

Guide de l'utilisateur BPA Mise à niveau OS v5.1

- [Introduction](#)
 - [Fonctionnalités clés](#)
 - [Flux de bout en bout](#)
 - [Proposition de valeur](#)
 - [Contrôleurs et plates-formes de périphériques pris en charge](#)
 - [Nouvelles fonctionnalités](#)
- [Conditions préalables](#)
- [Utilisation de l'application de mise à niveau OS](#)
 - [Gestion des images logicielles](#)
 - [Images logicielles](#)
 - [Synchronisation des images logicielles et des métadonnées](#)
 - [Ajout de métadonnées d'image logicielle](#)
 - [Téléchargement en masse des métadonnées des images logicielles](#)
 - [Modification des métadonnées d'image logicielle existantes](#)
 - [Suppression de métadonnées d'image logicielle](#)
 - [Gestion du serveur de distribution d'images](#)
 - [Serveur de distribution d'images](#)
 - [Ajout des détails du serveur d'images](#)
 - [Modification des détails du serveur d'images](#)
 - [Suppression des détails du serveur d'images](#)
 - [Aperçu des logiciels](#)
 - [Conditions préalables](#)
 - [Récupération des données Software Insights dans BPA](#)
 - [Affichage et gestion des avis de sécurité](#)
 - [Affichage et gestion des bogues de priorité](#)
 - [Affichage des informations logicielles](#)
 - [Affichage et sélection des versions logicielles suggérées par le fournisseur](#)
 - [Identification des périphériques nécessitant une mise à niveau logicielle](#)
 - [Conformité logicielle](#)
 - [Conditions préalables](#)
 - [Création de données de module EPLD dans l'application de gestion des données de référence](#)
 - [Affichage et gestion de la conformité des logiciels](#)
 - [Création de stratégies de conformité logicielle](#)
 - [Exécution de contrôles de conformité logicielle à la demande](#)
 - [Planification de l'exécution des contrôles de conformité logicielle](#)
 - [Mise à jour des stratégies de conformité logicielle](#)
 - [Suppression des stratégies de conformité logicielle](#)
 - [Affichage et téléchargement des résultats de conformité](#)
 - [Politique de mise à niveau](#)
 - [Conditions préalables](#)
 - [Affichage et gestion des stratégies de mise à niveau](#)

- [Création de stratégies de mise à niveau](#)
- [Pont SMU](#)
- [Modification des stratégies de mise à niveau](#)
- [Affichage des stratégies de mise à niveau](#)
- [Suppression des stratégies de mise à niveau](#)
- [Contrôle de l'accès aux stratégies de mise à niveau](#)
- [Tâches de mise à niveau](#)
 - [Conditions préalables](#)
 - [Affichage et gestion des travaux de mise à niveau](#)
 - [Planification des travaux de mise à niveau](#)
 - [Modification d'un lot dans une tâche](#)
 - [Exécution des tâches de mise à niveau et surveillance de la progression](#)
 - [Téléchargement du rapport de mise à niveau logicielle](#)
 - [Archiver des tâches](#)
 - [Suppression de travaux](#)
 - [Supprimer des lots dans les ordres de fabrication](#)
 - [Annulation de travaux](#)
 - [Annulation des travaux ou des mises à niveau terminés](#)
- [Paramètres](#)
 - [Conformité logicielle](#)
 - [Restauration](#)
- [Configuration du déploiement](#)
- [Contrôle d'accès](#)
 - [Contrôle d'accès basé sur les rôles](#)
 - [Groupes de ressources](#)
 - [Paramètre d'indicateur de confiance zéro](#)
- [Résolution des problèmes de mise à niveau OS](#)
 - [Impossible de voir le modèle de périphérique cible lors de la création d'une stratégie de conformité](#)
 - [La conformité du logiciel indique un état de non-fonctionnement](#)
 - [L'état du résultat de la conformité logicielle de certains périphériques est inconnu](#)
 - [Pourcentage de progression de la tâche de mise à niveau](#)
 - [Planification des tâches atteinte, les périphériques sont bloqués dans l'état En attente](#)

Introduction

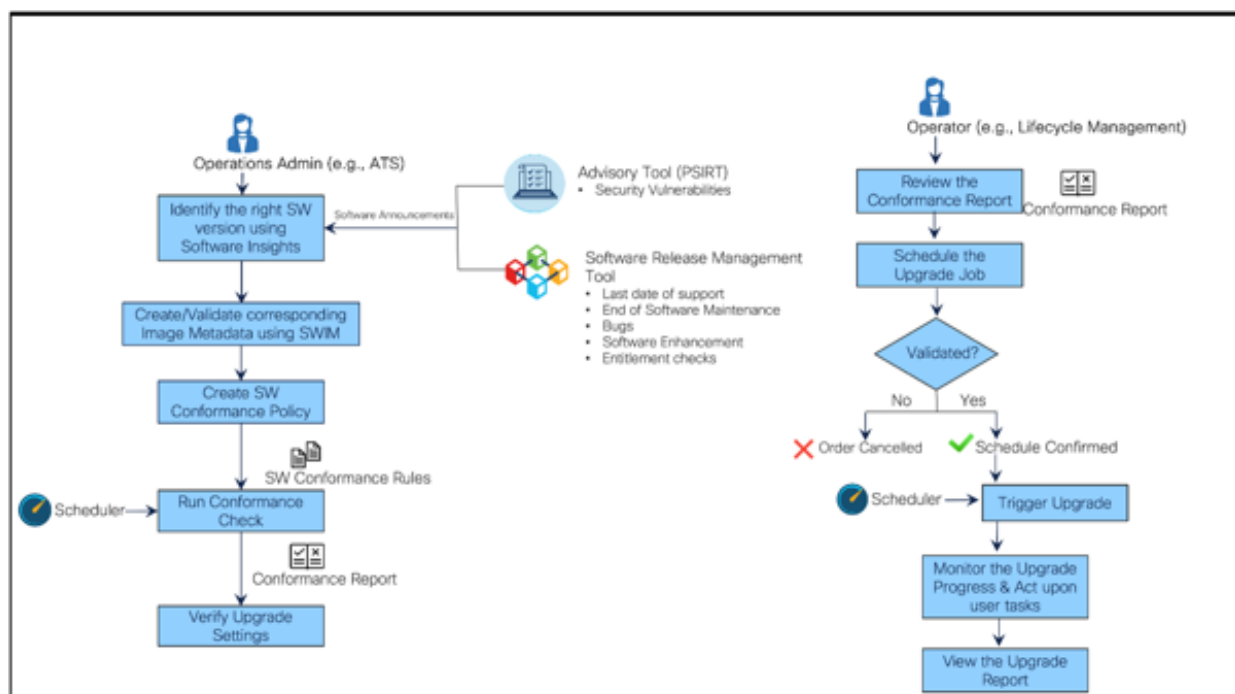
L'application de mise à niveau du système d'exploitation Business Process Automation (BPA) fournit une solution d'automatisation complète pour assurer la conformité logicielle et les mises à niveau des périphériques réseau sur différents domaines. Il prend en charge plusieurs contrôleurs de domaine et offre une expérience utilisateur unifiée. Il prend en charge les mises à niveau de base du système d'exploitation et les mises à jour de correctifs SMU (Software Maintenance Update) ou RPM Package Manager (RPM).

Fonctionnalités clés

L'application Mise à niveau du système d'exploitation offre les fonctionnalités d'automatisation suivantes :

- Gestion des images logicielles : Une liste centralisée des images logicielles et de leurs versions (de tous les fournisseurs) pour le processus de mise à niveau logicielle à utiliser
- Informations sur les logiciels : Identifie les risques et les vulnérabilités des logiciels exposés aux ressources réseau et obtient des informations sur les versions logicielles recommandées par le fournisseur
- Conformité logicielle : Identifie toutes les ressources du réseau dont les images logicielles doivent être mises à niveau
- Méthode de mise à niveau de la procédure (MOP) Définition : Prédéfinit le processus de mise à niveau, ainsi que les vérifications préalables et postérieures pour chaque modèle ou famille de périphériques fournisseur
- Tâches de mise à niveau : Planifie les mises à niveau des ressources non conformes pendant les fenêtres de maintenance dans les différentes zones géographiques, surveille la progression de la mise à niveau et obtient des rapports détaillés

Flux de bout en bout



Flux de bout en bout

La figure ci-dessus illustre les flux d'appels de l'application de mise à niveau du système d'exploitation pour deux utilisateurs différents : Administrateur des opérations et Opérateur réseau, qui est prêt à l'emploi (OOB). Référez-vous à [Contrôle d'accès](#) pour plus d'informations sur les

rôles OOB et les autorisations correspondantes.

Persona	Description	Espace de travail
Administrateur des opérations	Détecte les vulnérabilités logicielles (par exemple, les avis, les bogues, les bulletins de fin de vie) affectant les ressources réseau	BPA: Mise à niveau du système d'exploitation/Gestion des images logicielles/Conseils
Administrateur des opérations	Identifie la version du logiciel et les ressources affectées et détermine la version cible correcte en fonction des suggestions fournies par le fournisseur	BPA: Mise à niveau du SE/Gestion des images logicielles/Informations
Administrateur des opérations	Crée les métadonnées d'image logicielle requises	BPA: Mise à niveau du système d'exploitation/Gestion des images logicielles/Images logicielles
Administrateur des opérations	Crée l'intention pour les modèles de périphériques affectés et exécute la stratégie à la demande ou lors de l'exécution planifiée de la stratégie	BPA: Stratégie de mise à niveau du SE/conformité logicielle
Administrateur des opérations	Identifie les actifs non conformes ou affectés	BPA: Mise à niveau du système d'exploitation/Conformité logicielle/Afficher les résultats
Administrateur des opérations	Crée ou modifie la politique de mise à niveau conformément à la MOP de mise à niveau ; cela inclut la prédéfinition des contrôles préalables et postérieurs, des workflows pour la distribution ou l'activation, le détournement ou l'inversion du trafic et la restauration pour les mises à niveau en une ou plusieurs étapes	BPA: Mise à niveau/Stratégie de mise à niveau
Opérateur de réseau	Planifie une tâche de mise à niveau de tous les périphériques non conformes	BPA: Tâches de mise à niveau/mise à niveau OS
Opérateur de réseau	Surveille la progression du travail de mise à niveau	BPA: Travaux de mise à niveau/de mise à niveau du SE/Détails du travail
Opérateur de réseau	Agit sur les tâches des utilisateurs, le cas échéant, pour résoudre les problèmes et permet au processus	BPA: Mise à niveau/Mise à niveau du système d'exploitation

Proposition de valeur

Les valeurs ajoutées suivantes sont fournies par l'application de mise à niveau du système d'exploitation :

- Une première approche par API pour faciliter la consommation de services à partir des systèmes OSS (Operations Support Systems) et BSS (Business Support Systems) Northbound
- Validation rapide de la conformité logicielle des périphériques réseau sur les réseaux gérés par divers contrôleurs de domaine
- Les opérateurs contrôlent mieux les tâches de mise à niveau en utilisant des mécanismes de traitement par lots, de mise en file d'attente et de planification
- Les tâches de mise à niveau peuvent être créées tôt pour les révisions et exécutées ultérieurement
- Un mécanisme de mise en file d'attente qui permet un débit plus rapide et amélioré avec des pannes minimales à nulles
- Sauvegardes automatiques de la configuration avant la mise à niveau, permettant des restaurations transparentes en cas de panne
- Exécutions avant et après vérification, garantissant la réussite des mises à niveau sans interruption du service
- Une approche basée sur des politiques qui offre la flexibilité de prédéfinir la MOP de mise à niveau avec des contrôles de pré- et post-validation, la distribution ou l'activation, le détournement ou l'inversion du trafic et les processus de restauration, permettant de les personnaliser selon les besoins

Contrôleurs et plates-formes de périphériques pris en charge

Les plates-formes suivantes ont été validées en BPA et sont prises en charge en mode hors connexion. Cependant, le cadre est générique et peut être étendu à de nouvelles plates-formes. La prise en charge de plates-formes supplémentaires par OOB sera assurée dans les versions futures en fonction de la priorité.

Contrôleur(s) de domaine	Plates-formes de périphériques
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS, Cisco IOS-XE
vManage v20.12.4	- Cisco IOS, Cisco IOS-XE

Contrôleur(s) de domaine

Plates-formes de périphériques

Remarque : Les périphériques doivent être v17.9.x ou supérieur pour que la distribution de serveur distant fonctionne

Contrôleur de fabric de tableau de bord
Nexus (NDFC) v12.1.2e et v12.2.2

- Cisco-NXOS (N9k)

Centre de gestion des pare-feu (FMC)
v7.4.1

- Firepower 3140

- Cisco-IOSXR (NCS540, NCS560, ASR9K)

- Cisco-NXOS (N9K)

Network Services Orchestrator (NSO)
v6.3

Remarque : NX-OS NED v5.25.17 ou supérieur est requis

Contrôleur de réseau croisé (CNC) v6.0

- Cisco-IOSXR (NCS540, ASR9K)

ANSIBLE v2.9.18 (AWX - 17.1.0)

- Cisco-IOSXR (NCS540, ASR9K)

Direct-to-Device (via Telnet (Teletype
Network) et SSH (Secure Shell))

- Cisco-IOSXR (NCS540, ASR9K)

Nouvelles fonctionnalités

Pour connaître les fonctionnalités incrémentielles mises à disposition pour l'exemple d'utilisation Mise à niveau du système d'exploitation pour cette version, reportez-vous aux [Notes de version BPA](#).

Conditions préalables

Les conditions préalables suivantes doivent être remplies avant d'utiliser l'application Mise à niveau du système d'exploitation :

- Mise à niveau du système d'exploitation, sauvegarde et restauration, services du planificateur et tous les services de plate-forme ou d'agent de contrôleur requis sont opérationnels
- Les artefacts requis (par exemple, les workflows, les modèles de processus, les stratégies de mise à niveau par défaut, etc.) sont chargés
- Les contrôleurs requis sont ajoutés et les périphériques sont correctement synchronisés ; référez-vous à [Contrôleurs et plates-formes de périphériques pris en charge](#) pour plus d'informations

Utilisation de l'application de mise à niveau OS

L'application Mise à niveau du système d'exploitation comprend les composants suivants :

- Gestion des images logicielles (SWIM)
- Gestion du serveur de distribution d'images
- Aperçu des logiciels
- Conformité logicielle
- Politique de mise à niveau
- Tâches de mise à niveau
- Paramètres

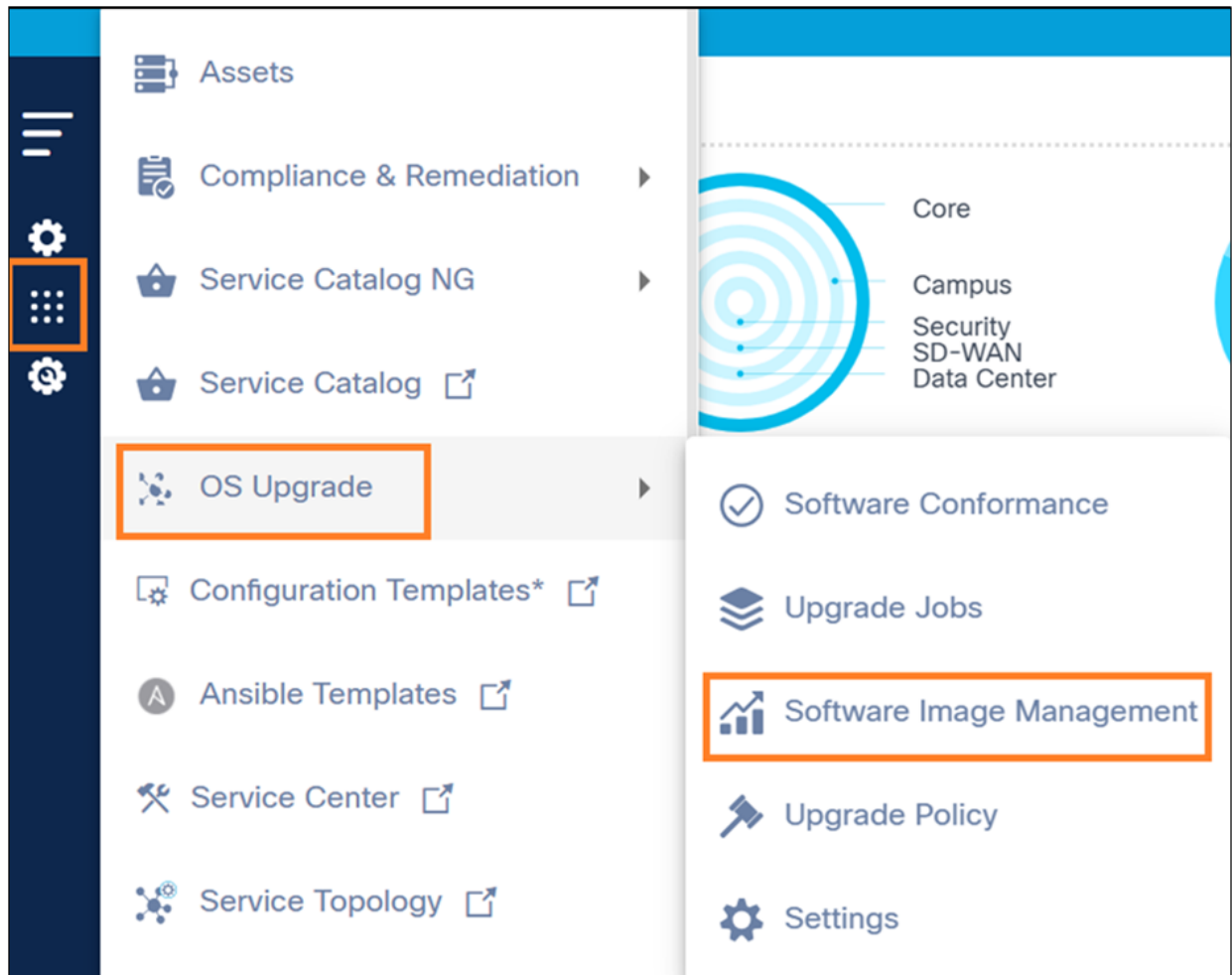
Gestion des images logicielles

Le composant SWIM permet aux utilisateurs Operations de conserver les détails de l'image logicielle pour les contrôleurs tels que NSO, ANSIBLE, CNC, FMC et Direct-to-Device qui ne prennent pas en charge la gestion des images OOB. Il répertorie également les détails de l'image logicielle gérés par des contrôleurs tels que vManage, NDFC et Cisco Catalyst Center, fournissant une liste centralisée des logiciels gérés sur tous les contrôleurs de domaine. Les images logicielles et le serveur de distribution d'images sont les deux principaux sous-composants du module SWIM.

Images logicielles

Pour accéder à la page Images logicielles :

1. Connectez-vous à BPA avec des informations d'identification ayant accès à Software Image Management.



Gestion des images logicielles Navigation

2. Sélectionnez Mise à niveau du SE > Gestion des images logicielles.

La page Gestion des images comporte les onglets suivants : Images logicielles, serveur de distribution d'images, conseils et informations.

Software Images

Image Distribution Server

Advisories

Insights

38

Device Models

195 - Base

33 - EPLD

77 - SMU

Images

154 - vManage

149 - NDFC

2 - NSO

Controller Types

305 - Cisco

Vendor

All

Search

☐	Device Model	Vendor	Image Name	Image Version	Image Type	Software Image Server	Added By	Last Modified On	Action
☐	ASR9K	Cisco	asr9k-x64-7.8.2.CSCwc11910.tar	7.8.2	SMU	NSO-FTP-2-Server	admin	Jul 14, 2025, 1:40 PM	
☐	N9K-C93180YC-FX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C93180YC-FX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C93180YC-EX	Cisco	nxos64-cs.10.2.2.F.bin	10.2.2	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C9364C-GX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C93180YC-EX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C93180YC-EX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C9364C-GX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	
☐	N9K-C9364C-GX	Cisco	nxos64-cs.10.2.2.F.bin	10.2.2	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	

Onglet Images logicielles

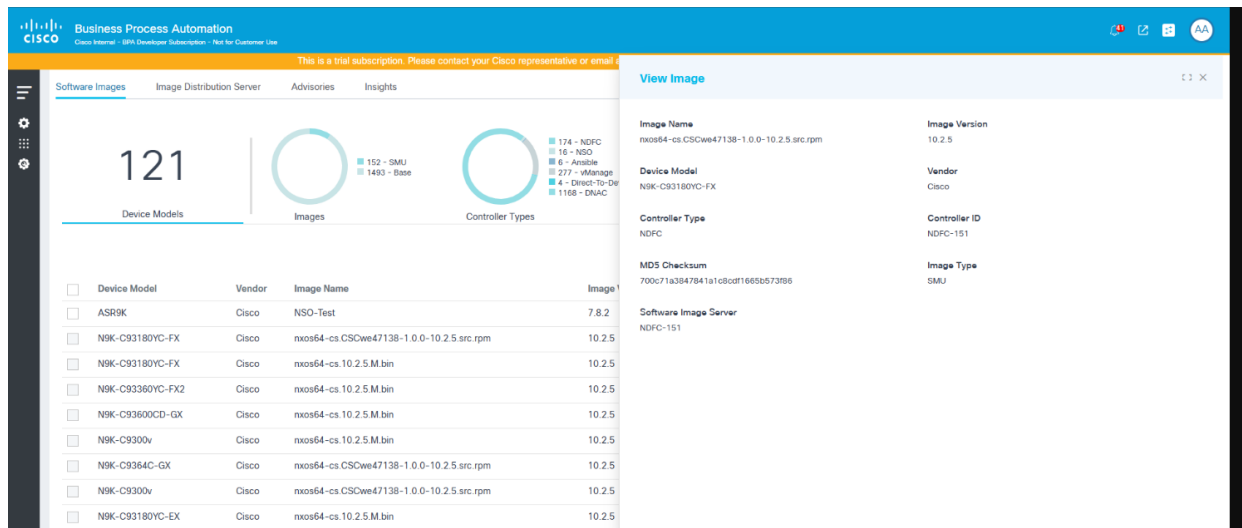
L'onglet Images logicielles contient les éléments suivants :

- Une section d'analyse, affichée en haut, qui fournit les informations suivantes :
 - Nombre total de modèles de périphériques et d'images logicielles associées
 - Un filtre rapide Images qui permet de filtrer les images en fonction du type (par exemple, base, SMU); le nombre indique le nombre total d'images associées à un type d'image respectif
 - Un filtre rapide de types de contrôleurs qui permet de filtrer les images en fonction du type de contrôleur (par exemple, Cisco Catalyst Center, vManage, NSO ou NDFC, Direct-to-Device, CNC, ANSIBLE, FMC) pour lequel les images sont hébergées ; le nombre indique le nombre total d'images associées à un type de contrôleur respectif
 - Un filtre rapide Fournisseur qui permet de filtrer les images en fonction du fournisseur qui a publié le logiciel
- L'icône Autres options propose les fonctionnalités suivantes :
 - Ajouter des détails d'image : Ajouter de nouvelles métadonnées d'image
 - Téléchargement en masse : Métadonnées d'image de téléchargement en masse au format .csv
 - Synchroniser les images : Synchroniser les métadonnées d'image des contrôleurs (par exemple, Cisco Catalyst Center, vManage, NDFC et FMC)
 - Supprimer tout : Suppression en bloc des images sélectionnées

 Remarque : L'ajout, la suppression et le téléchargement en masse des détails de l'image ne sont autorisés que pour les contrôleurs NSO, ANSIBLE, CNC et Direct-to-Device.

- Le filtre Rechercher peut être utilisé pour rechercher des images et inclut les filtres de recherche exclusifs suivants :
 - Tous : Rechercher dans tous les champs
 - Nom de l'image : Rechercher les images avec un nom d'image spécifique
 - Modèle de périphérique : Rechercher les images avec un modèle spécifié
 - Version de l'image : Rechercher des images avec une version logicielle spécifique
 - Serveur d'images logicielles : Rechercher les images associées à un serveur d'images spécifique
- L'icône Actualiser actualise la page et efface les filtres sélectionnés.
- Les images existantes sont affichées dans un tableau de grille avec les colonnes suivantes :
 - Modèle de périphérique : Modèle de périphérique pour lequel les détails de l'image sont applicables
 - Fournisseur : Fournisseur qui publie les images logicielles
 - Nom de l'image : Nom de fichier de l'image
 - Version de l'image : Version logicielle de l'image
 - Type d'image : Détermine le type d'image (p. ex. base, SMU, EPLD (Electronic Programmable Logic Device))

- Serveur d'images logicielles : Serveur d'images où l'image actuelle existe
- Ajouté par : Utilisateur ayant ajouté les métadonnées de l'image
- Dernière modification le : Horodatage de la dernière mise à jour des détails de l'image
- Action : Fournit une icône Plus d'options à partir de laquelle des actions spécifiques à une ligne (par exemple, modifier, supprimer) peuvent être sélectionnées
- Trier les images en cliquant sur un en-tête de colonne respectif



Afficher l'image

- Cliquez sur une ligne pour ouvrir la fenêtre Afficher l'image

Synchronisation des images logicielles et des métadonnées

Pour effectuer une synchronisation à la demande des images logicielles :



Synchroniser les images

1. Cliquez sur l'icône Autres options > Synchroniser les images. Les métadonnées d'image de vManage, Cisco Catalyst Center, NDFC et FMC sont découvertes et conservées dans BPA.

 Remarque : Pour les contrôleurs FMC, les données existantes sont conservées chaque fois qu'une synchronisation est exécutée. Seules les nouvelles images sont ajoutées.

2. Si le nom de l'image du contrôleur FMC inclut le mot « FTD » ou « Firepower Threat_Defense », le deviceModel de cette image est mappé en tant que FTD.

OU

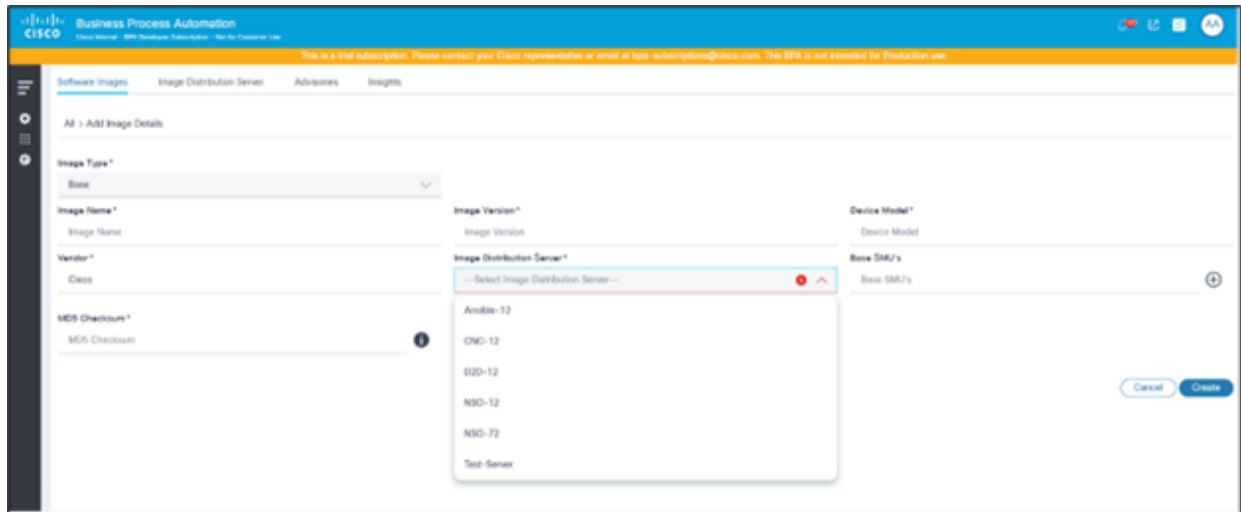
Si le nom de l'image du contrôleur FMC inclut le mot « FMC », « FW_Mgmt_Center » ou « Firewall_Management_Center », le deviceModel de cette image est mappé en tant que FMC.

 Remarque : FMC n'associe pas les informations de modèle aux métadonnées d'image. Une fois la synchronisation terminée, modifiez les métadonnées d'image respectives et mettez à jour le modèle si nécessaire. Le processus de mise à niveau FMC ne fonctionne pas comme prévu sans la mise à jour du modèle.

3. Les images des serveurs distants vManage ont initialement l'identificateur unique universel (UUID) mappé dans la colonne Version après l'opération de synchronisation. Les opérateurs doivent modifier manuellement les métadonnées de serveur distant requises et les mettre à jour avec la version d'image appropriée. Si ce mappage n'est pas effectué, les autres composants de mise à niveau du système d'exploitation (par exemple, conformité logicielle, stratégies de mise à niveau, tâches de mise à niveau, etc.) ne fonctionnent pas comme prévu.
4. Pour planifier la synchronisation automatique des métadonnées SWIM à intervalles réguliers, reportez-vous à [Configuration du déploiement](#).

Ajout de métadonnées d'image logicielle

1. Cliquez sur l'icône Autres options > Ajouter les détails de l'image. La page Add Image Details s'affiche.



Ajouter des détails d'image

2. Saisissez les informations dans les champs suivants :

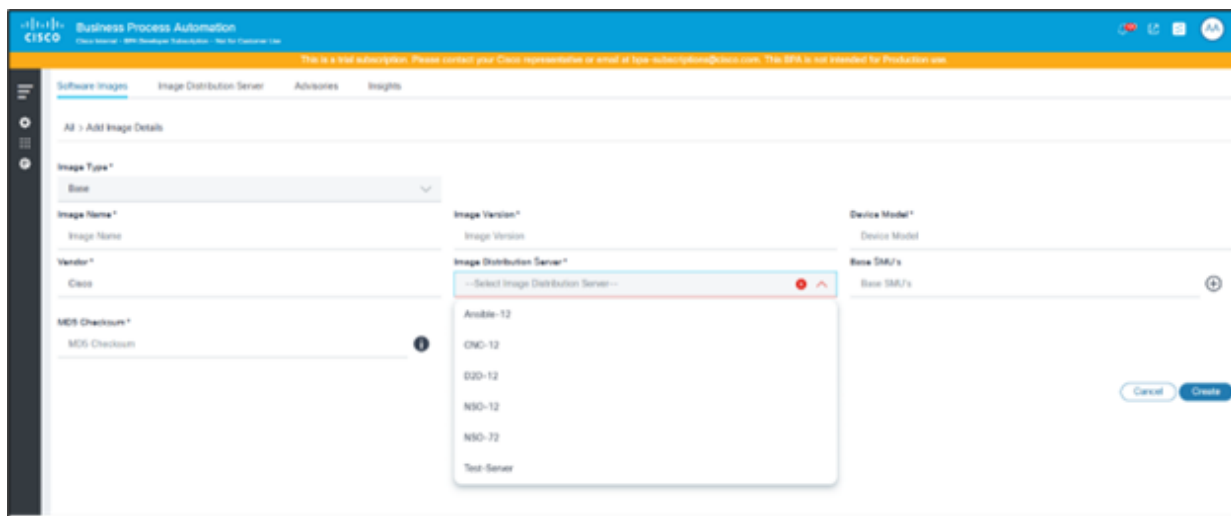
- Type d'image : Type d'image (par exemple, base, SMU, EPLD)
- Nom de l'image : Nom du fichier image ; les utilisateurs peuvent entrer un chemin d'accès relatif ou absolu de l'image dans le champ Nom. Si les utilisateurs fournissent un chemin absolu, l'image est extraite directement de ce chemin ; si les utilisateurs fournissent un chemin relatif, le système résout le chemin complet en ajoutant le chemin de base défini dans le serveur de référentiel lors de la distribution
- Version de l'image : Version logicielle de l'image
- Modèle de périphérique : Modèle de périphérique pour lequel l'image est marquée

 Remarque : Le modèle de périphérique doit correspondre aux informations fournies par le contrôleur CNC, NSO, Direct-To-Device ou ANSIBLE pour les périphériques concernés.

- Fournisseur : Le fournisseur ou le fournisseur qui a publié l'image ; la valeur par défaut est Cisco, mais elle peut être modifiée si nécessaire
- Serveur de distribution d'images : Sélectionnez le serveur de distribution d'images qui héberge le fichier logiciel indiqué dans le champ Nom de l'image. Lors de la sélection d'un serveur de distribution d'images, des images sont générées pour tous les ID de contrôleur associés au type de contrôleur spécifié défini dans le serveur de distribution d'images. Si un utilisateur ajoute ou supprime des instances de contrôleur sous le serveur de distribution d'images, les images logicielles correspondantes sont ajoutées ou supprimées pour ces instances de contrôleur.
- SMU de base : SMU qui sont présents dans l'image dorée de base ; cette option est applicable uniquement si le type d'image est Base
- Somme de contrôle MD5 : Somme de contrôle MD5 de l'image pour vérification

3. Cliquez sur Create. La notification Progress s'affiche, suivie d'un message de confirmation.

 Remarque : Les métadonnées d'image des SMU Bridge doivent être ajoutées avant de les utiliser dans une stratégie de mise à niveau. Pour ajouter des SMU de pont, sélectionnez SMU dans la liste déroulante Type d'image.



Ajouter des métadonnées d'image SMU Bridge

Téléchargement en masse des métadonnées des images logicielles

	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

Exemple de fichier CSV avec informations sur l'image

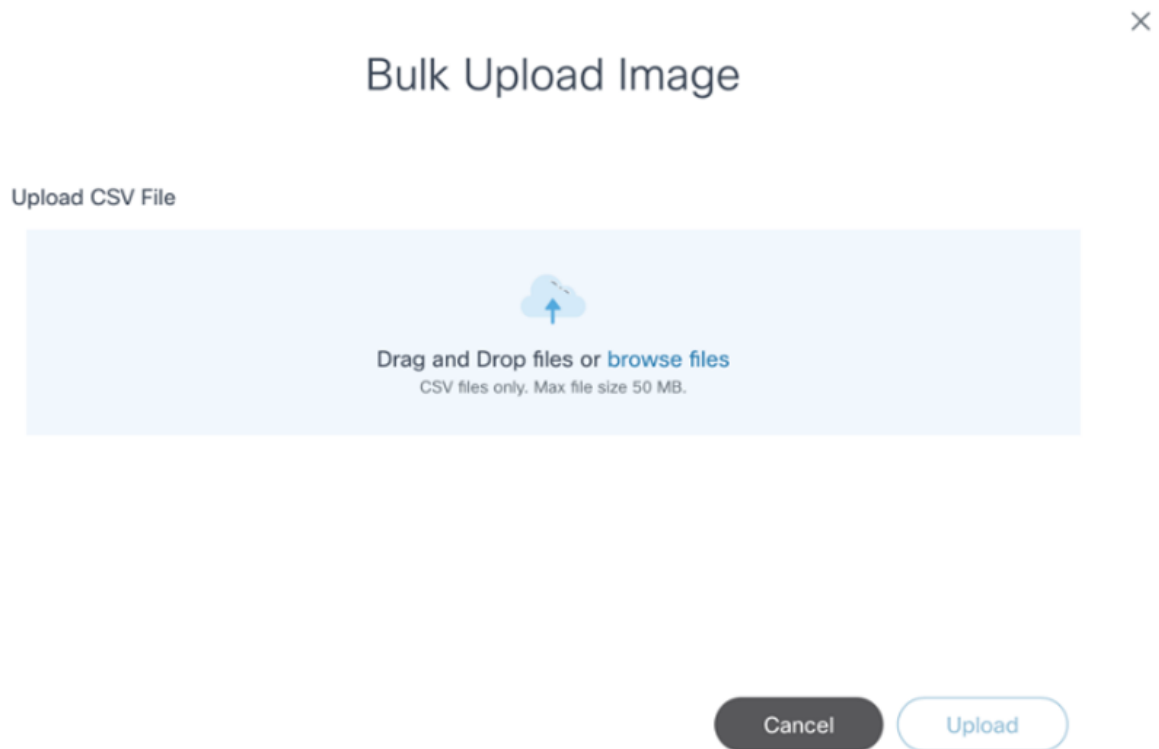
1. Préparez un fichier .csv avec les détails d'image nécessaires et les noms de colonne suivants :

- Nom de l'image
- Version
- Modèle de périphérique
- Fournisseur
- Type d'image

 Remarque : Seules les valeurs Base, SMU et EPLD sont prises en charge.

