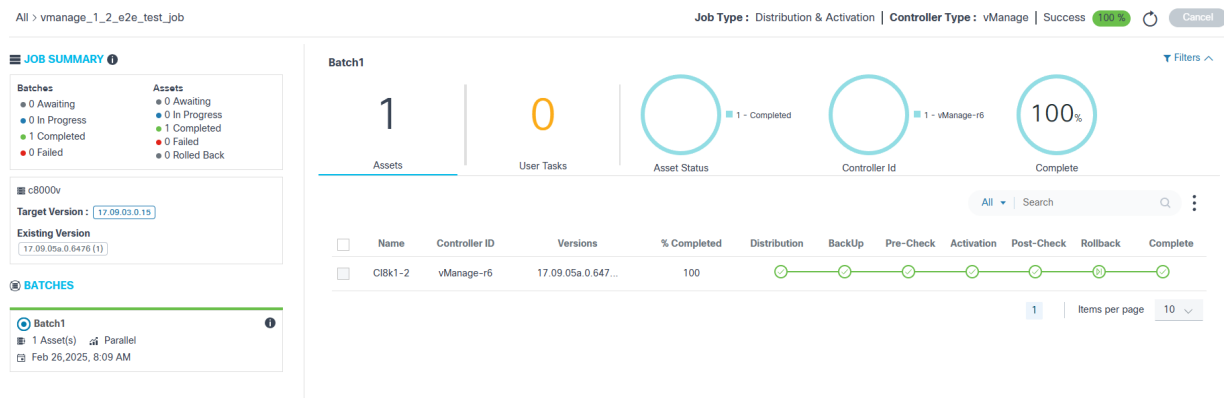
- 当前作业的痕迹导航 (例如 , All > vmanage_1_2_e2e) 。 All选项切换到作业控制面板

- 作业类型
- 控制器类型
- 作业状态及完成百分比：
 - 成功:升级作业成功
 - 失败:升级作业由于某种原因失败
 - 进行中:升级作业正在进行



注意：即使达到一个批的计划，作业状态也会移至进行中

- 等待:作业已提交，但正在等待达到一个或多个批处理计划



作业摘要

Job Summary页上提供了以下选项：

- Refresh图标允许用户按需检索更新
- “取消”用于取消“拟定”和“提交”阶段中的作业，除非达到任何批的计划
- “激活”将在“拟定”状态下创建与之前完成的任务相同的批和资产的新激活作业
 - 仅在作业类型为“分配”且已成功完成时，激活才可用
 - 如果激活作业已创建，并且点击了Activate，将显示一条消息，显示先前创建的作业的状态，并提供一个选项重定向已创建的作业；在新创建的作业中，用户可以选择编辑或删除批处理或资产，但作业类型、控制器类型和一致性策略不可编辑。
- 分析部分下方会显示已分页的资产列表
- Search字段允许对列进行常规和字段特定搜索，例如：
 - 设备名
 - 控制器Id
 - Serial Number

AllSearch

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

1Items per page10

下载批处理报告

- 通过选择More Options图标> Download下载批处理级报告的选项；该报告包含批次级别详细信息以及设备详细信息

	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							

1Items per page10

排序 — 单步升级

	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 — 多步骤升级

JOB SUMMARY

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 IdComplete

AllSearch

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

1Items per page10

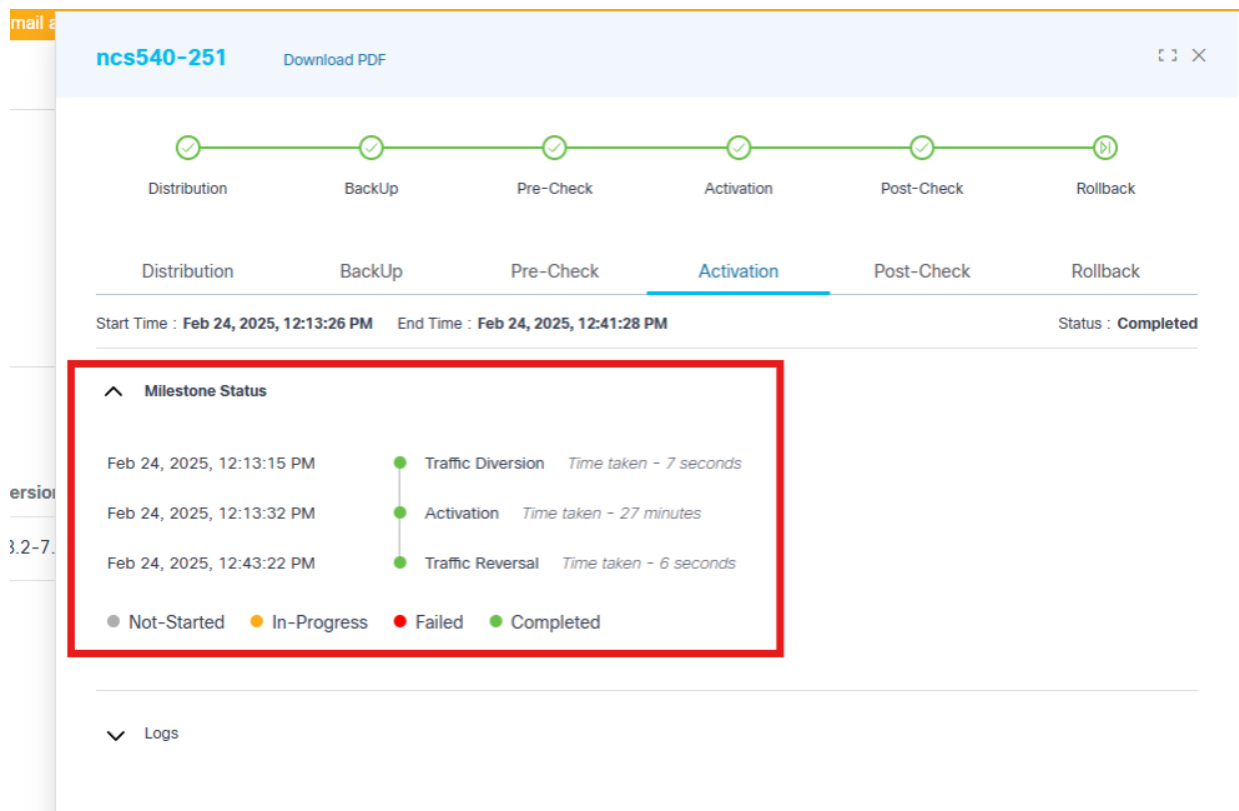
排序 — 网桥SMU升级

- 可通过单击列名来执行排序
- 每个设备的以下升级里程碑以及Name、Controller ID、Versions和% Completed一起显示：
 - 分布
 - 备份
 - 预检查

