Déployer EVPN VXLAN, multisite via DCNM 11.2(1)

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Topologie physique créée
- Déployer l'OVA/OVF dans vCenter
- Déploiement du premier fabric : fabric RTP
  - Ajout de commutateurs dans le fabric
  - Déploiement de la configuration du fabric
- Déployer le deuxième fabric : SJ
- Créer un réseau (VLAN/L2VNI) et des VRF (L3VNI)
- Configuration multisite
- Déployer des politiques d'accès/trunk hôte
- Opérations du jour 2
  - Mise à niveau du logiciel NX-OS via DCNM
  - Installer Endpoint Locator
- Problèmes Rencontrés Lors De Ce Déploiement
  - Câblage incorrect
  - Échec de la configuration d'une fonctionnalité
  - Chevaucher les sous-réseaux de gestion de différents fabrics
  - Interfaces de répartition
  - Erreur de fabric lors du déploiement vers une fonctionnalité non prise en charge
- Quelles sont les nouveautés de DCNM 11.2 ?
- Informations connexes

Introduction

Ce document décrit comment déployer deux fabrics EVPN VXLAN individuels ainsi que comment fusionner ces deux fabrics dans un déploiement de fabric EVPN multisite à l'aide de Cisco Data Center Manager (DCNM) 11.2(1).

MSD (Multi-Site Domain), introduit dans la version 11.0(1) de DCNM, est un conteneur multifabric créé pour gérer plusieurs fabrics membres. Il s'agit d'un point de contrôle unique pour la définition des réseaux de superposition et du routage et transfert virtuels (VRF) qui sont partagés entre les

fabrics membres.

Remarque : ce document ne décrit pas les détails relatifs aux fonctions/propriétés de chaque onglet dans DCNM. Veuillez consulter les références à la fin qui couvre les explications détaillées.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- vCenter/UCS pour déployer la machine virtuelle DCNM
- Connaissance de NX-OS et Nexus 9000s
- Nexus 9000s ToR, EoR connectés en mode Leaf/Spine

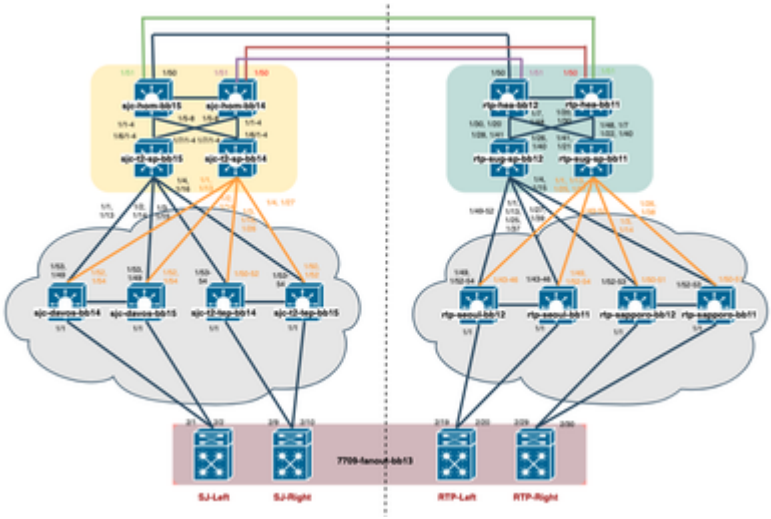
Composants utilisés

Les informations contenues dans ce document sont basées sur les logiciels et le matériel suivants :

- DCNM 11.2(1)
- NX-OS 7.0(3)I7(7) et NX-OS 9.2(3)
- Spines : N9K-C9508 / N9K-X97160YC-EX et N9K-C9508 / N9K-X9636PQ
- Leafs : N9K-C9372TX, N9K-C93180YC-EX, N9K-C9372TX-E, N9K-C92160YC-X
- Passerelles de périphérie : N9K-C93240YC-FX2 et N9K-C93180YC-FX
- 7 000 "hôtes" : N77-C709