- Serveur de distribution d'images
- Somme de contrôle MD5

2. Cliquez sur l'icône Autres options > Téléchargement en masse. La fenêtre Téléchargement en masse de l'image s'ouvre.



Télécharger une image en masse

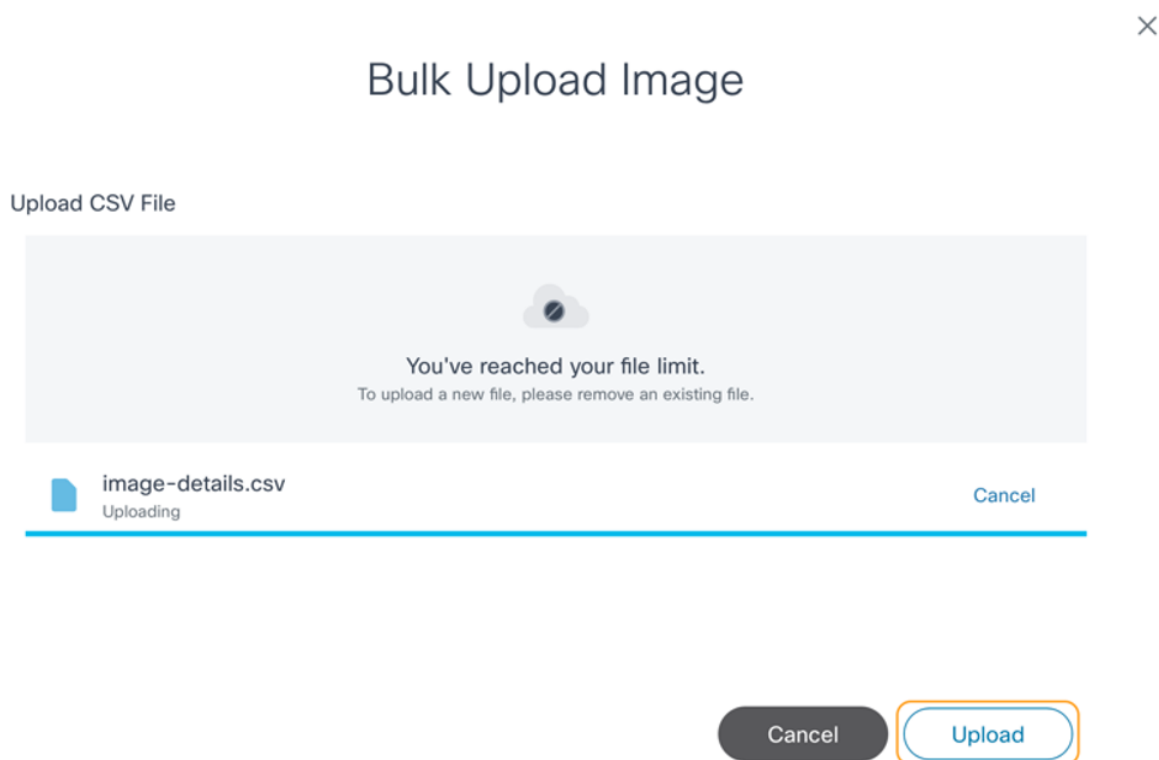
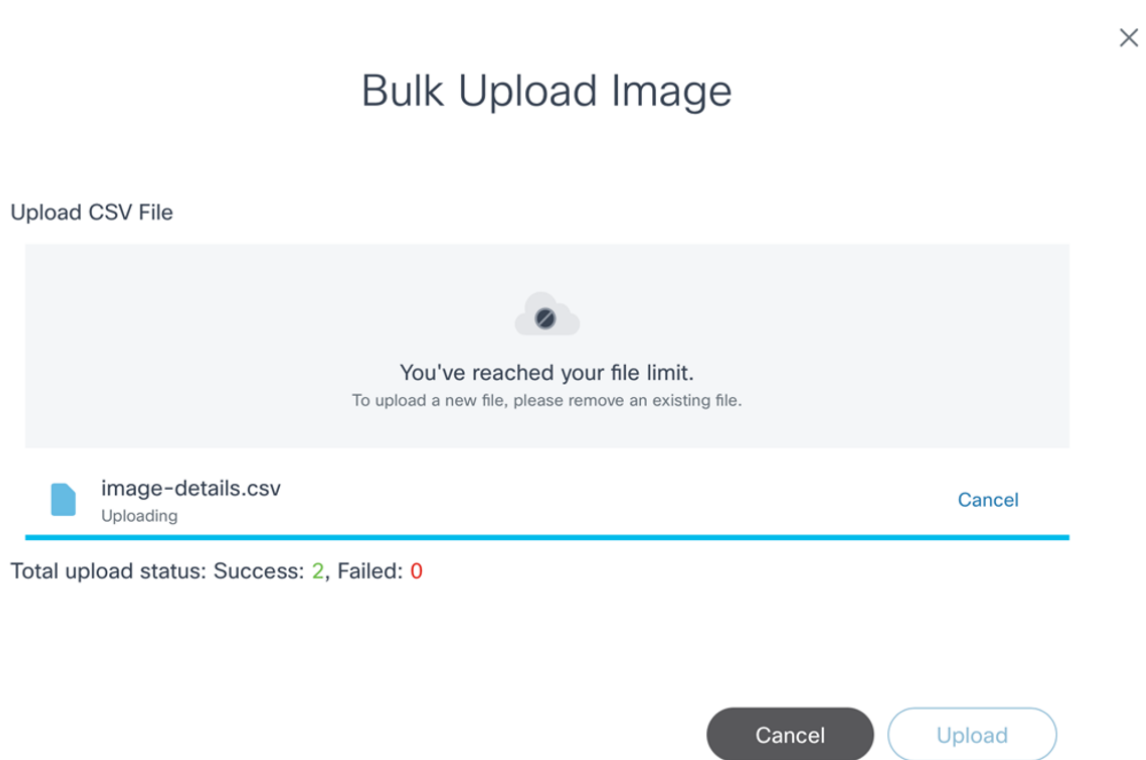


Image de téléchargement en masse - Téléchargement CSV

3. Sélectionnez un fichier .csv préparé et cliquez sur Upload. Les détails de l'image du fichier

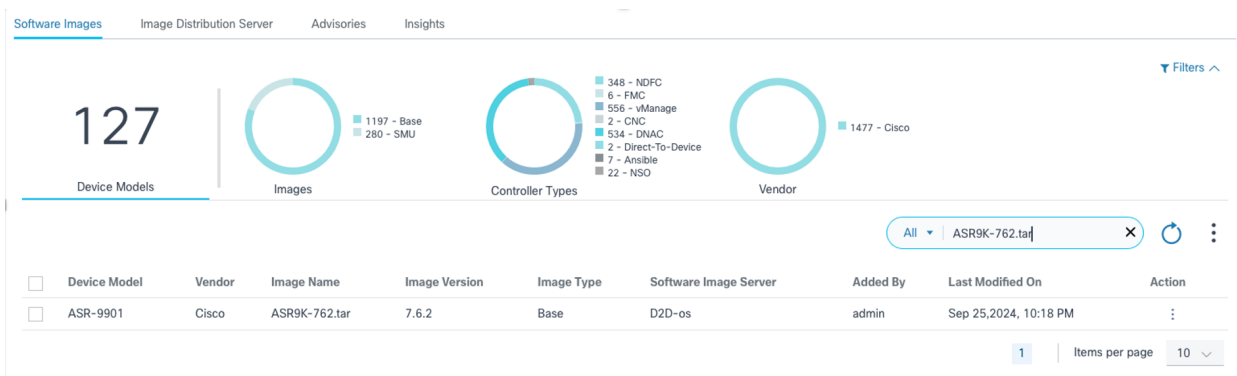
.csv sont validés, puis traités. Une fois le fichier téléchargé, l'état final du téléchargement en masse s'affiche.



État de téléchargement d'image en masse réussi

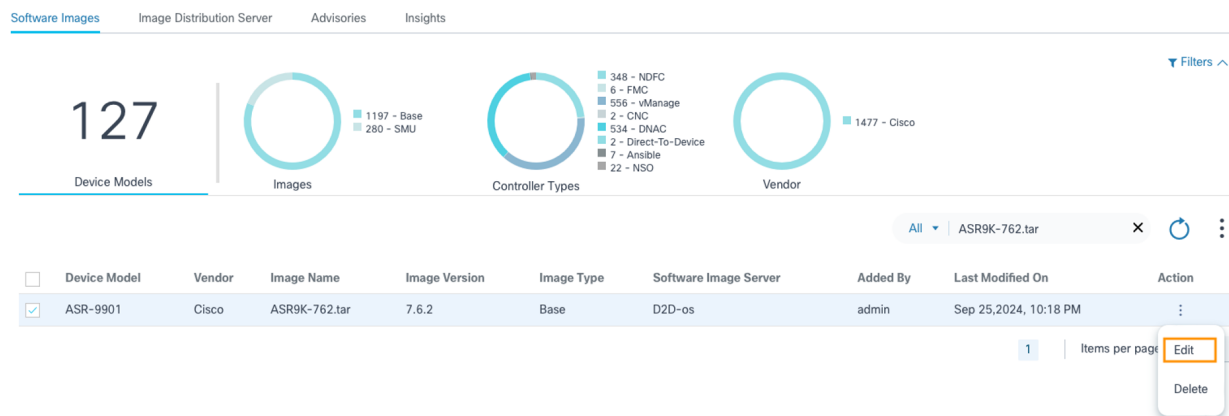
 Remarque : En cas d'erreurs de validation des données (par exemple, enregistrements en double ou paramètres non valides), les messages d'erreur s'affichent sous la forme d'une grille dans la fenêtre Bulk Upload Image. Les utilisateurs peuvent corriger les valeurs du fichier .csv et le télécharger à nouveau.

Modification des métadonnées d'image logicielle existantes



Rechercher dans les métadonnées d'image logicielle

1. Localisez l'image qui doit être mise à jour à l'aide du filtre Rechercher.



Modifier

2. Dans la colonne Action de l'image souhaitée, sélectionnez l'icône More Options > 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

Modifier les images logicielles

3. Mettez à jour les paramètres requis et cliquez sur Save pour enregistrer les modifications ou cliquez sur Cancel pour annuler les modifications. La notification de progression s'affiche, suivie d'un message de confirmation pour la mise à jour de l'image.

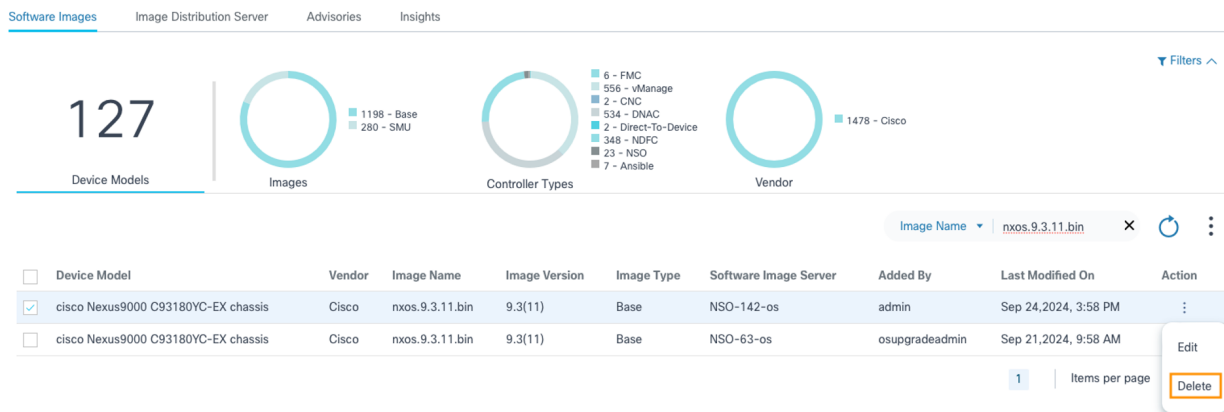
 Remarque : La liste suivante doit être notée.

- L'édition est disponible pour les contrôleurs CNC, NSO, D2D, ANSIBLE, FMC et vManage (applicable uniquement pour les métadonnées d'image de serveur distant)
- La mise à jour du modèle de périphérique est uniquement prise en charge pour les images de serveur distant vManage
- Seul le champ Version du logiciel peut être mis à jour pour les métadonnées d'image du serveur distant vManage
- Pour les images vManage, les utilisateurs peuvent afficher le serveur d'images logicielles à la place des instances de contrôleur

Suppression de métadonnées d'image logicielle

Rechercher dans les métadonnées d'image logicielle

1. Utilisez le champ Rechercher pour localiser une image souhaitée.



DELETE

2. Dans la colonne Action de l'image souhaitée, sélectionnez l'icône Plus d'options > Supprimer pour supprimer une image.

OU



Supprimer tout

Sélectionnez les images souhaitées et sélectionnez l'icône Plus d'options > Supprimer tout pour supprimer plusieurs images.

Une confirmation s'affiche.



Delete Image

Are you sure you want to delete the selected images?

Cancel

Ok

Confirmation

3. Cliquez sur OK. Une notification de progression s'affiche, suivie d'un message de confirmation.



Remarque : La liste suivante doit être notée.

- Les métadonnées d'image ne peuvent être ajoutées que pour les contrôleurs NSO, ANSIBLE, Direct-to-Device et CNC. Pour tous les autres contrôleurs d'entreprise, la fonctionnalité SWIM intégrée est exploitée et des images sont découvertes à partir des contrôleurs respectifs
- La fonctionnalité de découverte d'images n'est pas prise en charge pour les serveurs d'images des contrôleurs NSO, ANSIBLE, Direct-to-Device et CNC.
- Par défaut, les métadonnées de l'image du serveur distant vManage contiennent l'UUID pour la post-synchronisation du paramètre de version. Les utilisateurs doivent modifier les métadonnées et mettre à jour l'UUID avec la version correspondante. La version d'image correspondante peut être identifiée à partir du contrôleur vManage ou en se connectant au périphérique où l'image existe.

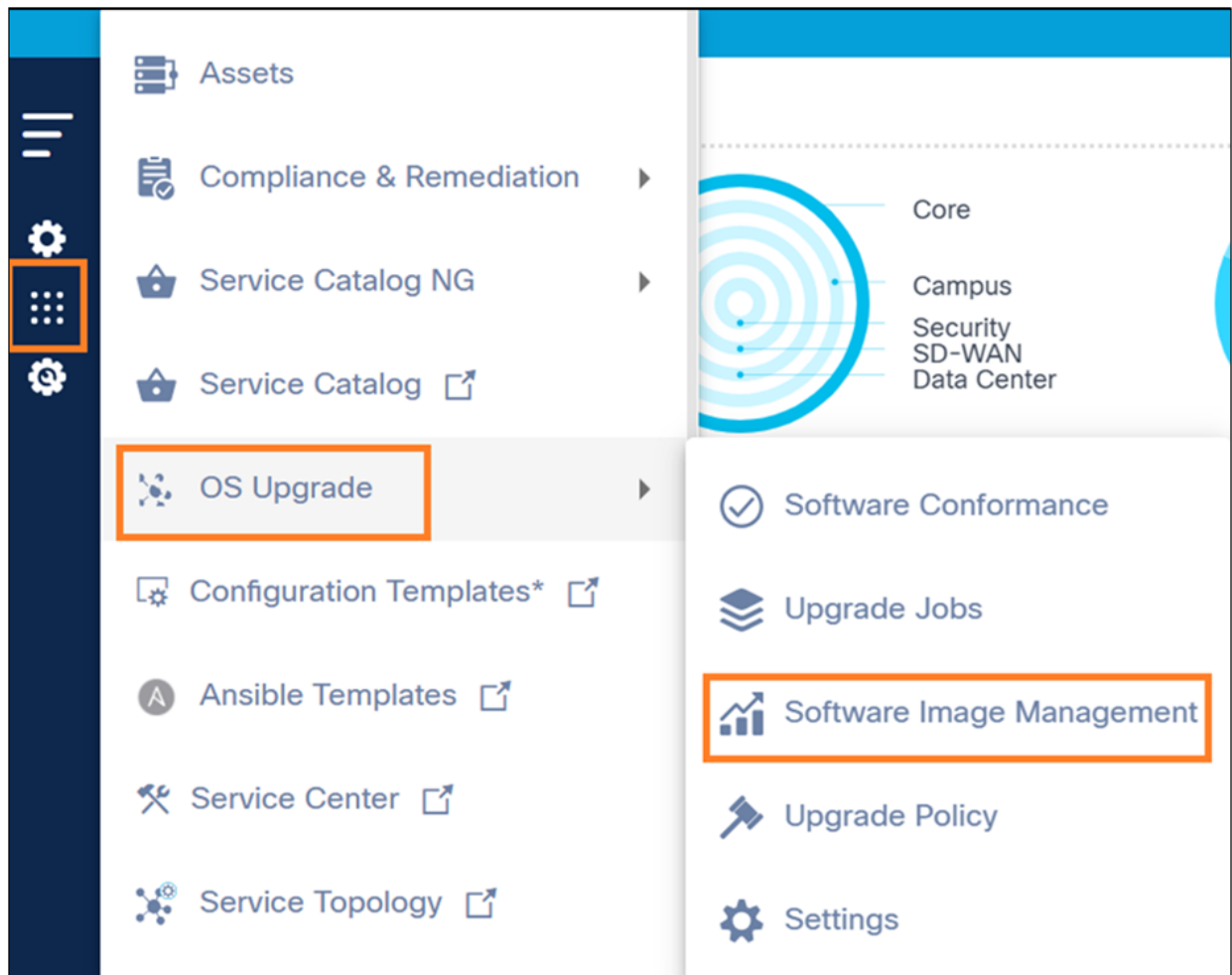
Gestion du serveur de distribution d'images

Serveur de distribution d'images

Le composant permet aux utilisateurs Operations de conserver les détails du serveur de référentiel d'images pour les contrôleurs CNC, NSO, ANSIBLE, FMC et Direct-To-Device qui ne prennent pas en charge la gestion du référentiel d'images OOB.

Pour accéder à la page Serveur de distribution d'images :

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré au serveur de distribution d'images.



Gestion des images logicielles

2. Sélectionnez Mise à niveau du SE > Gestion des images logicielles.

SW Images Image Distribution Server

2

Image Servers

CONTROLLER TYPE

1 - Direct-To-Device
1 - NSO

Filters

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

1 | Items per page 10

Onglet Serveur de distribution d'images

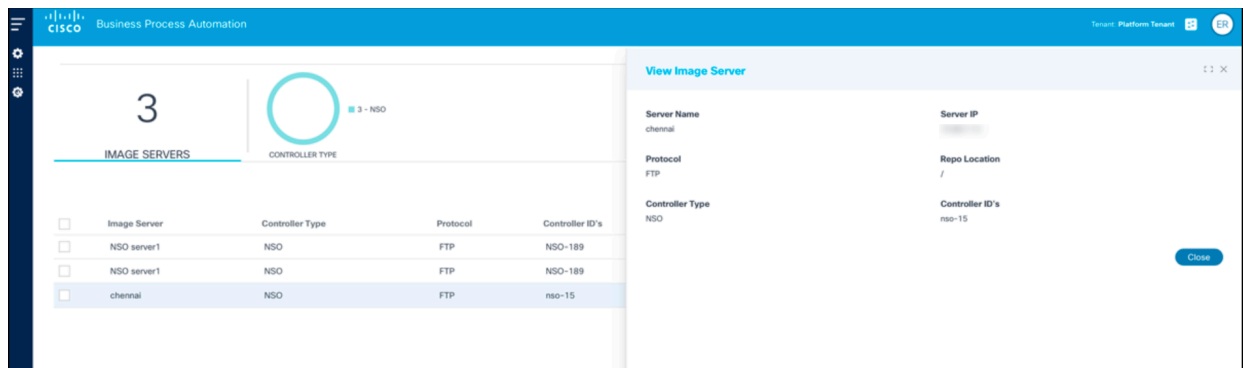
3. Cliquez sur l'onglet Image Distribution Server.

L'onglet Serveur de distribution d'images contient les éléments suivants :

- Une section d'analyse, affichée en haut, qui fournit les informations suivantes :
 - Nombre total de serveurs d'images intégrés sur cette instance BPA
 - Un filtre rapide de type contrôleur qui permet de filtrer les serveurs d'images en fonction du type de contrôleur (par exemple, NSO, Direct-to-Device, CNC, ANSIBLE, FMC) ; le nombre indique le nombre total de serveurs de distribution d'images associés à ce type de contrôleur
- Une icône Autres options qui fournit les fonctionnalités suivantes :
 - Ajouter un serveur d'images : Ajouter un nouveau serveur de distribution d'images
 - Supprimer tout : Suppression en bloc des serveurs de distribution sélectionnés
- Un filtre de recherche qui peut être utilisé pour rechercher les serveurs de distribution et inclut les filtres de recherche exclusifs suivants :
 - Tous : Recherche dans tous les champs
 - Serveur d'images : Recherche les serveurs portant un nom spécifique
 - ID du contrôleur : Recherche les serveurs associés à un ID de contrôleur spécifique
- Une icône Actualiser qui peut être utilisée pour actualiser la page et effacer les filtres sélectionnés
- Les serveurs de distribution existants sont affichés dans une table de grille avec les colonnes suivantes :
- Serveur d'images : Nom unique du serveur de référentiel
 - Type de contrôleur : Type de contrôleur auquel ce serveur d'images s'applique
 - Protocole : Copier le protocole pris en charge par le serveur de référentiel

 Remarque : Seuls FTP, SCP et SFTP (Secure File Transfer Protocol) sont pris en charge

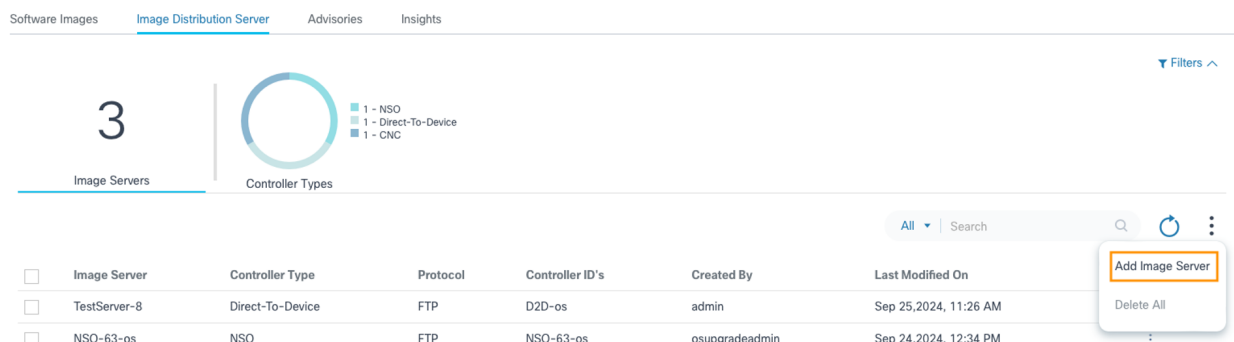
- ID du contrôleur : les instances de contrôleur pour lesquelles le serveur de référentiel actuel est utilisable ou applicable ; instance de contrôleur fait référence aux périphériques gérés via ce contrôleur
- Créé par : Utilisateur qui a intégré le serveur de référentiel
- Dernière modification le : Horodatage de la dernière mise à jour des détails du serveur
- Action : Propose des actions propres aux lignes, telles que Modifier et Supprimer



Panneau Afficher le serveur d'images

- Cliquez sur une ligne pour ouvrir la fenêtre View Image Server

Ajout des détails du serveur d'images



Ajouter un serveur d'images

4. Cliquez sur l'icône Autres options > Ajouter un serveur d'images. La page Add Image Server s'affiche.

Software Images **Image Distribution Server** Advisories Insights

All > Add Image Server

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

Ajouter les détails du serveur d'images

Ajouter un serveur d'images avec des exemples de détails

5. Saisissez les informations dans les champs suivants :

- Nom de serveur: Nom unique du serveur de référentiel d'images
- Adresse IP du serveur : Adresse IPv4 du serveur de référentiel

Remarque : Assurez-vous que cette adresse IP est accessible à partir des périphériques réseau avant d'ajouter.

- Protocole : Pris en charge par le serveur de référentiel d'images pour la copie d'image

Remarque : Seuls les protocoles FTP, SCP et SFTP sont pris en charge.

- Emplacement de la reprise : Chemin d'accès de base des fichiers image dans le serveur de référentiel

Remarque : Si des fichiers image sont présents à la racine du dossier du référentiel du serveur d'images, « / » fonctionne comme une valeur.

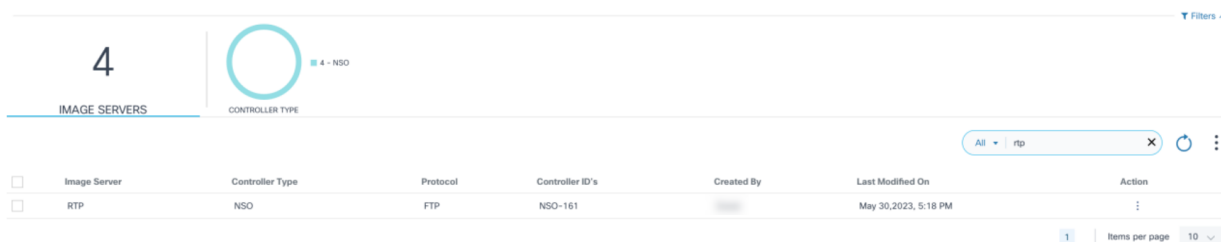
- Type de contrôleur : Type de contrôleur pour lequel le serveur d'images actuel est applicable

Remarque : Seuls NSO, Direct-To-Device, CNC et ANSIBLE sont pris en charge.

- Instances de contrôleur : Une ou plusieurs instances de contrôleur applicables en fonction des périphériques qu'elles gèrent pour lesquels le serveur de référentiel d'images donné doit être utilisé pour copier l'image
- Utilisateur : Identifiants personnalisés à utiliser pour accéder aux fichiers image à partir du référentiel

6. Cliquez sur Create. La notification de progression s'affiche, suivie d'un message de confirmation.

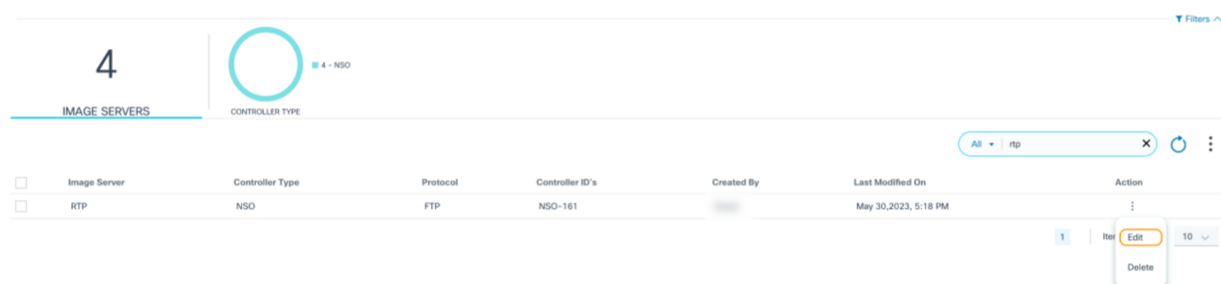
Modification des détails du serveur d'images



☐	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	

Recherche du serveur d'images

7. A l'aide du champ Search, localisez le serveur de distribution qui doit être mis à jour.



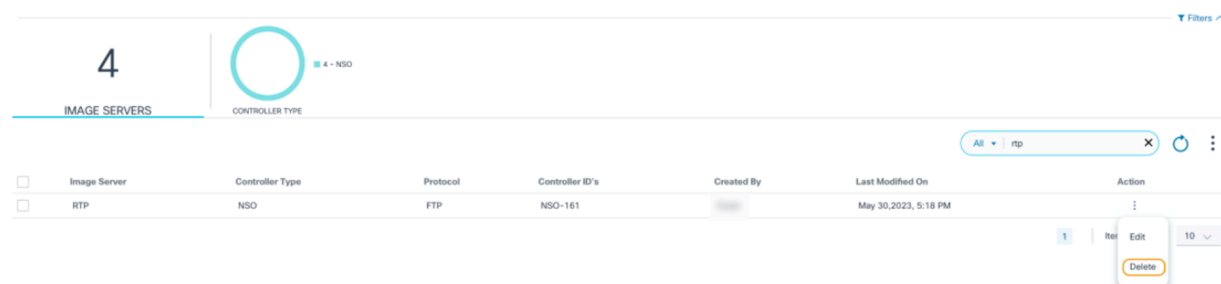
☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐	RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	Edit

Modifier le serveur d'images

8. Dans la colonne Action, sélectionnez l'icône More Options > Edit.
9. Mettez à jour les paramètres requis.
10. Cliquez sur Save. La notification de progression s'affiche, suivie d'un message de confirmation.

Suppression des détails du serveur d'images

1. A l'aide du filtre Search, localisez le ou les serveurs souhaités.



☐	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	Delete

Supprimer le serveur d'images

2. Dans la colonne Action, sélectionnez l'icône More Options > Delete pour supprimer un serveur de distribution unique.

OU

☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On
☒	TestServer-8	Direct-To-Device	FTP	D2D-os		Sep 25, 2024, 11:26 AM
☒	NSO-63-os	NSO	FTP	NSO-63-os		Sep 24, 2024, 12:34 PM

Suppression de plusieurs serveurs d'images

Sélectionnez les serveurs souhaités et cliquez sur l'icône Plus d'options > Supprimer tout pour supprimer plusieurs serveurs de distribution.

Une confirmation s'affiche.

Delete Image Server

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

Cancel Ok

Confirmation de suppression

3. Cliquez sur OK. Les notifications de progression s'affichent, suivies d'un message de confirmation.

Aperçu des logiciels

Software Insights détecte toutes les vulnérabilités de sécurité, telles que les avis de sécurité, les bogues et la fin de vie des logiciels exposés par les ressources réseau. Il fournit également des suggestions logicielles pour les modèles de périphériques gérés par Cisco Catalyst Center et les contrôleurs NDFC. Il permet aux administrateurs de sélectionner la version logicielle suggérée pour les ressources réseau et crée une stratégie de conformité pour les modèles de périphériques

si la suggestion est disponible.

Conditions préalables

- Activez l'adaptateur pour obtenir des informations. L'adaptateur pour le serveur Cisco Insights, appelé « Cisco-Insights-Adapter », est disponible en ligne. Pour intégrer certains serveurs Insights externes tiers, vous devez créer les adaptateurs correspondants. Référez-vous à Configuration de l'adaptateur Insights dans le [Guide du développeur BPA](#) pour plus d'informations.
 - Une connectivité Internet est requise pour que le système BPA puisse se connecter au cloud Cisco.
 - Vérifiez que client_id et client_secret se trouvent dans la configuration de l'adaptateur avant de poursuivre l'opération de synchronisation.
 - Si nécessaire, le proxy pour Internet peut être configuré en suivant les étapes ci-dessous.
 - Pour le type de système d'exploitation IOS-XR, le mappage série/modèle personnalisé des périphériques peut être effectué dans la gestion des données de référence (RefD), selon les besoins. Pour plus d'informations sur le mappage série-à-modèle personnalisé, référez-vous au [Guide du développeur BPA](#).
 - Les pods BPA Kubernetes nécessitent un accès Internet pour recueillir les conseils, les bogues et les informations de fin de vie de Cisco. Si le réseau BPA n'a pas d'accès direct à Internet, mais est disponible via un proxy, suivez les étapes ci-dessous pour que Kubernetes Pods utilise le proxy pour Internet.
1. Mettez à jour le script en remplaçant <<http://proxy-domain.com:port>> par l'adresse proxy réelle.
 2. Configurez les paramètres d'environnement pour chaque pod dans les graphiques YAML ou de barre de déploiement.
 3. Exécutez le script ci-dessous dans le noeud Kubernetes en ajoutant tous les noms de déploiement dans la configuration NO_PROXY ou no_proxy.

```
#!/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

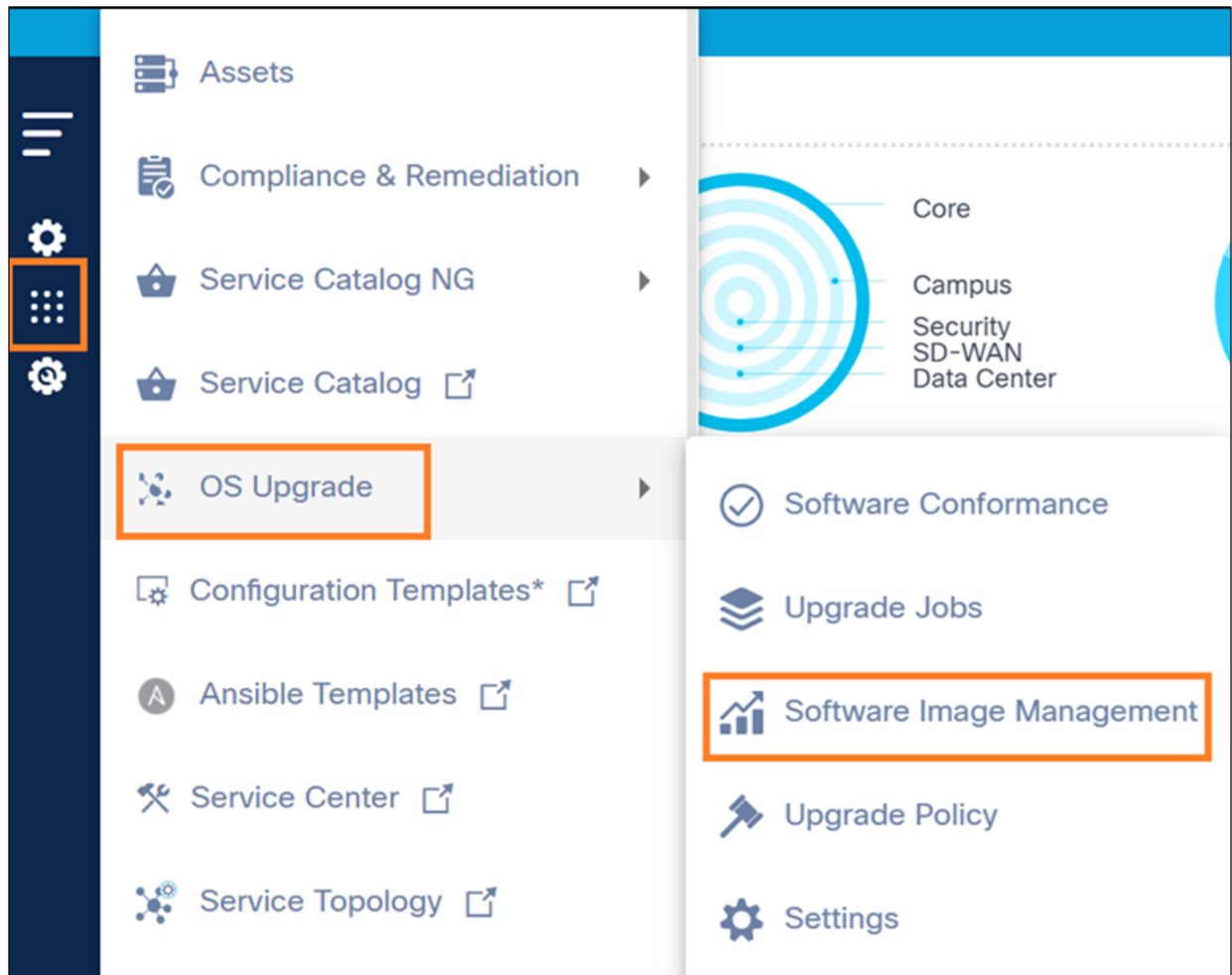
```

 Remarque : En configurant le proxy comme décrit ci-dessus, l'adaptateur de données peut atteindre le réseau Cisco et télécharger les données Software Insights requises dans le BPA. Pour vous connecter à un autre serveur Insights externe directement sans proxy, veuillez à les ajouter à la variable no_proxy.

Récupération des données Software Insights dans BPA

Pour synchroniser les données d'analyse logicielle dans BPA :

1. Connectez-vous à BPA avec des informations d'identification qui ont accès à la synchronisation des données d'analyse logicielle.



Gestion des images logicielles Navigation

2. Sélectionnez OS Upgrade > Software Image Management dans le panneau latéral.



Onglet Conseils

3. Cliquez sur l'onglet Conseils.

Synchronisation pour récupérer des informations logicielles dans BPA



Synchronisation pour récupérer des informations logicielles dans BPA

4. Cliquez sur Synchroniser.

Cette opération permet de détecter tous les avis de sécurité, les bogues prioritaires, les bulletins

de fin de vie et les suggestions de logiciels associés aux ressources présentes dans l'inventaire. Les avis de sécurité et les dates de fin de vie des logiciels sont déterminés en fonction du type de système d'exploitation et de la version du logiciel. Les bogues prioritaires et les suggestions de logiciels sont déterminés en fonction de l'ID de produit et de la version du logiciel.

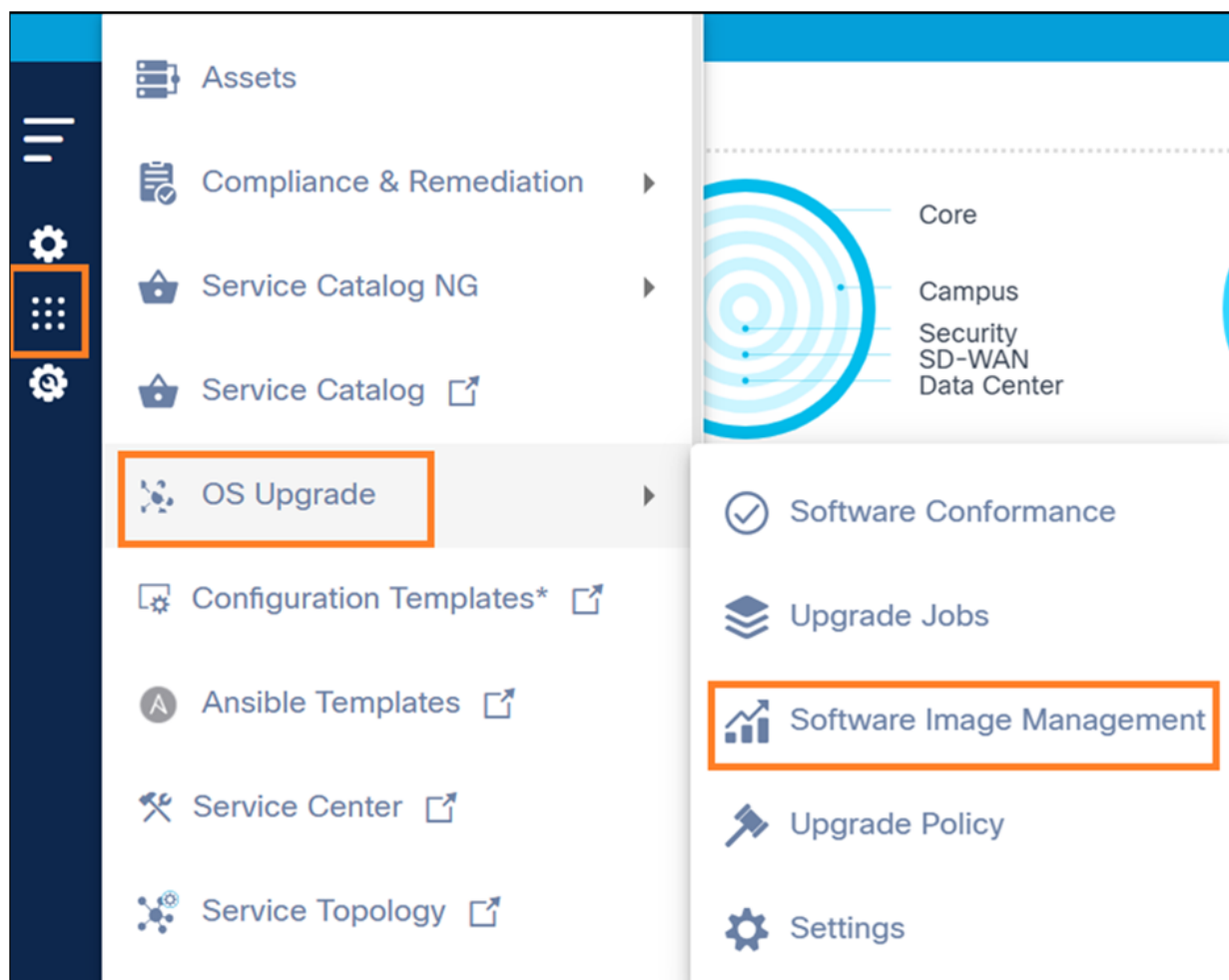
Dernière mise à jour indique la date et l'heure de la dernière synchronisation des données d'aperçus et le champ État de synchronisation affiche l'état de la dernière synchronisation.

 Remarque : Tous les conseils, bogues, notes de version et suggestions applicables sont extraits du cloud Cisco via le fichier « Cisco-Insights-Adapter ».

Affichage et gestion des avis de sécurité

Pour accéder à la page Avis :

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré aux conseils.



Gestion des images logicielles Navigation

2. Sélectionnez Mise à niveau du SE > Gestion des images logicielles.

Software Images Image Distribution Server **Advisories** Insights

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

Priority Bugs

Filters

Impacts

- All
- Critical
- High
- Medium
- Low

Last Updated

- All
- <30 Days
- 31-60 Days
- 61-90 Days
- >90 Days

Clear All

Security Advisories 214 Total

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

Bulletins de renseignements de sécurité

3. Cliquez sur l'onglet Conseils. La page Avis de sécurité s'ouvre par défaut.

Les options suivantes s'affichent pour filtrer les données des conseils :

- Les impacts permettent un filtrage basé sur la gravité des avis ; Tout est sélectionné par défaut
- Dernière mise à jour permet un filtrage basé sur la date de la dernière mise à jour de l'avis ; Tout est sélectionné par défaut
- Clear All réinitialise les filtres sélectionnés
- Le filtre Rechercher est utilisé pour rechercher les conseils et inclut les filtres de recherche exclusifs suivants :
 - Tous : Effectue des recherches dans des colonnes telles que Advisory, CVE et Software Versions
 - Avis : Recherche les conseils avec les termes spécifiés dans la recherche
 - CVE : Recherche les avis comportant des vulnérabilités et des expositions courantes (CVE) spécifiques
 - Versions logicielles : Recherche les conseils associés à des types de système d'exploitation ou à des versions logicielles spécifiques
- L'icône Actualiser est utilisée pour actualiser la page et effacer les filtres sélectionnés
- Les conseils existants s'affichent dans les colonnes suivantes :
 - Avis : Résumé de l'avis
 - Incidence: Gravité consultative
 - CVE : CVE attribués
 - Versions logicielles : Type de système d'exploitation et versions logicielles concernés
 - Dernière mise à jour Date et heure de la dernière mise à jour de l'avis
 - Version : Version consultative
 - Ressources potentiellement affectées : Nombre de ressources susceptibles d'être affectées par l'avis

- Cliquez sur le champ d'en-tête pour trier les conseils



Remarque : Le tri n'est pas une option pour les ressources potentiellement affectées.