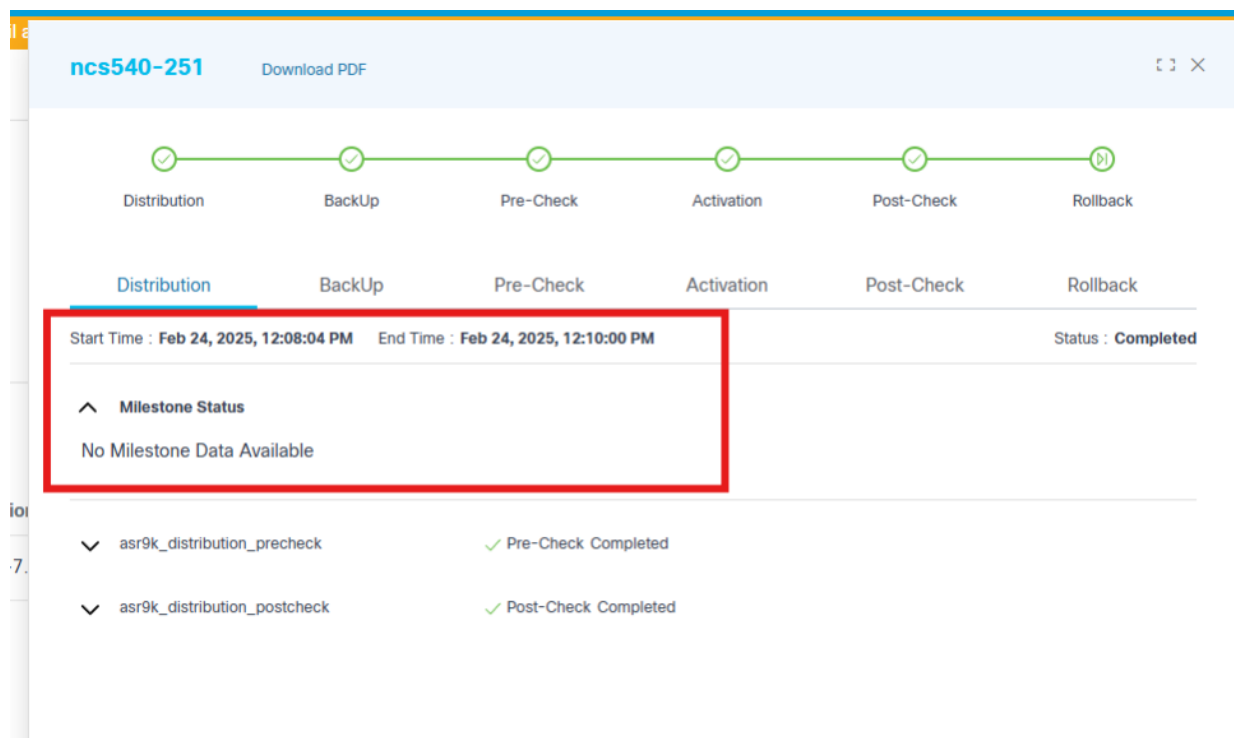
- 流量分流
- 激活
- 后检查
- 流量反转
- 回滚
- 完成

 注意：已完成%根据设备完成的里程碑数显示进度。系统会合计批中的所有设备层完成百分比，以计算批完成百分比。然后，汇总所有批完成百分比以计算任务层完成百分比。

子里程碑（也称为自定义里程碑）是在添加时在标准里程碑下执行和查看的中间重要步骤。有关添加自定义里程碑的详细信息，请参阅[BPA开发人员指南](#)。



子里程碑视图（如果在标准里程碑名称下添加子里程碑）



子里程碑视图（如果未在标准里程碑名称下添加子里程碑）



注意：里程碑因所选作业类型而异。TrafficReversal里程碑不可用于分发作业。

流量转移和流量反转在激活里程碑下移动。

里程碑颜色图例，由以下内容组成：

- 灰色检查:待处理
- 蓝色勾选:进行中
- 绿色标志:已跳过
- 绿色勾选:Completed
- 橙色检查:用户任务