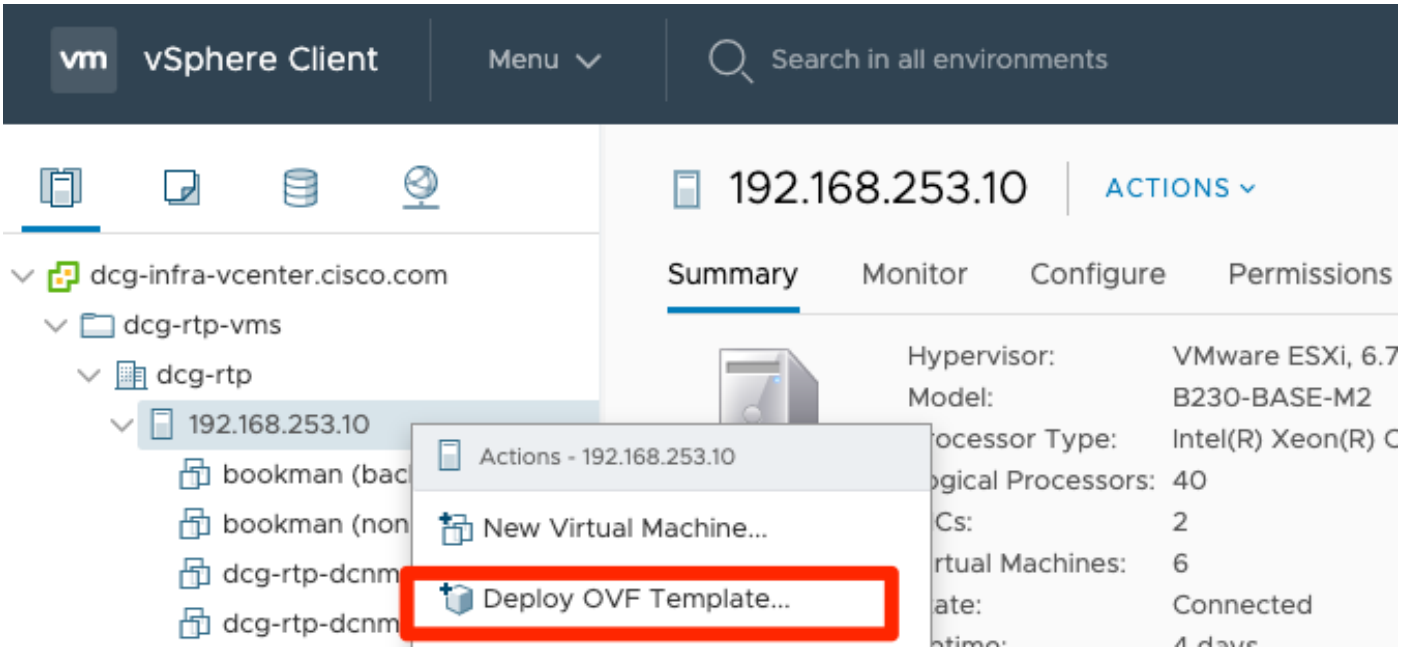
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Topologie physique créée