Filters

Impacts

☒ All

☐ Critical

☐ High

☐ Medium

☐ Low

Last Updated

☒ All

☐ <30 Days

☐ 31-60 Days

☐ 61-90 Days

☐ >90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
...		
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
...		
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
...		
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
...		
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
...		
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
...		
Cisco IOx for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
...		
Cisco IOx for IOS XE Software Command Injection V	Medium	CVE-2021-1384
...		
Cisco IOx Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2018,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE CVE-2022-20823

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

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

Version 1.0

[View Security Advisory](#)

[Summary](#) [Affected Assets \(2\)](#)

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

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

Vue détaillée des conseils

- La sélection d'une ligne de conseil ouvre la vue détaillée d'un conseil qui comprend les onglets suivants :
 - Résumé: Affiche un résumé de l'avis sélectionné ; affiche par défaut
 - Ressources affectées : Affiche les détails des ressources potentiellement affectées, tels que le nom de la ressource, le numéro de série, le nom du modèle, la version du logiciel, l'adresse IP et l'ID du contrôleur ; vous pouvez trier et rechercher les ressources dans cet onglet

Filters

Impacts

☒ All

☐ Critical

☐ High

☐ Medium

☐ Low

Last Updated

☒ All

☐ <30 Days

☐ 31-60 Days

☐ 61-90 Days

☐ >90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
...		
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
...		
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
...		
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
...		
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
...		
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
...		
Cisco IOx for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
...		
Cisco IOx for IOS XE Software Command Injection V	Medium	CVE-2021-1384
...		
Cisco IOx Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2018,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE CVE-2022-20823

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

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

Version 1.0

[View Security Advisory](#)

[Summary](#) [Affected Assets \(2\)](#)

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

2 Total Assets

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

1 Items per page 10

Afficher les conseils de sécurité

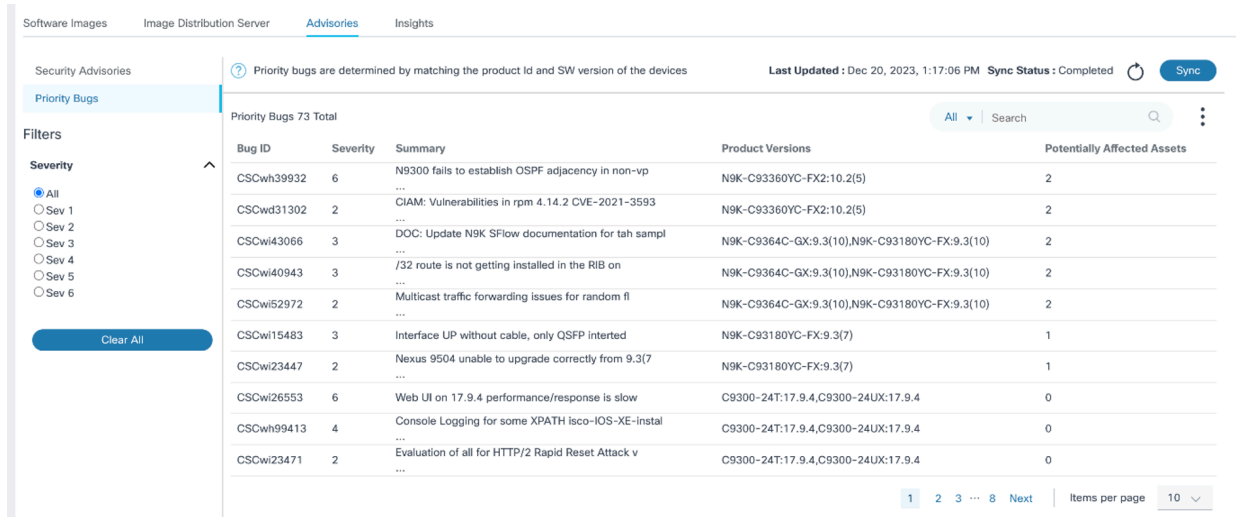
- Afficher le lien Security Advisory : Accède à la page de conseil officielle

Affichage et gestion des bogues de priorité



Sélectionner les bogues prioritaires

Après avoir ouvert la page Avis comme décrit dans la section précédente, cliquez sur l'onglet Priorité des bogues. La page Priority Bugs s'affiche.



Bogues prioritaires

Les options suivantes sont disponibles sur la page Priority Bugs :

- Un filtre Severity qui permet le filtrage basé sur la gravité du bogue ; Tout est sélectionné par défaut
- Le filtre Search peut être utilisé pour rechercher les bogues et inclut les filtres de recherche exclusifs suivants :
 - Tous : Recherche dans tous les champs
 - ID de bogue: Recherche les bogues avec un ID de bogue spécifié
 - Résumé: Recherche les bogues avec des mots-clés spécifiques présents dans le résumé
 - Versions du produit : Recherche les bogues associés à un ID de produit ou à une version de logiciel spécifique
- L'icône Actualiser peut être utilisée pour actualiser la page et effacer les filtres sélectionnés
- Les bogues de priorité sont affichés dans le tableau avec les colonnes suivantes :
 - ID de bogue
 - Gravité : Gravité du bogue
 - Résumé: Résumé des détails du bogue
 - Versions du produit : ID de produit et versions logicielles affectés
 - Ressources potentiellement affectées : Nombre de ressources qui pourraient être

affectées par le bogue

- Le tri peut être effectué en cliquant sur un en-tête de colonne, à l'exception des ressources potentiellement affectées

The screenshot shows the Cisco Security Advisories interface. On the left, there's a sidebar with 'Security Advisories' and 'Priority Bugs' tabs. The 'Priority Bugs' tab is active, showing a list of bugs with columns for Bug ID, Severity, and Summary. The main content area displays the details for bug CSCwh39932, including its severity (6), description, symptom, conditions, and workaround.

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-2019-11352
CSCwi43066	3	DOC: Update N9K SFlow documentation for N9K 9504
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for random
CSCwi15483	3	Interface UP without cable, only QSFP interface
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from
CSCwi26553	6	Web UI on 17.9.4 performance/response issues
CSCwh99413	4	Console Logging for some XPATH isco-IO
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset At

Sev 6
CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

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:

Vue détaillée du bogue

- Cliquer sur un bogue ouvre la vue détaillée du bogue qui comprend les éléments suivants :
 - Onglet Résumé : Affiche la gravité du bogue, la description et les détails de la solution de contournement

The screenshot shows the Cisco Security Advisories interface, specifically the 'Affected Assets' tab for bug CSCwh39932. The main content area displays a table of assets affected by the bug, including columns for Asset Name, Serial Number, Model Name, Version, Role, IP Address, and Controller ID. The table shows two assets: CNXS-N93360YC-2 and CNXS-N93360YC-1.

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

Onglet Actifs affectés

- Onglet Actifs affectés : Affiche tous les détails des ressources potentiellement affectées, tels que le nom de la ressource, le numéro de série, le nom du modèle, la version du logiciel, l'adresse IP et l'ID du contrôleur ; vous pouvez trier et rechercher les ressources dans cet onglet

Software Images Image Distribution Server **Advisories** Insights

Security Advisories
Priority Bugs

Filters

Severity

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

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-20
CSCwi43066	3	DOC: Update N9K SFlow documentation fo
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for rande
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

Sev 6
CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

View Priority Bugs

Summary **Affected Assets (2)**

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

2 Total Assets

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
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

Afficher les bogues prioritaires

- Lien Afficher les bogues prioritaires : Accède à l'outil de recherche de bogues officiel

Assets

29 Total

Domain

Core
Campus
Data Center
Security
SD-WAN

Controller Type

Controller

ANSIBLE-156
NSO-183

Filters

... All Search

Name	ControllerType	Ip Address	Location	Managed By	Product Description	Product Family	Software Type	Software Version	Action
ASR9K-12	NSO			NSO-183	ASR9K-13	ASR9K	IOS-XR	7.6.2	
ASR9K-13	NSO			NSO-183	ASR9K-13	ASR9K	IOS-XR	7.6.2	
ASR9K-154	NSO			NSO-183	ASR9K	IOS-XR	7.6.2		
ASR9K-155	NSO			NSO-183	ASR9K	IOS-XR	7.7.2		
asr9k-154	NSO			NSO-183	ASR9K	IOS-XR	7.6.2		

Actifs

Dans le Gestionnaire d'actifs, les utilisateurs peuvent afficher la liste de tous les actifs. Lors de la sélection d'une ressource, un panneau affiche des informations au niveau de la ressource, notamment des détails sur les vulnérabilités logicielles de la ressource, organisés en deux onglets : Avis et EOX.

29 Total

Domain

Core
Campus
Data Center
Security
SD-WAN

Controller Type

Controller

ANSIBLE-156
NSO-183

Summary Backups **Advisories** **EOX**

Admin State
unlocked

Controller Type
NSO

Platform Serial Number
...

Domain
Core

IsCompliant

Auth Group
cxlabb

Current Version
7.6.2

Device-Type
cli

Ip Address
...

Managed By
...

Avis et EOX

L'onglet Avis contient deux sous-onglets, Avis de sécurité et Bogue de priorité. Vous trouverez plus de détails sur ces onglets dans les sections ci-dessous.

Bulletins de renseignements de sécurité

CI9k-CP-T2.fra-lab.net

IP Address: [REDACTED]

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

Summary Backups Advisories EOX

Security Advisories Priority Bugs

All Search

Advisory	Impact	CVE	Last Updated	Version
Cisco IOS Application Hosting Environment Privs	Medium	CVE-2023-20335	7 months ago	1.0
Cisco IOS and IOS XE Software Internet Key Exchange	High	CVE-2024-20337, CVE-2024-20300	2 months ago	1.0
Cisco IOS XE Software Auxiliary Asynchronous Port	Medium	CVE-2024-20339	2 months ago	1.0
Cisco IOS XE Software DHCP Snooping with Endpoint	High	CVE-2024-20259	2 months ago	1.0

Avis de sécurité pour les ressources sélectionnées

Dans le sous-onglet Avis de sécurité, les utilisateurs peuvent afficher tous les avis de sécurité ayant un impact sur une ressource sélectionnée. Les colonnes du tableau Avis de sécurité incluent Avis, Impact, CVE, Dernière mise à jour et Version.

CI9k-CP-T2.fra-lab.net

IP Address: [REDACTED]

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

Summary Backups Advisories EOX

Security Advisories Priority Bugs

All ASR

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

1 Items per page 10

Recherche d'avis de sécurité

CI9k-CP-T2.fra-lab.net

IP Address: [REDACTED]

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

Summary Backups Advisories EOX

Security Advisories Priority Bugs

Impact Critical

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

Recherche d'avis de sécurité - Option Impact

Les utilisateurs peuvent rechercher des conseils en fonction des valeurs des colonnes Conseils, Impact, CVE, Dernière mise à jour et Version. La pagination permet aux utilisateurs de naviguer entre les pages.

Bogues prioritaires

The screenshot shows the Cisco Prime Infrastructure interface. On the left, the 'Assets' page displays a summary of 1 asset and a list of assets. The main panel shows the 'Priority Bugs' sub-tab for the device 'CI9k-CP-T2.fra-lab.net'. The table lists the following bugs:

Bug ID	Severity	Summary
CSCwd80753	4	CCO flow does not support forward slash in the pa...

Bogues prioritaires affectant une ressource sélectionnée

Dans le sous-onglet Priority Bugs, les utilisateurs peuvent accéder à tous les bogues prioritaires affectant une ressource donnée. Les colonnes de cet onglet incluent l'ID de bogue, la gravité et le résumé.

The screenshot shows the 'Priority Bugs' sub-tab for the device 'CI9k-CP-T2.fra-lab.net'. A search filter '9800' is applied to the 'Summary' column. The table lists the following bugs:

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

Recherche de bogues prioritaires par résumé

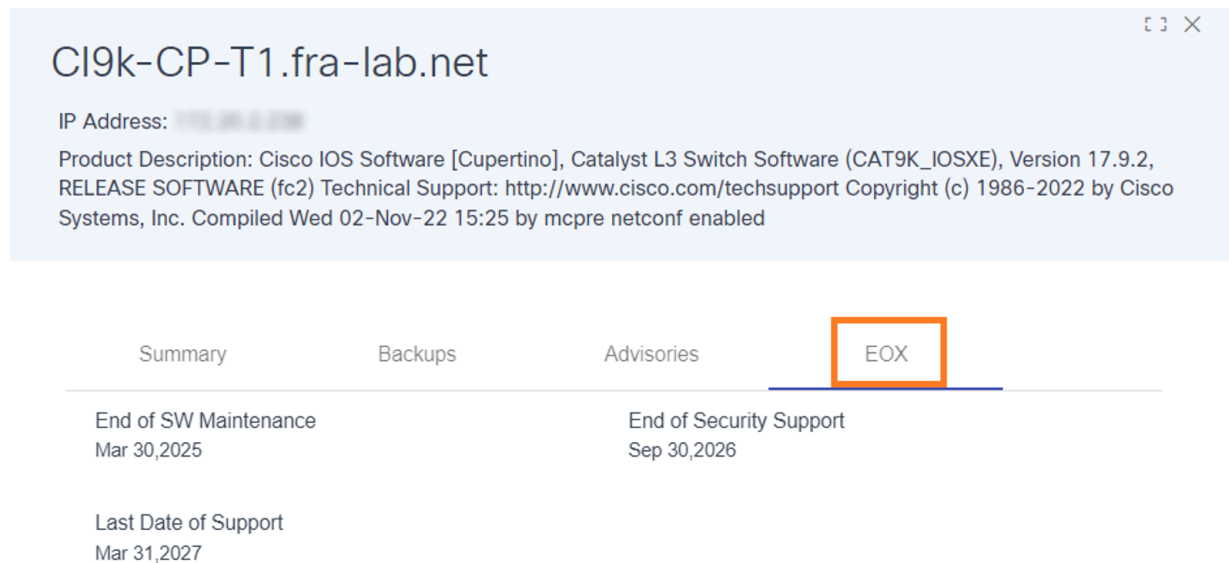
The screenshot shows the 'Priority Bugs' sub-tab for the device 'CI9k-CP-T2.fra-lab.net'. A search filter '6' is applied to the 'Severity' column. The table lists the following bugs:

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

Recherche de bogues prioritaires par gravité

Les utilisateurs peuvent rechercher des bogues prioritaires en fonction des valeurs des colonnes ID de bogue, Gravité et Résumé. La pagination facilite la navigation entre les pages.

EOX



CI9k-CP-T1.fra-lab.net

IP Address: 192.168.1.100

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

Summary	Backups	Advisories	EOX
End of SW Maintenance Mar 30, 2025		End of Security Support Sep 30, 2026	
Last Date of Support Mar 31, 2027			

Onglet EOX

L'onglet EOX affiche les données de fin de vie des logiciels spécifiques à une ressource, y compris trois dates importantes :

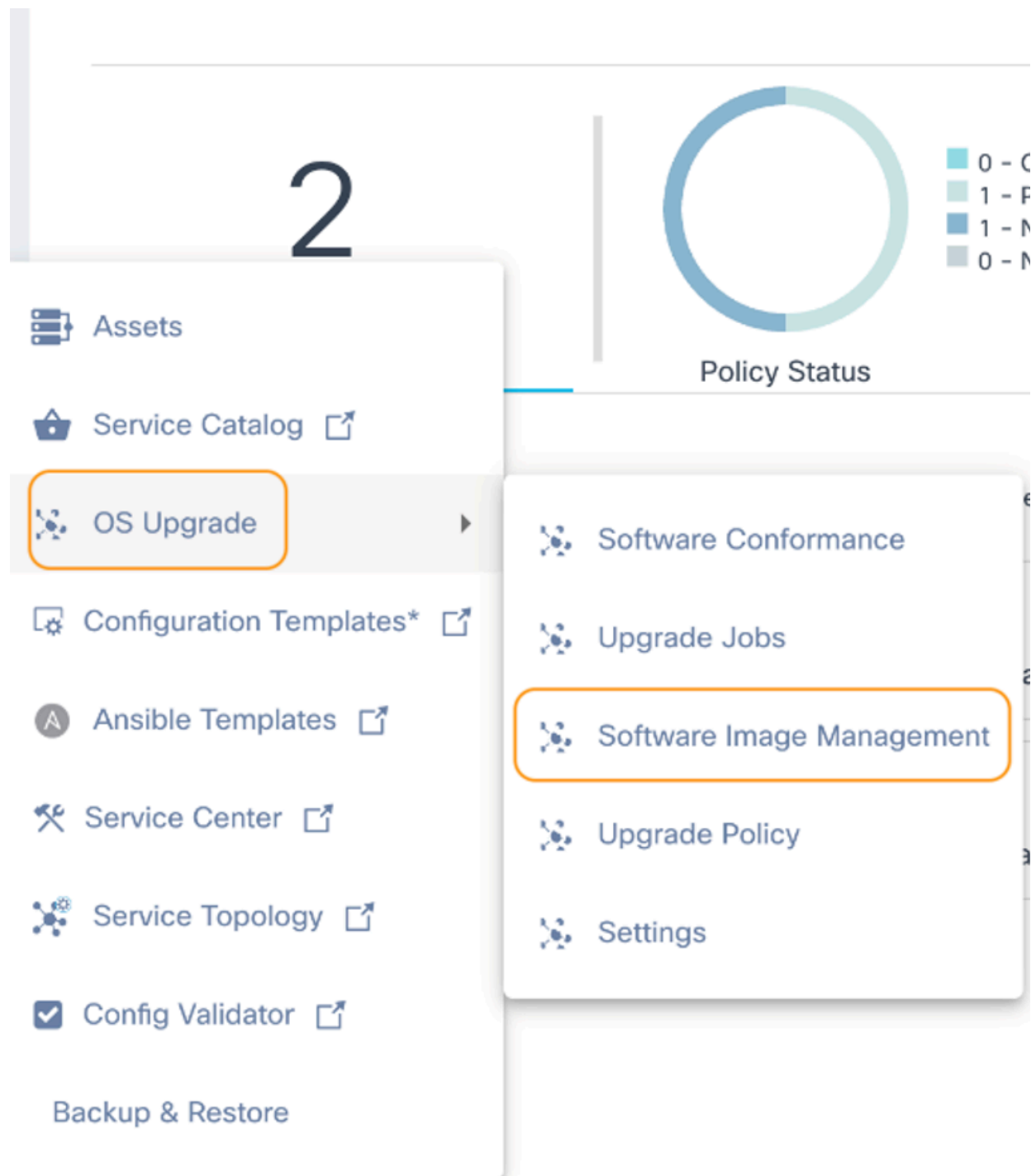
- Fin de la maintenance logicielle
- Fin du support de sécurité
- Dernière date de soutien

Affichage des informations logicielles

Software Insights fournit des suggestions logicielles pour les modèles de périphériques gérés par Cisco Catalyst Center et les contrôleurs NDFC, ce qui permet aux utilisateurs administrateurs de créer une stratégie de conformité pour les modèles de périphériques si la suggestion est disponible.

Pour accéder à Software Insights :

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré à Insights.



Gestion des images logicielles

2. Sélectionnez OS Upgrade > Software Image Management dans le panneau latéral.

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

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

1 2 3 Next | Items per page 10

Onglet Insights

3. Cliquez sur l'onglet Insights.

L'onglet Insights contient les éléments suivants :

- Filtre qui permet aux utilisateurs de filtrer les données en fonction des suggestions. Tout est sélectionné par défaut.
 - Oui filtre les données pour les modèles de périphériques avec des suggestions
 - Aucun filtre les données pour les modèles de périphériques sans suggestions

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

29 Total Device Models

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

Export to CSV

Exporter au format CSV

- L'icône Plus d'options fournit une option Exporter au format CSV pour exporter les données affichées dans la page
 - L'icône Actualiser actualise la page et efface les filtres sélectionnés
 - Le filtre Rechercher est utilisé pour rechercher les données et inclut les filtres de recherche exclusifs suivants :
 - Tous : Recherche dans toutes les colonnes (par exemple, Modèle de périphérique, Gamme de produits et Type de logiciel)
 - Modèle de périphérique : Recherche des données avec un nom de modèle de périphérique spécifique
 - Gamme de produits Recherche les données avec le nom de famille de produits spécifique
 - Type de logiciel : Recherche des données avec un nom de type de logiciel spécifique

- Les modèles de périphériques existants sont affichés avec les colonnes suivantes :
- Modèle de périphérique : Nom du modèle de périphérique
- Gamme de produits : Nom de la famille de produits à laquelle appartient le modèle de périphérique
- Type de logiciel : Nom du type de logiciel auquel le modèle de périphérique appartient
- Versions actuelles : Liste des versions logicielles uniques actuellement présentes dans l'inventaire pour le modèle de périphérique
- Version sélectionnée : Version de version suggérée qui a été sélectionnée comme version facultative à partir des suggestions fournies par Cisco
- Ressources : Nombre de ressources présentes dans le Gestionnaire d'actifs pour le modèle de périphérique
- Suggestions : Affiche Oui ou Non pour toutes les suggestions disponibles pour le modèle de périphérique

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

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

Prev 1 2 3 Next Items per page 10

Navigation dans les suggestions

- Action : Fournit des actions spécifiques à une ligne via l'icône Plus d'options (par exemple, Afficher les suggestions et Afficher les ressources)

 Remarque : L'option Afficher les suggestions est désactivée si le modèle de périphérique ne comporte aucune suggestion.

Affichage et sélection des versions logicielles suggérées par le fournisseur

Software Images
Image Distribution Server
Advisories
Insights

Filters

Suggestions

- All
- No
- Yes

Clear All

24 Total Device Models

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

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

Suggestions
Affected Assets (1)

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

Release Version & Date	CURRENT	OPTIMAL - 1
	10.2(6) Sep 1, 2023 Release Notes	10.2(6) Sep 1, 2023 Release Notes
Conformance Policy		Create
Bugs	Current Exposure : 7 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

Onglet Suggestion

Si vous sélectionnez l'icône Plus d'options > Afficher les suggestions dans la colonne Action, un panneau latéral contenant tous les détails de l'aperçu s'ouvre. L'onglet Suggestions contient les détails de version actuels et suggérés pour le modèle de périphérique sélectionné ; il est possible qu'un modèle d'appareil contienne plusieurs suggestions. Les données suivantes sont disponibles :

- Version et date de publication : La version, la date et les détails des notes s'affichent pour les versions actuelles et suggérées, si elles sont disponibles dans le cloud Cisco ; si les immobilisations du stock appartiennent à plusieurs versions, toutes les versions applicables sont affichées sous forme de valeurs séparées par des virgules dans la colonne Actuel
- Créer une stratégie de conformité : Permet aux administrateurs de créer une stratégie de conformité pour une version spécifique avec le rôle de périphérique Any

 Remarque : La création de stratégie de conformité est uniquement prise en charge pour les modèles de périphériques contrôleur NDFC

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

Supprimer une option de stratégie

 Remarque : Si une stratégie existe déjà pour le modèle de périphérique, une erreur s'affiche. S'il n'existe aucune stratégie, une stratégie est créée à l'état Activé. Si une stratégie est créée à partir d'Insights, les utilisateurs ont la possibilité de la supprimer.

- Bogues : Affiche un nombre consolidé de bogues pour chaque version
- Avis de sécurité : Affiche un nombre consolidé de conseils pour chaque version
- EoX : Affiche les dates de fin de maintenance logicielle, de fin de support de sécurité et de fin de support pour chaque version

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

Onglet Actifs affectés

Si vous sélectionnez l'icône Plus d'options > Afficher les actifs dans la colonne Action, un panneau latéral s'ouvre, où l'onglet Actifs affectés s'affiche par défaut. L'onglet Actifs affectés affiche les détails des actifs potentiellement affectés dans des colonnes telles que le nom de l'actif, le numéro de série, le nom du modèle, la version du logiciel, l'adresse IP et l'ID du contrôleur. Cet onglet permet de trier et de rechercher les ressources.

Identification des périphériques nécessitant une mise à niveau logicielle

Référez-vous à [Conformité logicielle](#) pour plus d'informations.

Conformité logicielle

La conformité logicielle permet d'identifier les ressources d'un réseau qui ne sont pas conformes à la version logicielle cible prévue. La validation est basée sur des politiques et des règles par lesquelles les intentions de conformité logicielle sont définies. Ces politiques peuvent être exécutées sur une base planifiée ou à la demande. Lors de l'exécution réussie de la politique de conformité, le résultat de conformité est obtenu, ce qui fournit l'état des actifs applicables. La portée de la conformité dépend de divers critères, tels que le rôle du périphérique, la gestion de l'instance du contrôleur, etc.

Conditions préalables

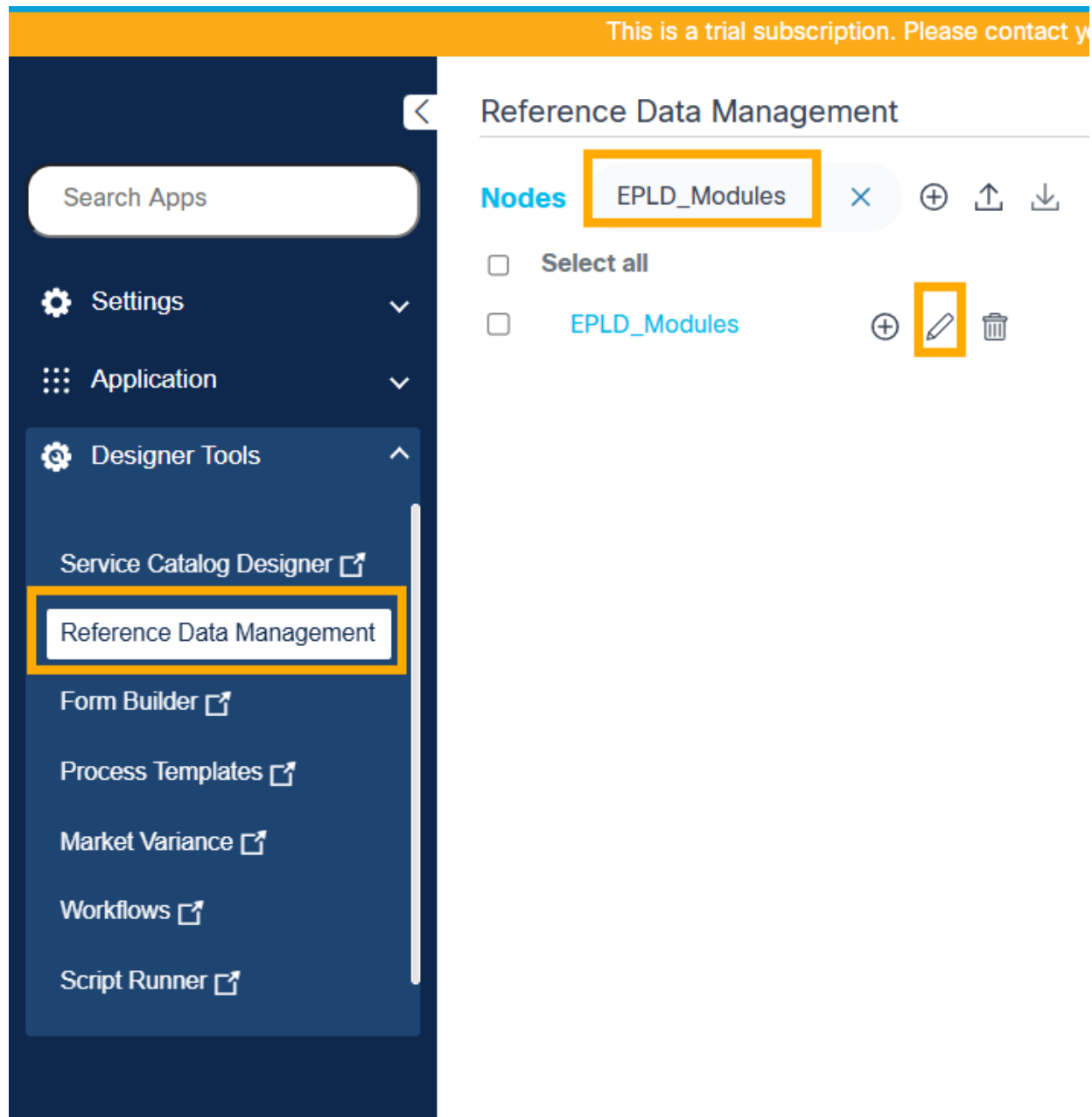
- Les images logicielles des contrôleurs tels que Cisco Catalyst Center, vManage, NDFC et FMC doivent être synchronisées. Référez-vous à [Synchronisation des images logicielles et des métadonnées](#) pour plus d'informations.
- Les métadonnées d'image logicielle nécessaires pour les contrôleurs tels que NSO, CNC, Direct-to-Device et ANSIBLE doivent être ajoutées. Référez-vous à [Ajout de métadonnées d'image logicielle](#) pour plus d'informations.
- Les utilisateurs doivent avoir accès à l'application RefD pour gérer les données du module EPLD.
- Les informations du module EPLD pour les versions requises doivent être préremplies dans l'application RefD
- Les utilisateurs doivent ajouter manuellement les informations du module EPLD dans l'application RefD si elle n'est pas disponible en mode hors connexion

Création de données de module EPLD dans l'application de gestion des données de référence

Avant de créer une stratégie de conformité, créez des données de référence de module EPLD dans l'application RefD. L'application RefD inclut des informations sur le module EPLD pour les versions du logiciel Nexus v10.2(8) et v10.4(5), respectivement. Pour les autres versions de

périphériques, les informations du modèle EPLD doivent être ajoutées manuellement dans l'application RefD.

Procédez comme suit pour ajouter d'autres versions aux métadonnées du module EPLD :



Gestion des données de référence

1. Accédez à l'application Reference Data Management et recherchez « EPLD_Modules ».
2. Sélectionnez le fichier « EPLD_Modules » et cliquez sur l'icône Edit.

Edit Node

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

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

EPLD_Modules.json Cancel Save Upload Download

Modifier le noeud

3. Ajoutez les métadonnées du module EPLD de la nouvelle version en ajoutant une nouvelle entrée avec la structure suivante :

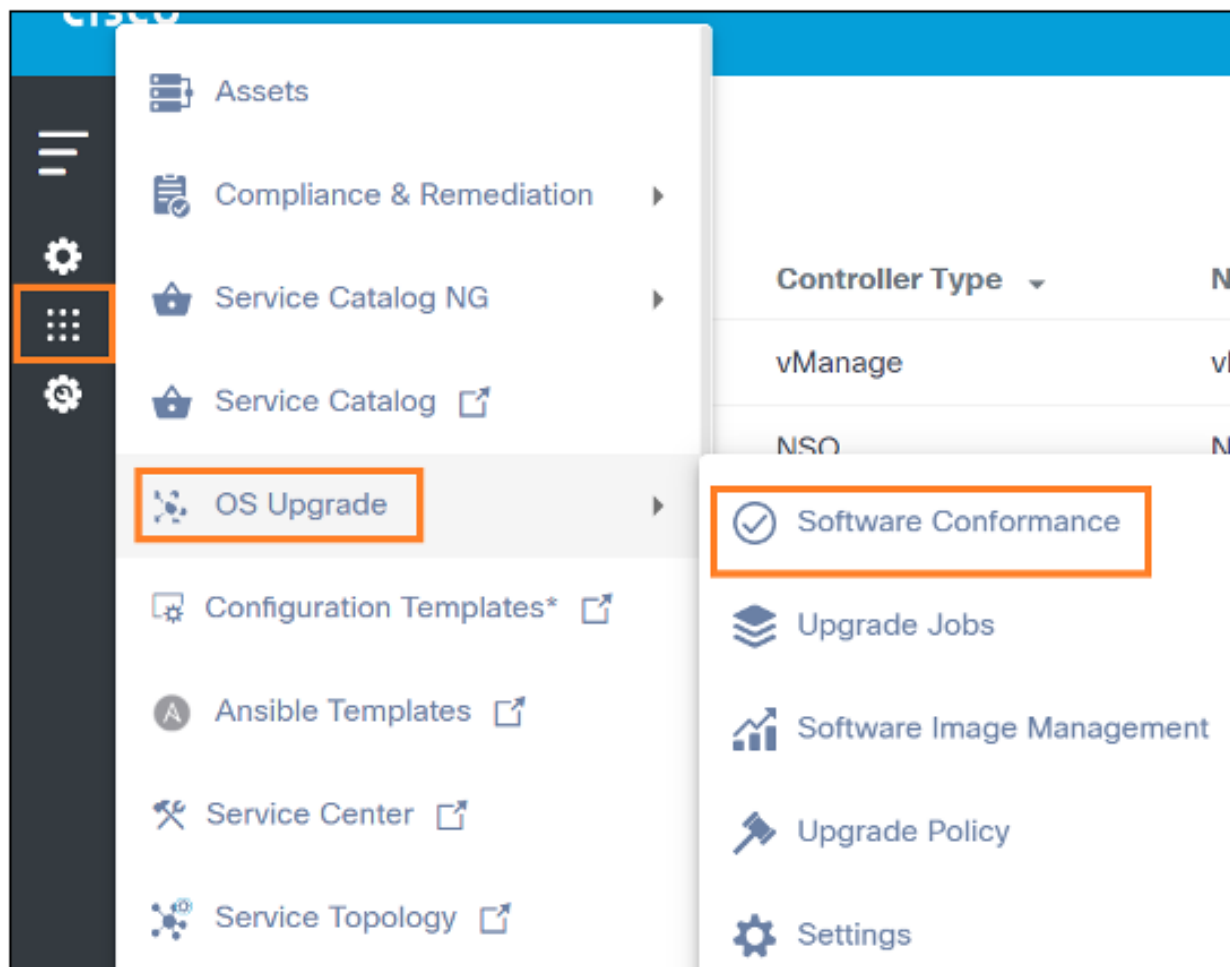
structure:

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

4. Cliquez sur Save et validez les nouvelles métadonnées du module EPLD qui sont disponibles pour la sélection dans la stratégie de conformité. Les données EPLD des versions prises en charge sont préremplies.

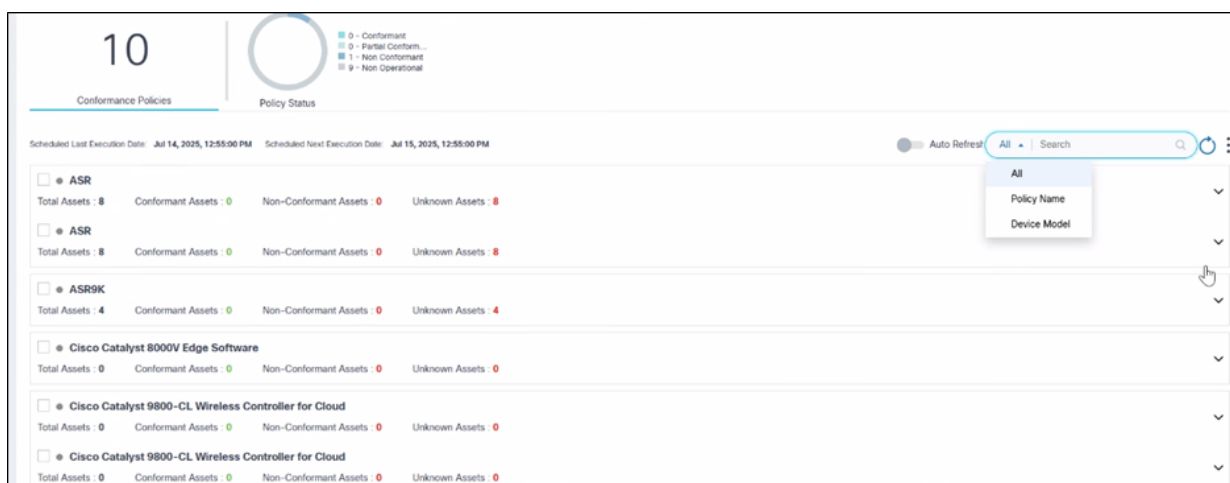
Affichage et gestion de la conformité des logiciels

1. Connectez-vous à BPA avec des informations d'identification ayant accès à Software Conformance.



Navigation de conformité logicielle

2. Sélectionnez Mise à niveau du système d'exploitation > Conformité logicielle. La page Conformité logicielle s'affiche.



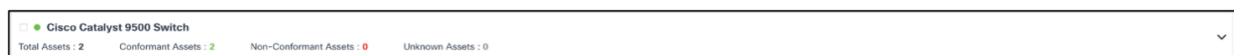
Conformité logicielle

La page Conformité logicielle contient les éléments suivants :

- Une section d'analyse, affichée en haut, qui fournit les informations suivantes :

- Nombre total de stratégies de conformité existantes dans le système
- Un filtre rapide d'état de stratégie pour filtrer en fonction des critères suivants :
 - Conformité : Tous les périphériques gérés par BPA avec un modèle spécifié se trouvent sur la version logicielle définie
 - Conformité partielle : Certains périphériques gérés par BPA avec un modèle spécifié se trouvent sur la version logicielle définie ; les périphériques restants se trouvent dans des versions logicielles différentes
 - Non conforme : Tous les périphériques gérés par BPA avec un modèle spécifié sont sur des versions logicielles différentes par rapport à une version logicielle donnée
 - Non opérationnel : Aucun périphérique applicable n'a été trouvé en fonction du modèle de périphérique spécifié dans la stratégie
- Date de la dernière exécution planifiée et date de la prochaine exécution planifiée qui indiquent la date et l'heure des contrôles de conformité planifiés précédemment exécutés et la date du prochain contrôle de conformité planifié pour toutes les stratégies
- Un champ de recherche qui est utilisé pour filtrer les politiques en fonction du modèle de périphérique, du nom de la politique ou de tout ; les utilisateurs peuvent sélectionner All pour effectuer une recherche sur tous les paramètres
- Une bascule Actualisation automatique permet l'actualisation automatique de la stratégie de conformité en cours à intervalles définis par l'utilisateur lorsqu'elle est activée. Pour activer la bascule :
 - Accédez à Mise à niveau du système d'exploitation > Paramètres pour modifier l'intervalle d'actualisation
 - Modifier l'intervalle d'actualisation automatique avec une valeur souhaitée
 - Cliquez sur Save (enregistrer)
- Le tableau de bord de stratégie de conformité logicielle est actualisé au nouvel intervalle lorsque l'option Actualisation automatique est activée
- Une icône Actualiser pour actualiser la page et effacer les filtres sélectionnés
- Une icône Autres options qui fournit les options suivantes :
 - Créer une stratégie
 - Exécuter toutes les stratégies
 - Supprimer plusieurs stratégies sélectionnées

Les stratégies sont regroupées en fonction des modèles de périphériques et s'affichent sous forme de panneaux extensibles pour fournir une vue unique sur les modèles de périphériques gérés par différents contrôleurs.



Vue réduite de la stratégie de conformité

Dans la vue réduite, le panneau affiche le modèle de périphérique et des statistiques rapides

telles que Total Assets, Conformant Assets, Non-Conformant Assets et 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

Vue étendue de la politique de conformité

Dans la vue étendue, toutes les politiques liées au modèle de périphérique s'affichent. Pour chaque stratégie, des actions supplémentaires, notamment Exécuter, Modifier la stratégie, Afficher les résultats, etc., peuvent être effectuées en sélectionnant l'icône Autres options dans la colonne Action.

Création de stratégies de conformité logicielle

1. Connectez-vous au BPA avec des informations d'identification qui ont un accès géré à la conformité logicielle.
2. Sélectionnez Mise à niveau du système d'exploitation > Conformité logicielle. La page Conformité logicielle s'affiche.

10

0 - Conformant

0 - Partial Conform...