- 红色复选:失败

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	7.6.2-7.7
		7.7.2-7.8

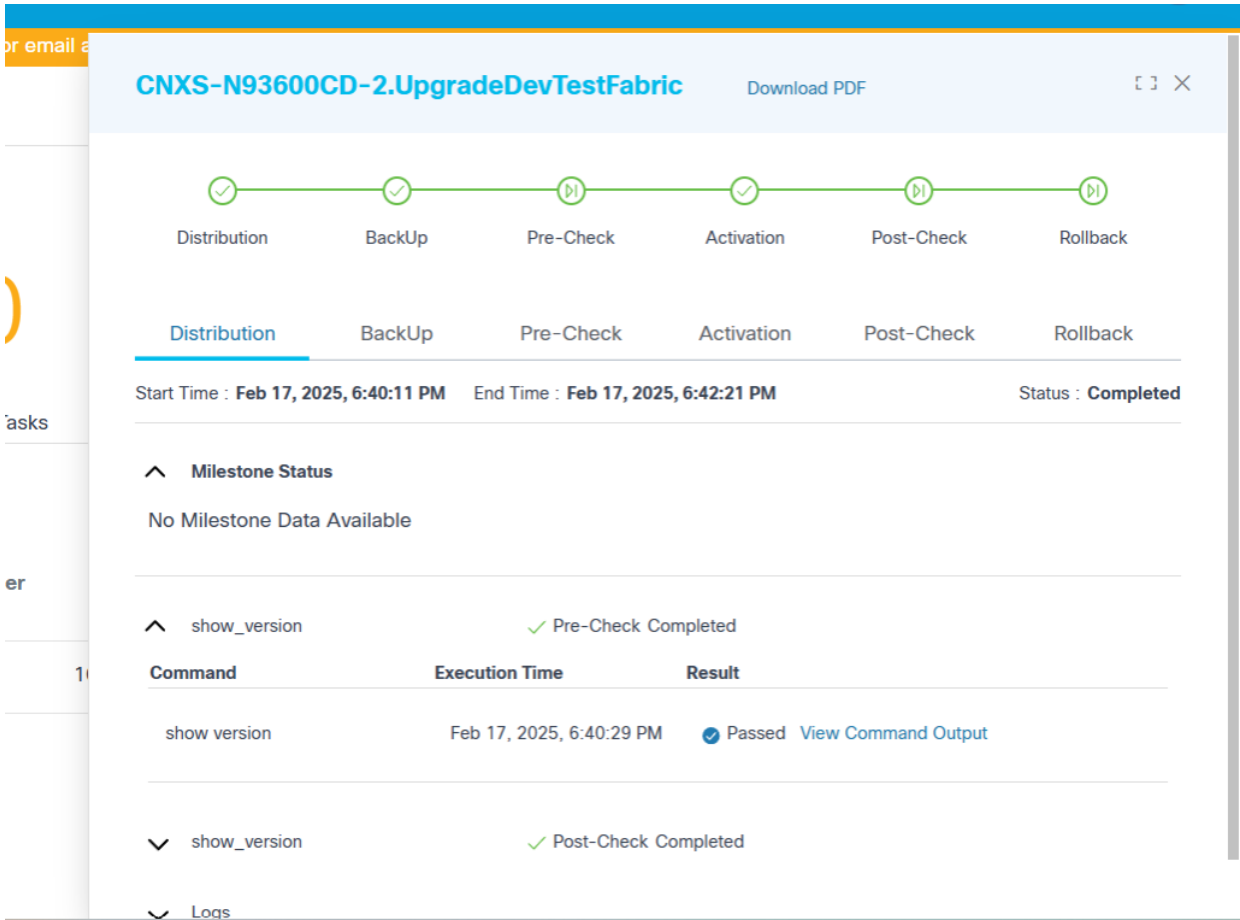
ASR9K-75

Download PDF



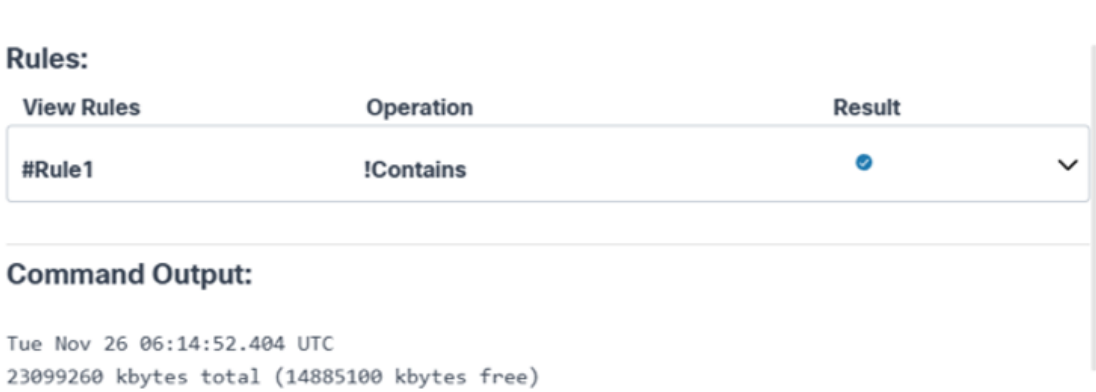
检查前和检查后里程碑视图

对于执行检查前或检查后阶段的事件，用户可以查看完整的命令输出以及各个流程模板中配置的所有命令的验证规则及其状态。



带有预检查命令输出的分布里程碑视图

- 1. 要查看命令输出以及与检查前和检查后命令相关的规则，请单击查看命令输出链接。



检查前和检查后命令输出和相关规则

- 2. 选择Expand图标以查看每个规则的完整详细信息。

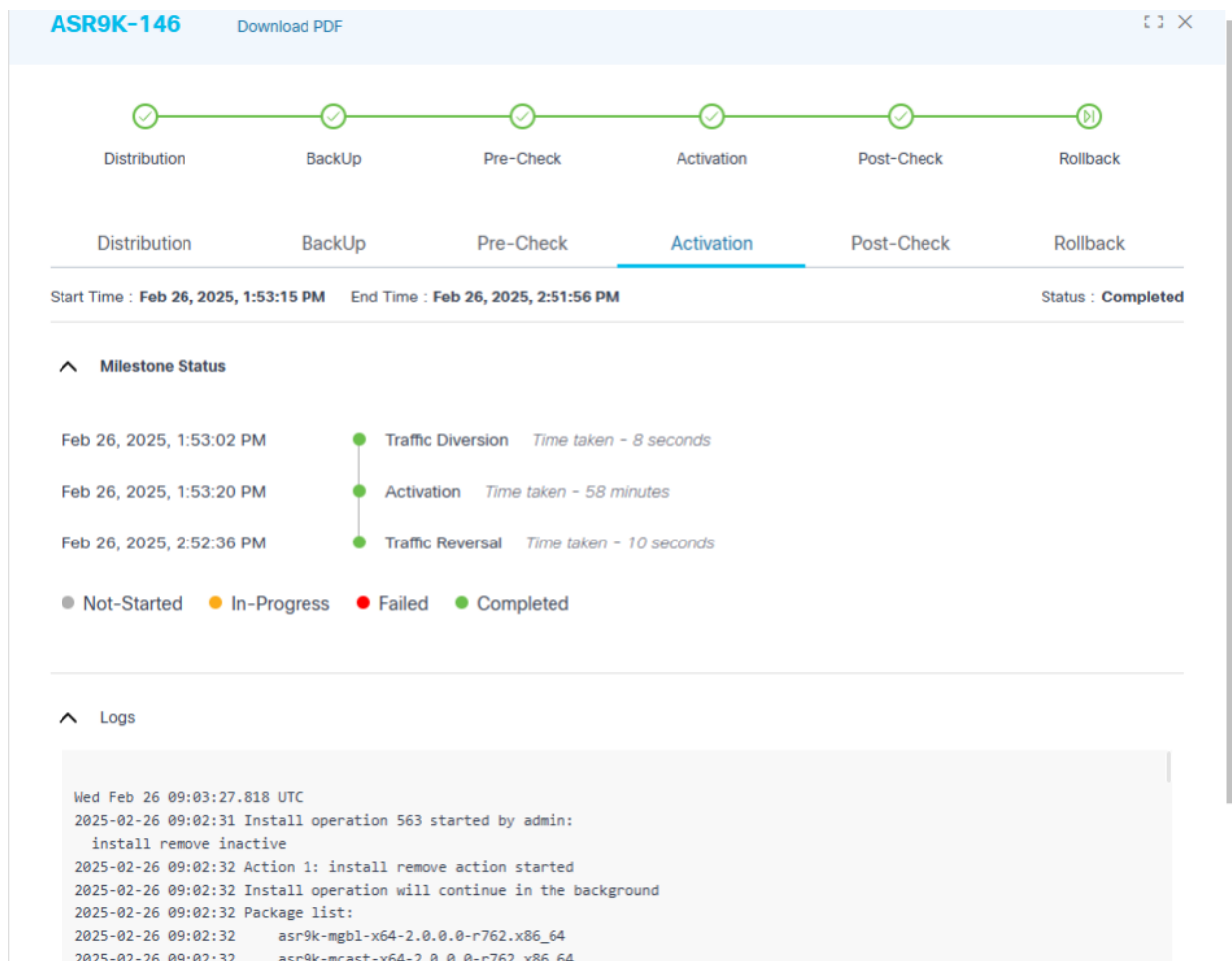
Rules:

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__%%
!
```

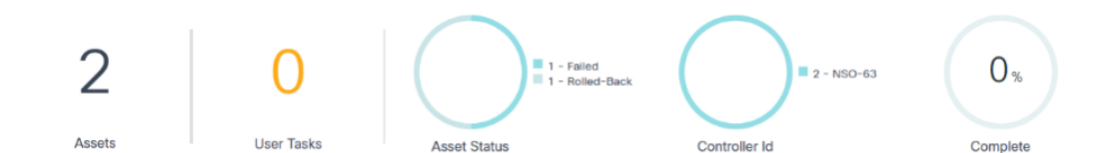
带验证规则的检查前和检查后命令输出



使用实时日志的激活里程碑视图

上图提供了激活里程碑的详细信息，包括实时日志，以帮助监控特定设备的软件激活进度。

当里程碑开始或完成时，单击里程碑将显示详细信息。



Analytics部分

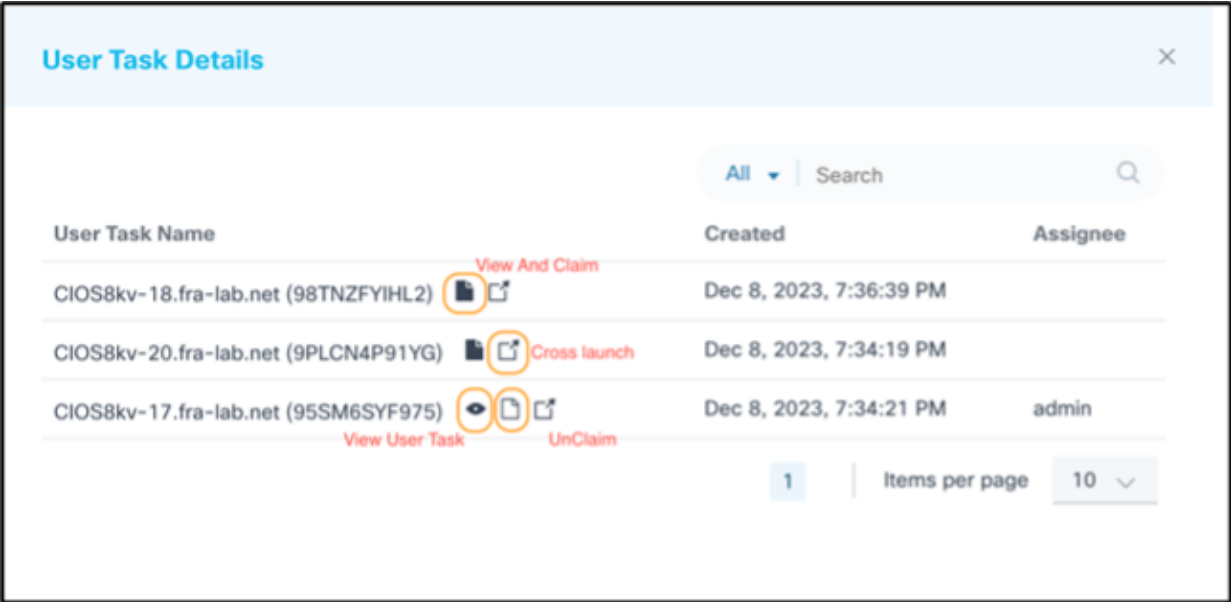
作业摘要页面顶部显示的分析部分显示与当前所选作业相关的以下信息：

- 批次名称（例如，Asia）
- 筛选器^折叠和展开分析部分
- 以下批次详细信息按顺序显示：
 - 资产:资产总数
 - 用户任务:等待操作用户或管理员输入的用户任务总数
 - 资产状态:根据批处理设备状态过滤这些设备。已添加Rollback过滤器以帮助识别已成

功回滚的设备。

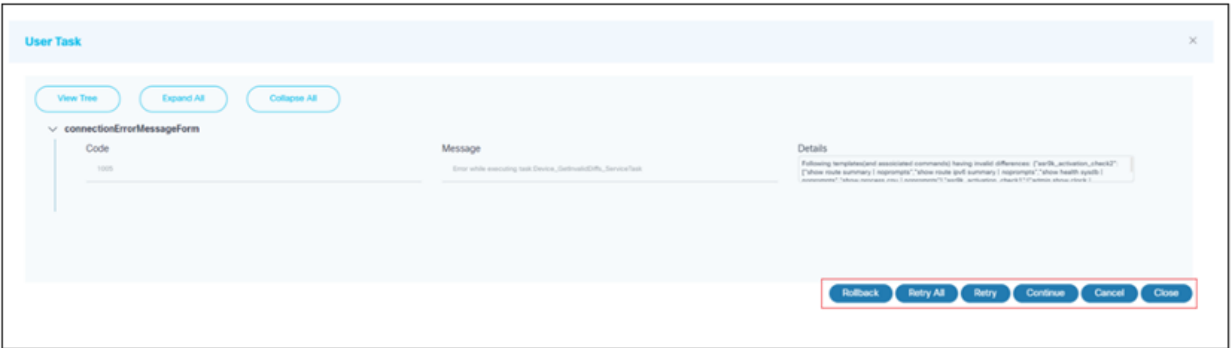
- 控制器ID:过滤属于所选控制器ID的批处理设备
- 完成:整体批处理完成百分比

要处理任何用户任务，请点击用户任务计数。将打开User Task Details窗口，显示以下内容：



用户任务详细信息

- 与需要注意的相应设备相对应的用户任务列表
- 用户任务选项的以下图标：
 - 查看和领款申请:查看用户任务详细信息
 - 交叉启动:在传统UI中查看BPA工作流程任务
 - 取消申请：删除用户任务分配
 - 查看用户任务:查看用户任务详细信息



用户任务

用户任务的视图选项

- 根据任务的上下文显示以下选项：

- 重试:重新执行该任务
 - 全部重试:重新执行所有预先检查和事后检查
 - 继续:继续下一个任务
 - 回滚:回滚到前一版本；当激活或后检查失败或发现前/后检查之间的差异无效时，此选项可用
 - 取消:取消当前作业
 - 关闭:关闭“用户任务”窗口。
- 执行用户任务（如果有），并选择刷新图标以刷新用户任务总数
 - 批次完成百分比合计
 - 按控制器ID过滤的可点击图表



注意：控制器ID之前的数字表示由相应控制器管理的设备总数。

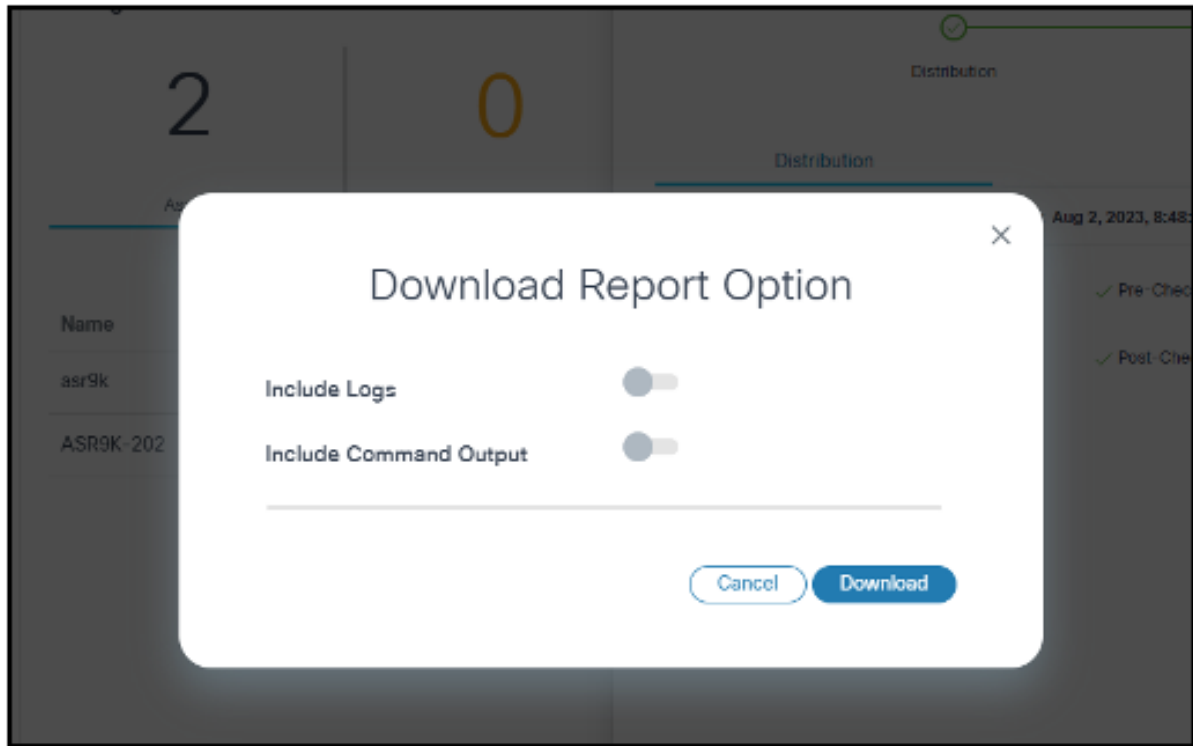
下载软件升级报告

The screenshot shows a software upgrade interface. On the left, there's a 'JOB SUMMARY' section with 'Batches' and 'Assets' counts. The 'Batches' section shows 0 Awaiting, 0 In Progress, 1 Completed, and 0 Failed. The 'Assets' section shows 0 Awaiting, 0 In Progress, 1 Completed, 0 Failed, and 0 Rolled Back. Below this, there's a 'BATCHES' section with a 'Batch1' entry. On the right, there's a progress bar for 'Batch1' with steps: Distribution, Backup, Pre-Check, Activation, Post-Check, and Rollback. The 'Rollback' step is highlighted with a red box and labeled 'Download PDF'. Below the progress bar, there's a 'Milestone Status' section with 'No Milestone Data Available'.

下载 pdf文档

设备名称后接详细视图标题中的下载PDF。用户可以生成并下载当前所选设备的PDF格式的升级报告。要以PDF格式下载升级报告，请执行以下操作：

1. 单击下载PDF。Download Report Option窗口打开。



下载报告选项

2. 启用Include Logs和Include Command Outputs切换。

- 包括日志:在报告中包括实时日志（如果有）