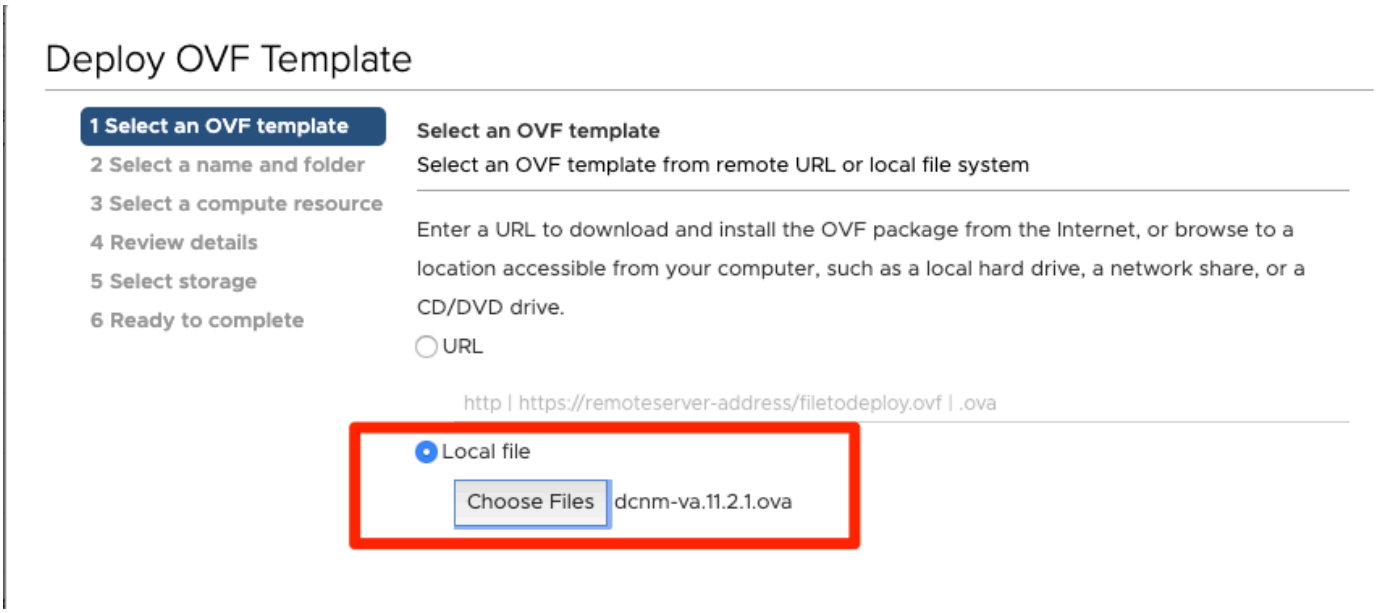


Déployer l'OVA/OVF dans vCenter

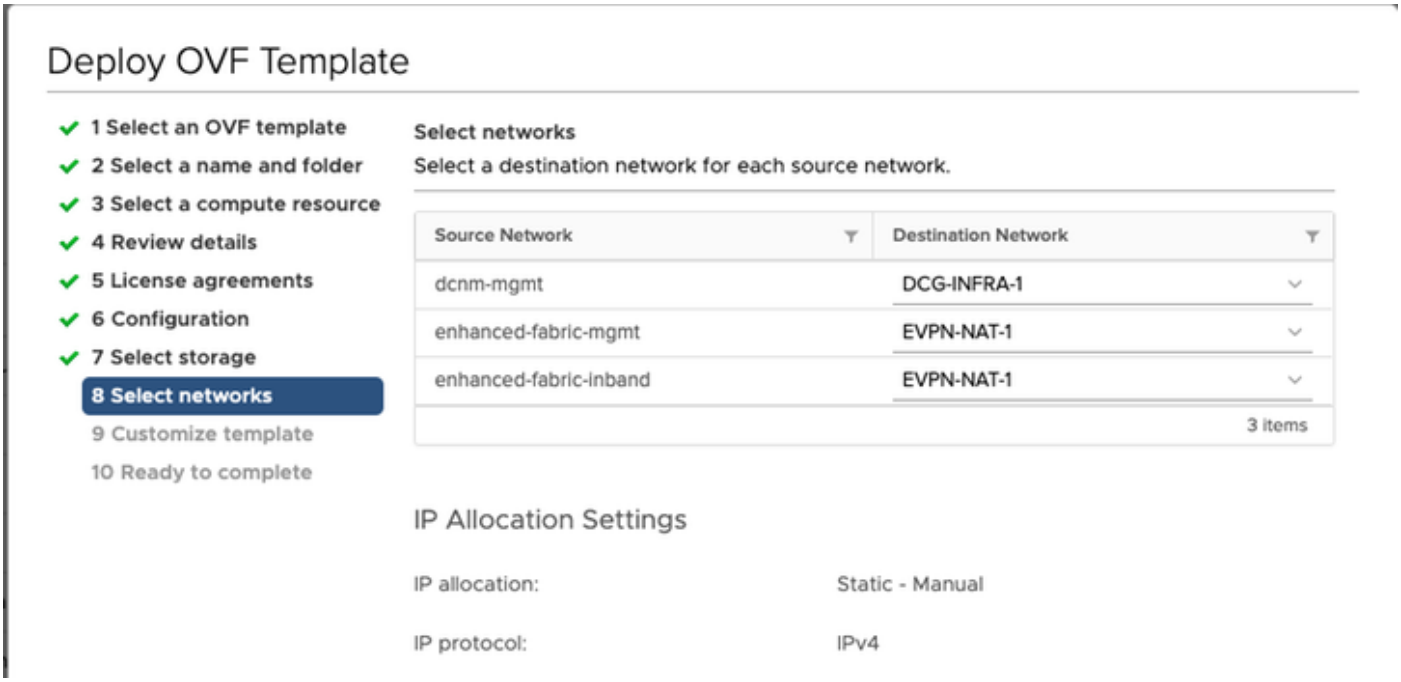
Étape 1. Sous vCenter, déployez le modèle OVF (Open Virtualization Format) sur le serveur/hôte de votre choix, comme illustré dans l'image.