1 - Non Conformant

9 - Non Operational

Conformance Policies

Policy Status

Scheduled Last Execution Date: Jul 14, 2025, 12:55:00 PM

Scheduled Next Execution Date: Jul 15, 2025, 12:55:00 PM

Auto Refresh

All

Search

Q

ASR

Total Assets : 8

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 8

ASR

Total Assets : 8

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 8

ASR9K

Total Assets : 4

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 4

Cisco Catalyst 8000V Edge Software

Total Assets : 0

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 0

Cisco Catalyst 9800-CL Wireless Controller for Cloud

Total Assets : 0

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 0

Create Policy

Delete

Run All

Créer une stratégie

3. Cliquez sur l'icône Autres options > Créer une stratégie.

Créer un formulaire de stratégie

4. Saisissez les informations dans les champs Nom de la politique, Modèle(s) de périphérique, Version cible, SMU, EPLD, Rôle du périphérique, Groupes d'actifs et Modèle de vérification de conformité supplémentaire. Les champs SMU, Groupe(s) d'actifs et Modèle supplémentaire de contrôle de conformité sont facultatifs.



Remarque : Les utilisateurs peuvent désormais sélectionner plusieurs modèles de périphériques dans le formulaire Créer une stratégie de conformité.



Remarque : Le cadre de conformité logicielle peut exécuter des vérifications de conformité sur la version du système d'exploitation de base et les correctifs SMU par rapport aux périphériques d'un modèle, d'un rôle ou d'une instance de contrôleur spécifique qui gère le périphérique. Si des vérifications personnalisées supplémentaires sont nécessaires, un modèle de processus peut être créé avec les commandes et les règles de validation requises qui peuvent être mappées avec le champ Modèle de vérification de conformité supplémentaire.

5. Cliquez sur Create. Une confirmation s'affiche.

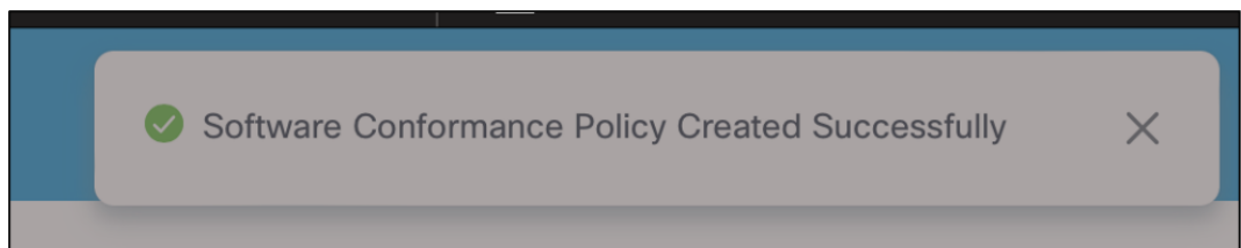


Remarque : La liste suivante doit être notée.

- Cas d'utilisation Les administrateurs ont la possibilité de créer plusieurs stratégies avec différents rôles de périphérique pour un modèle de périphérique sélectionné. Il est possible de sélectionner plusieurs rôles dans une même stratégie.
- Si Any est sélectionné dans la liste déroulante Device Role(s), tous les autres rôles de périphériques (par exemple, Access, Core, etc.) sont désactivés. Si un autre rôle de périphérique est sélectionné, alors Any est désactivé.
- Pour les périphériques gérés par des contrôleurs tels que CNC, NSO, ANSIBLE et Direct-to-Device, le rôle Any (sélectionné dans la liste déroulante Device Role(s)) peut être utilisé pour

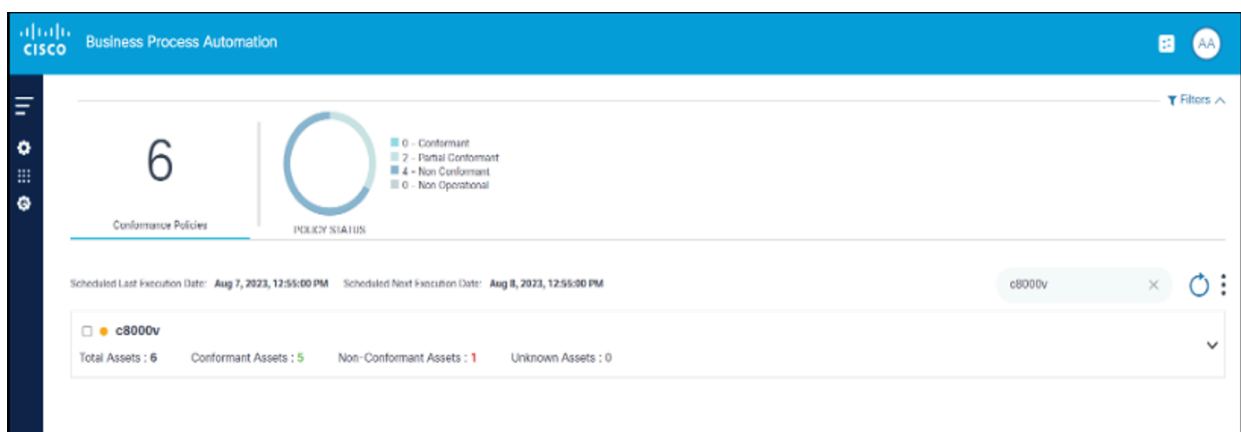
effectuer la vérification de conformité car les périphériques ne disposent pas d'informations de rôle.

- Si Any est sélectionné dans la liste déroulante Device Role(s) pour FMC, alors la conformité logicielle est exécutée sur tous les périphériques, ce qui inclut les périphériques autonomes, de contrôle et de données.
- La conformité et les mises à niveau SMU sont uniquement prises en charge pour les contrôleurs CNC, NSO, ANSIBLE, FMC, Direct-to-Device et NDFC.
- Seule la liste déroulante Global de la région est prise en charge dans cette version
- Les utilisateurs peuvent sélectionner Groupe(s) d'actifs dans la liste déroulante. Tout est sélectionné par défaut. Les utilisateurs ont la possibilité de sélectionner un ou plusieurs groupes d'actifs. Si un groupe d'actifs spécifique est sélectionné, la stratégie est exécutée uniquement sur les périphériques du groupe d'actifs sélectionné.
- Si les valeurs attendues pour les champs Device Model, Target Version, et SMU(s) ne sont pas affichées, cliquez sur Discover Images et réessayez.
- Les champs Device Model, Asset Group(s) et Role forment ensemble une stratégie unique ; les stratégies en double ne sont pas autorisées.
- Le champ EPLD renseigne les valeurs uniquement lorsque les métadonnées de l'image EPLD sont disponibles pour les modèles de périphériques et la version cible sélectionnés.
- Le nom de la stratégie est unique et les noms de stratégie en double ne sont pas autorisés.



Confirmation de création de stratégie de conformité

- Les modèles de processus balisés pour Mise à niveau du système d'exploitation nouvelle génération (nouvelle génération) s'affichent dans le champ Modèle de contrôle de conformité supplémentaire.



Résultat de la recherche de stratégie de conformité

6. Recherchez la stratégie créée en entrant le modèle de périphérique dans le champ Rechercher.

The screenshot displays the Cisco Business Process Automation interface. On the left, a list of policies is shown, including 'ASR9K', 'N9K-C93180YC-FX', and 'N9K-C93360YC-FX2'. The right panel shows the details for the 'Multi-Model-Policy-Demo' policy. The policy name is 'Multi-Model-Policy-Demo', the region is 'Global', and the target version is '10.2.5'. The device model(s) are 'N9K-C93180YC-FX, N9K-C93360YC-FX...', and the device role(s) are 'N9K-C93180YC-FX'. The controller ID(s) is 'NDFC-OS'. The additional conformance check template is 'NA'. The policy is enabled. The SMUs section shows 'No Record Found'.

Afficher la stratégie de conformité

7. Cliquez sur Policy pour afficher la vue détaillée de la stratégie.

Exécution de contrôles de conformité logicielle à la demande

1. Connectez-vous à BPA avec des informations d'identification ayant un accès d'exécution.
2. Sélectionnez Mise à niveau du système d'exploitation > Conformité logicielle. La page Conformité logicielle s'affiche.

The screenshot displays the Cisco Business Process Automation interface. The top bar shows the Cisco logo and 'Business Process Automation'. The main content area shows a 'Conformance Policies' section with a large number '9' and a 'POLICY STATUS' section with a donut chart. The donut chart shows the following status distribution: 1 - Conformant, 1 - Partial Conformant, 5 - Non Conformant, and 2 - Non Operational. Below the chart, there is a table of policies. The first policy is 'N9K-C93360YC-FX2' with a total of 2 assets, 0 conformant, 2 non-conformant, and 0 unknown. The second policy is 'N9K-C9336C-FX2' with a total of 1 asset, 1 conformant, 0 non-conformant, and 0 unknown. A search bar at the top right contains the text 'N9K'.

Recherche de stratégie

3. Recherchez la politique à exécuter à la demande à l'aide du champ Rechercher.

1

0 - Conformant

1 - Partial Conformant

0 - Non Conformant

0 - Non Operational

Policy Status

Conformance Policies

Scheduled Last Execution Date: Apr 25, 2024, 12:55:00 PM

Scheduled Next Execution Date: Apr 26, 2024, 12:55:00 PM

Search Device M

Run

View Results

Edit

Delete

ASR9K

Total Assets : 13

Conformant Assets : 4

Non-Conformant Assets : 9

Unknown Assets : 0

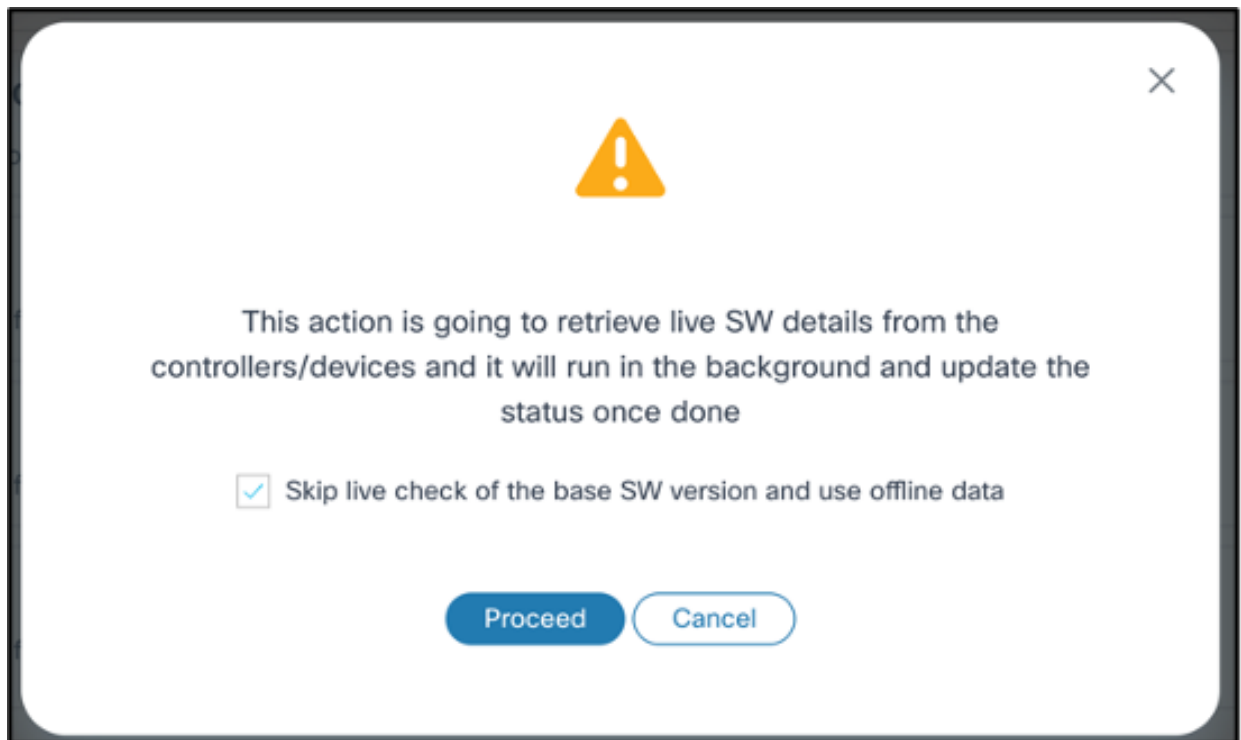
Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status
ASR9k	Global	Any	7.7.2	admin	Apr 24,2024, 7:57 PM	Apr 25,2024, 12:55 PM	Completed	Partial Conformant

1

Items per page 10

Exécutez la commande

4. Dans la colonne Action de la stratégie, sélectionnez More Options > Run. Une confirmation s'affiche pour confirmer si une vérification de l'inventaire en direct doit être effectuée pour les périphériques.



Confirmation de l'exécution de la stratégie de conformité

5. Si une synchronisation d'inventaire en direct est requise avant d'exécuter des vérifications de conformité, désactivez la case à cocher Ignorer la vérification en direct de la version du logiciel de base et utiliser les données hors connexion et cliquez sur Continuer. Dans ce cas, le contrôle de conformité n'est exécuté qu'après la synchronisation. Une notification s'affiche dans l'angle supérieur droit.



Software Conformance policy execution initiated



Notification d'exécution de stratégie de conformité



Remarque : La liste suivante doit être notée.

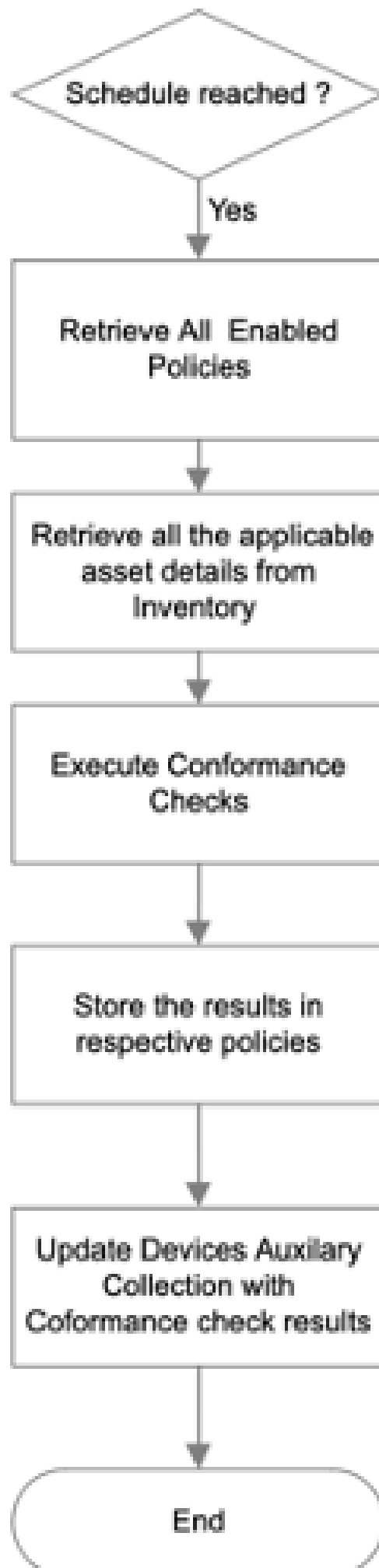
- Une vérification de conformité est effectuée par défaut à l'aide des données d'inventaire des ressources.
- Au cours de ce processus, si l'inventaire ou la synchronisation du périphérique échoue, le périphérique de stratégie correspondant est marqué comme Inconnu et la vérification SMU est ignorée.
- Pour les SMU, les données en temps réel sont récupérées du périphérique avant d'effectuer des vérifications de conformité si la case à cocher Ignorer la vérification en direct de la version du logiciel de base et utiliser les données hors connexion est activée ou non.
- Lorsqu'une stratégie inclut plusieurs modèles de périphérique, son exécution pour un modèle de périphérique lance l'exécution de toutes les stratégies associées.

Planification de l'exécution des contrôles de conformité logicielle

Les vérifications de conformité logicielle peuvent être effectuées automatiquement à intervalles réguliers à l'aide du service de planification. Les vérifications de conformité planifiées peuvent être configurées pour s'exécuter :

- Quotidien
- Deux fois par jour
- Hebdo
- Une fois

Une fois la planification atteinte, toutes les stratégies à l'état Activé sont exécutées automatiquement et les résultats de conformité sont stockés dans les stratégies respectives.

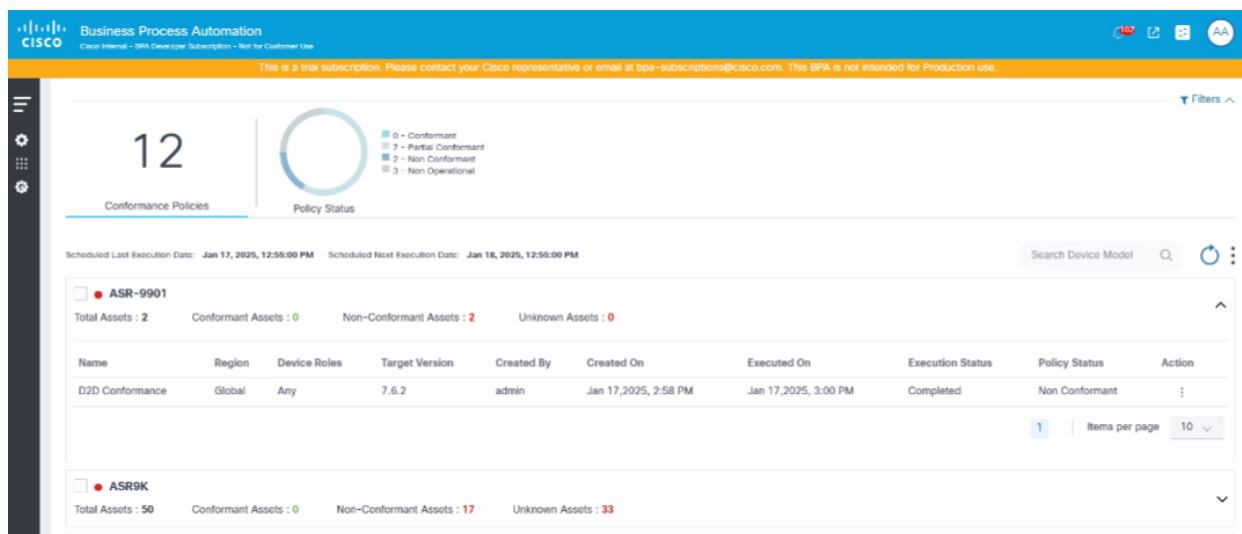


Exécution planifiée des contrôles de conformité logicielle Flux d'appels

Référez-vous à [Conformité logicielle](#) pour plus d'informations.

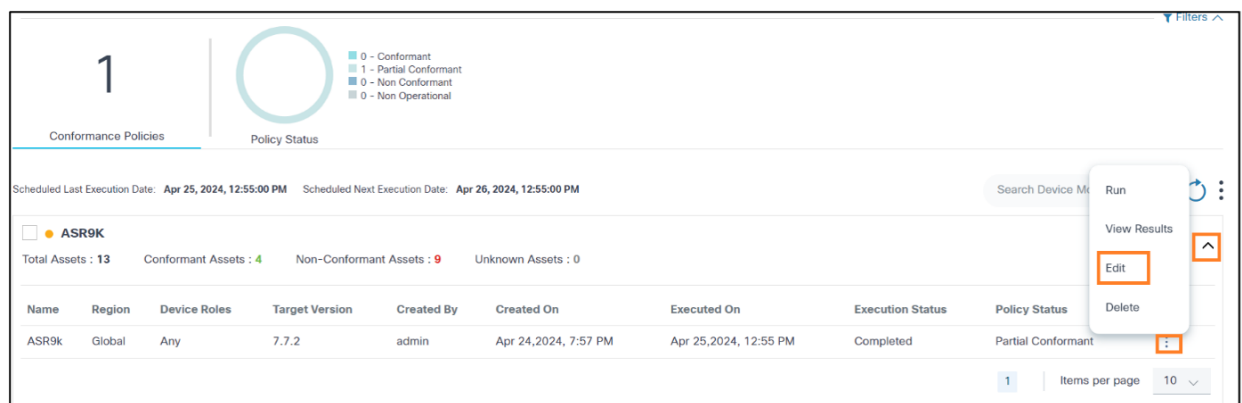
Mise à jour des stratégies de conformité logicielle

1. Connectez-vous au BPA avec des informations d'identification disposant d'un accès de gestion pour la conformité logicielle
2. Sélectionnez Mise à niveau du système d'exploitation > Conformité logicielle. La page Conformité logicielle s'affiche.



Conformité logicielle

3. Utilisez le champ Rechercher pour localiser la stratégie souhaitée.



Modifier

4. Dans la colonne Action de la stratégie, sélectionnez l'icône Autres options > Modifier.

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

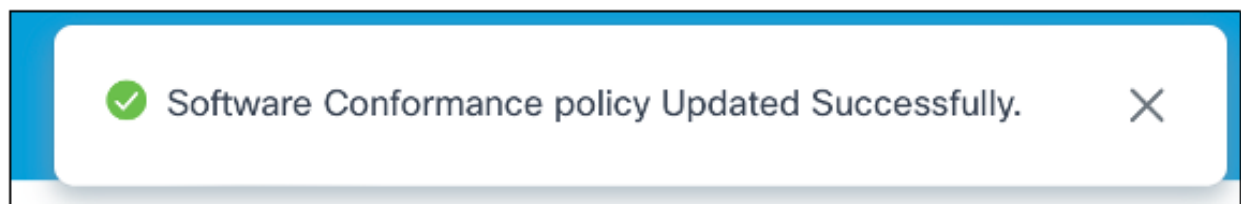
Policy Name*	Device Model*	Target Version*	SMU(s)
Multi-Model-Policy-Demo	N9K-C93180YC-FX, N9K-C93360YC-FX2 ✓	10.2.5	Select option(s)
Region*	Device Role(s)*	Controller ID(s)	Additional Conformance Check Template
Global	Any	NDFC-OS	Select option

State ☒ Enable

Cancel Save

Modifier la stratégie de conformité avec les détails remplis

5. Modifiez les champs Version cible, SMU, Rôles de périphérique, ID de contrôleur, État de la stratégie et Modèle de vérification de conformité supplémentaire si nécessaire.
6. Cliquez sur Save. Une confirmation s'affiche.

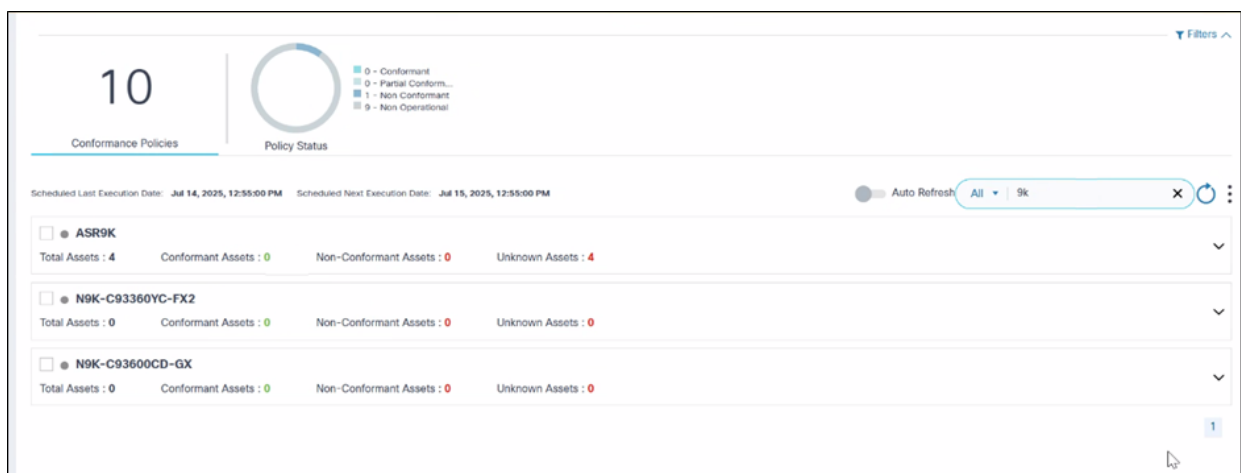


Confirmation de la mise à jour réussie

 Remarque : Lorsque la stratégie de conformité logicielle est utilisée pour une tâche de mise à niveau en cours, elle ne peut pas être modifiée.

Suppression des stratégies de conformité logicielle

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré.
2. Sélectionnez OS Upgrade > Software Conformance. La page Software Conformance s'affiche.



Résultat de la recherche de stratégie de conformité

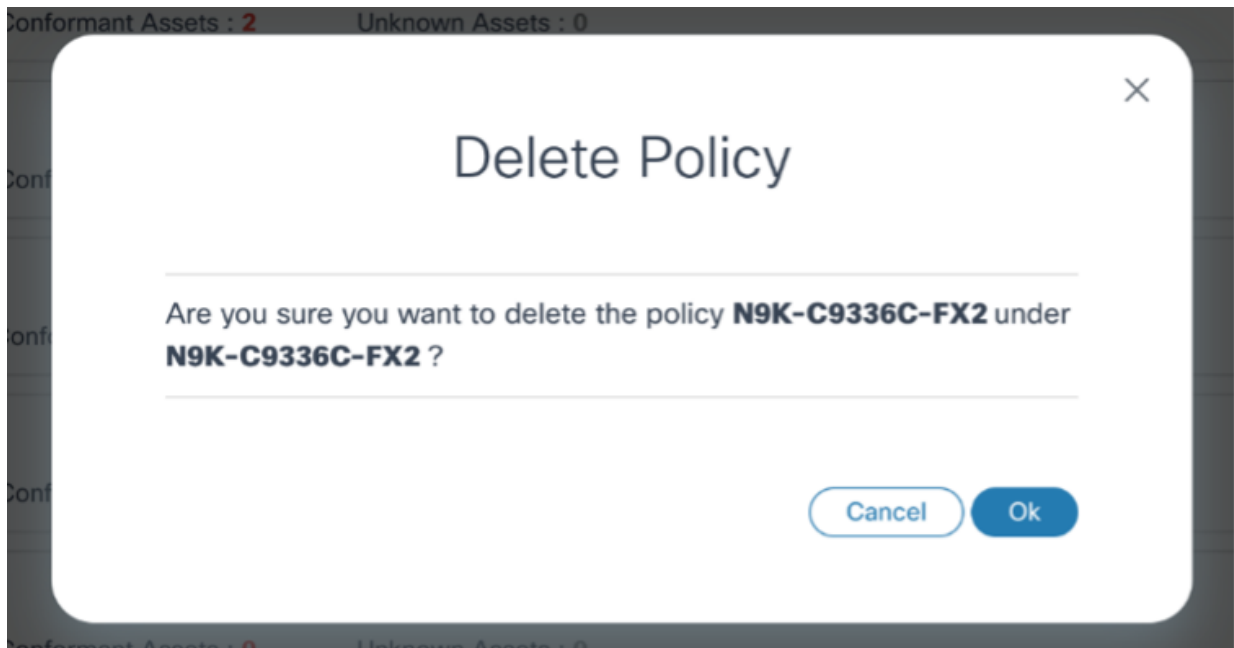
3. Utilisez le champ Rechercher pour localiser la stratégie souhaitée.

The screenshot shows the 'Conformance Policies' interface. At the top, there's a summary for '3' policies. Below this, a table lists policies. The first policy is 'PDF-Font-Testing-Policy' with a status of 'Non Conformant'. A context menu is open over the 'Delete' column, showing options: 'Run', 'View Results', 'Edit', and 'Delete'.

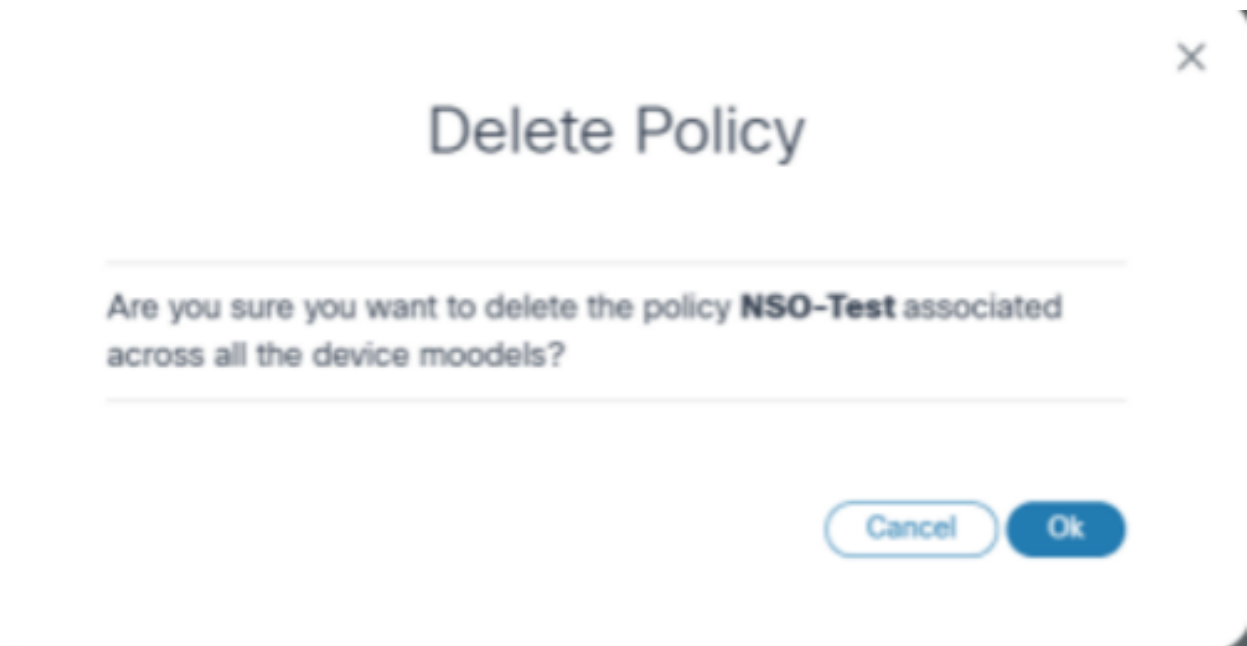
Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status	Action
PDF-Font-Testing-Policy	Global	Any	7.8.2	admin	Jul 7, 2025, 5:51 PM	Jul 14, 2025, 4:03 PM	Completed	Non Conformant	Delete

DELETE

4. Dans la colonne Action de la stratégie, sélectionnez l'icône Autres options > Supprimer. Une fenêtre de confirmation s'ouvre.



Confirmation de suppression



Confirmation de suppression de stratégie (si la stratégie est associée à plusieurs modèles)

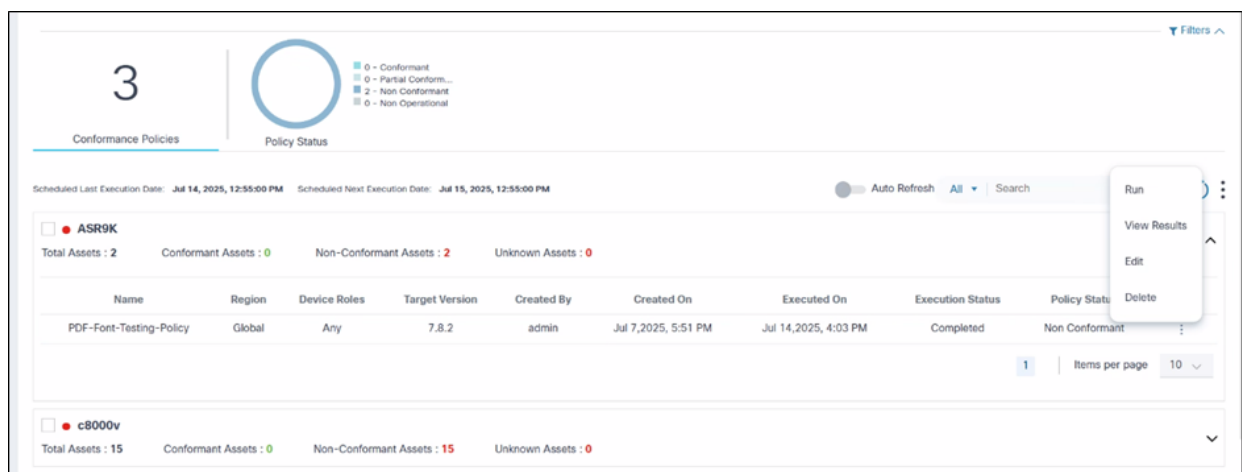
5. Click OK. La stratégie est supprimée.

 Remarque : La liste suivante doit être notée.

- Si une stratégie est associée à plusieurs modèles de périphériques, la suppression d'une stratégie supprime toutes les stratégies associées pour chaque modèle associé.
- Lorsque la stratégie de conformité logicielle est utilisée pour une tâche de mise à niveau en cours, elle ne peut pas être supprimée.

Affichage et téléchargement des résultats de conformité

Une fois qu'une stratégie est exécutée :



3 Conformance Policies

Policy Status

- 0 - Conformant
- 0 - Partial Conformant
- 2 - Non Conformant
- 0 - Non Operational

Scheduled Last Execution Date: Jul 14, 2025, 12:55:00 PM Scheduled Next Execution Date: Jul 15, 2025, 12:55:00 PM

Auto Refresh All Search

☐ **ASR9K**

Total Assets : 2 Conformant Assets : 0 Non-Conformant Assets : 2 Unknown Assets : 0

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

1 Items per page 10

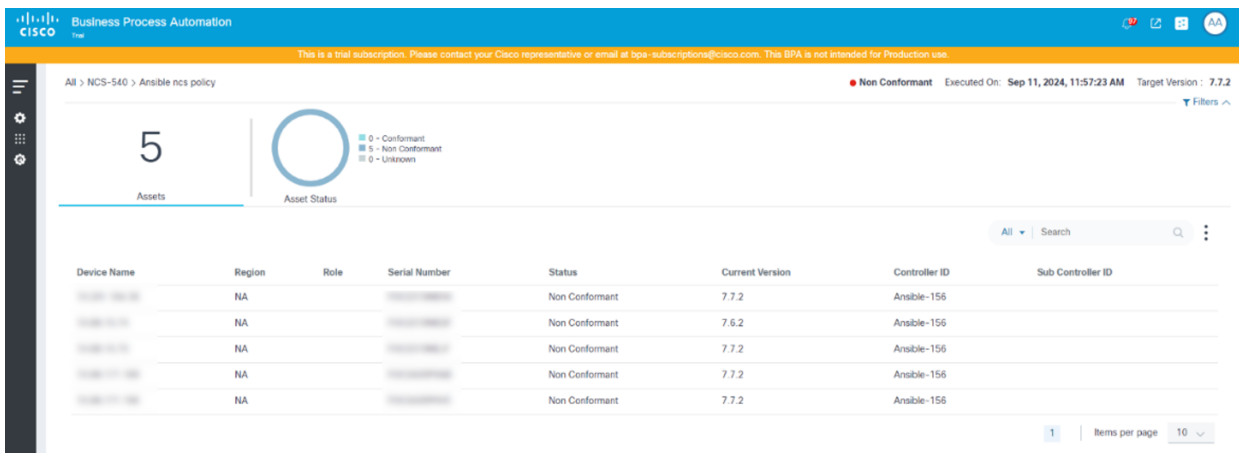
☐ **c8000v**

Total Assets : 15 Conformant Assets : 0 Non-Conformant Assets : 15 Unknown Assets : 0

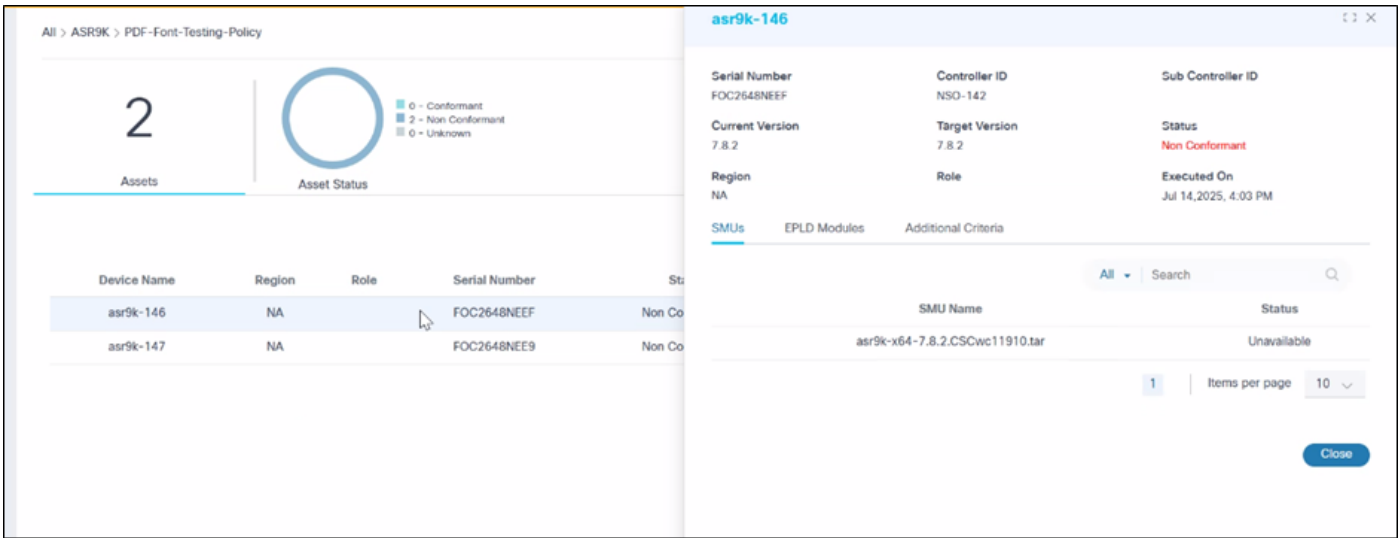
Run View Results Edit Delete

Option Afficher les résultats

1. Sur la page Software Conformance, sélectionnez l'icône More Options > View Results. La page Results s'affiche, où les utilisateurs peuvent afficher l'état de conformité des périphériques.



Afficher les résultats



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]

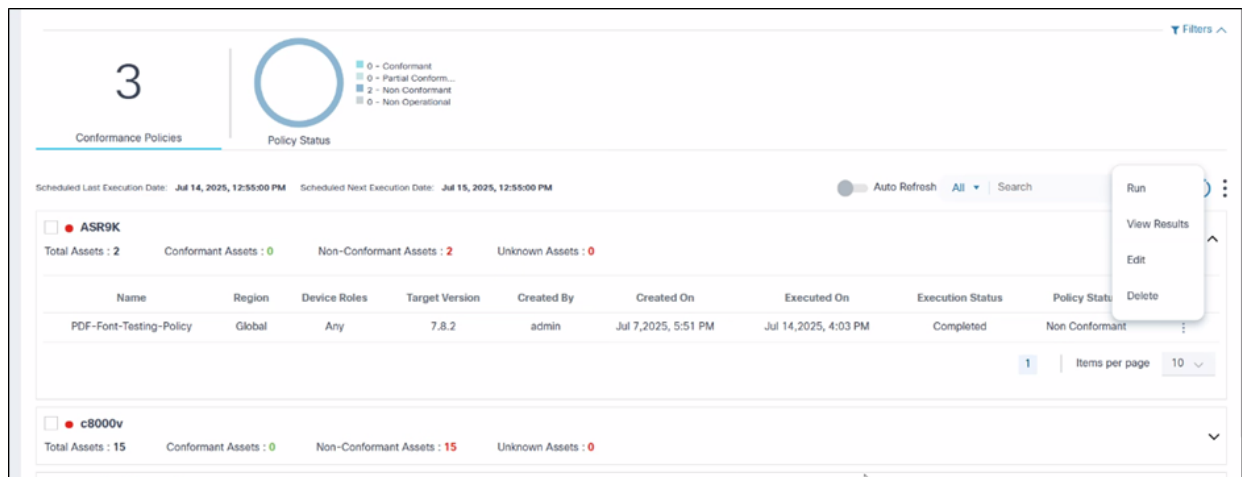
Boot Partition: xr_lcp_lv32

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. Sélectionnez une ligne pour afficher des détails spécifiques sur les ressources, ainsi que l'état SMU et d'autres critères.

 Remarque : Les détails SMU s'affichent uniquement pour les ressources des contrôleurs NSO, CNC, ANSIBLE, Direct-to-Device et NDFC. Les modules EPLD s'affichent uniquement pour les contrôleurs NDFC.