- 包含命令输出:在报告中包括预检查和后检查的命令输出；在本例中，规则后跟命令输出

3. 单击 Download。报告生成开始。

 注意：同时启用Include Logs和Include Command Output切换会增加报告生成和报告的处理时间。仅在需要详细报告时使用这些切换。无论命令输出切换为On或Off，命令规则都包括在报告中。

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
<pre>Rules : Rule View Rules Operation Result #Rule1 Invalid input detected !Contains Passed #Rule2 asdf Contains Failed #Rule3 qwerty !Contains Passed</pre>		

设备报告

存档作业

1. 使用具有足够升级作业访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。
3. 将Search过滤器与可用的图表过滤器结合使用以过滤作业。
4. 选择一个或多个作业。



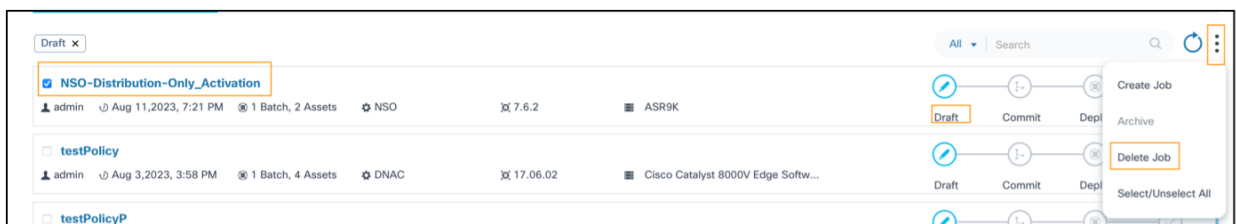
存档作业

5. 选择更多选项图标> 存档。

 注意：只能存档已完成的作业。

删除作业

1. 使用具有足够升级作业访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。
3. 将Search过滤器与可用的图表过滤器结合使用以过滤作业。
4. 选择一个或多个作业。



删除作业

5. 选择更多选项图标> 删除作业。

 注意：只有作业处于草稿阶段时，才能删除作业。

删除作业中的批次

 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

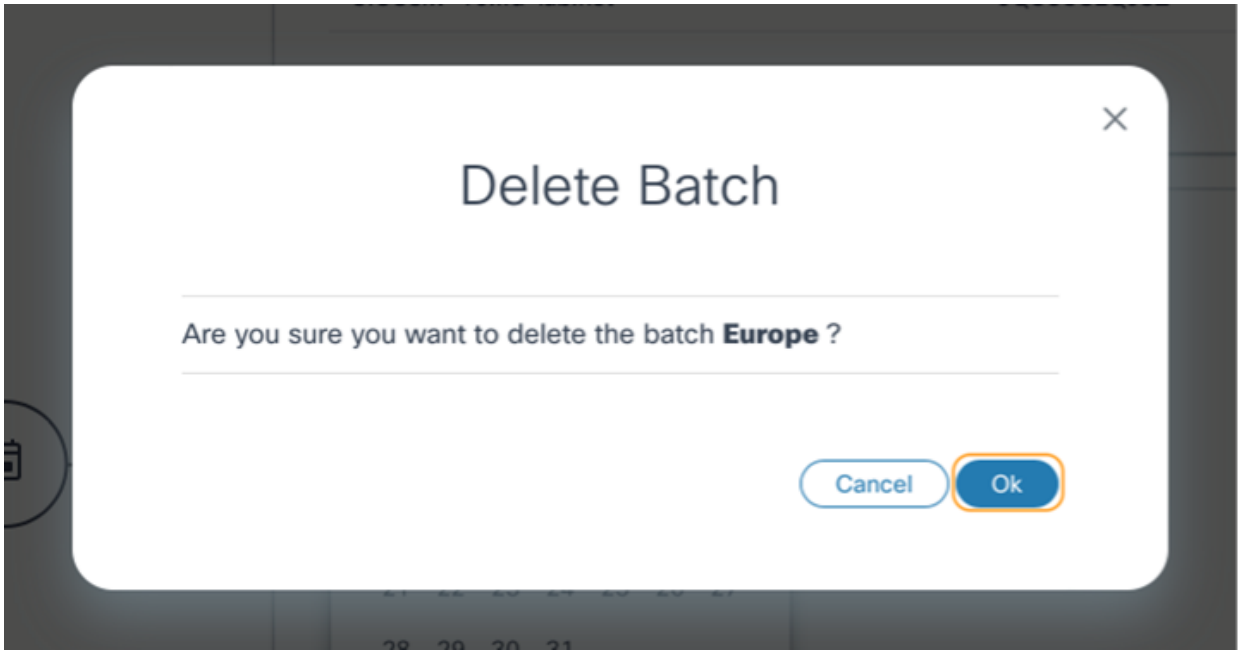
Batch Name *

Europe



删除作业中的批

1. 在侧面板中选择所需批的Delete图标。确认窗口即会打开。



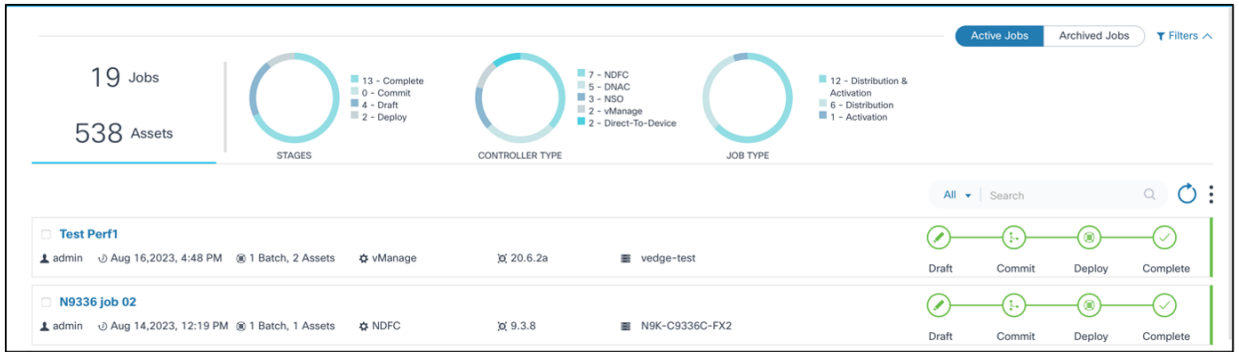
删除批确认

2. Click OK.

与已删除批相关联的资产将返回待定资产池，并且可在新批或现有批中进行选择。

取消作业

- 1. 使用具有足够升级作业访问权限的凭证登录到BPA。
- 2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。



升级作业

- 3. 将Search过滤器与可用的图表过滤器结合使用，以过滤所需的作业。
- 4. 单击所需的作业。系统将显示Job Summary页面。

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

Save Job

Commit Job

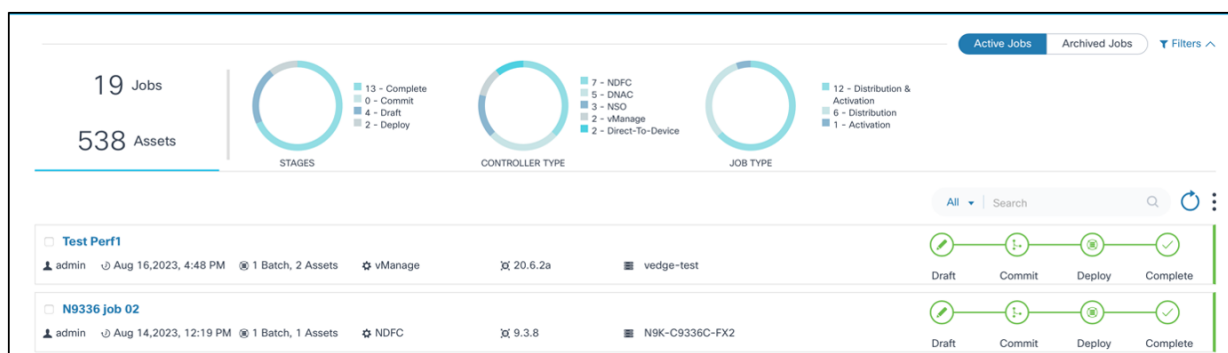
Cancel

取消

5. 单击Cancel (取消) 。

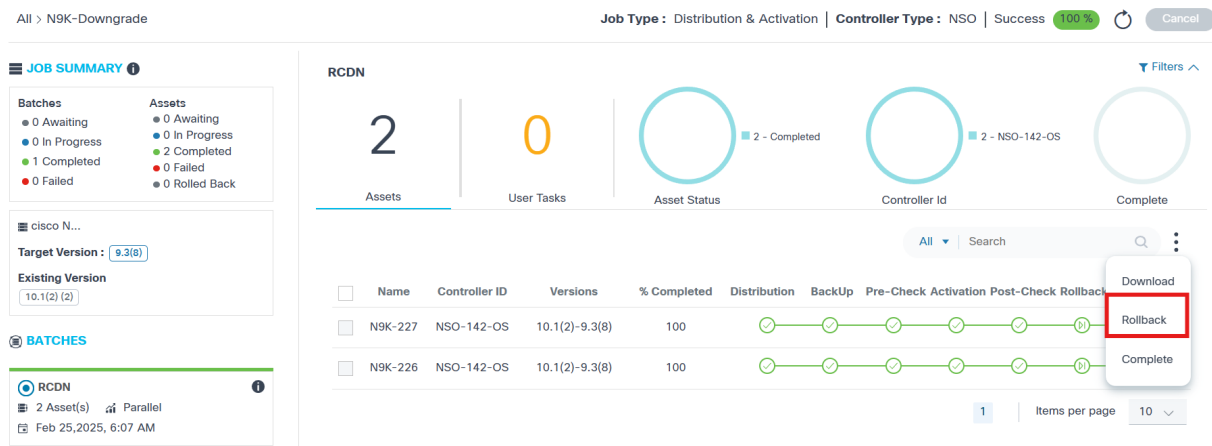
回滚已完成的作业或升级

1. 使用具有足够升级作业访问权限的凭证登录到BPA。
2. 选择OS Upgrade > Upgrade Jobs。系统将显示Upgrade Job页面。



升级作业

3. 将Search过滤器与可用的图表过滤器结合使用，以过滤所需的作业。
4. 单击所需的作业。系统将显示Job Summary页面。在左侧窗格中选择所需的批处理，并在右侧面板上选择需要完全确认/回滚的所需设备
5. 选择More Options图标，然后根据需要点击Rollback或Complete菜单操作。



回滚

 注意：只有在满足以下前提条件时，才能选择设备：

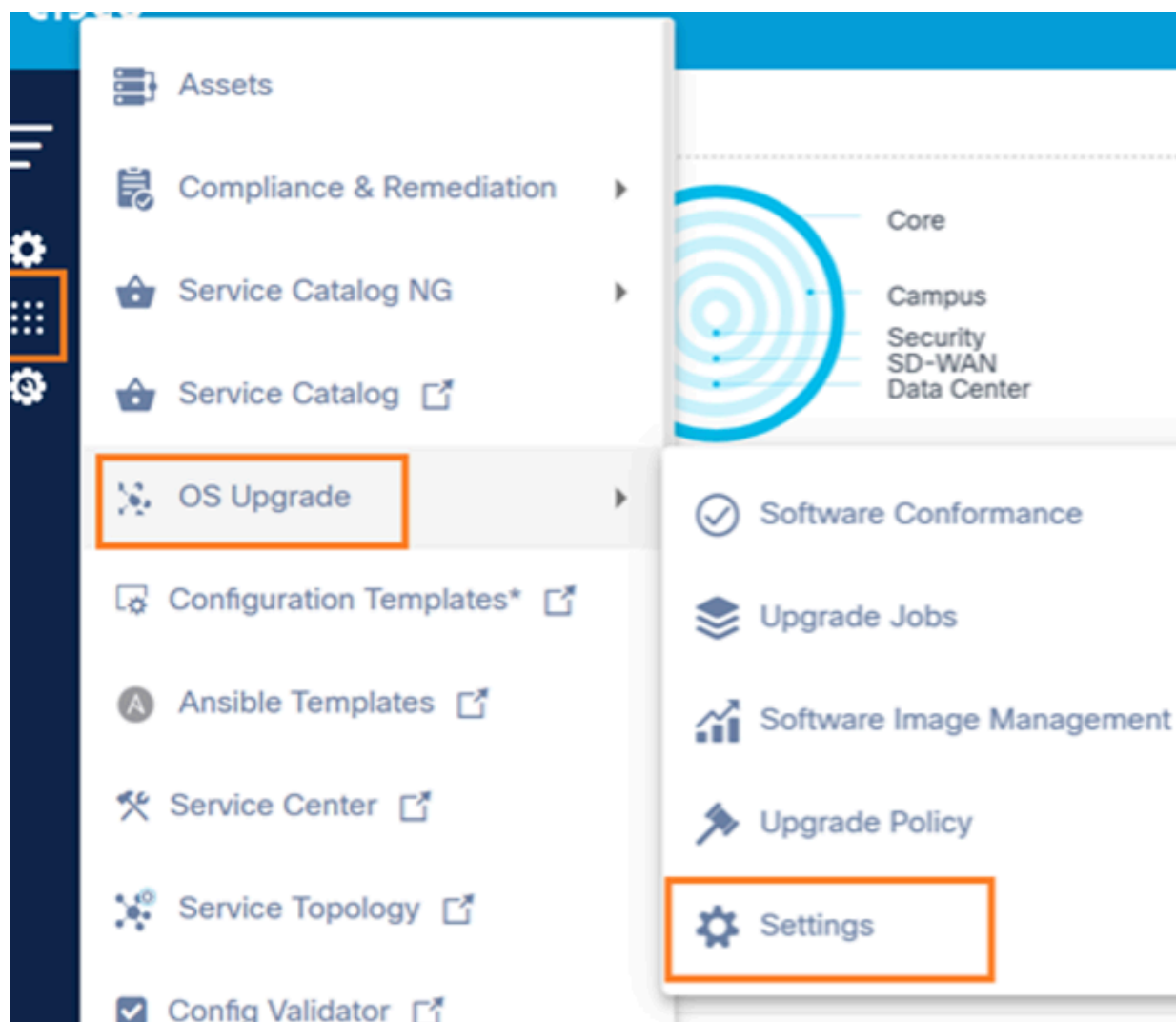
- 必须配置设置以启用已完成升级作业的回滚选项；有关详细信息，请参阅[设置](#)。
- 如果在此期间未执行任何操作，设备将自动转到“完成”状态
- 如果之前已完成回滚，或者回滚里程碑处于“正在等待”状态，则设备可用于按需回滚操作

设置

OS升级设置提供了一个占位符，用于保存在OS升级应用程序的其他组件中使用的常用设置。