Afficher les résultats

3. Dans la colonne Action d'un périphérique, sélectionnez l'icône More Options > View Results.

Device Name	Region	Role	Serial Number	Status	Current Version	Controller ID	Sub Controller ID	Action
10.255.160.156	NA	Ansible-156	10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		Download
10.255.160.156	NA	Ansible-156	10.255.160.156	Conformant	7.7.2	ANSIBLE-156		
10.255.160.156	NA	Ansible-156	10.255.160.156	Conformant	7.7.2	ANSIBLE-156		
10.255.160.156	NA	Ansible-156	10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		
10.255.160.156	NA	Ansible-156	10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		
10.255.160.156	NA	Ansible-156	10.255.160.156	Non Conformant	7.6.2	NSO-183		

Télécharger

4. Sélectionnez l'icône Plus d'options > Télécharger pour télécharger les résultats au format .csv avec l'état de disponibilité SMU.

Device Name	Serial Num	Controller	Sub Contr	Region	Device Rol	Current Ve	Target Ver	Device Sta	Execution	Compliance	Compliance	Remarks
10.255.160.156	10.255.160.156	Ansible-156	NA	NA	7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl show_inst:Success	Device conformance check completed along with Process Template		
10.255.160.156	10.255.160.156	Ansible-156	NA	NA	7.6.2	7.7.2	Non Confo	11 Sep 202	Unavailabl show_inst:NA	Device conformance check completed		
10.255.160.156	10.255.160.156	Ansible-156	NA	NA	7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl show_inst:Success	Device conformance check completed along with Process Template		
10.255.160.156	10.255.160.156	Ansible-156	NA	NA	7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl show_inst:Success	Device conformance check completed along with Process Template		
10.255.160.156	10.255.160.156	Ansible-156	NA	NA	7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl show_inst:Success	Device conformance check completed along with Process Template		

Affichage Feuille Excel

Remarque : Afficher les résultats affiche uniquement les résultats de la dernière vérification de conformité exécutée. Les utilisateurs peuvent uniquement afficher les ressources auxquelles ils ont accès. Pour les stratégies non opérationnelles, Afficher les résultats est désactivé.

États possibles des périphériques :

- Conformité : Indique que le périphérique est conforme à la stratégie définie
- Non conforme : Indique que le périphérique n'est pas conforme lorsqu'il remplit les conditions suivantes :

Version cible	SMU	Contrôle de conformité	Status (état)
Non Conforme	S. O.	S. O.	Non Conforme
Conforme	Indisponible	Échec des règles	Non Conforme
Conforme	Disponible	Échec des règles	Non Conforme
Conforme	Indisponible	Règles réussies	Non Conforme

- Inconnu : Indique que la vérification de la conformité du logiciel du périphérique n'a pas pu être effectuée car le périphérique ne dispose pas des informations de version du logiciel actuelles.

Les critères d'état Inconnu sont les suivants :

Version cible	SMU	EPLD	Contrôle de conformité	Status (état)
Non Conforme	S. O.	S. O.	S. O.	Non Conforme
Conforme	Indisponible	Non Conforme	Échec des règles	Non Conforme
Conforme	Indisponible	Conforme	Échec des règles	Non Conforme
Conforme	Disponible	Conforme	Échec des règles	Non Conforme
Conforme	Disponible	Non Conforme	Échec des règles	Non Conforme
Conforme	Indisponible	Conforme	Règles réussies	Non Conforme
Conforme	Indisponible	Conforme	Règles réussies	Non Conforme

États SMU possibles :

- Disponible : Indique que la SMU est présente dans le périphérique et dans un état actif
- Indisponible : Indique que la SMU n'existe peut-être pas ou qu'elle existe, mais qu'elle est à l'état Inactif

États possibles du module EPLD :

- Conformité : Indique que le module EPLD est présent dans le périphérique avec la version cible attendue
- Non conforme : Indique que le module EPLD est présent dans le périphérique avec une version cible attendue sans correspondance
- Module manquant : Indique que les modules EPLD ne sont pas configurés ou abonnés dans le périphérique

États possibles du modèle de vérification de conformité :

- Réussite : Indique que le périphérique a correctement exécuté le modèle de processus avec des commandes et des règles valides
- Échec : Indique que le périphérique n'a pas pu exécuter le modèle de processus (par exemple, lorsque les commandes sont incorrectes)
- S. O.: Indique que le périphérique ne peut pas exécuter le modèle de processus (par exemple, lorsqu'il n'est pas conforme à la version cible définie)



Remarque : La liste suivante doit être notée.

- Les contrôles de conformité logicielle fonctionnent uniquement avec les périphériques appartenant au locataire par défaut
- Les contrôles de conformité logicielle s'appuient sur l'inventaire des ressources comme source de vérité pour les versions logicielles actuelles des périphériques. Si les données d'inventaire des ressources sont périmées, les résultats des contrôles de conformité du logiciel le sont également. Pour éviter le problème des données périmées, utilisez la fonction de vérification de l'inventaire en direct lors du démarrage de l'exécution de la stratégie de conformité
- La planification par défaut peut être modifiée dans Mise à niveau du système d'exploitation > Paramètres > Conformité logicielle
- Après la mise à niveau vers BPA 5.1, toutes les politiques préexistantes sont déplacées vers un état désactivé ; les utilisateurs doivent modifier chaque stratégie, sélectionner les valeurs appropriées, l'activer, puis enregistrer les modifications pour une utilisation ultérieure

Politique de mise à niveau

Le composant de stratégie de mise à niveau prend en charge deux types de stratégies :

- Stratégie en une étape :
 - Any-Any
 - <version source spécifique (7.7.1)> - <version cible spécifique (7.7.2)>
- Stratégie en plusieurs étapes :
 - v7.7.1 - 7.7.2
 - v7.7.2 - 7.7.8

- La mise à niveau en plusieurs étapes peut inclure des SMU Bridge, comme indiqué dans l'exemple ci-dessous :
 - v7.7.1 - v7.7.1[SMU de pont]
 - V7.7.1[SMU de pont] - 7.7.8

Le composant de stratégie de mise à niveau offre la flexibilité nécessaire pour prédéfinir les artefacts spécifiques à la plate-forme suivants :

- Chemins de mise à niveau
- Modèles ou workflows de pré-validation et de post-validation
- Workflow de distribution
- Workflow d'activation
- Workflow de sauvegarde
- Valeurs de délai
- Workflow de restauration
- Différences valides avant et après l'achat
- Workflow de réacheminement ou d'inversion du trafic

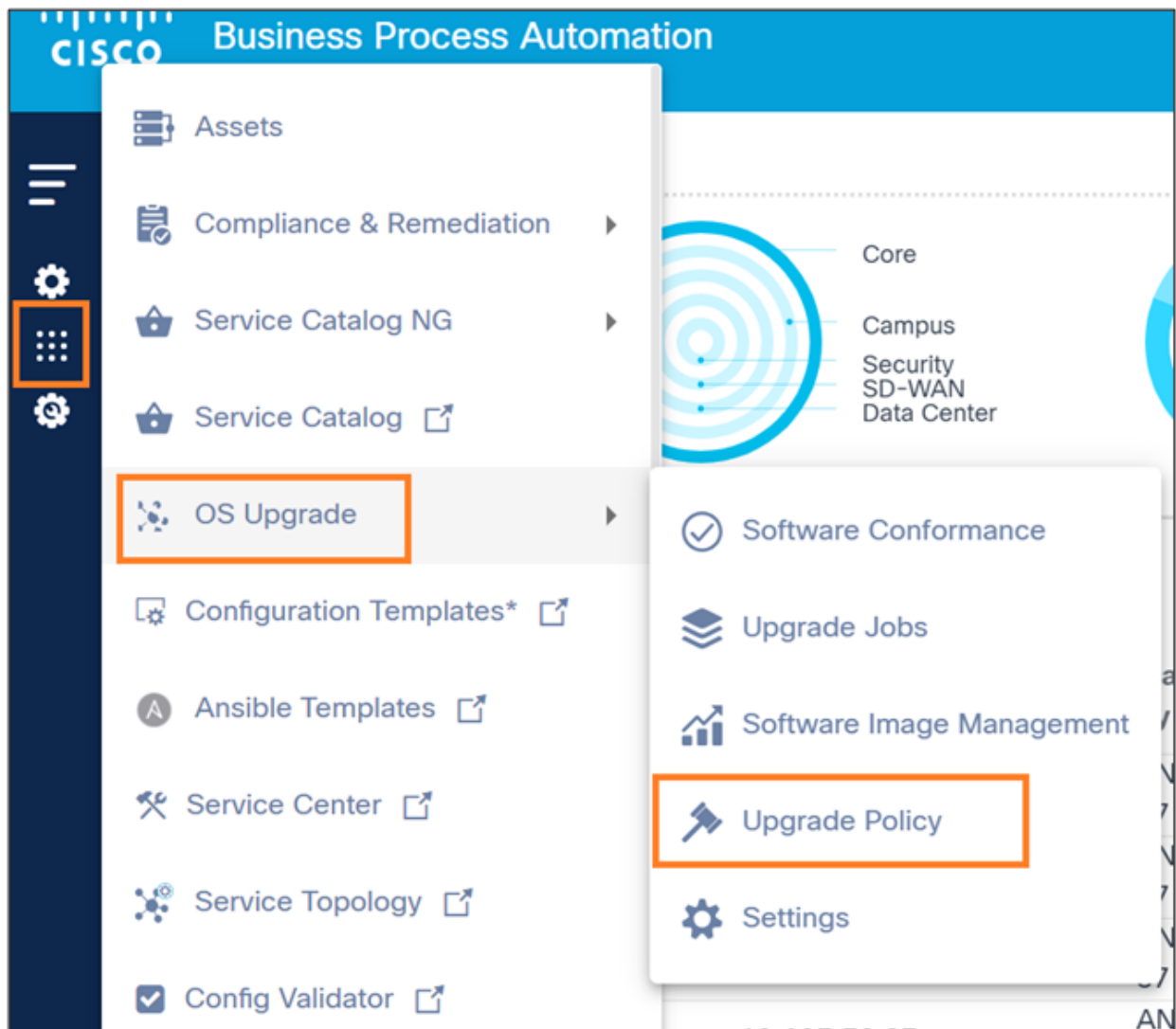
Conditions préalables

- Modèles ou workflows de processus requis avant et après validation
- Workflows de sauvegarde, de distribution, d'activation et de restauration requis
- Métadonnées d'image requises

Affichage et gestion des stratégies de mise à niveau

Pour accéder à la page Stratégie de mise à niveau :

1. Connectez-vous à BPA avec des informations d'identification disposant d'un accès suffisant à la stratégie de mise à niveau.



Mise à niveau de la navigation

- Sélectionnez Mise à niveau du SE > Stratégie de mise à niveau. La page Stratégie de mise à niveau s'affiche.

8

Policies

1 - CNC

1 - DNAC

1 - Direct-To-Device

1 - FMC

1 - NDFC

1 - vManage

1 - Ansible

1 - NSO

Controller Types

All

Search

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	

Politique de mise à niveau

La page Upgrade Policy contient les éléments suivants :

- Une section d'analyse, affichée en haut, qui fournit les informations suivantes :

- Nombre total de stratégies de mise à niveau dans le système
- Un filtre rapide Types de contrôleurs qui permet de filtrer par type de contrôleur
- Une icône Plus d'options qui permet de créer une stratégie et des actions de traitement en masse telles que Supprimer toutes les stratégies sélectionnées
- Un filtre Rechercher pour rechercher des stratégies qui peuvent être filtrées comme suit :
 - Tous : Rechercher dans tous les champs
 - Modèle de périphérique : Rechercher des stratégies avec un modèle spécifié
 - Name : Rechercher des stratégies avec un nom de stratégie spécifié
 - Créé par : Rechercher des stratégies avec un utilisateur spécifié
- Trier les stratégies en cliquant sur les noms de colonne ou les champs de table correspondants

The screenshot displays the Cisco Business Process Automation (BPA) interface. On the left, a sidebar shows a menu with a 'Policies' section. The main area features a summary card with the number '61' and a donut chart showing the distribution of strategies by controller type. Below this is a table listing strategies with columns for checkboxes, Device Model, Controller Type, and Name. The table lists several strategies, including 'D2d_any_without_TD', 'D2D-ASR-9901-Default', and 'Ansible_multi_step_123'. On the right, a detailed view of the 'Ansible_TR_TD_workflow_check' strategy is shown, including its description, max batch count, default policy, and a list of workflow details.

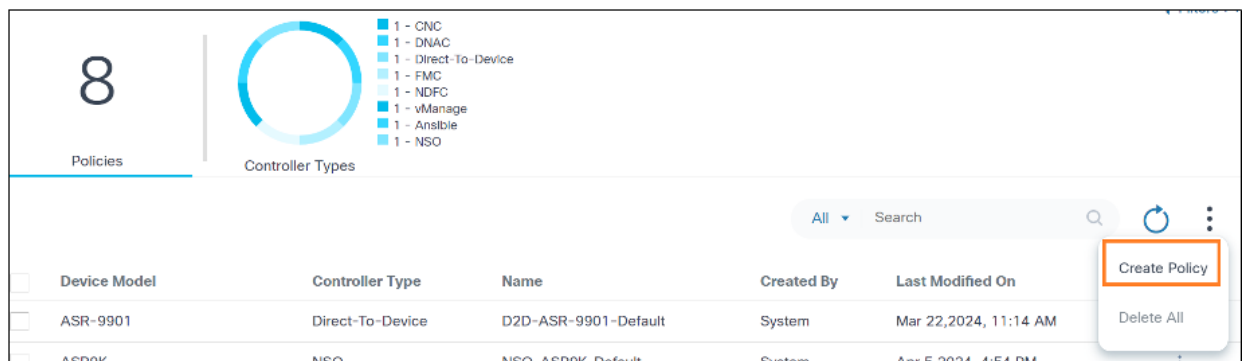
Vue détaillée des stratégies

- Cliquer sur une stratégie particulière ou afficher la vue détaillée d'une stratégie

 Remarque : Le même modèle de périphérique et le même type de contrôleur peuvent avoir un nombre quelconque de stratégies si les noms de stratégie sont uniques.

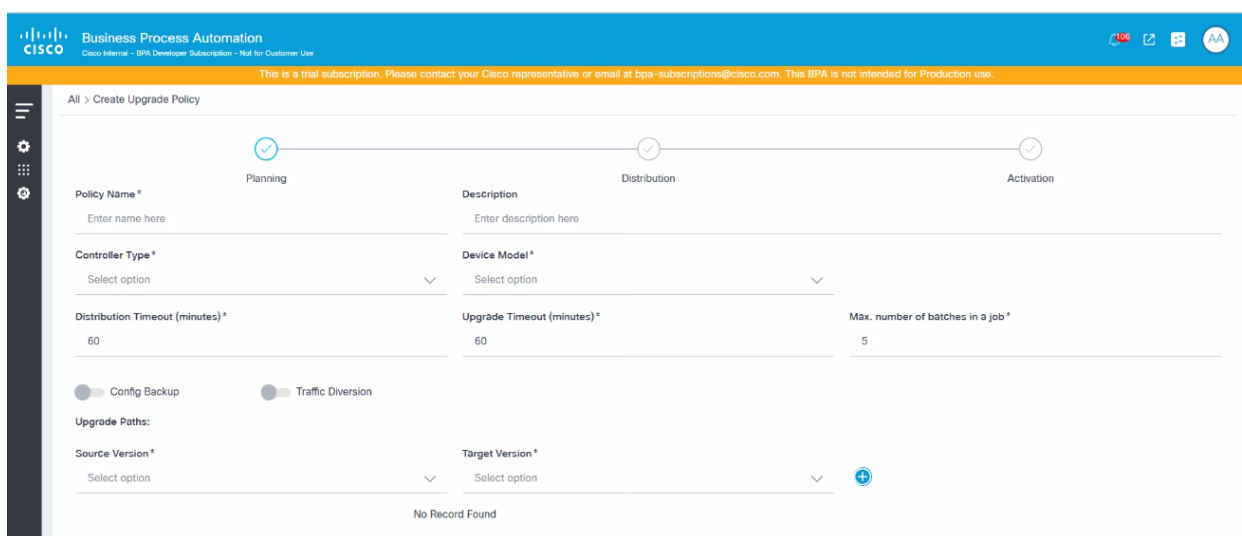
Création de stratégies de mise à niveau

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré pour les stratégies de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Stratégie de mise à niveau. La page Stratégie de mise à niveau s'affiche.



Créer une stratégie

- Sélectionnez Autres options > Créer une stratégie. La page Créer une stratégie de mise à niveau s'affiche.



Créer une stratégie de mise à niveau

Planification

- Configurez les paramètres liés à la stratégie globale. Le tableau ci-dessous fournit une brève description de chaque champ.

Champ	Description
Nom de stratégie	Nom de la stratégie
Description	Brève description de la politique
Type de contrôleur	Contrôleur approprié utilisé pour effectuer la mise à niveau du système d'exploitation
Modèle de périphérique	Modèle de périphérique utilisé pour effectuer la mise à niveau du système d'exploitation
Délai de distribution (minutes)	Temps d'attente maximal en minutes pour l'activité de

Champ	Description
	distribution d'image
Délai de mise à niveau (minutes)	Durée d'attente maximale en minutes pour l'activité d'activation d'image
Nombre maximal de lots dans une tâche	Nombre de lots pouvant être ajoutés à un ordre de fabrication ; le nombre maximal de lots autorisés est de 20 Activez cette option si une sauvegarde est requise et renseignez les champs suivants dans la fenêtre pour les contrôleurs vManage et Direct-to-Device : - Nom du workflow : Workflow de sauvegarde applicable Remarque : Si les flux de travail sont introuvables, vérifiez qu'ils sont correctement balisés avec la balise NextGen Mise à niveau du système d'exploitation - Utiliser le dernier workflow : Si cette option est sélectionnée, la dernière version du workflow sélectionné est utilisée - Version du workflow : La version personnalisée du workflow ; ne peut être sélectionné que si l'option Utiliser le dernier workflow n'est pas sélectionnée.
Basculement de sauvegarde de configuration	Pour les contrôleurs NDFC, NSO, CNC et Cisco Catalyst Center, la sauvegarde est effectuée via le service de sauvegarde et de restauration. Par conséquent, une stratégie de sauvegarde et de restauration doit être sélectionnée dans la fenêtre Détails de la sauvegarde. Remarque : Les utilisateurs doivent sélectionner la stratégie appropriée pour le type de contrôleur. Référez-vous à la section Sauvegarde et restauration pour plus d'informations sur les politiques de sauvegarde et de restauration. Pour activer la sauvegarde des périphériques Nexus, la configuration de la fonction scp-server doit être présente sur les périphériques cibles.

Champ	Description
	Activez cette option si le détournement de trafic est requis et renseignez les champs suivants dans la fenêtre Traffic Diversion : - Workflow de déviation du trafic : Workflow de déviation de trafic applicable. Remarque : Si les flux de travail sont introuvables, vérifiez qu'ils sont correctement balisés avec la balise NextGen Mise à niveau du système d'exploitation
Basculement de déviation du trafic	- Workflow d'inversion du trafic : Workflow d'inversion du trafic applicable. Remarque : Si les flux de travail sont introuvables, vérifiez qu'ils sont correctement balisés avec la balise NextGen Mise à niveau du système d'exploitation - Utiliser le dernier workflow : Dernière version du workflow sélectionné ci-dessus - Version du workflow : La version personnalisée du workflow ; ne peut être sélectionné que si Utiliser le dernier workflow n'est pas sélectionné Les chemins de mise à niveau définissent les chemins de mise à niveau d'étape applicables ; il est possible d'ajouter plusieurs versions source et cible dans les champs suivants pour répondre à différentes demandes - Version source : Version de début du chemin de mise à niveau - Version cible : Version finale du chemin de mise à niveau
Chemins de mise à niveau	- Version source (Any) à Version cible (Any) : Pour ce faire, sélectionnez Any dans les champs Source Version et Target Version, qui est la valeur par défaut pour tous les modèles de périphériques ; dans ce scénario, les pages Distribution et Activation fournissent un processus unifié pour la mise à niveau - Version source (version spécifique) vers Version cible (version spécifique) : Pour ce faire, il est possible de sélectionner des versions d'image spécifiques disponibles pour le modèle d'appareil ; plusieurs

Champ	Description
	versions source et cible peuvent être ajoutées ; le nombre d'entrées du processus de mise à niveau de distribution et d'activation correspond au nombre de versions source et cible ajoutées, et chacune est présentée sous la forme d'une section réductible étiquetée avec les versions source et cible correspondantes. Un chemin de mise à niveau nécessite que les SMU obligatoires soient appliqués à la version source avant la mise à niveau vers la version cible en les ajoutant comme SMU de pont au chemin de mise à niveau respectif. Pour plus d'informations sur les SMU Bridge, reportez-vous à la section suivante.

Pont SMU

Les SMU de pont, également appelés SMU de mise à niveau ou de rétrogradation obligatoires, sont une condition préalable et doivent être installés avant la mise à niveau ou la rétrogradation vers une autre version logicielle de la même plate-forme ou du même modèle.

Ajout de SMU de pont dans un chemin de mise à niveau

✓

Planning

✓

Distribution

✓

Activation

Policy Name*

Enter name here

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
7.6.2		7.7.2	⋮
			1

Delete Path

Add Bridge SMUs

Cancel

Next

Options du chemin de mise à niveau

1. Après avoir ajouté un chemin de mise à niveau, sélectionnez l'icône Autres options. Les options Delete Path et Add Bridge SMU s'affichent.

Progress bar: Planning (checked), Distribution (unchecked), Activation (unchecked)

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

Ajouter des SMU de pont

- Sélectionnez Add Bridge SMU. La fenêtre Add Bridge SMUs s'affiche. Tous les SMU de pont disponibles s'affichent pour le chemin de mise à niveau spécifié.

Close button (X)

Add Bridge SMUs

Select option(s)

- ☒ asr9k-x64-7.6.2.CSCwf77420.tar
- ☐ asr9k-x64-7.6.2.CSCwc41614.tar

Ajouter des SMU de pont

- Dans la fenêtre Add Bridge SMUs, activez la ou les cases à cocher appropriées pour ajouter des Bridge SMU ou désactivez les cases à cocher pour les supprimer. Une fois les SMU de pont ajoutés, le chemin de mise à niveau est mis à jour avec les détails SMU de pont sélectionnés.

✓ Planning
✓ Distribution
✓ Activation

Policy Name*

ASR9kPolicy

Controller Type*

NSO

Distribution Timeout (minutes)*

60

Upgrade Paths:

Source Version

Select option

Description

Enter description here

Device Model*

ASR9K

Upgrade Timeout (minutes)*

60

Max. number of batches in a job*

5

☐ Config Backup ☐ Traffic Diversion

Target Version

Select option

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2	asr9k-x64-7.6.2.CSCw77420.tar	7.7.2	⋮

Chemin de mise à niveau avec Bridge SMU

Remarque : Chaque chemin de mise à niveau incluant des SMU de pont est considéré comme une mise à niveau en deux étapes. Pour le chemin de mise à niveau illustré dans la figure ci-dessus, le chemin de mise à niveau final est le suivant :

- 7.6.2 - 7.6.2 [SMU de pont]

Ce chemin représente la mise à jour du périphérique exécuté sur v7.6.2 avec les SMU Bridge.

- 7.6.2 [SMU de pont] - 7.7.2

Ce chemin représente la mise à niveau du périphérique de v7.6.2 vers v7.7.2. Dans ce cas, la version source du périphérique est 7.6.2, y compris les SMU de pont qui lui sont appliqués.

Modification des SMU de pont

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

Chemin de mise à niveau avec Bridge SMU

1. Dans la section Upgrade Paths, sélectionnez l'icône More Options > Edit Bridge SMUs. La fenêtre Edit Bridge SMUs s'affiche.

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

Modifier les SMU de pont

2. Activez ou désactivez les cases à cocher appropriées pour mettre à jour les SMU de pont.
3. Cliquez sur OK. Un résumé des modifications s'affiche.

Policy Name *	Planning	Description	Distribution	Activation
ASR9K bridge 772		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

Résumé des modifications

4. Vérifiez le résumé des modifications et cliquez sur Next.

Suppression des SMU de pont

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

Delete Path

Edit Bridge SMUs

Cancel Next

Modifier les SMU de pont

1. Dans la section Upgrade Paths, sélectionnez l'icône More Options > Edit Bridge SMUs. La fenêtre Edit Bridge SMUs s'affiche.

×

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

Modifier les SMU de pont

2. Désactivez les cases à cocher appropriées pour supprimer les SMU de pont.
3. Cliquez sur OK. Un résumé des modifications s'affiche.

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

Device Model *

ASR9K

Upgrade Timeout (minutes) *

60

Max. number of batches in a job *

5

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	:

1Items per page25

Cancel

Next

Résumé des modifications

Distribution

La distribution prend les paramètres d'entrée liés à la distribution d'image (c'est-à-dire la copie d'image). Les images suivantes sont les paramètres d'entrée requis pour chaque type de chemin de mise à niveau.

Planning

Distribution

Activation

Workflow Name *

ASR9K_Device_SW_Distribution

Workflow Version *

Select option

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asr9k_distribution_precheck

Post Check Templates

asr9k_distribution_postcheck

Pre/Post Workflow

Previous

Next

Section Distribution d'images - Mise à niveau en une étape

✓

✓

✓

Planning

Distribution

Activation

Workflow Name *

ASR9K_Device_SW_Distribution

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

☒ Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓ ✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Post check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓ ✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Previous

Next

Section de distribution d'images - Mise à niveau en une étape avec activation du workflow pré/post

All > D2D_multi_step_policy > Edit Upgrade Policy

✓

✓

✓

Planning

Distribution

Activation

7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

asr9k_distribution_precheck

✓

Post Check Templates

asr9k_distribution_postcheck

✓

☒ Pre/Post Workflow

☐ Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

asr9k_distribution_precheck

✓

Post Check Templates

asr9k_distribution_postcheck

✓

☒ Pre/Post Workflow

Previous

Next

Section Distribution - Mise à niveau en plusieurs étapes

✓

✓

✓

Planning

Distribution

Activation

7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

☒ Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓ ✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Post check Workflow *

Select option

▼

☐ Use latest workflow

Workflow Version *

Select option

▼

☐ Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASR9K_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

▼

Section Distribution - Mise à niveau en plusieurs étapes

Section Distribution - Mise à niveau Bridge SMU

1. Configurez les paramètres liés à la distribution d'images.
2. Le tableau suivant fournit une brève description de chaque champ.

Champ	Description
Nom du workflow	Workflow de distribution applicable
Utiliser le dernier workflow	Sélectionner la dernière version du workflow sélectionné
Version du workflow	La version personnalisée du workflow ; cette option ne peut être sélectionnée que si la case à cocher Utiliser le dernier workflow n'est pas activée
Modèles communs avant/après	Modèles de processus qui sont exécutés aux deux étapes (c.-à-d. vérification préalable et vérification postérieure) Remarque : Les vérifications ne sont spécifiques qu'au jalon de distribution.
Basculement pré/post workflow	Référez-vous à Modèles de processus pour plus d'informations Permet aux utilisateurs de sélectionner l'exécution de workflows de pré-vérification ou de post-vérification dans le jalon de distribution. Lorsque la bascule est activée, seuls les workflows de pré-vérification ou de post-vérification peuvent être configurés.
Vérification préalable du workflow	Inclut les commandes exécutées uniquement au cours de la phase de pré-vérification. Remarque : Ces vérifications sont spécifiques à l'étape de distribution.

Champ	Description
Workflow post-contrôle	Le workflow de post-contrôle comprend les commandes exécutées de manière unique au cours de la phase de post-contrôle.
Modèles de pré-vérification	Remarque : Ces vérifications sont spécifiques à l'étape de distribution. Les modèles de processus qui contiennent des commandes exclusives de pré-vérification ; les modèles ne sont exécutés qu'au cours de la phase de pré-vérification.
Modèles de post-vérification	Remarque : Les vérifications ne sont spécifiques qu'au jalon de distribution. Les modèles de processus qui contiennent des commandes exclusives de post-vérification ; les modèles ne sont exécutés qu'au cours de la phase de post-vérification.
Utilisez les mêmes propriétés pour tous les chemins de mise à niveau ci-dessous	Remarque : Les vérifications ne sont spécifiques qu'au jalon de distribution. Des propriétés cohérentes sont appliquées sur tous les chemins de mise à niveau dans des mises à niveau à sélection multiple. Remarque : Si cette option est sélectionnée, les mêmes propriétés sont appliquées à tous les chemins de mise à niveau dans la mise à niveau à sélection multiple.



Remarque : Les flux de travail ou les modèles de processus doivent être correctement balisés avec la balise de nouvelle génération Mise à niveau du système d'exploitation.

3. Cliquez sur Next pour passer à la section Activation.

Activation

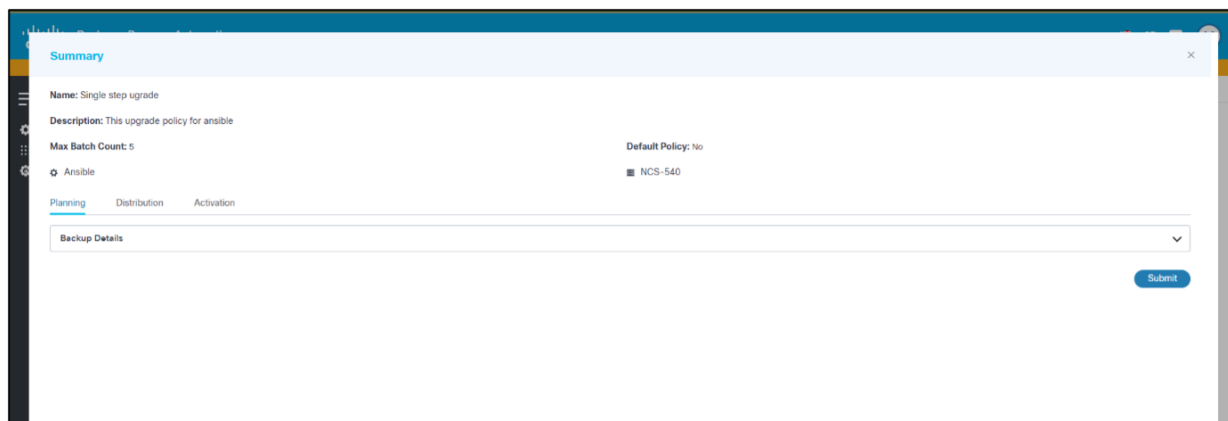
Champ	Description
Nom du workflow	Workflow d'activation applicable
Utiliser le dernier workflow	Sélectionner la dernière version du workflow sélectionné
Version du workflow	La version personnalisée du workflow ; ne peut être sélectionné que si la case Utiliser le dernier workflow n'est pas cochée
Modèles communs avant/après	Modèles de processus qui sont exécutés aux deux étapes (c.-à-d. vérification préalable et vérification postérieure). Remarque : Les vérifications ne sont spécifiques qu'au jalon d'activation.
Modèles de pré-vérification	Référez-vous à Modèles de processus pour plus d'informations Les modèles de processus qui contiennent des commandes exclusives de pré-vérification ; les modèles ne sont exécutés qu'au cours de la phase de pré-vérification.
Modèles de post-contrôle	Remarque : Les vérifications ne sont spécifiques qu'au jalon d'activation. Les modèles de processus qui contiennent des commandes exclusives de post-vérification ; les modèles ne sont exécutés qu'au cours de la phase de post-vérification.
Différence valide avant/après	Remarque : Les vérifications ne sont spécifiques qu'au jalon d'activation. Modèles de processus sélectionnés pour ignorer les différences.
Workflow de restauration	Remarque : Les vérifications ne sont spécifiques qu'au jalon d'activation. Workflow de restauration applicable.
Vérification préalable du workflow	Remarque : Si l'un des chemins de mise à niveau avec le workflow de restauration est sélectionné dans la mise à niveau à sélection multiple, toutes les autres étapes de mise à niveau sont sélectionnées avec le workflow de restauration par défaut. Ce workflow de pré-vérification personnalisé est constitué de commandes spécifiques dont les résultats d'exécution peuvent être sélectionnés et révisés. Elle n'est effectuée que lors de la phase de contrôle préalable.
Workflow post-contrôle	Remarque : Ces vérifications sont spécifiques au jalon d'activation. Ce workflow de post-vérification personnalisé se compose de commandes spécifiques dont les résultats d'exécution peuvent être sélectionnés et révisés. Elle n'est effectuée que lors de la phase de post-contrôle.
Utilisez les mêmes propriétés pour tous les chemins de mise	Remarque : Ces vérifications sont spécifiques au jalon d'activation. Des propriétés cohérentes sont appliquées sur tous les chemins de mise à niveau dans des mises à niveau à sélection multiple.
	Remarque : Si cette option est sélectionnée, les mêmes propriétés sont

Champ	Description
à niveau ci-dessous	appliquées à tous les chemins de mise à niveau dans la mise à niveau à sélection multiple.

 Remarque : Il convient de noter ce qui suit :

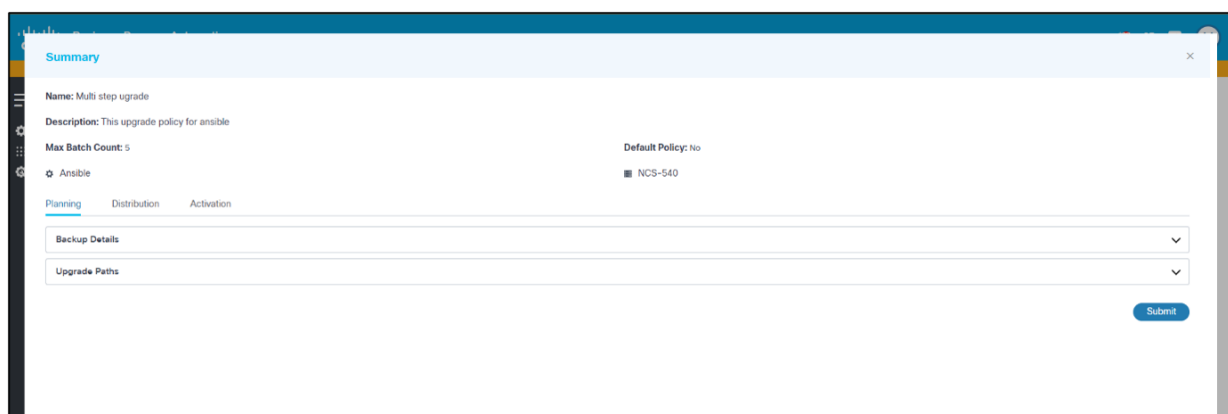
- L'algorithme de clé publique requis pour les périphériques Nexus doit être configuré dans NSO.
- Configurez les fonctionnalités de bgp, bfd et hsrp pour exécuter des modèles de pré-vérification et de post-vérification dans les périphériques Nexus.

3. Cliquez sur Create. Un résumé des champs s'affiche.



The screenshot shows the 'Summary' window for a 'Single step upgrade' policy. The 'Name' is 'Single step upgrade' and the 'Description' is 'This upgrade policy for ansible'. The 'Max Batch Count' is 5. The 'Default Policy' is 'No'. The 'Ansible' checkbox is checked. The 'NCS-540' checkbox is also checked. The 'Planning' tab is selected, and the 'Backup Details' dropdown is visible. A 'Submit' button is at the bottom right.

Résumé - Politique de mise à niveau en une étape



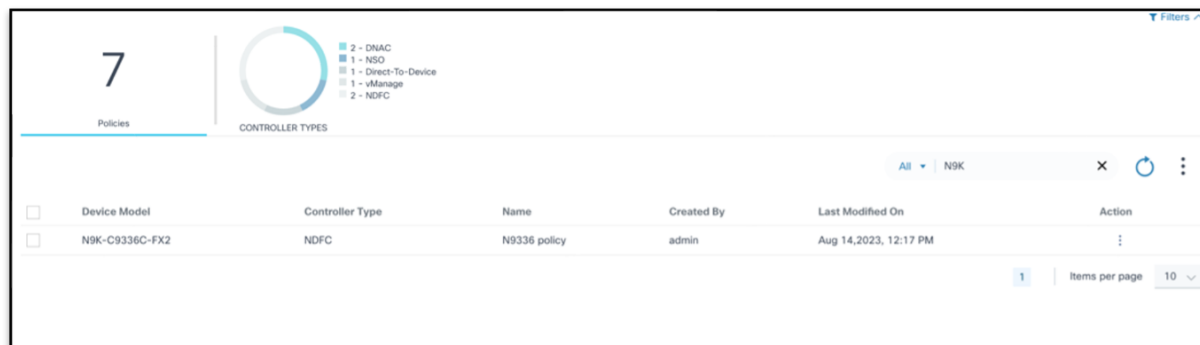
The screenshot shows the 'Summary' window for a 'Multi step upgrade' policy. The 'Name' is 'Multi step upgrade' and the 'Description' is 'This upgrade policy for ansible'. The 'Max Batch Count' is 5. The 'Default Policy' is 'No'. The 'Ansible' checkbox is checked. The 'NCS-540' checkbox is also checked. The 'Planning' tab is selected, and the 'Backup Details' and 'Upgrade Paths' dropdowns are visible. A 'Submit' button is at the bottom right.

Résumé - Politique de mise à niveau en plusieurs étapes

4. Vérifiez le résumé des champs et cliquez sur Submit. Une notification de progression s'affiche, suivie d'un message de confirmation. Les stratégies sont visibles sur la page dès leur création.

Des politiques de mise à niveau supplémentaires pour d'autres modèles de périphériques peuvent être créées si nécessaire.

Modification des stratégies de mise à niveau



7 Policies

CONTROLLER TYPES

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

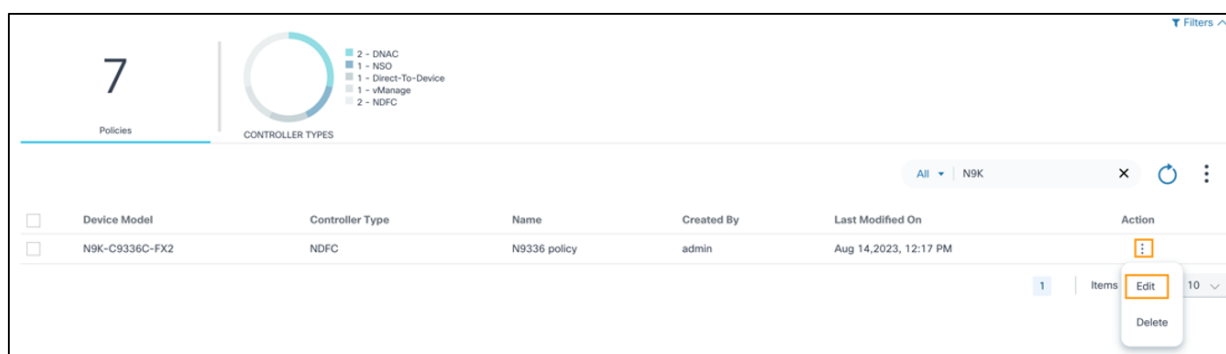
All N9K

☐	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

Résultat de la recherche de stratégie de mise à niveau

1. Dans la page Upgrade Policy, recherchez la stratégie souhaitée à l'aide du champ Search.



7 Policies

CONTROLLER TYPES

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

All N9K

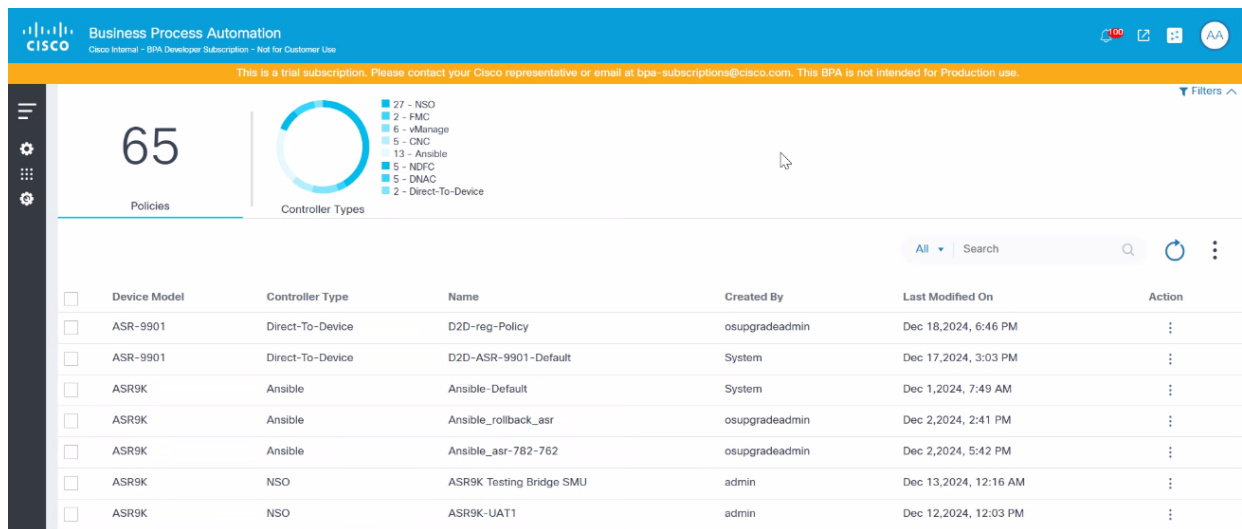
☐	Device Model	Controller Type	Name	Created By	Last Modified On	Action
☐	N9K-C9336C-FX2	NDFC	N9336 policy	admin	Aug 14, 2023, 12:17 PM	⋮ Edit Delete

1 Items per page 10

Modifier la stratégie de mise à niveau

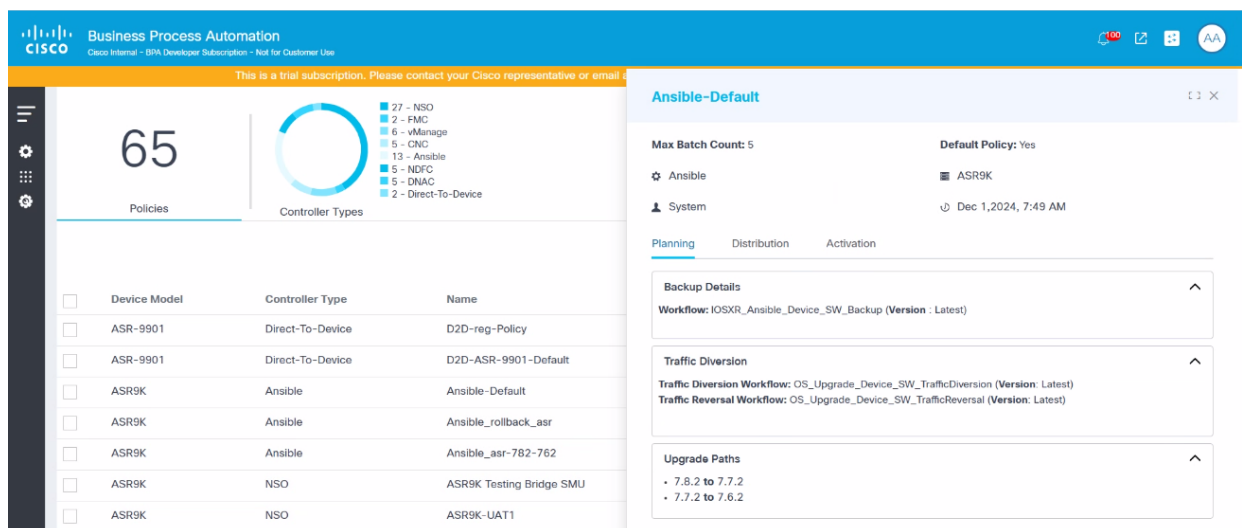
2. Dans la colonne Action de la stratégie, sélectionnez l'icône Autres options > Modifier.
3. Mettez à jour les champs appropriés et cliquez sur Update. Un résumé des modifications s'affiche.
4. Vérifiez le résumé des modifications et cliquez sur Submit. Les notifications de progression s'affichent, suivies d'un message de confirmation.

Affichage des stratégies de mise à niveau



Politique de mise à niveau

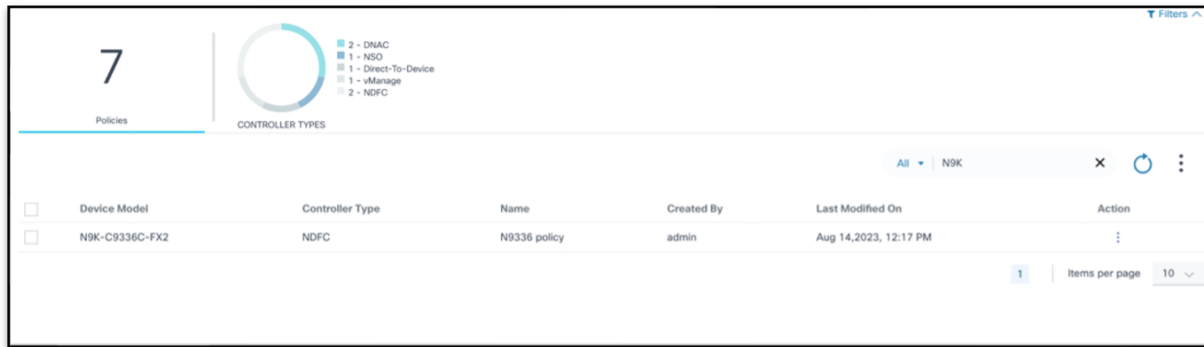
1. Dans la page Stratégie de mise à niveau, sélectionnez la ligne de la stratégie de mise à niveau souhaitée. La vue détaillée de la stratégie s'ouvre.



Vue détaillée des stratégies de mise à niveau

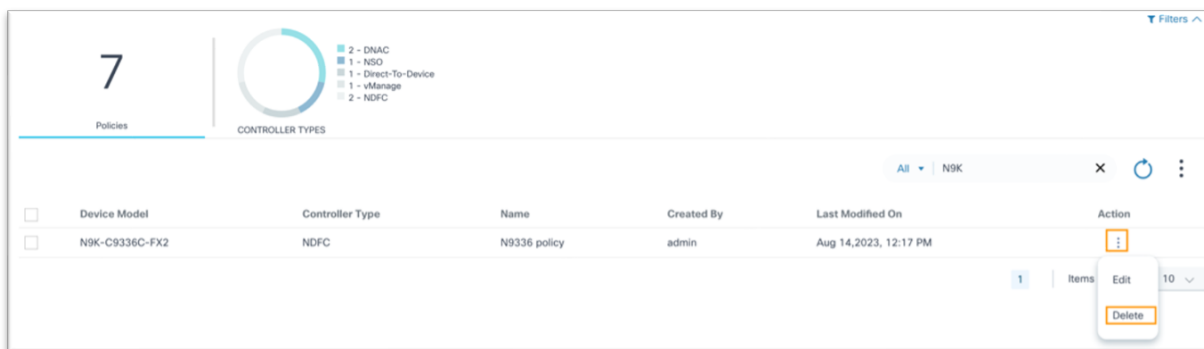
Suppression des stratégies de mise à niveau

 **Remarque :** Les stratégies par défaut ne peuvent pas être supprimées, mais les utilisateurs peuvent modifier les modèles de processus et les workflows.



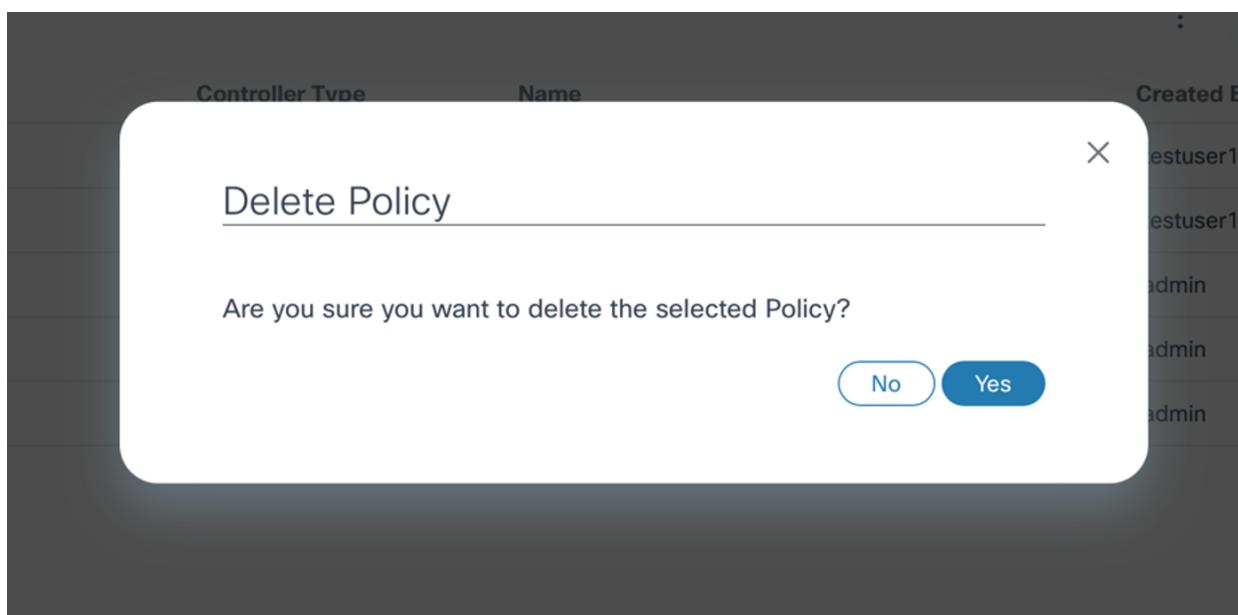
Politique de mise à niveau

1. Dans la page Upgrade Policies, localisez la stratégie souhaitée à l'aide du champ Search**.



Supprimer la stratégie de mise à niveau

2. Dans la colonne Action de la stratégie, sélectionnez Autres options > Supprimer. Une fenêtre de confirmation s'ouvre



Confirmation de suppression

3. Cliquez sur Yes.

Contrôle de l'accès aux stratégies de mise à niveau

Cette fonctionnalité permet de contrôler l'accès aux stratégies de mise à niveau, ce qui empêche les utilisateurs non autorisés de mettre à jour les stratégies définies dans l'application Mise à niveau du système d'exploitation. Les administrateurs peuvent restreindre l'accès en définissant un groupe de ressources avec des stratégies accessibles.

Pour créer un groupe de ressources :

1. Accédez à Paramètres > Groupes de ressources.
2. Créez un groupe de ressources avec des stratégies auxquelles les utilisateurs non administrateurs peuvent accéder. Les utilisateurs non administrateurs appartenant à ce groupe d'utilisateurs ont désormais uniquement accès aux stratégies disponibles dans ce groupe de ressources.
3. Créez une stratégie d'accès pour associer le groupe de ressources à un groupe d'utilisateurs.

Référez-vous à [Contrôle d'accès](#) pour plus d'informations.



Remarque : Il convient de noter ce qui suit.

- Les utilisateurs peuvent sélectionner les flux de travail incorrects pour la distribution et l'activation, ce qui entraîne un comportement involontaire. Il incombe à l'utilisateur de mapper correctement le workflow et de vérifier l'applicabilité des jalons tels que la distribution, l'activation, la restauration et les modèles de périphériques.
- Les flux de travail et les modèles de processus doivent être mappés avec la balise de nouvelle génération Mise à niveau du système d'exploitation pour pouvoir être sélectionnés lors de la création ou de la mise à jour des stratégies.
- Les stratégies OOB par défaut créées par l'utilisateur système ne peuvent pas être supprimées, mais les utilisateurs peuvent modifier les modèles de processus et les flux de travail.

Tâches de mise à niveau

Les mises à niveau logicielles sont gérées à l'aide de l'application Travail de mise à niveau, qui est composée d'un ou de plusieurs lots, chaque lot comportant un ou plusieurs périphériques réseau. Une tâche peut être créée en mode brouillon et enregistrée plusieurs fois. Les mises à niveau ne peuvent commencer qu'une fois le travail validé, ce qui permet aux opérateurs de planifier les

modifications à l'avance.

Conditions préalables

- Fenêtre Maintenance réservée pour les mises à niveau
- Pré-approbations pour demande de modification de mise à niveau
- Le service de sauvegarde et de restauration de la configuration doit être actif et opérationnel
- Le service de planification doit être opérationnel
- Les adaptateurs BPA pour les systèmes externes (par exemple, un système de billetterie), le cas échéant, doivent être intégrés

Affichage et gestion des travaux de mise à niveau

1. Connectez-vous à BPA avec des informations d'identification ayant accès aux travaux de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.



Tâche de mise à niveau

La page Travail de mise à niveau contient les éléments suivants :

 Remarque : Par défaut, dix tâches s'affichent. Les numéros de page peuvent être utilisés pour accéder à d'autres pages de travail.

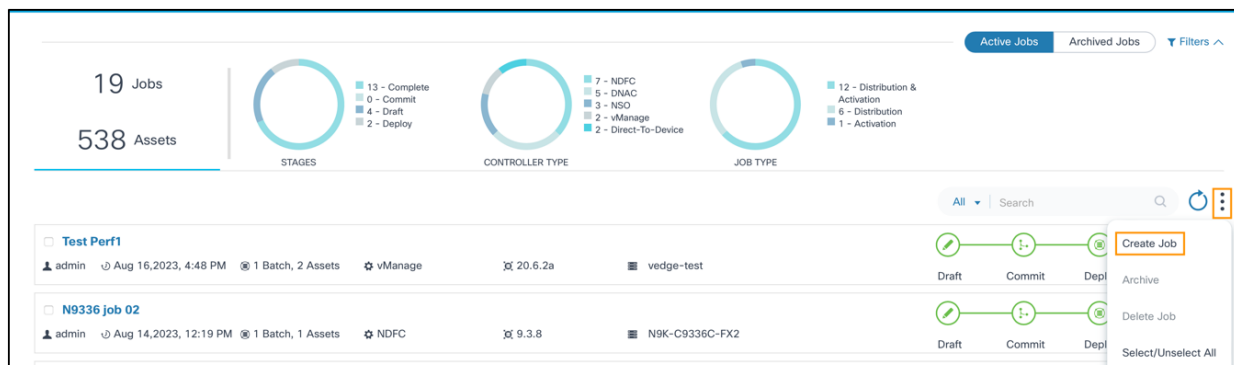
- Une bascule Tâches actives et Tâches archivées qui peut être utilisée pour basculer entre les tâches actives et archivées
- Une section d'analyse, affichée en haut, qui fournit les informations suivantes :

- Total des tâches et des actifs associés aux tâches
- Graphique des étapes avec les filtres suivants :
 - Brouillon : Le travail est en phase de rédaction et n'est pas encore validé
 - Valider : Le travail est validé avec tous les périphériques, lots ou plannings nécessaires jusqu'à ce que le planning soit atteint
 - Déploiement: L'activité de mise à niveau a démarré pour un ou plusieurs lots
 - Terminé : La mise à niveau est terminée pour tous les périphériques appartenant à tous les lots
- Graphique Type de contrôleur : Filtrage des tâches par type de contrôleur Cisco Catalyst Center, vManage, NSO, NDFC, Direct-to-Device, CNC, ANSIBLE et FMC
- Graphique Types de travaux avec les filtres suivants :
 - Distribution : Tâches qui effectuent le transfert ou la copie d'images d'un contrôleur vers des périphériques
 - Activation : Tâches qui effectuent l'activation ou la mise à niveau du logiciel d'un périphérique
 - Distribution et activation : Tâches qui effectuent à la fois le transfert ou la copie et l'activation ou la mise à niveau du logiciel d'un périphérique
- Le champ Rechercher qui peut être utilisé pour effectuer une recherche générique sur toutes les métadonnées ou par les champs Nom du travail et Créé par
- L'icône Actualiser qui peut être utilisée pour actualiser le résumé du travail et effacer les filtres de graphique ou toute recherche personnalisée dans le champ Rechercher
- L'icône Plus d'options qui fournit des options pour Créer un nouveau travail de mise à niveau et pour Archiver ou Supprimer les travaux sélectionnés ; Les utilisateurs peuvent sélectionner ou désélectionner Tout
- Les tâches s'affichent sous forme de panneaux et fournissent un aperçu rapide des informations suivantes :
 - L'icône Tâche utilisateur s'affiche avec le nombre de tâches utilisateur si des tâches utilisateur sont disponibles
 - L'utilisateur qui a créé le travail
 - Date de création de la tâche
 - Nombre de lots et d'immobilisations
 - Le type de contrôleur (par exemple, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, ANSIBLE ou FMC)
 - La version cible
 - Le modèle de périphérique applicable
 - Une vue jalon des étapes du travail (c'est-à-dire Brouillon, Valider, Déployer et Terminer) avec une légende de couleur pour chaque jalon :
 - Gris : Le jalon n'a pas commencé
 - Bleu : L'étape est en cours
 - Rouge : Problème majeur
 - Vert: Jalon terminé
 - Une légende de couleur à la fin des jalons qui affiche le statut de la tâche :

- Vert: Le travail est terminé
- Rouge : Le travail présente des problèmes
- Bleu : La tâche est en cours

Planification des travaux de mise à niveau

Pour créer une tâche :



Créer une option de travail de mise à niveau

1. Sur la page Mettre à niveau le travail, sélectionnez l'icône Autres options > Créer un travail. La page Créer un travail de mise à niveau s'affiche.

Créer un travail de mise à niveau

2. Saisissez un nom de tâche dans le champ Nom.
3. Sélectionnez le type de contrôleur (par exemple, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE ou NSO).
4. Sélectionnez une politique de conformité comportant des périphériques non conformes.

 Remarque : Seules les politiques de conformité qui sont exécutées au moins une fois et ont au moins un dispositif non conforme sont disponibles dans la liste, identifiant automatiquement la politique de mise à niveau applicable à utiliser une fois qu'une politique est sélectionnée.

Les détails suivants s'affichent sur le côté gauche du formulaire Créer un travail sous Résumé du travail :

- Modèle(s) de périphérique affecté(s)



Remarque : Plusieurs modèles de périphériques sont affichés lorsque la stratégie de conformité sélectionnée comporte plusieurs modèles de périphériques associés.

- Version cible
- Agrégation des versions existantes et de leur nombre correspondant
- Nombre maximal de lots autorisé
- Nombre total d'actifs non conformes



Remarque : Si la stratégie de conformité sélectionnée est associée à plusieurs modèles de périphériques, elle affiche l'ensemble des actifs non conformes pour tous les modèles associés.

- Option d'ajout de lot

5. Sélectionnez l'un des types de travaux de mise à niveau suivants :

- Distribution : Les tâches de distribution uniquement sont utiles lorsque la préparation de l'image logicielle se produit avant l'activation réelle
- Activation : Les tâches d'activation uniquement sont utiles pour effectuer les mises à niveau des périphériques pour lesquels la distribution est déjà effectuée via une tâche de distribution uniquement
- Distribution et activation : La distribution ou la préparation et l'activation des images se font au sein du même travail, ce qui est utile dans les scénarios où une fenêtre de maintenance étendue est disponible pour couvrir à la fois la copie d'images sur un périphérique et la mise à niveau

6. Sélectionnez la commande de mise à niveau. Plusieurs périphériques sont traités en même temps en mode parallèle tandis que les périphériques sont traités un par un en mode séquentiel.



Remarque : Le nombre maximal de périphériques pouvant être traités en mode parallèle dépend de la configuration du déploiement. L'ordre de mise à niveau sélectionné s'applique à l'ensemble du travail, mais peut être remplacé dans un lot particulier en fonction des besoins.

7. Ajoutez le numéro de demande de modification dans le champ Numéro de ticket ITSM (IT Service Management).
8. Sélectionnez le nom de la stratégie de mise à niveau. Seules les stratégies de mise à niveau applicables s'affichent en fonction du type de contrôleur et du modèle de périphérique de stratégie de conformité ; les utilisateurs peuvent sélectionner l'une des stratégies de mise à niveau. Si plusieurs modèles sont associés à la stratégie de conformité logicielle, toutes les stratégies de mise à niveau associées à chaque modèle sont affichées. Les utilisateurs doivent sélectionner avec soin la stratégie de mise à niveau qui fonctionne pour tous les modèles.
9. Sélectionnez le serveur d'images logicielles pour spécifier le référentiel d'images vManage (par exemple, local ou distant) à utiliser.



Remarque : Cette entrée s'applique uniquement au type de contrôleur vManage.

The screenshot shows the Cisco Business Process Automation (BPA) interface for configuring a vManage Job. The sidebar on the left includes a 'Job Summary' section with 'c8000v' as the target version and '17.09.03a.0.15' as the existing release. The main form contains the following fields:

- Name ***: vManage Job
- Controller Type ***: vManage
- Conformance Policy ***: vmanage c8000v policy
- Job Type ***: Distribution & Activation
- Deployment Order ***: Parallel
- ITSM Ticket Number**: Enter ITSM Ticket Number
- Upgrade Policy Name ***: vManage-Default
- Software Image Server**: vmanage-r3

The 'Add New Batch' button is located at the bottom right of the form.

Créer un travail de mise à niveau avec des détails remplis (la stratégie de conformité a un modèle)

The screenshot shows the Cisco Business Process Automation (BPA) interface for configuring a vManage Job. The sidebar on the left includes a 'Job Summary' section with 'N9K-C93...N9K-C93...' as the target version and '10.2.5' as the existing release. The main form contains the following fields:

- Name ***: test
- Controller Type ***: NDFC
- Conformance Policy ***: policy-demo
- Job Type ***: Distribution & Activation
- Deployment Order ***: Parallel
- ITSM Ticket Number**: Enter ITSM Ticket Number
- Upgrade Policy Name ***: NDFC-Default

The 'Add New Batch' button is located at the bottom right of the form.

Créer un travail de mise à niveau avec des détails remplis (la stratégie de conformité a plusieurs modèles)

10. Cliquez sur Save Job pour enregistrer le brouillon jusqu'à ce que le travail soit prêt à être validé.

All > vManage Job Save Job Commit Job

Job Summary

c8000v

Target Version : 17.09.03.0.15

Existing Release
17.06.03a.0.3 [6]

Batches (Max Limit : 5)

[Add Batch](#)

6 Assets Pending

Name *
vManage Job ✓

Job Type *
Distribution & Activation ✓ ✓

Upgrade Policy Name *
vManage-Default ✓

Controller Type *
vManage ✓ ✓

Deployment Order *
Parallel ✓ ✓

Software Image Server
vManage-r3 ✓ ✓

Conformance Policy *
vmanage sw conformance

ITSM Ticket Number
Enter ITSM Ticket Number

To get started Add New Batch

Ajouter un lot et Ajouter un nouveau lot

- Pour ajouter un lot, cliquez sur le lien Ajouter un lot ou sur Ajouter un nouveau lot. La fenêtre Création de lot s'ouvre.

CISCO 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 : 17.09.03.0.15

Existing Release
17.06.03a.0.3 [3] | 17.09.03a.0.6476 [1]

Batches (Max Limit : 5)

[Add Batch](#)

4 Assets Pending

Batch Name *
Enter Batch Name

Deployment Order
Parallel

Software Image Server
vmanage-r3

Select Assets Upload Assets Add Asset

☐ Distribute Now & Activate Later

August 2024

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Start Time: Image Distribution & Activation

Création de lots

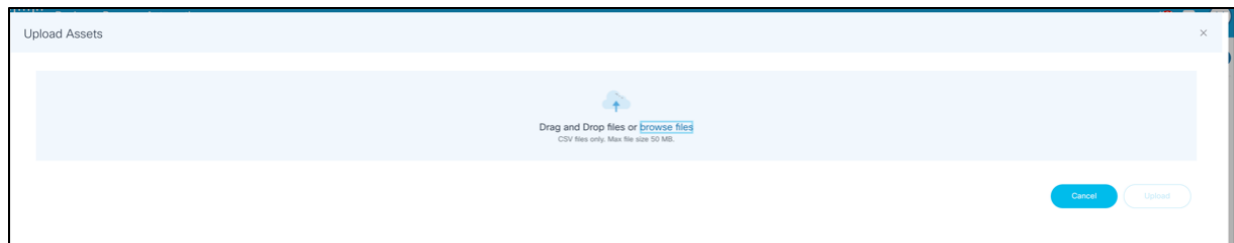
- Saisissez un nom de lot approprié et sélectionnez l'ordre de déploiement.

 Remarque : Le type de mise à niveau sélectionné ici est prioritaire sur celui sélectionné sur la page Création de tâche

- Sélectionnez le serveur d'images logicielles pour spécifier le référentiel vManage (par exemple, local ou distant) à utiliser.

 Remarque : Ce champ s'applique uniquement au type de contrôleur vManage. Le serveur d'images logicielles sélectionné ici est prioritaire sur celui sélectionné sur la page Création de tâche

14. Ajoutez des immobilisations aux lots. Les immobilisations peuvent être ajoutées aux lots de deux manières :



Télécharger des ressources

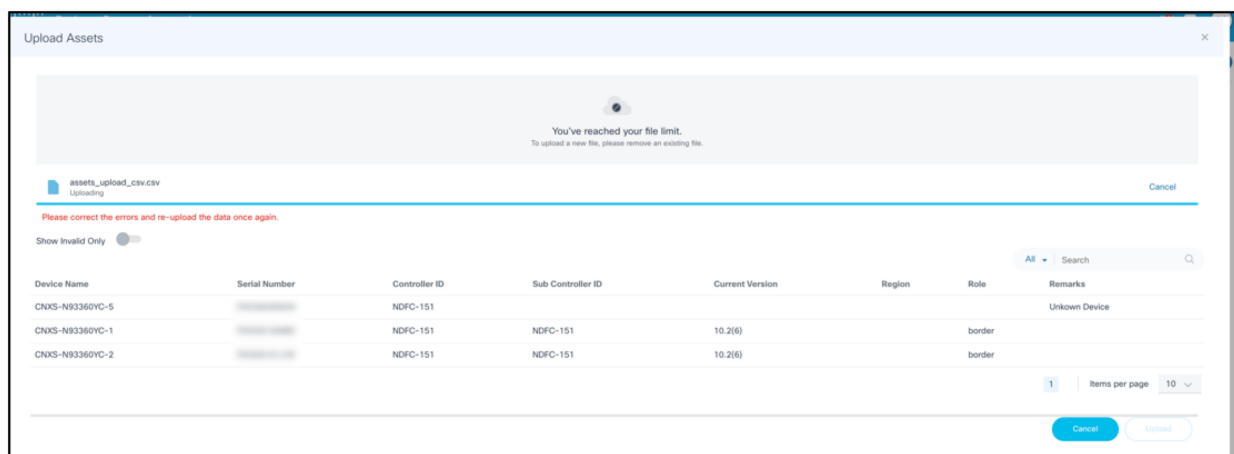
Option 1 :

- Cliquez sur Upload Assets. La fenêtre Charger des immobilisations s'affiche.
- Sélectionnez un fichier .csv à télécharger.



Remarque : Le fichier .csv doit comporter les informations suivantes :

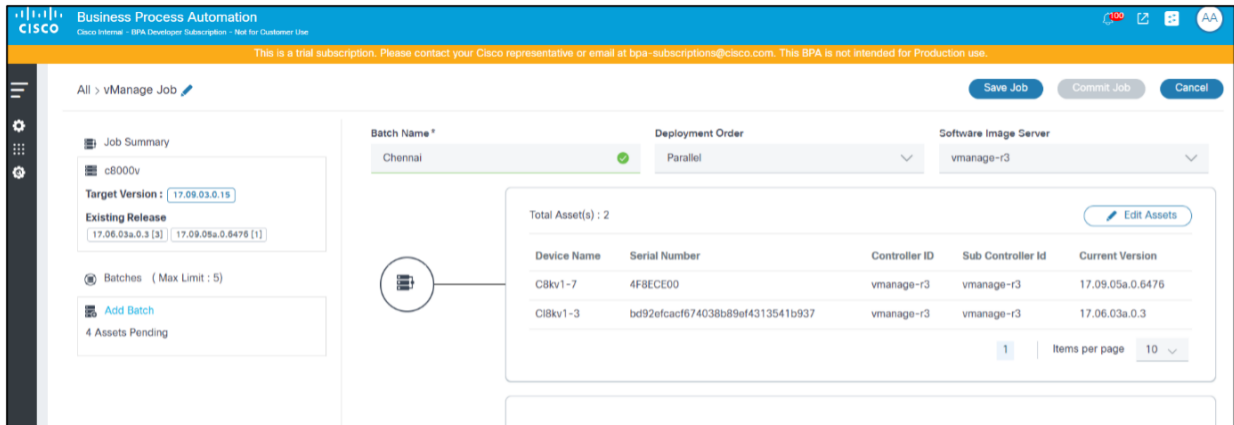
- Nom du périphérique: Nom du périphérique ou de la ressource
 - Numéro de série: Numéro de série du périphérique
 - ID du contrôleur : Nom du contrôleur qui gère le périphérique
 - ID du sous-contrôleur : Nom de l'ID du sous-contrôleur gérant le périphérique
- c. Cliquez sur Upload (charger). Les données du fichier .csv sont validées et les données valides et non valides s'affichent. L'option Show Invalid Only peut être utilisée pour filtrer les périphériques non valides à partir des détails des ressources téléchargées.



Exemples de ressources téléchargées via un fichier CSV

- Si le fichier téléchargé contient des erreurs, corrigez-les et téléchargez-le à nouveau.

 Remarque : Les utilisateurs peuvent uniquement poursuivre la sélection des ressources si tous les périphériques téléchargés sont valides.



Ajouter un lot - Ressources sélectionnées

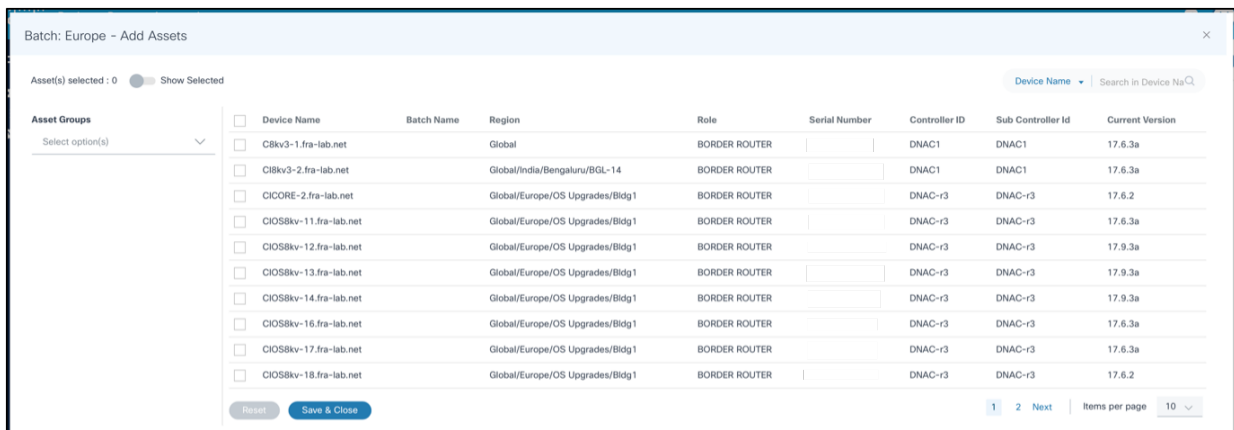
Option 2 :

a. Cliquez sur Ajouter des ressources. La fenêtre Sélection des équipements s'ouvre.

 Remarque : Télécharger des ressources et Ajouter des ressources ne peuvent pas être utilisés simultanément.

b. Pour le type de contrôleur FMC uniquement, sélectionnez le noeud de contrôle ou le noeud autonome pour effectuer la mise à niveau.

 Remarque : Les périphériques de données ne sont pas autorisés dans le travail de mise à niveau car la mise à niveau des noeuds de données est gérée par son noeud de contrôle.



Sélection du périphérique

c. Sélectionnez le ou les périphériques appropriés à inclure dans le lot en cours.

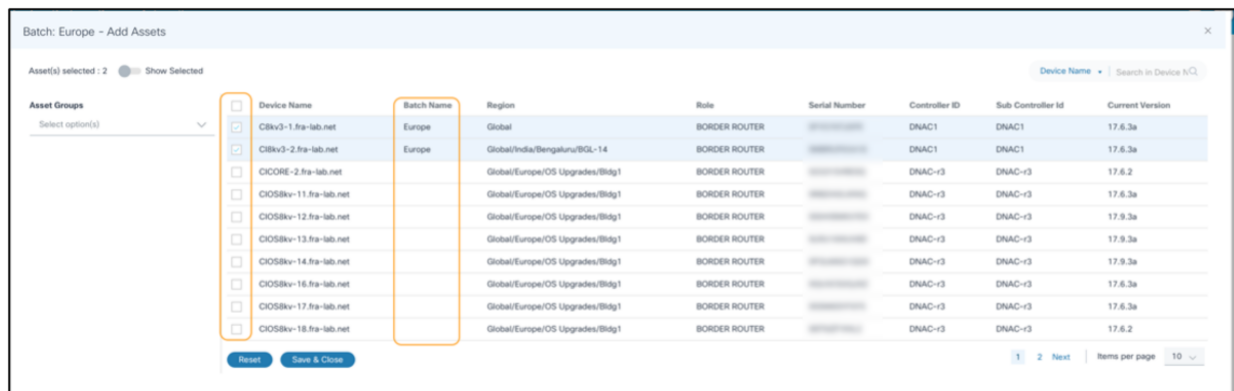
Le filtre Rechercher peut être utilisé pour filtrer les périphériques en fonction de différents attributs et tous les périphériques correspondant aux critères de filtrage peuvent être sélectionnés en bloc en cochant la case dans l'en-tête de la colonne Nom du périphérique. Les utilisateurs ont également la possibilité de filtrer par groupes d'actifs.

L'option Afficher la sélection peut être activée pour afficher uniquement les ressources sélectionnées.

 Remarque : Lorsque la bascule Afficher la sélection est activée, le filtre Groupes d'actifs est désactivé.

d. Cliquez sur Enregistrer et fermer.

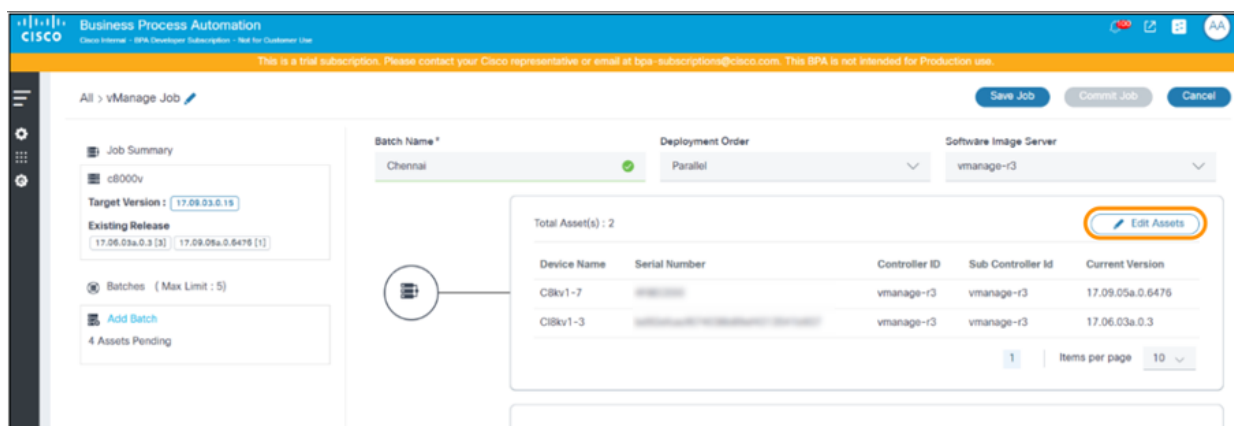
Cliquez sur Réinitialiser pour annuler les sélections et conserver l'état d'origine de la sélection d'actifs.



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

reset

e. Si la sélection d'actifs doit être modifiée, cliquez sur Modifier les actifs.



Business Process Automation

Job Summary

Target Version: 17.09.03.0.19

Existing Release: 17.06.03a.0.3 [3] 17.09.06a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

4 Assets Pending

Batch Name: Chennai

Deployment Order: Parallel

Software Image Server: vmanage-r3

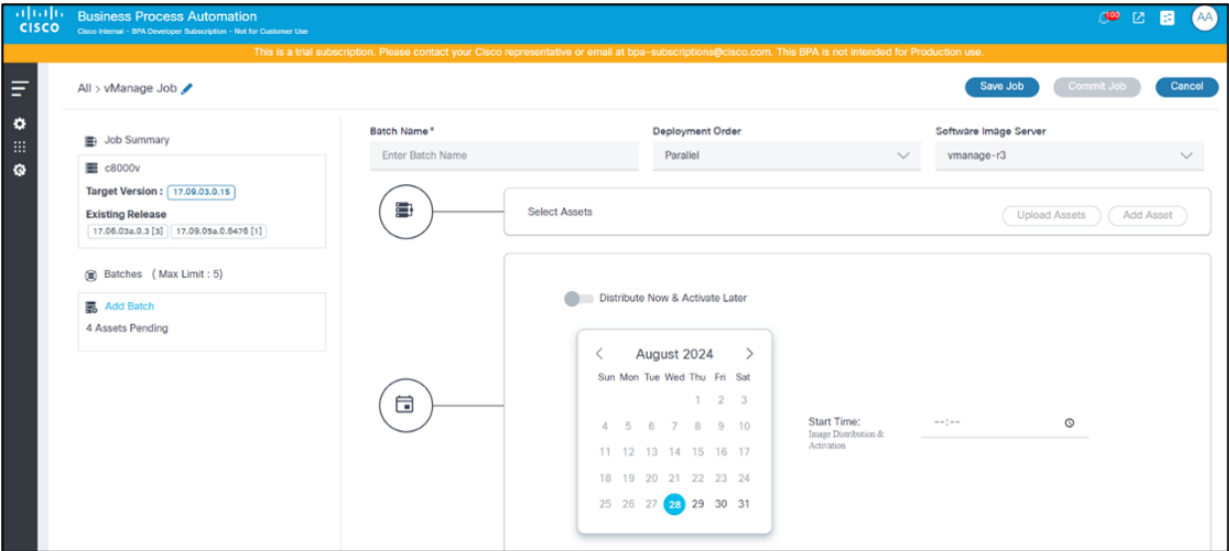
Total Asset(s): 2

Edit Assets

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

Modifier les ressources par lots

- f. Sélectionnez ou effacez les ressources pour effectuer les modifications nécessaires et cliquez sur Enregistrer et fermer. Lors de la modification des actifs du lot, les actifs actuellement sélectionnés qui font partie d'un ordre de fabrication et d'un lot différents peuvent être identifiés à l'aide de coches et le nom du lot s'affiche dans la colonne Nom du lot.



Planificateur de travaux de mise à niveau

15. Sélectionnez une date dans le sélecteur de dates et une heure dans le sélecteur de temps pour planifier une heure de déclenchement du type de mise à niveau sélectionné pour le lot actuel.

 Remarque : Le type de tâche sélectionné change le type de plannings disponibles.