要访问“设置”(Settings)页面：

1. 使用具有设置管理访问权限的凭证登录到BPA。



设置

2. 选择OS Upgrade > Settings。将打开Settings页面。

Settings页面包含以下两个选项卡：

- 软件一致性:可以在此选项卡中更新允许自动一致性执行计划的配置
- 回滚:允许回滚完整设备升级的配置可以在此选项卡中更新

软件一致性

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

“软件一致性”选项卡

Software Conformance选项卡提供以下内容：

- 计划一致性检查:启用或禁用计划
- 开始日期:选择MM/DD/YYYY



注意：开始日期应为将来日期。

- Cron模式：提供以下详细信息：
 - 分钟(0-59)
 - 小时(0-23)
 - 天 (月) (1-31)
 - 月(1-12)
 - 天 (周) (1-7)
- 添加自动刷新闻隔:默认值为30秒
- 保存：保存更改

回滚

“回滚”选项卡

Rollback选项卡提供以下内容：

- 用户验证切换:启用或禁用用户验证
 - 启用状态：升级作业中的设备等待用户确认回滚或完成升级，直到达到在配置阈值时间（小时）中配置的阈值时间；到达时，设备会自动进入Completed状态
 - 禁用状态：升级作业中的设备自动完成升级，无需等待用户确认
- 确认阈值时间：添加阈值等待时间（以小时为单位）
- 保存：保存更改

部署配置

- 合规性策略检查和SWIM元数据的默认时间表每天本地时间上午7:25。
- 要更改SWIM映像元数据同步的默认计划，请导航到BPA安装目录“<BPA install directory>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json”并使用Cron表达式更新schedule.swimSchedule属性。可以在部署后更新计划。有关详细信息，请参阅[软件一致性](#)。
- 要增加或减少不同控制器类型在并行模式下处理的最大设备数量，请执行以下操作：

1. 更新以下文件：

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

2. 导航到Update throttling > capabilities > image-activation，image-distribute以增加并发激活或分发限制。



注意：在更新这些限制之前，请参阅[支持的控制器和设备平台](#)。

访问控制

基于角色的访问控制

BPA支持基于角色的访问控制(RBAC)。 在RBAC模型中，角色封装用户可执行的一组权限（即操作）。对于访问控制，管理员可以将预定义角色或新创建的具有权限的角色分配给用户组。一个用户可属于一个或多个用户组，每个用户组可分配给一个或多个角色，这些角色赋予该组中的用户特定的访问权限。

下表概述了OOB操作系统升级角色和相关权限。

服务	组	意图	超级管理 员	用例管理 员	只读用户 (操作系 统升级使 用案例只 读用户)	操作员
OSUpgradeService	ui_app	显示或隐藏升级作 业应用程序	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	显示或隐藏软件一 致性应用程序	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	显示或隐藏 SWIM应用程序	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	显示或隐藏软件升 级策略应用	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	显示或隐藏软件升 级设置	Yes	Yes	Yes	Yes
OSUpgradeService	升级作业	管理升级作业（例 如，创建、更新、 删除和提交）	Yes	Yes	无	Yes
OSUpgradeService	升级作业	取消升级作业	Yes	Yes	无	Yes
OSUpgradeService	升级作业	按需存档作业	Yes	Yes	无	Yes
OSUpgradeService	升级作业	手动审批	Yes	Yes	无	Yes
OSUpgradeService	软件一致性策略	查看软件一致性策 略和执行结果	Yes	Yes	Yes	Yes