Les scénarios possibles sont les suivants :

Type de tâche	Bascule Distribuer maintenant	Date et heure de planification	Détails de distribution
Distribution	Désactivé par défaut	Actif	La distribution a lieu à la date et à l'heure planifiées spécifiées
Distribution	Activée	Désactivé	La distribution a lieu après validation du travail
Activation	S/O	Actif	L'activation a lieu à la date et à l'heure

Type de tâche	Bascule Distribuer maintenant	Date et heure de planification	Détails de distribution spécifiées
Distribution et activation	Désactivé par défaut	Actif	La distribution et l'activation ont lieu à la date et à l'heure spécifiées
Distribution et activation	Activée	Actif	La distribution a lieu après la validation du travail et les déclencheurs d'activation à la date et l'heure planifiées spécifiées

Options de planification du type de tâche de distribution

Options de planification du type de tâche Activation

☒ Distribute Now & Activate Later

< August 2023 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Start Time: Image Distribution & Activation 13:10 ✓

Create Batch

Options de planification du type de tâche Distribution et activation

CISCO Business Process Automation

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

All > vManage Upgrade

Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.06.02.0.2788

Existing Release: 17.06.03a.0.2 [2] 17.09.03.0.15 [2] 17.09.05a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name* Enter Batch Name

Deployment Order Parallel

Software Image Server Select option

Select Assets

Upload Assets Add Asset

☒ Distribute Now & Activate Later

< September 2024 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Start Time: Image Activation 13:10

Create Batch

Options de planification des types de tâche de distribution et d'activation avec l'option Distribuer maintenant et activer plus tard activée

Remarque : La liste suivante doit être notée.

- Lorsque vous planifiez plusieurs lots, prévoyez un intervalle de temps entre les deux lots afin d'éviter une surcharge du système. Si plusieurs lots se chevauchent, pensez à les ajouter à un seul lot.
- Lorsque l'option Distribuer maintenant et activer plus tard est activée, fournissez un intervalle de temps entre l'heure de validation du travail et la planification d'activation. Dans le cas contraire, les workflows d'activation peuvent créer des tâches utilisateur nécessitant une intervention manuelle (c'est-à-dire que les utilisateurs doivent attendre la fin de la distribution

et réessayer).

16. Cliquez sur Créer un lot. Le lot peut être affiché sur le côté gauche de la page.

The screenshot displays the Cisco Business Process Automation (BPA) interface. At the top, there's a header with the Cisco logo and a warning: "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." The main interface is divided into several sections. On the left, there's a sidebar with a menu. The central area is titled "All > vManage Job". It includes a "Job Summary" panel on the left with fields for "Job Name" (c8000v), "Target Version" (17.09.03.0.15), and "Existing Release" (17.08.03a.0.3 [3], 17.09.05a.0.6476 [1]). Below this is a "Batches" section with "Add Batch" and "4 Assets Pending". The main area shows a "Batch Name" (Chennai), "Deployment Order" (Parallel), and "Software Image Server" (vmanage-r3). A table lists assets: C8kv1-7 and C8kv1-3, both with version 17.09.05a.0.6476. A "Distribute Now & Activate Later" toggle is visible, and a calendar shows August 2024.

Créer un travail - Valider le travail

Créez autant de lots que nécessaire. Un travail peut être à l'état Brouillon jusqu'à ce que toutes les informations requises soient disponibles.

 Remarque : Pour éviter la perte de données de tâche, cliquez sur Save Job pour enregistrer le brouillon.

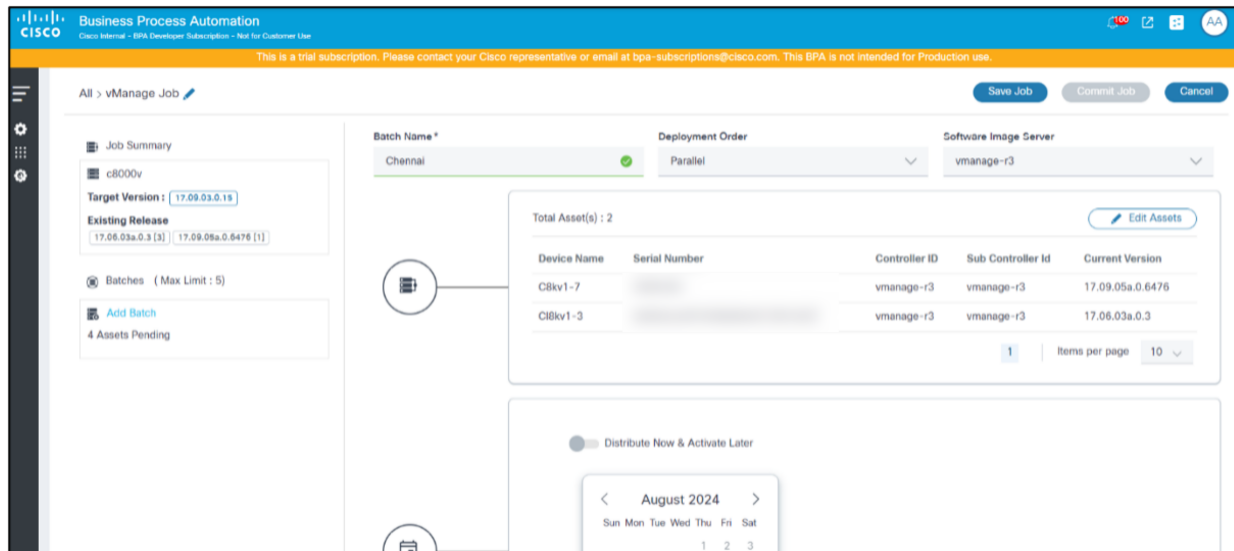
17. Cliquez sur Valider le travail pour finaliser la création du travail. Le travail passe à l'état Déployer lorsque la planification est déclenchée pour l'un des lots.

 Remarque : Le seuil du nombre maximal de lots peut être étendu ou mis à jour sur la page Stratégie de mise à niveau.

Modification d'un lot dans une tâche

 Remarque : Les lots ne peuvent être mis à jour que lorsque le travail est en phase Brouillon.

1. Sélectionnez le lot souhaité dans le panneau de gauche.



Modifier les ressources

2. Cliquez sur Modifier les ressources.
3. Apportez les modifications nécessaires en sélectionnant ou en effaçant des immobilisations dans Ajouter des immobilisations ou Charger des immobilisations ou en modifiant le programme de lots en modifiant la date ou l'heure de début.
4. Cliquez sur Mettre à jour le lot.

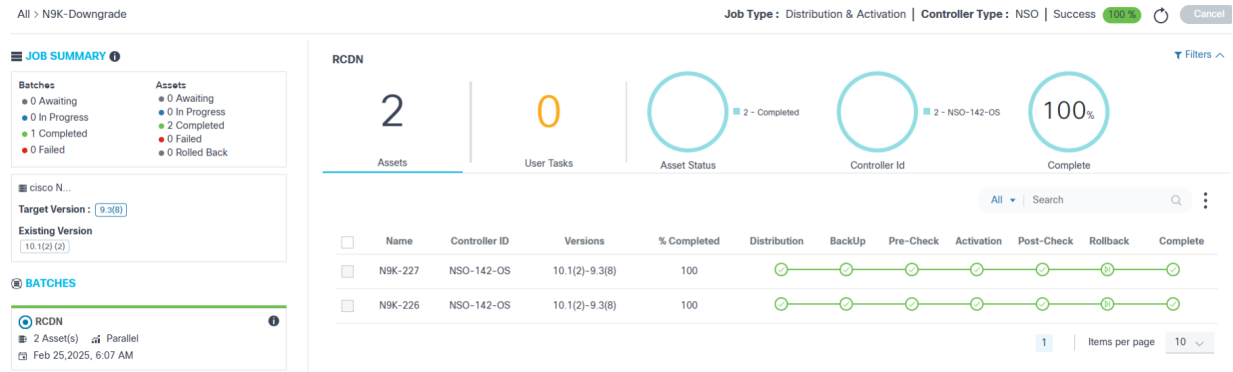
Exécution des tâches de mise à niveau et surveillance de la progression

1. Connectez-vous à BPA avec des informations d'identification ayant accès aux travaux de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.

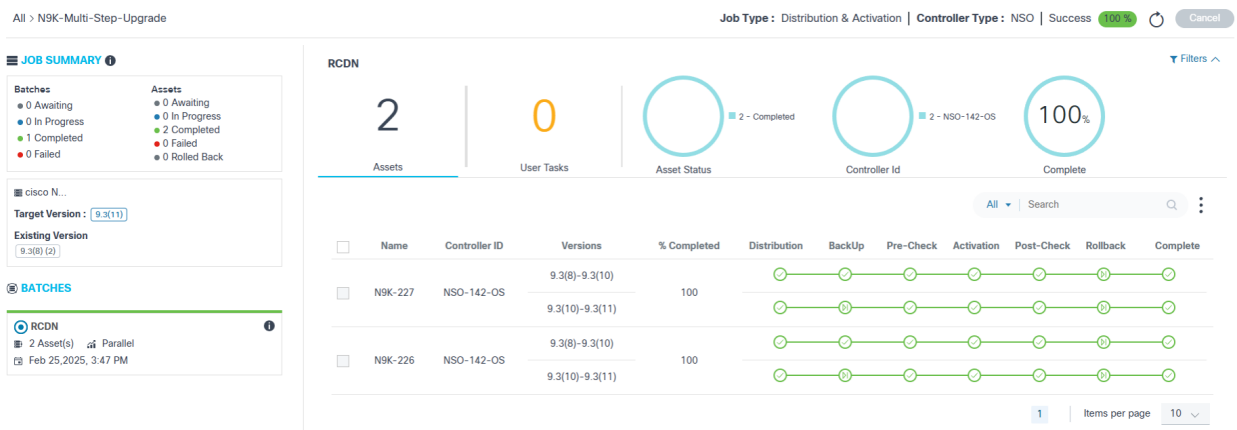


Tâche de mise à niveau

3. Utilisez le filtre Rechercher en combinaison avec les filtres de graphique disponibles pour filtrer rapidement la tâche.
4. Cliquez sur la tâche souhaitée. La page Récapitulatif des tâches s'affiche.



Mise à niveau pas à pas



Mise à niveau en plusieurs étapes

Le panneau de gauche fournit les informations suivantes :

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

Récapitulatif des tâches

- Synthèse rapide des lots et des immobilisations respectives

 c8000v

Target Version : 17.09.01a.0.240

Existing Version
17.09.03.0.15 (1)

Détails de la stratégie de conformité (si la stratégie a un modèle)

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

Target Version :

10.2.5

Existing Release

9.3(7) [4]

Détails de la stratégie de conformité (si la stratégie comporte plusieurs modèles)

- Le modèle de périphérique affecté par la tâche, la version du logiciel cible et la version existante
- Liste des lots faisant partie de cette tâche

BATCHES

chennai

1 Asset(s)

Parallel

Aug 14,2023, 12:20 PM

Détails du lot

- Détails du lot :
 - La bordure supérieure grise indique que le lot est en attente de planification
 - La bordure supérieure bleue indique que le déploiement par lots est en cours
 - La bordure supérieure verte indique que le déploiement par lots est terminé

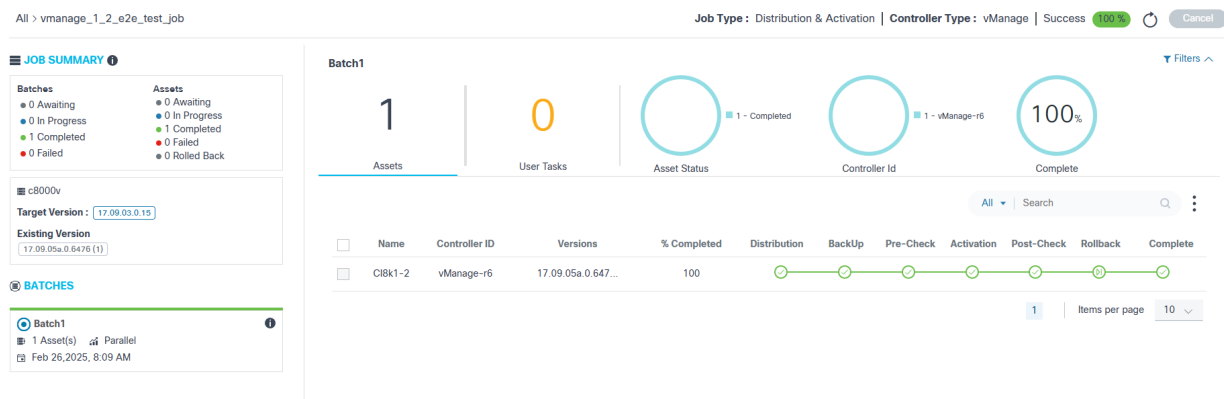
Les informations suivantes s'affichent en haut de la page Récapitulatif des tâches :

Résumé du haut de la tâche

- La navigation dans le plan du pain de la tâche en cours (par exemple, Tous > vmanage_1_2_e2e). L'option Tous bascule vers Tableau de bord des tâches
- Type de travail
- Le type de contrôleur
- Statut du travail avec pourcentage de réalisation :
 - Réussite : Le travail de mise à niveau a réussi
 - Échec : La mise à niveau a échoué pour une raison quelconque
 - En cours : Tâche de mise à niveau en cours

 Remarque : L'état du travail est déplacé vers En cours même si la planification d'un lot est atteinte

- En attente : Le travail est validé mais en attente d'un ou plusieurs planifications de lots



Récapitulatif des tâches

Les options suivantes sont disponibles sur la page Résumé du travail :

- L'icône Actualiser permet aux utilisateurs de récupérer des mises à jour à la demande
- Annuler permet d'annuler les tâches aux étapes Brouillon et Valider, sauf si la planification de l'un des lots est atteinte
- L'option Activer crée un travail d'activation à l'état Provisoire avec les lots et les immobilisations qui faisaient partie du travail précédemment terminé
 - L'activation est disponible uniquement si le type de travail est Distribution et s'il est terminé avec succès
 - Si le travail d'activation est déjà créé et que l'on clique sur Activate, un message s'affiche avec le statut du travail précédemment créé et fournit une option pour rediriger le travail déjà créé ; dans le travail nouvellement créé, les utilisateurs ont la possibilité de modifier ou de supprimer les lots ou les ressources, mais le type de travail, le type de contrôleur et la stratégie de conformité ne sont pas modifiables.
- Une liste paginée des ressources s'affiche sous la section Analytics
- Le champ Rechercher permet d'effectuer des recherches générales et spécifiques aux

champs pour des colonnes telles que :

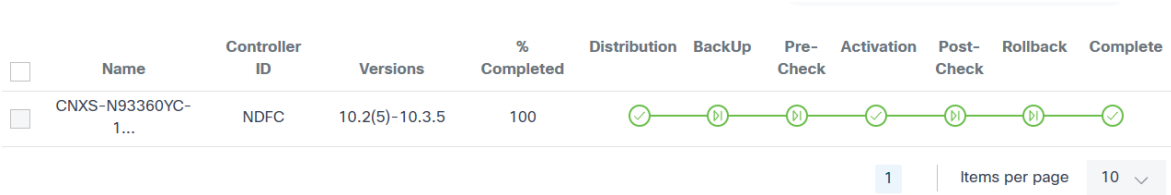
- Nom du périphérique
- ID contrôleur
- Numéro de série



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

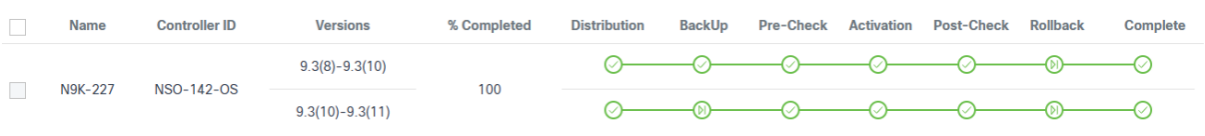
Télécharger le rapport par lots

- L'option de télécharger le rapport au niveau du lot en sélectionnant l'icône Plus d'options > Télécharger ; le rapport comprend les détails au niveau du lot et les détails sur le périphérique



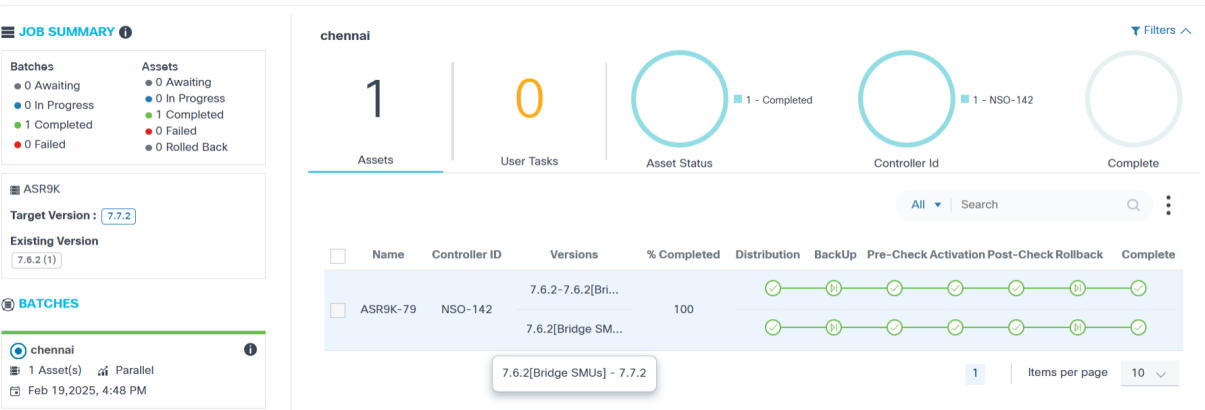
☐	Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
☐	CNXS-N93360YC-1...	NDFC	10.2(5)-10.3.5	100							

Trier - Mise à niveau en une étape



☐	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)								

Trier - Mise à niveau en plusieurs étapes



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

chennal

1 Asset(s) Parallel

Feb 19, 2025, 4:48 PM

chennal

1

Assets

0

User Tasks

1 - Completed

Asset Status

1 - NSO-142

Controller Id

Complete

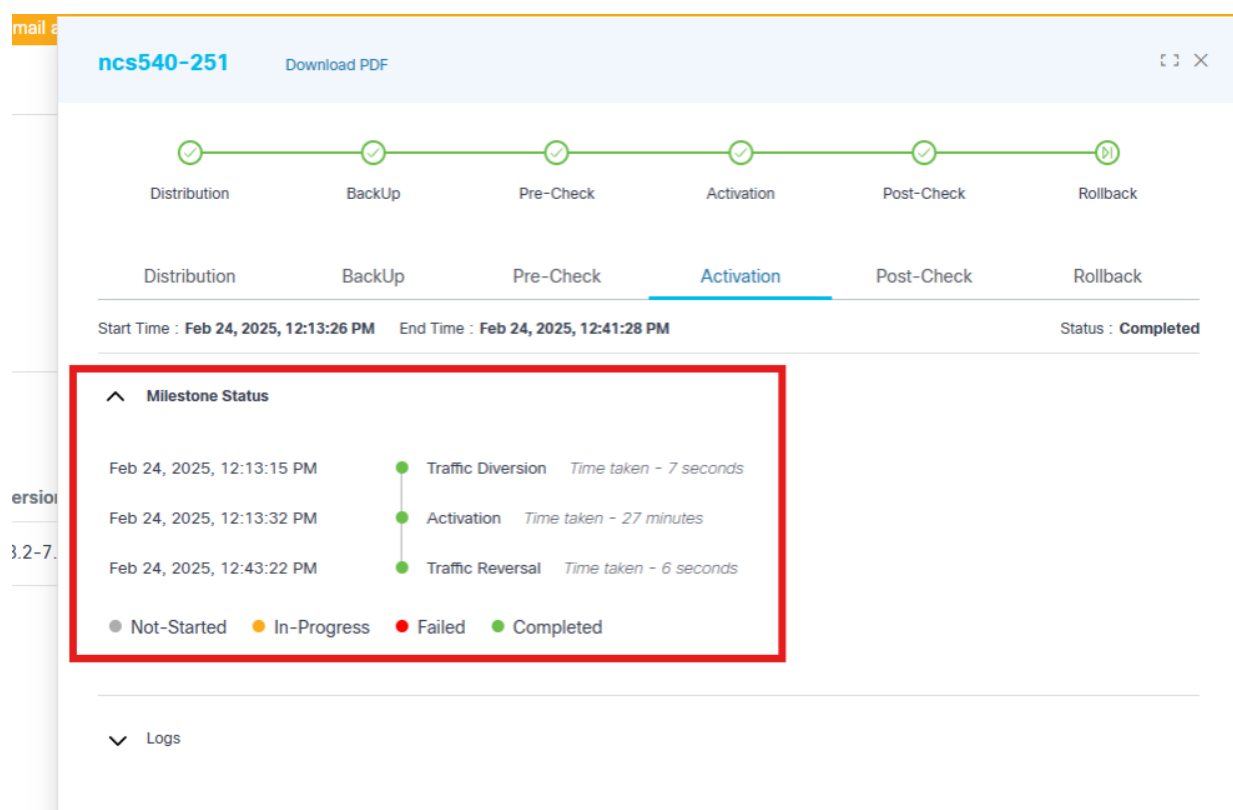
☐	Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
☐	ASR9K-79	NSO-142	7.6.2-7.6.2[Bri...]	100							
☐			7.6.2[Bridge SM...]								

Tri - Mise à niveau Bridge SMU

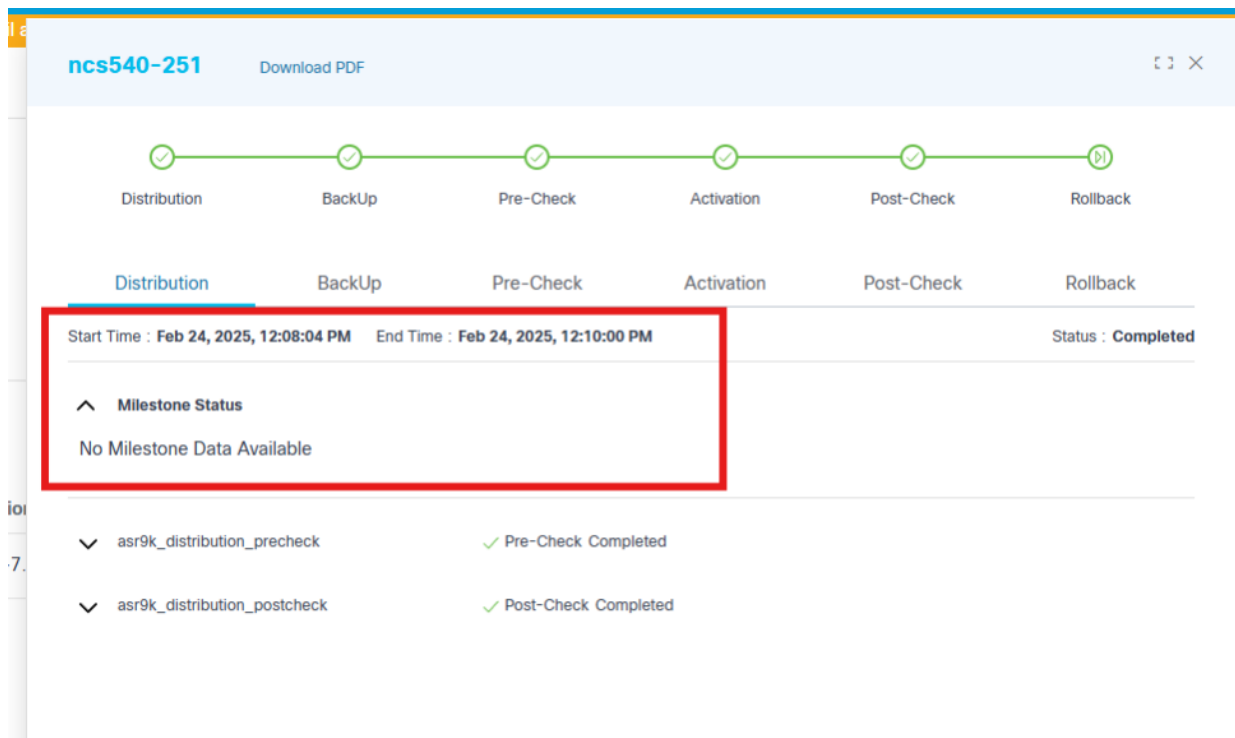
- Vous pouvez effectuer le tri en cliquant sur les noms des colonnes
- Les jalons de mise à niveau suivants sont affichés pour chaque périphérique avec Nom, ID de contrôleur, Versions et % Terminé :
 - Distribution
 - Sauvegarde
 - Contrôle Préalable
 - Dérivation Du Trafic
 - Activation
 - Contrôle A Posteriori
 - Inversion De Trafic
 - Restauration
 - Terminer

 Remarque : % terminé affiche la progression en fonction du nombre d'étapes terminées pour un périphérique. Tous les pourcentages de fin de traitement au niveau du périphérique dans un lot sont agrégés pour calculer le pourcentage de fin de traitement du lot. A son tour, tous les pourcentages de fin de traitement par lots sont consolidés pour calculer le pourcentage de fin de traitement au niveau OF.

Les sous-jalons, également appelés jalons personnalisés, sont les étapes intermédiaires importantes exécutées et affichées sous le jalon standard lorsqu'elles sont ajoutées. Pour plus d'informations sur l'ajout de jalons personnalisés, référez-vous au [Guide du développeur BPA](#).



Vue des sous-jalons (si des sous-jalons sont ajoutés sous un nom de jalon standard)



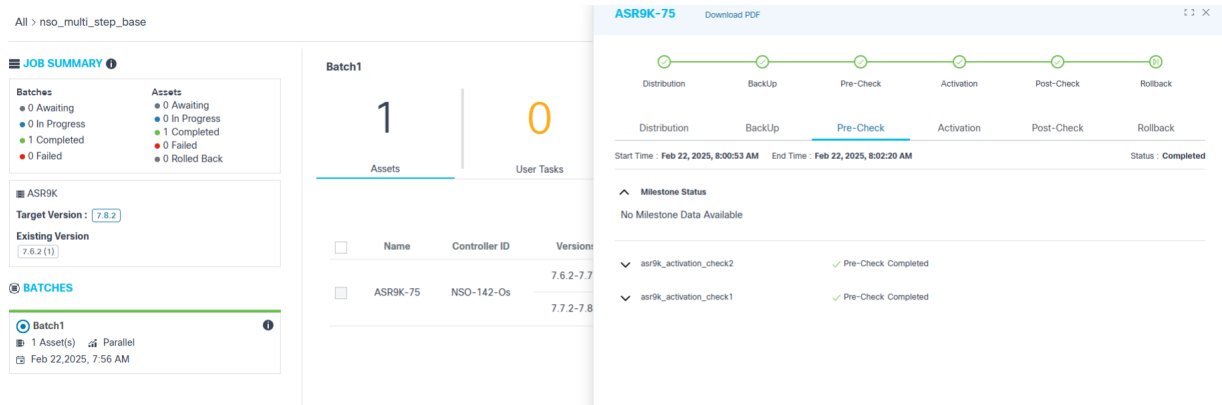
Vue des sous-jalons (si les sous-jalons ne sont pas ajoutés sous le nom de jalon standard)



Remarque : Les jalons varient en fonction du type de tâche sélectionné. Le jalon TrafficReversal n'est pas disponible pour les tâches de distribution.

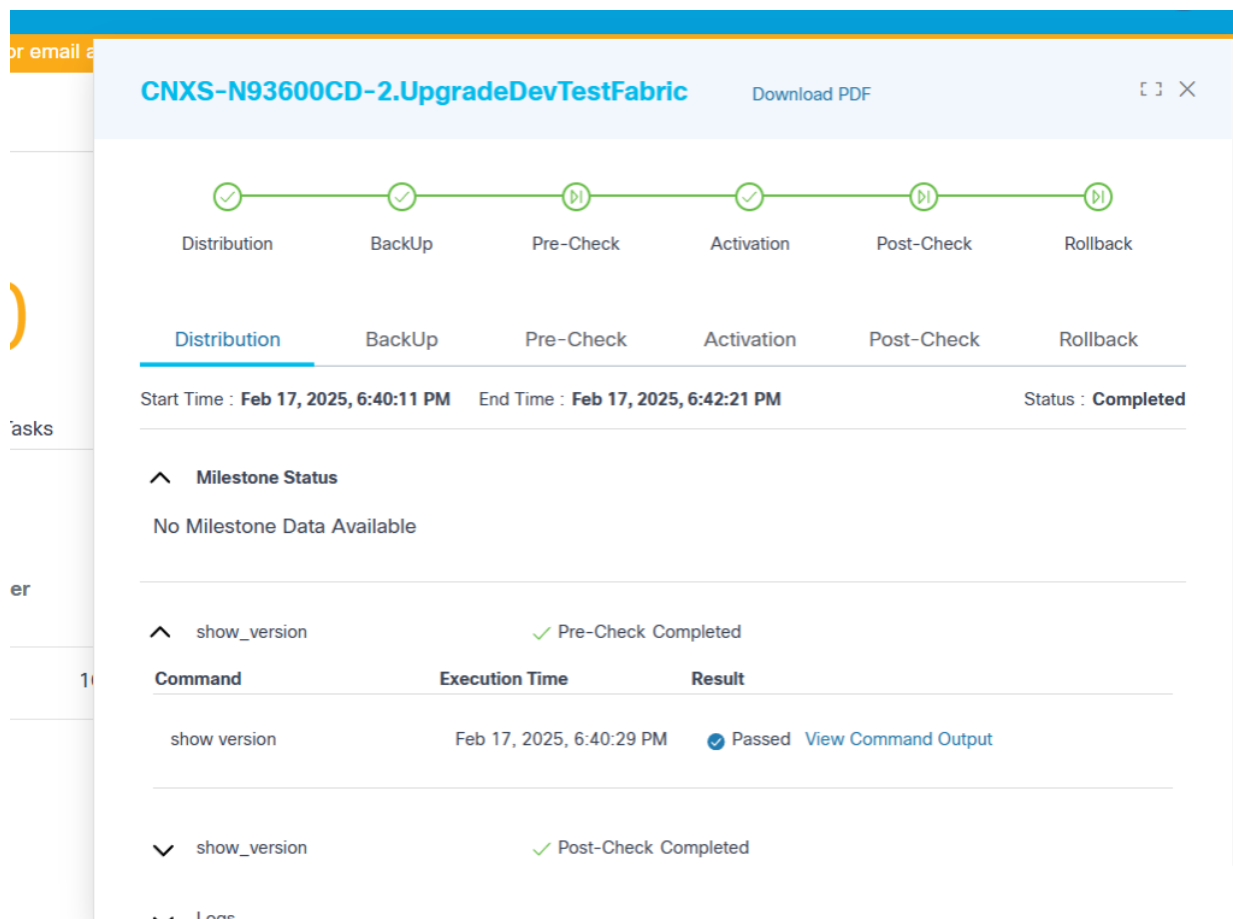
Le détournement et l'inversion du trafic sont déplacés sous le jalon d'activation.

- Une légende de couleur de jalon qui se compose des éléments suivants :
 - Coche grise : En attente
 - Vérification bleue : En cours
 - Indicateur vert : Ignoré
 - Coche verte : Terminé
 - Chèque orange : Tâche utilisateur
 - Vérification rouge : Échec



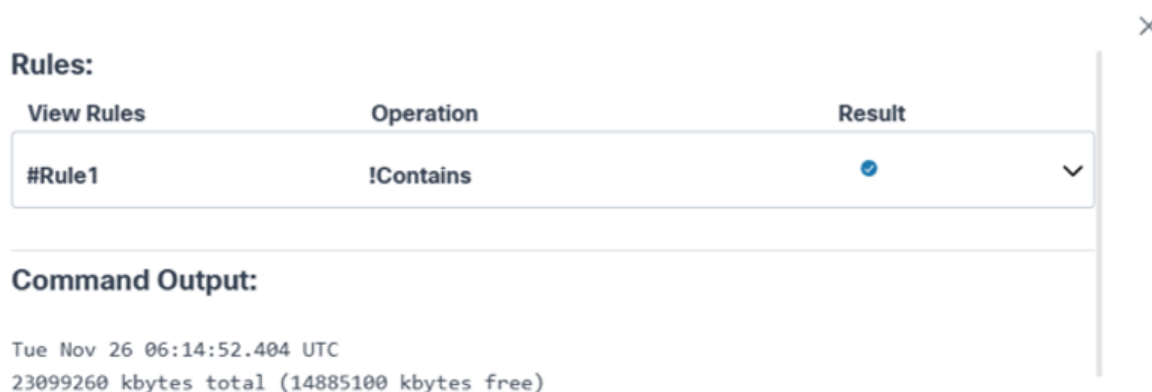
Vue Jalons avant et après vérification

Pour les jalons avec une exécution de pré- ou post-vérification, les utilisateurs peuvent afficher le résultat complet de la commande ainsi que les règles de validation et leur état pour toutes les commandes configurées dans le modèle de processus respectif.



Vue Jalon de distribution avec sortie de la commande de pré-vérification

1. Pour afficher le résultat de la commande et les règles associées aux commandes de pré-vérification et de post-vérification, cliquez sur le lien Afficher le résultat de la commande.



Sortie des commandes de pré-vérification et de post-vérification et règles associées

2. Cliquez sur l'icône Développer pour afficher tous les détails de chaque règle.

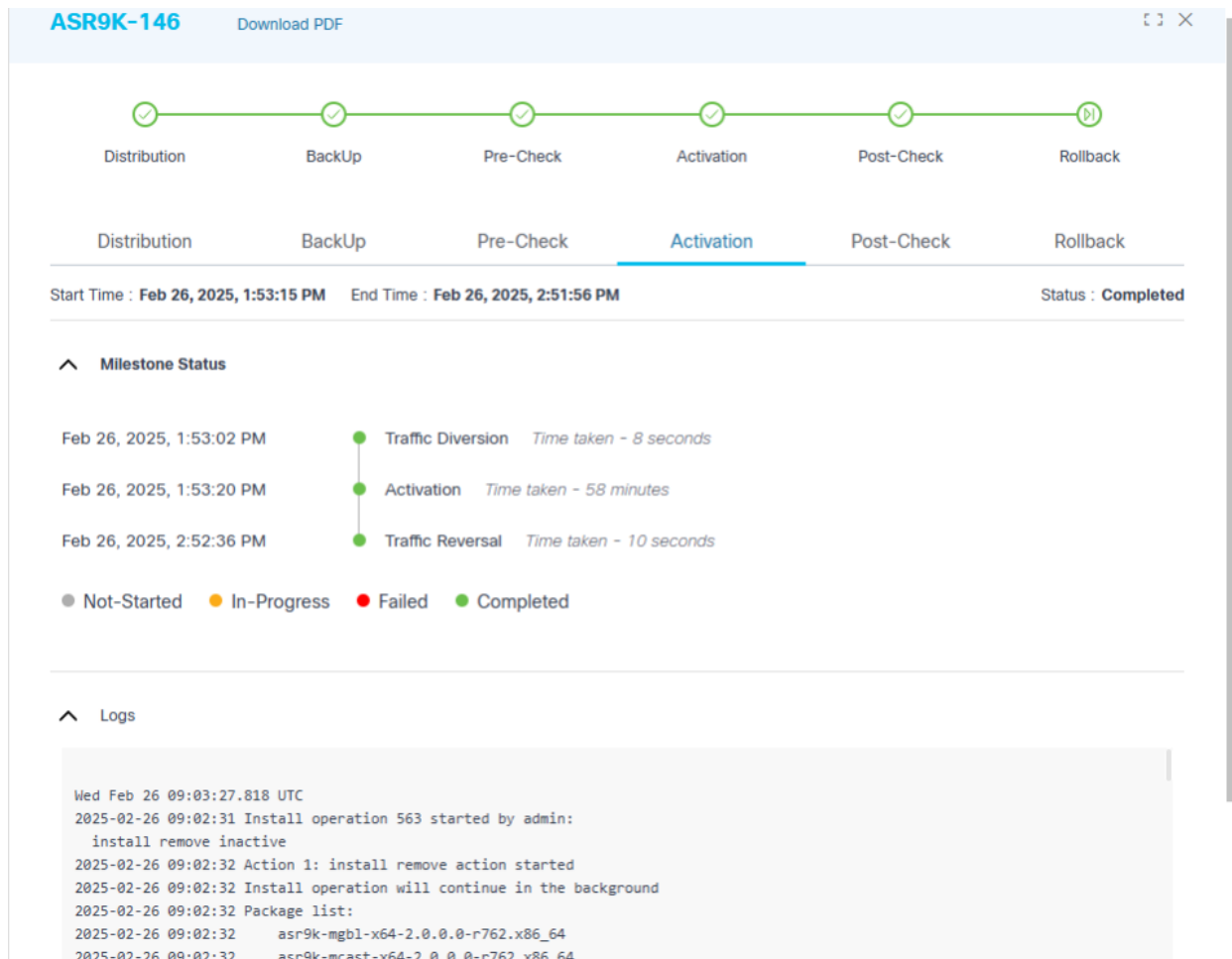
Rules:

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__%
```

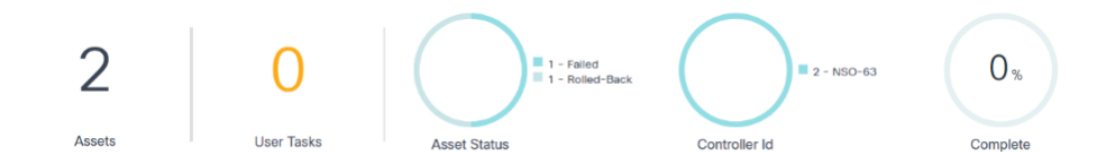
Sortie des commandes de pré-vérification et de post-vérification avec règles de validation



Vue Jalon d'activation avec journaux en direct

La figure ci-dessus fournit des détails sur le jalon d'activation, qui inclut des journaux en direct pour vous aider à surveiller la progression de l'activation logicielle d'un périphérique particulier.

Lorsqu'un jalon démarre ou se termine, cliquez sur le jalon pour afficher plus d'informations.



Section Analytique

Une section d'analyse, affichée en haut de la page Résumé du travail, affiche les informations suivantes relatives au travail actuellement sélectionné :

- Nom du lot (par exemple, Asie)
- Filtres ^ réduit et développe la section d'analyse
- Les détails de lot suivants sont affichés dans l'ordre :
 - Ressources : Nombre total d'actifs

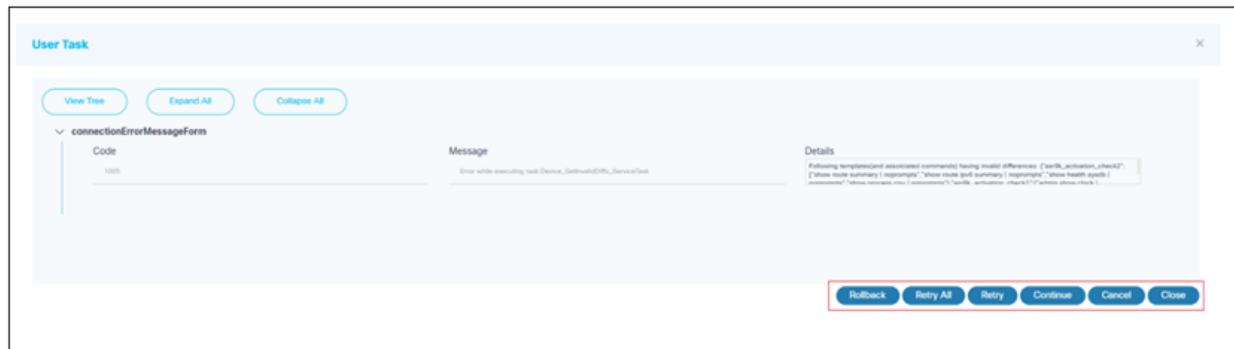
- Tâches utilisateur : Nombre total de tâches utilisateur en attente de l'entrée de l'utilisateur ou de l'administrateur Operations
- État des ressources : Filtre les périphériques par lots en fonction de leur état. Le filtre de restauration a été ajouté pour aider à identifier les périphériques qui ont été restaurés avec succès.
- ID du contrôleur : Filtre les périphériques par lots appartenant à l'ID de contrôleur sélectionné
- Terminé : Pourcentage global d'achèvement du lot

Pour effectuer des tâches utilisateur, cliquez sur le nombre de tâches utilisateur. La fenêtre Détails de la tâche utilisateur s'ouvre et affiche les informations suivantes :

User Task Details			All ▾ Search	
User Task Name		Created	Assignee	
CIO8kv-18.fra-lab.net (98TNZFYIHL2)	 View And Claim	Dec 8, 2023, 7:36:39 PM		
CIO8kv-20.fra-lab.net (9PLCN4P91YG)	 Cross launch	Dec 8, 2023, 7:34:19 PM		
CIO8kv-17.fra-lab.net (95SM6SYF975)	 View User Task  UnClaim	Dec 8, 2023, 7:34:21 PM	admin	
		1	Items per page	10 ▾

Détails des tâches utilisateur

- Liste de tâches utilisateur correspondant aux dispositifs respectifs nécessitant une attention particulière
- Les icônes suivantes pour les options des tâches utilisateur :
 - Afficher et demander : Afficher les détails des tâches utilisateur
 - Lancement croisé : Afficher les tâches de workflow BPA dans l'interface utilisateur classique
 - Annuler la demande : Supprimer l'affectation de tâche utilisateur
 - Afficher la tâche utilisateur : Afficher les détails des tâches utilisateur



Tâche utilisateur

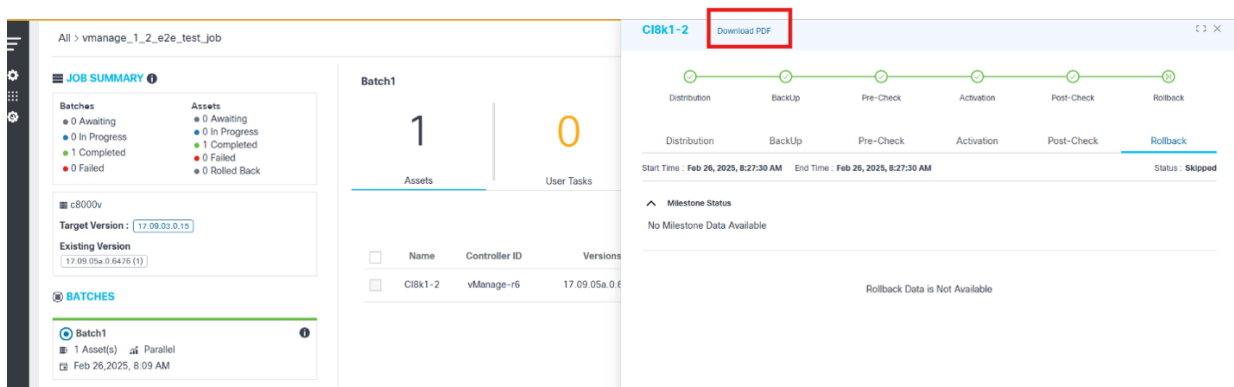
Afficher l'option de tâche utilisateur

- Les options suivantes s'affichent en fonction du contexte de la tâche :
 - Réessayer : Réexécute la tâche.
 - Réessayer tout : Réexécute toutes les vérifications avant et après l'exécution
 - Continuer : Passe à la tâche suivante
 - Restauration : Revient à la version précédente ; Cette option est disponible en cas d'échec de l'activation ou de la post-vérification, ou lorsque des différences non valides sont trouvées entre les pré-vérifications et les post-vérifications
 - Annuler : Annule la tâche en cours
 - Fermer : Ferme la fenêtre Tâche utilisateur.
- Agissez sur les tâches utilisateur, le cas échéant, et sélectionnez l'icône Actualiser pour actualiser le nombre total de tâches utilisateur
- Pourcentage total de fin du lot
- Graphique cliquable pour filtrer par ID de contrôleur



Remarque : Le nombre avant l'ID du contrôleur indique le nombre total de périphériques gérés par le contrôleur respectif.

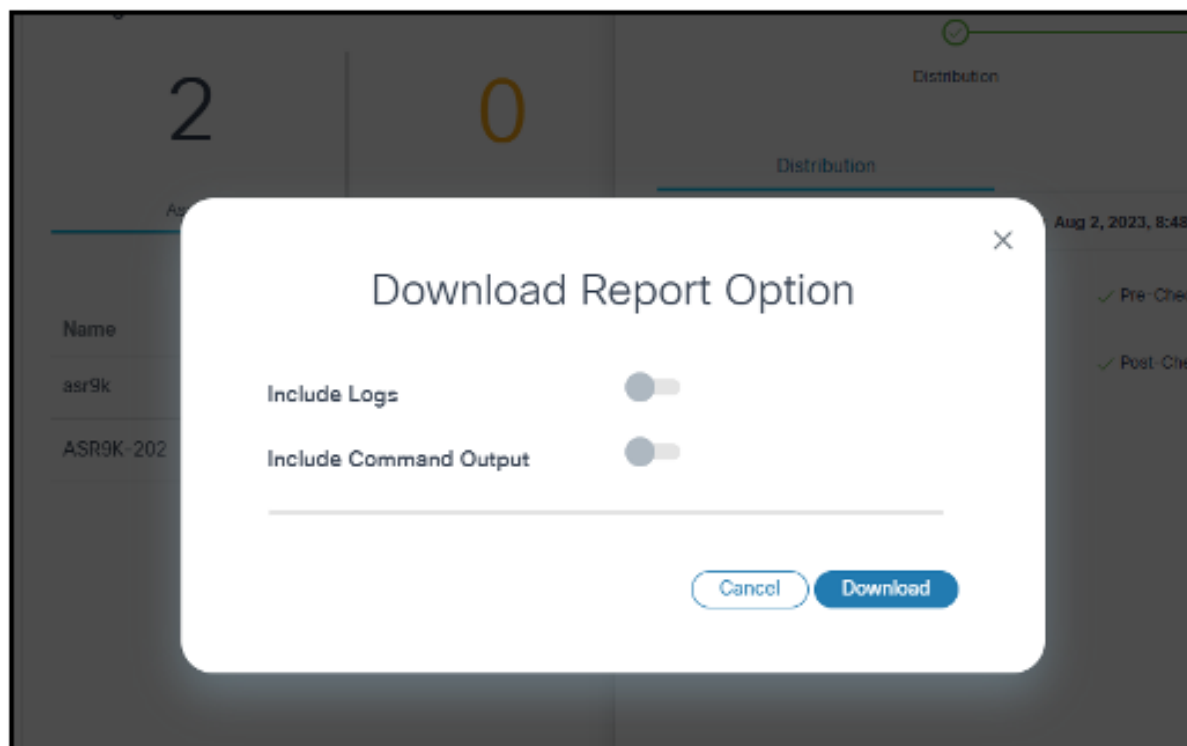
Téléchargement du rapport de mise à niveau logicielle



Télécharger le PDF

Le nom du périphérique s'affiche, suivi de Download PDF dans l'en-tête de la vue détaillée. Les utilisateurs peuvent générer et télécharger le rapport de mise à niveau au format PDF pour le périphérique actuellement sélectionné. Pour télécharger le rapport de mise à niveau au format PDF :

1. Cliquez sur Download PDF. La fenêtre Download Report Option s'affiche.



Option Télécharger le rapport

2. Activez les bascules Include Logs et Include Command Outputs.
 - Inclure les journaux : Inclut les journaux actifs, le cas échéant, dans le rapport
 - Inclure le résultat de la commande : Inclut dans le rapport le résultat de la commande des vérifications préalables et postérieures ; Dans ce cas, les règles sont suivies par le résultat de la commande
3. Cliquez sur Download. La génération du rapport commence.

 Remarque : L'activation des bascules Include Logs et Include Command Output augmente le temps de traitement pour la génération et la taille du rapport. N'utilisez ces bascules que lorsqu'un rapport détaillé est nécessaire. Les règles de commande sont incluses dans le rapport, que le basculement de sortie de commande soit activé ou désactivé.

Device Report

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

Software Upgrade Version: 7.8.2 - 7.7.2

Milestone: Distribution

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

Pre-Check

Process Template precheck_passfailrules

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

Rapport de périphérique

Archiver des tâches

1. Connectez-vous à BPA avec des informations d'identification disposant d'un accès suffisant aux travaux de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.
3. Utilisez le filtre Rechercher en combinaison avec les filtres de graphique disponibles pour filtrer le ou les travaux.
4. Sélectionnez une ou plusieurs tâches.



Travail d'archivage

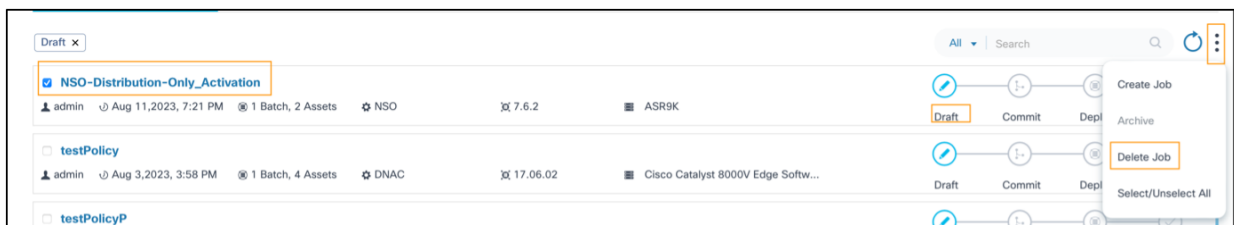
5. Cliquez sur l'icône Autres options > Archiver.



Remarque : Seules les tâches terminées peuvent être archivées.

Suppression de travaux

1. Connectez-vous à BPA avec des informations d'identification disposant d'un accès suffisant aux travaux de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.
3. Utilisez le filtre Rechercher en combinaison avec les filtres de graphique disponibles pour filtrer le ou les travaux.
4. Sélectionnez une ou plusieurs tâches.



Supprimer le travail

5. Cliquez sur l'icône Autres options > Supprimer le travail.



Remarque : Les tâches ne peuvent être supprimées que lorsqu'elles sont à l'étape Brouillon.

Supprimer des lots dans les ordres de fabrication

 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

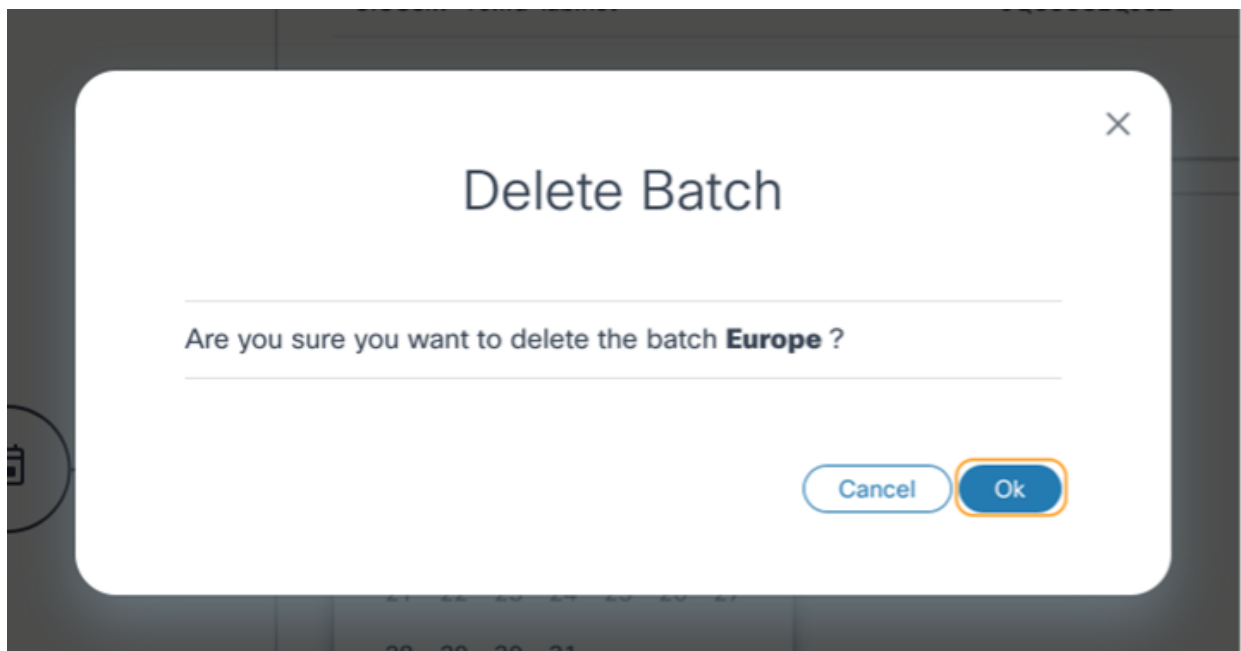
Batch Name *

Europe



Supprimer un lot dans une tâche

1. Sélectionnez l'icône Supprimer du lot souhaité dans le panneau latéral. Une fenêtre de confirmation s'ouvre.



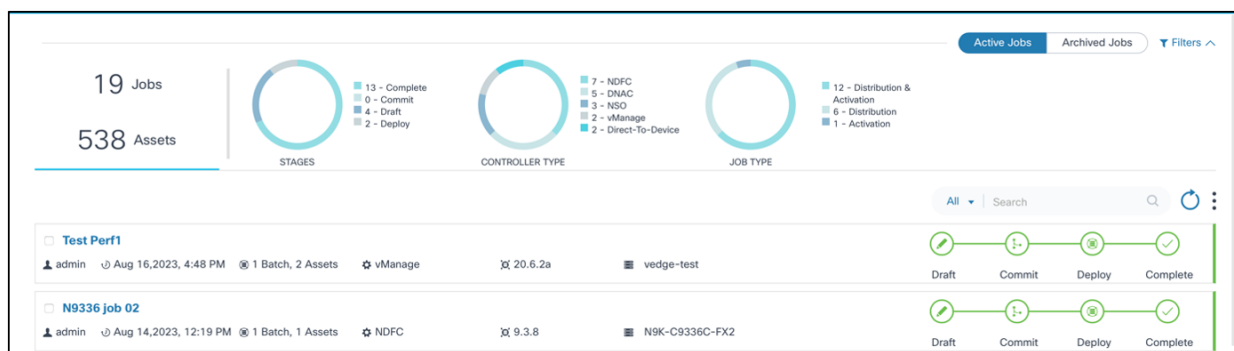
Confirmation de suppression de lot

2. Cliquez sur OK.

Les immobilisations associées au lot supprimé retournent dans le pool d'immobilisations en attente et peuvent être sélectionnées dans des lots nouveaux ou existants.

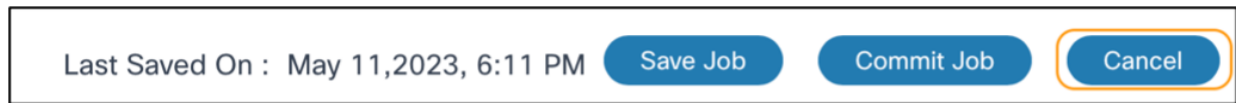
Annulation de travaux

1. Connectez-vous à BPA avec des informations d'identification disposant d'un accès suffisant aux travaux de mise à niveau.
2. Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.



Tâche de mise à niveau

- Utilisez le filtre Rechercher en combinaison avec les filtres de graphique disponibles pour filtrer la tâche souhaitée.
- Cliquez sur la tâche souhaitée. La page Récapitulatif des tâches s'affiche.

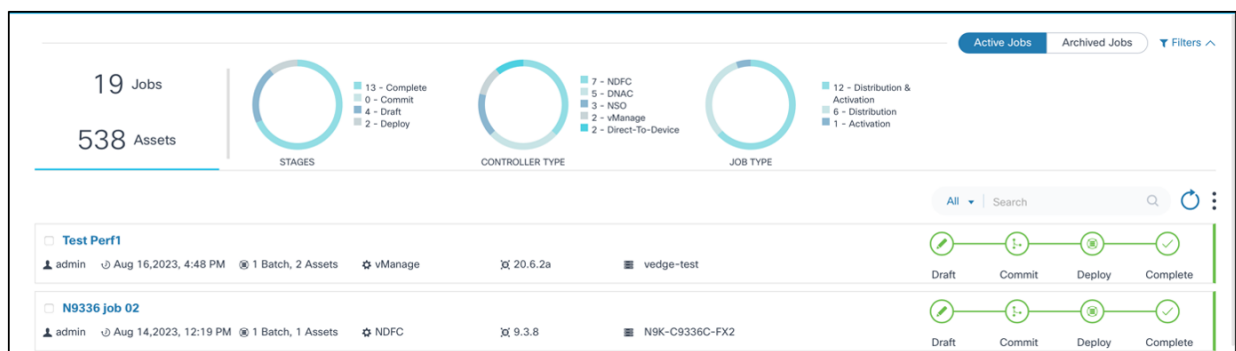


Annuler

- Cliquez sur Annuler.

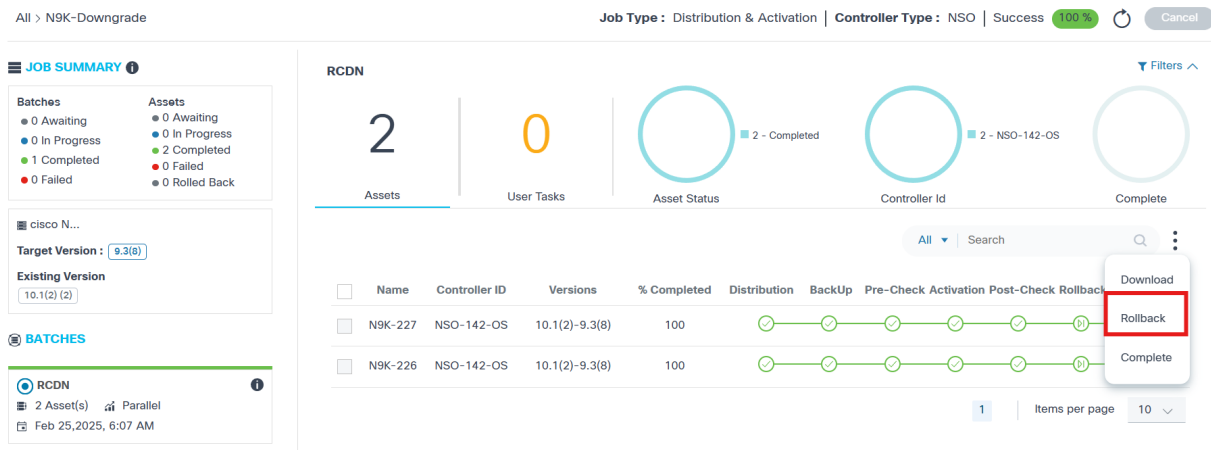
Annulation des travaux ou des mises à niveau terminés

- Connectez-vous à BPA avec des informations d'identification disposant d'un accès suffisant aux travaux de mise à niveau.
- Sélectionnez Mise à niveau du SE > Tâches de mise à niveau. La page Travail de mise à niveau s'affiche.



Tâche de mise à niveau

- Utilisez le filtre Rechercher en combinaison avec les filtres de graphique disponibles pour filtrer la tâche souhaitée.
- Cliquez sur la tâche souhaitée. La page Récapitulatif des tâches s'affiche. Sélectionnez le lot requis dans le volet de gauche et sélectionnez les périphériques souhaités qui nécessitent une confirmation complète/restauration dans le volet de droite
- Sélectionnez l'icône Plus d'options et cliquez sur Restaurer ou Terminer les actions de menu selon le besoin.



Restauration

Remarque : Les périphériques ne peuvent être sélectionnés que si les conditions suivantes sont remplies :

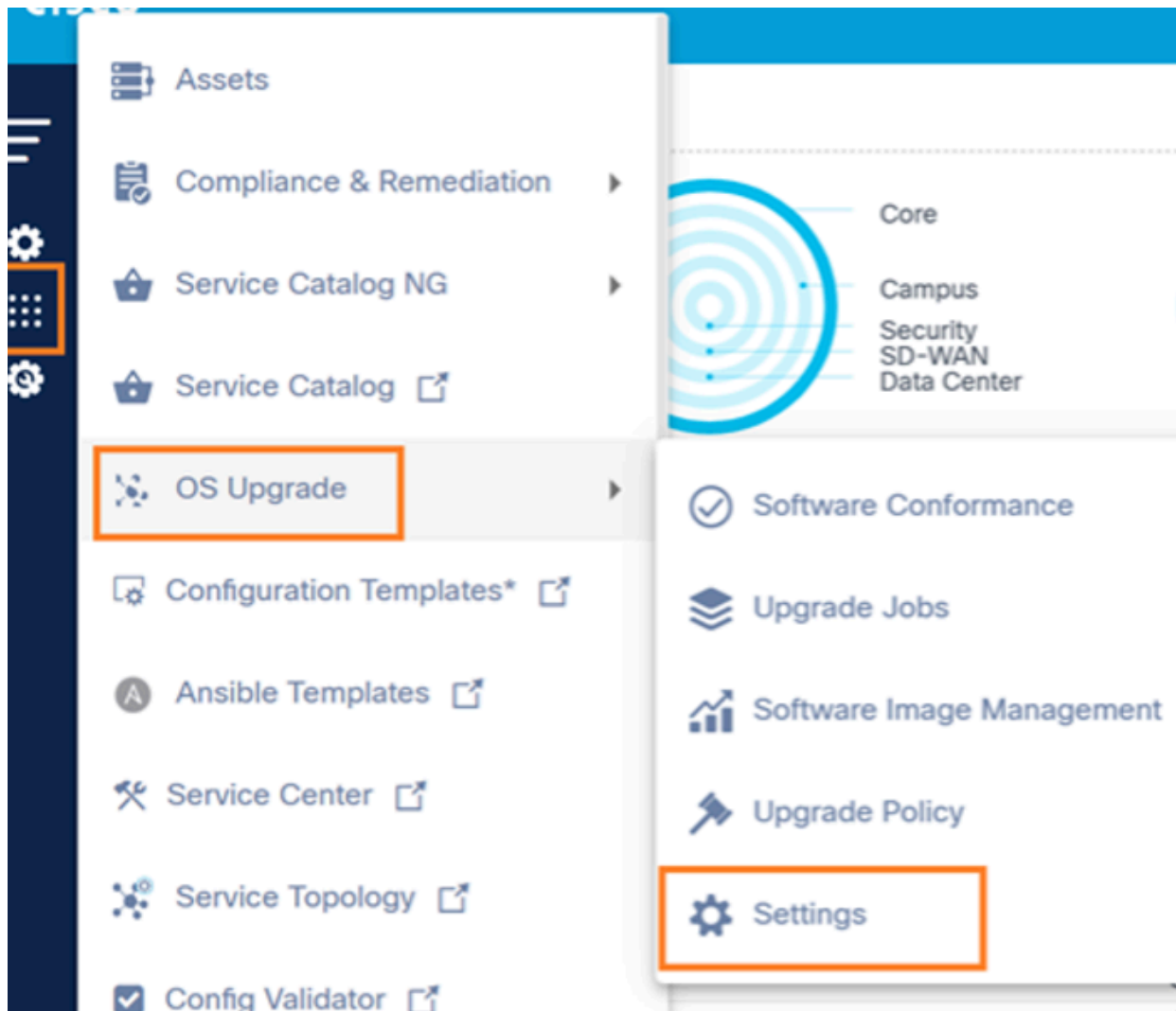
- Les paramètres doivent être configurés pour activer l'option de restauration d'une tâche de mise à niveau terminée ; référez-vous à [Paramètres](#) pour plus d'informations.
- Si aucune action n'est entreprise dans le délai imparti, les périphériques passent automatiquement à l'état Terminé
- Les périphériques sont disponibles pour l'action de restauration à la demande si la restauration a déjà été effectuée ou si le jalon de restauration est à l'état En attente

Paramètres

Les paramètres de mise à niveau du système d'exploitation fournissent un espace réservé pour contenir les paramètres communs utilisés dans d'autres composants de l'application de mise à niveau du système d'exploitation.

Pour accéder à la page Paramètres :

1. Connectez-vous à BPA avec des informations d'identification qui ont un accès géré aux paramètres.



Paramètres

2. Sélectionnez Mise à niveau du SE > Paramètres. La page Paramètres s'ouvre.

La page Paramètres comporte les deux onglets suivants :

- Conformité logicielle : Les configurations qui autorisent les programmes d'exécution de conformité automatique peuvent être mises à jour dans cet onglet
- Restauration : Les configurations qui permettent la restauration d'une mise à niveau complète d'un périphérique peuvent être mises à jour dans cet onglet

Conformité logicielle

Onglet Conformité logicielle

L'onglet Conformité logicielle fournit les éléments suivants :

- Vérification de la conformité planifiée : Activer ou désactiver la planification
- Date de début : Sélectionnez le MM/JJ/AAAA



Remarque : La date de début doit être une date ultérieure.

- Modèle cron : Fournissez les informations suivantes :
 - Minutes (0-59)
 - Heure (0-23)
 - Jour (Mois) (1-31)
 - Mois (1-12)
 - Jour (Semaine) (1-7)
- Ajouter un intervalle d'actualisation automatique : La valeur par défaut est de 30 secondes
- Enregistrer : Sauvegardez les modifications

Restauration

Onglet Restauration

L'onglet Rollback fournit les éléments suivants :

- Bascule de vérification utilisateur : Activer ou désactiver la vérification utilisateur
 - État activé : Les périphériques dans la tâche de mise à niveau attendent la confirmation de l'utilisateur pour revenir en arrière ou terminer la mise à niveau jusqu'à ce que le délai de seuil configuré dans Configuration Threshold Time (hrs) soit atteint ; une fois atteints, les périphériques passent automatiquement à l'état Terminé
 - État désactivé : Les périphériques dans la tâche de mise à niveau terminent automatiquement la mise à niveau sans attendre la confirmation de l'utilisateur
- Durée du seuil de confirmation : Ajouter un délai d'attente de seuil en heures
- Enregistrer : Sauvegardez les modifications

Configuration du déploiement

- Les plannings par défaut pour la vérification de la stratégie de conformité et les métadonnées SWIM sont configurés quotidiennement à 7h25 heure locale.
- Pour modifier les planifications par défaut de la synchronisation des métadonnées de l'image SWIM, accédez au répertoire installé BPA « <répertoire d'installation BPA>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json » et mettez à jour la propriété schedule.swimSchedule avec l'expression Cron. Les planifications peuvent être mises à jour après le déploiement. Référez-vous à [Conformité logicielle](#) pour plus d'informations.
- Pour augmenter ou diminuer le nombre maximal de périphériques traités en mode parallèle pour différents types de contrôleurs :

1. Mettez à jour les fichiers suivants :

- Fichier Cisco Catalyst Center : « <RÉPERTOIRE_INSTALLATION_BPA>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json »
- Fichier vManage : « <RÉPERTOIRE_INSTALLATION_BPA>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json »
- Fichier NDFC : « <RÉPERTOIRE_INSTALLATION_BPA>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json »
- Fichier FMC : « <RÉPERTOIRE_INSTALLATION_BPA>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json »

2. Accédez à Update throttling > capabilities > image-activation, image-distribute pour augmenter la limite d'activation ou de distribution simultanée.

 Remarque : Référez-vous à [Contrôleurs et plates-formes de périphériques pris en charge](#) avant de mettre à jour ces limites.

Contrôle d'accès

Contrôle d'accès basé sur les rôles

BPA prend en charge le contrôle d'accès basé sur les rôles (RBAC). Dans le modèle RBAC, un rôle encapsule un ensemble d'autorisations (c'est-à-dire des actions) qu'un utilisateur peut effectuer. Pour le contrôle d'accès, les administrateurs peuvent attribuer des rôles prédéfinis ou des rôles nouvellement créés avec des autorisations sur des groupes d'utilisateurs. Un utilisateur peut appartenir à un ou plusieurs groupes d'utilisateurs et chaque groupe d'utilisateurs peut être affecté à un ou plusieurs rôles qui donnent aux utilisateurs de ce groupe certaines autorisations d'accès.

Le tableau ci-dessous présente les rôles OOB OS Upgrade et les autorisations associées.

Service	Groupe	Intention	Super admin	Exemple d'utilisation Administrateur	Utilisateur en lecture seule (exemple d'utilisation Mise à niveau du SE Utilisateur en lecture seule)		Opérateur
ServiceMiseÀNiveauOSU ui_app		Afficher ou masquer l'application Tâches de mise à niveau	Oui	Oui	Oui		Oui
ServiceMiseÀNiveauOSU ui_app		Afficher ou masquer l'application Conformité logicielle	Oui	Oui	Oui		Oui
ServiceMiseÀNiveauOSU ui_app		Afficher ou masquer l'application SWIM	Oui	Oui	Oui		Oui
ServiceMiseÀNiveauOSU ui_app		Afficher ou masquer l'application Stratégies de mise à niveau	Oui	Oui	Oui		Oui

Service	Groupe	Intention	Super admin	Exemple d'utilisation Administrateur	Utilisateur en lecture seule (exemple d'utilisation Mise à niveau du SE Utilisateur en lecture seule)	Opérateur
ServiceMiseÀNiveauOSU	ui_app	logicielle Afficher ou masquer les paramètres de mise à niveau logicielle	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Tâches de mise à niveau	Gérer les tâches de mise à niveau (par exemple, créer, mettre à jour, supprimer et valider)	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Tâches de mise à niveau	Annuler les travaux de mise à niveau	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Tâches de mise à niveau	Archivage à la demande des travaux	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Tâches de mise à niveau	Approbation manuelle	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Politique de conformité logicielle	Afficher les stratégies de conformité logicielle et les résultats d'exécution	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Politique de conformité logicielle	Créer, mettre à jour et supprimer des stratégies de conformité logicielle	Oui	Oui	Non	Non
ServiceMiseÀNiveauOSU	Politique de conformité logicielle	Exécution à la demande de politiques de	Oui	Oui	Non	Oui

Service	Groupe	Intention	Super admin	Exemple d'utilisation Administrateur	Utilisateur en lecture seule (exemple d'utilisation Mise à niveau du SE Utilisateur en lecture seule)	Opérateur
ServiceMiseÀNiveauOSU	Politique de mise à niveau	conformité logicielle Afficher les stratégies de mise à niveau OS	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Politique de mise à niveau	Gérer les stratégies de mise à niveau OS	Oui	Oui	Non	Non
ServiceMiseÀNiveauOSU	Gestion des images de natation	Créer, mettre à jour et supprimer des images logicielles	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Gestion des images de natation	Afficher SWIM	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Gestion des images de natation	Synchroniser les images logicielles	Oui	Oui	Non	Oui
ServiceMiseÀNiveauOSU	Recommandations logicielles	Synchroniser les métadonnées des recommandations logicielles	Oui	Oui	Non	Non
ServiceMiseÀNiveauOSU	Recommandations logicielles	Afficher les conseils ou les aperçus	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Recommandations logicielles	Gérer la stratégie de conformité	Oui	Oui	Non	Non
ServiceMiseÀNiveauOSU	Configuration de la conformité logicielle	Afficher les paramètres de conformité logicielle	Oui	Oui	Oui	Oui
ServiceMiseÀNiveauOSU	Configuration de la conformité	Gérer les paramètres de	Oui	Oui	Non	Non

Service	Groupe	Intention	Super admin	Exemple d'utilisation Administrateur	Utilisateur en lecture seule (exemple d'utilisation Mise à niveau du SE Utilisateur en lecture seule)	Opérateur
	logicielle	conformité logicielle				

 Remarque : Les rôles personnalisés et le mappage des autorisations peuvent être effectués selon les besoins. Reportez-vous à [Groupes de ressources](#).

Groupes de ressources

Cette fonctionnalité fournit un contrôle d'accès à grain fin pour les ressources BPA, telles que les politiques de mise à niveau, empêchant les utilisateurs non autorisés de mettre à jour les politiques définies dans l'application de mise à niveau du système d'exploitation. Les administrateurs peuvent restreindre l'accès en définissant un groupe de ressources avec des stratégies accessibles.

Pour créer un groupe de ressources :

1. Accédez à Paramètres > Groupes de ressources.

Add Resource Group

Resource Group name *
osupgrade-res-grp

Resource Type:
os-upgrade-policy

Description:
Enter resource group description

Resources:

Name	ASRK	NSO
Nso-qa1	ASRK	NSO
NSO-asrk-policy-2	ASRK	NSO
☒ NSO-any-to-any-policy	ASRK	NSO

1
Items per page
10

Cancel
Submit

Ajouter un groupe de ressources

2. Créez un groupe de ressources avec des stratégies auxquelles les utilisateurs non administrateurs peuvent accéder.
3. Sélectionnez os-upgrade-policy comme type de ressource. Les ressources correspondantes s'affichent.
4. Sélectionnez les stratégies de mise à niveau requises.
5. Cliquez sur Submit. Les utilisateurs non administrateurs appartenant à ce groupe d'utilisateurs ont désormais accès aux stratégies disponibles dans le groupe de ressources sélectionné uniquement.

Pour associer le groupe de ressources à un groupe d'utilisateurs, créez une stratégie d'accès.

Add Policy

Policy name *
osupgrade-access-policy

Description:
Enter policy description

Resource Groups:

All | osupg

Resource Groups
☐ Resource Groups
☒ osupgrade-res-grp

1 | Items per page 10

Asset Groups:

All | Search

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

1 | Items per page 10

User Groups:

All | osupgrade

User Groups
☐ User Groups
☒ osupgrade-user-grp

1 | Items per page 10

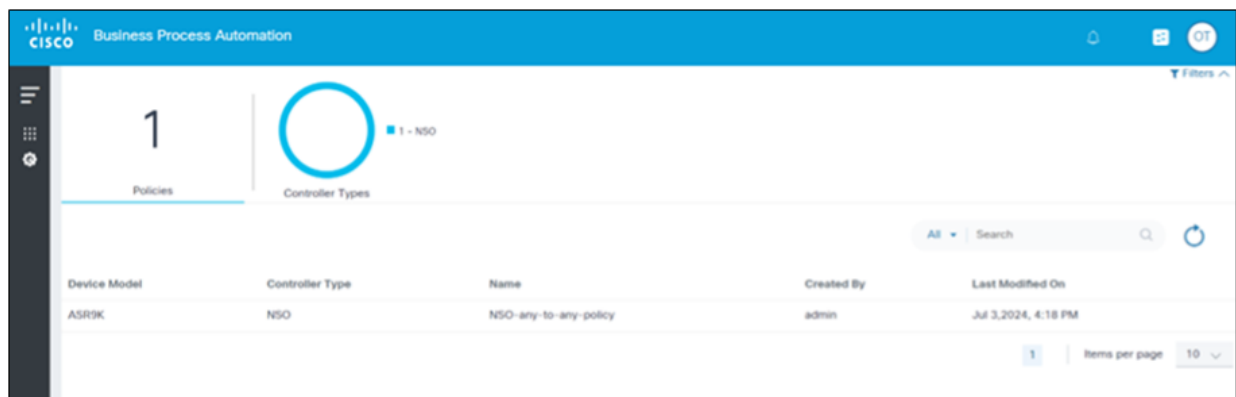
Ajouter une stratégie d'accès



Remarque : Une fois le groupe de ressources créé, il doit être associé à un groupe d'utilisateurs via des stratégies d'accès. Référez-vous à [Contrôle d'accès](#) pour plus d'informations sur les éléments suivants :

- Utilisateurs
- Rôles
- Groupes d'utilisateurs
- Politiques d'accès
- Groupes de ressources
- Groupes de ressources

Voici un exemple d'utilisateur non administrateur ayant accès à des ressources restreintes :



Utilisateur Non Administrateur Ayant Des Restrictions De Ressources

Paramètre d'indicateur de confiance zéro

Les ressources accessibles par un utilisateur peuvent varier en fonction du paramètre de l'indicateur d'approbation zéro. L'indicateur d'approbation zéro peut être défini sur true ou false. Le tableau suivant récapitule les possibilités d'accès aux ressources en fonction du paramètre d'indicateur d'approbation zéro.

Utilisateur	Groupe d'utilisateurs	Politique d'accès	Groupe de ressources	Ressources	Confiance Nulle	Activée
Utilisateur 1	UG1	AP1	RG1	2 ressources	2 ressources	2 ressources
Utilisateur 1	UG1	AP2	RG2	0 ressource	0 ressource	0 ressource
Utilisateur 1	UG1	AP3	Nul		0 ressource	Toutes les ressources
Utilisateur 1	UG1	Nul	Nul		0 ressource	Toutes les ressources

Pour activer ou désactiver l'indicateur de confiance zéro :

1. Accédez au chemin de configuration suivant :

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

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

2. Modifiez la valeur zeroTrustPolicies.
3. Accédez à l'offre groupée principale suivante :

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

4. Exécutez la commande suivante pour supprimer la barre principale :

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

5. Exécutez la commande suivante pour vérifier l'état des pods

```
kubectl get pods -n bpa-ns
```

6. Exécutez la commande suivante pour installer la barre principale une fois que tous les pods sont terminés :

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

7. Exécutez la commande suivante pour vérifier l'état des pods qui s'affichent :

```
kubectl get pods -n bpa-ns
```

Résolution des problèmes de mise à niveau OS

Cette section fournit des conseils de dépannage relatifs aux problèmes observés avec l'application Mise à niveau du système d'exploitation dans BPA.

Impossible de voir le modèle de périphérique cible lors de la création d'une stratégie de conformité

Assurez-vous que les métadonnées d'image correspondantes sont disponibles dans Images logicielles sous SWIM. Si cette option est introuvable, effectuez l'une des opérations suivantes :

- Synchroniser des images pour récupérer des métadonnées d'image à partir de contrôleurs tels que Cisco Catalyst Center, NDFC, vManage et FMC
- Créer les métadonnées d'image requises pour les contrôleurs tels que NSO, CNC, Direct-to-Device et ANSIBLE

La conformité du logiciel indique un état de non-fonctionnement

Cela peut être dû aux raisons suivantes :

- Aucune ressource n'a été trouvée avec le modèle sélectionné lors de la création de la stratégie de conformité logicielle
- Le nom du modèle dans SWIM ne correspond pas au modèle de périphérique conforme dans l'inventaire des périphériques pour tous les périphériques
- Si le SMU a été choisi dans le cadre de la création de la conformité logicielle et que la détection SMU a échoué pour tous les périphériques
- Le modèle de processus sélectionné pour l'exécution du modèle de contrôle de conformité a échoué ou est introuvable
- Le numéro de série ou la version actuelle n'est pas disponible pour tous les périphériques sous le modèle sélectionné lors de la création de la conformité logicielle

L'état du résultat de la conformité logicielle de certains périphériques est inconnu

Cela peut être dû aux raisons suivantes :

- Le nom du modèle dans SWIM ne correspond pas au modèle de périphérique conforme dans l'inventaire des périphériques
- Si le SMU a été choisi dans le cadre de la création de la conformité logicielle et que la détection SMU a échoué pour un périphérique
- Le modèle de processus sélectionné pour l'exécution du modèle de contrôle de conformité a échoué ou est introuvable
- Le numéro de série ou la version actuelle n'est pas disponible pour les périphériques

Pourcentage de progression de la tâche de mise à niveau

Si le pourcentage de progression de l'achèvement de la tâche de mise à niveau est inférieur à 100, même si la mise à niveau est terminée, vérifiez que les paramètres d'attente de restauration sont activés sous Mise à niveau du système d'exploitation > Paramètres > Restauration et que

l'option Vérification de l'utilisateur est activée. Si le pourcentage d'achèvement global reste inférieur à 100, sélectionnez Rollback ou Complete.

Planification des tâches atteinte, les périphériques sont bloqués dans l'état En attente

Si les périphériques sont bloqués dans un état En attente après le lancement du travail planifié, essayez de redémarrer les microservices Kafka, Camunda, Scheduler et Mise à niveau du système d'exploitation.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.