OSUpgradeService	软件一致性策略	创建、更新和删除 软件一致性策略	Yes	Yes	无	无
OSUpgradeService	软件一致性策略	按需执行软件一致 性策略	Yes	Yes	无	Yes
OSUpgradeService	升级策略	查看操作系统升级	Yes	Yes	Yes	Yes

服务	组	意图	超级管理 员	用例管理 员	只读用户 (操作系 统升级使 用案例只 读用户)	操作员
		策略				
OSUpgradeService	升级策略	管理操作系统升级策略	Yes	Yes	无	无
OSUpgradeService	Swim-image-management	创建、更新和删除软件映像	Yes	Yes	无	Yes
OSUpgradeService	Swim-image-management	查看SWIM	Yes	Yes	Yes	Yes
OSUpgradeService	Swim-image-management	同步软件映像	Yes	Yes	无	Yes
OSUpgradeService	软件建议	同步软件建议元数据	Yes	Yes	无	无
OSUpgradeService	软件建议	查看建议或见解	Yes	Yes	Yes	Yes
OSUpgradeService	软件建议	管理一致性策略	Yes	Yes	无	无
OSUpgradeService	软件一致性设置	查看软件一致性设置	Yes	Yes	Yes	Yes
OSUpgradeService	软件一致性设置	管理软件一致性设置	Yes	Yes	无	无

 注意：可以根据要求完成自定义角色和权限映射。请参阅[资源组](#)。

资源组

此功能为BPA资源提供精细的访问控制，例如升级策略，限制未经授权的用户更新操作系统升级应用中定义的策略。管理员可以通过定义具有可访问策略的资源组来限制访问。

要创建资源组，请执行以下操作：

1. 导航到设置 > 资源组。

Add Resource Group

Resource Group name *
osupgrade-res-grp

Resource Type:
os-upgrade-policy

Description:
Enter resource group description

Resources:

☐	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

添加资源组

2. 使用非管理员用户可以访问的策略创建资源组。
3. 选择os-upgrade-policy作为Resource Type。系统随即会显示相应的资源。
4. 选择所需的升级策略。
5. 单击 submit。属于此用户组的非管理员用户现在仅有权访问所选资源组中可用的策略。

要将资源组与用户组相关联，请创建访问策略。

Add Policy

Policy name *
osupgrade-access-policy

Description:
Enter policy description

Resource Groups:

osupg

Asset Groups:

ALL-ACCESS static
ReadOnly static
replacement-nodes static

User Groups:

osupgrade

osupgrade-user-grp

1 Items per page 10

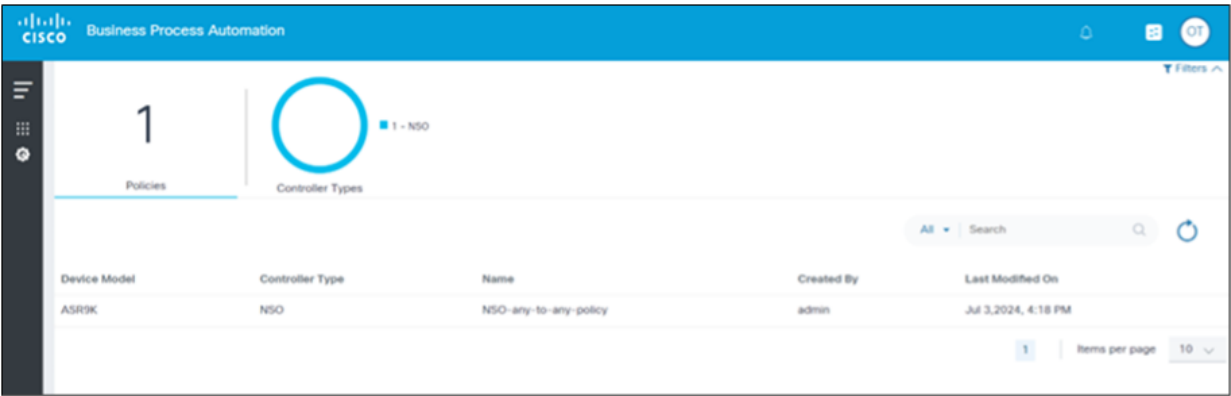
添加访问策略

 **注意：**创建资源组后，应通过访问策略将其与用户组关联。有关以下内容的详细信息，请参阅[访问控制](#)：

- 用户
- 角色
- 用户组
- 访问策略
- 资源组

- 资产组

以下是有权访问受限资源的非管理员用户的示例：



具有资源限制的非管理员用户

零信任标志设置

用户可访问的资源可能因零信任标志设置而异。零信任标志可以设置为true或false。下表汇总了基于零信任标志设置的资源访问可能性。

用户	用户组	访问策略	资源组	相关资源	零信任	启用
User 1	UG1	AP1	RG1	2资源	2资源	2资源
User 1	UG1	AP2	RG2	0资源	0资源	0资源
User 1	UG1	AP3	无		0资源	所有资源
User 1	UG1	无	无		0资源	所有资源

要启用或禁用零信任标志，请执行以下操作：

1. 导航到以下配置路径：

```
cd /opt/bpa/bpa-helm-chart-  
  
/charts/cisco-bpa-platform-mw-auth/public_conf/config.json
```

2. 修改zeroTrustPolicies值。
3. 导航至以下核心捆绑包：

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

4. 运行以下命令以删除核心掌舵：

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

5. 运行以下命令检查Pod的状态

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

6. 在终止所有Pod后，运行以下命令以安装核心控制板：

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

7. 运行以下命令以验证启动的Pod的状态：

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

操作系统升级问题故障排除

本节提供与BPA中观察到的操作系统升级应用程序相关的故障排除提示。

创建一致性策略时看不到目标设备型号

确保对应的映像元数据在SWIM下的软件映像中可用。如果未找到，请执行以下任一选项：

- 同步映像以从Cisco Catalyst Center、NDFC、vManage和FMC等控制器检索映像元数据
- 为NSO、CNC、直接到设备和ANSIBLE等控制器创建所需的映像元数据

软件一致性显示非运行状态

这可能是由于以下原因：

- 创建软件一致性策略时，找不到具有所选模型的资产
- SWIM中的型号名称与所有设备的设备清单中的一致性设备型号不匹配
- 如果选择SMU作为软件一致性创建的一部分，则所有设备的SMU发现均失败
- 为合规性检查模板执行选择的过程模板失败或找不到
- 创建软件符合性时，所选型号下的所有设备均无法使用序列号或当前版本

某些设备的软件符合性结果状态未知

这可能是由于以下原因：

- SWIM中的型号名称与设备资产中的一致性设备型号不匹配
- 如果选择SMU作为软件一致性创建的一部分，则设备的SMU发现失败
- 为合规性检查模板执行选择的过程模板失败或找不到
- 设备无法使用序列号或当前版本

升级作业完成进度百分比

如果升级作业完成进度百分比小于100，即使升级已经完成，请确认在OS Upgrade > Settings > Rollback下启用了Wait for Rollback设置，并且User Verification切换已启用。如果总体完成百分比保持低于100，请选择Rollback或Complete。

作业安排已达到，设备停滞在“等待”状态

如果设备在计划作业启动后停滞在“等待”状态，请尝试重新启动Kafka、Camunda、Scheduler和OS Upgrade micro服务。

关于此翻译

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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