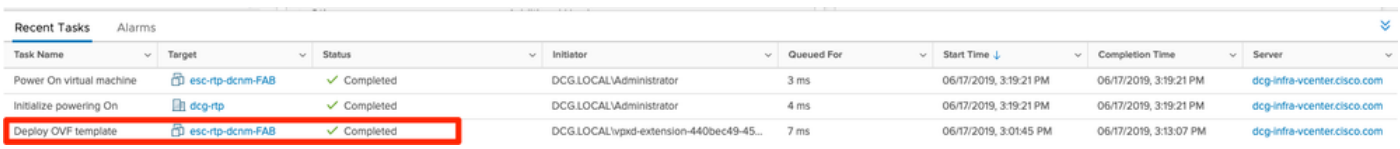
1. Ayez OVA/OVF, etc fichier localement et sélectionnez via Choose Files, comme indiqué dans l'image :

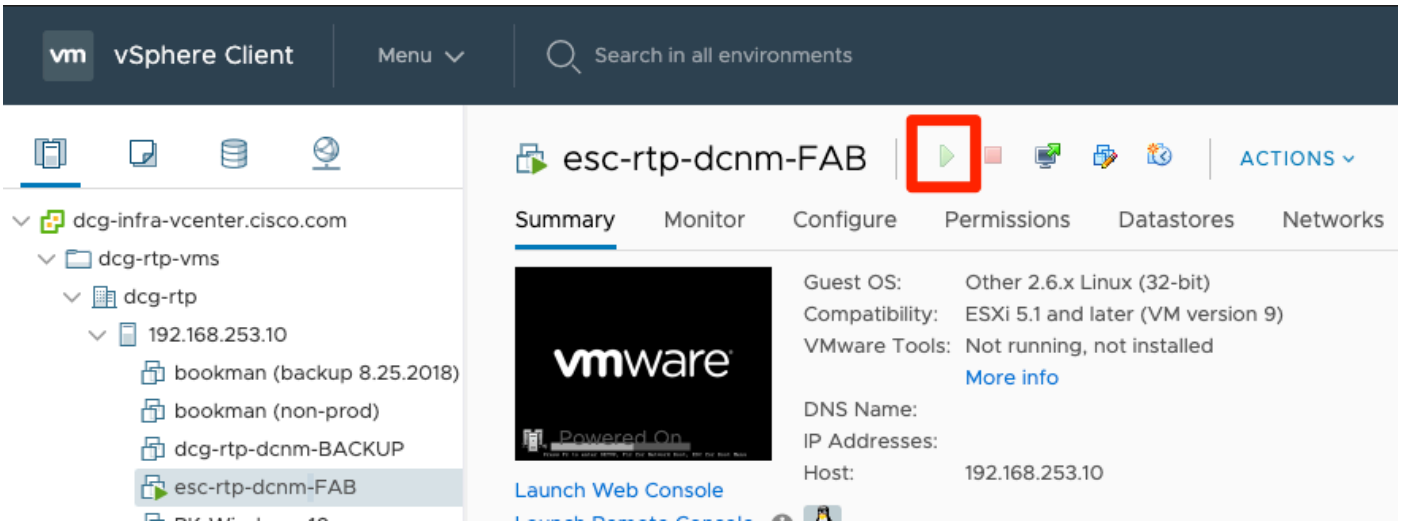


2. Suivez les autres invites (nom de la machine virtuelle, hôte, paramètres réseau, comme indiqué dans l'image) et cliquez sur Terminer.

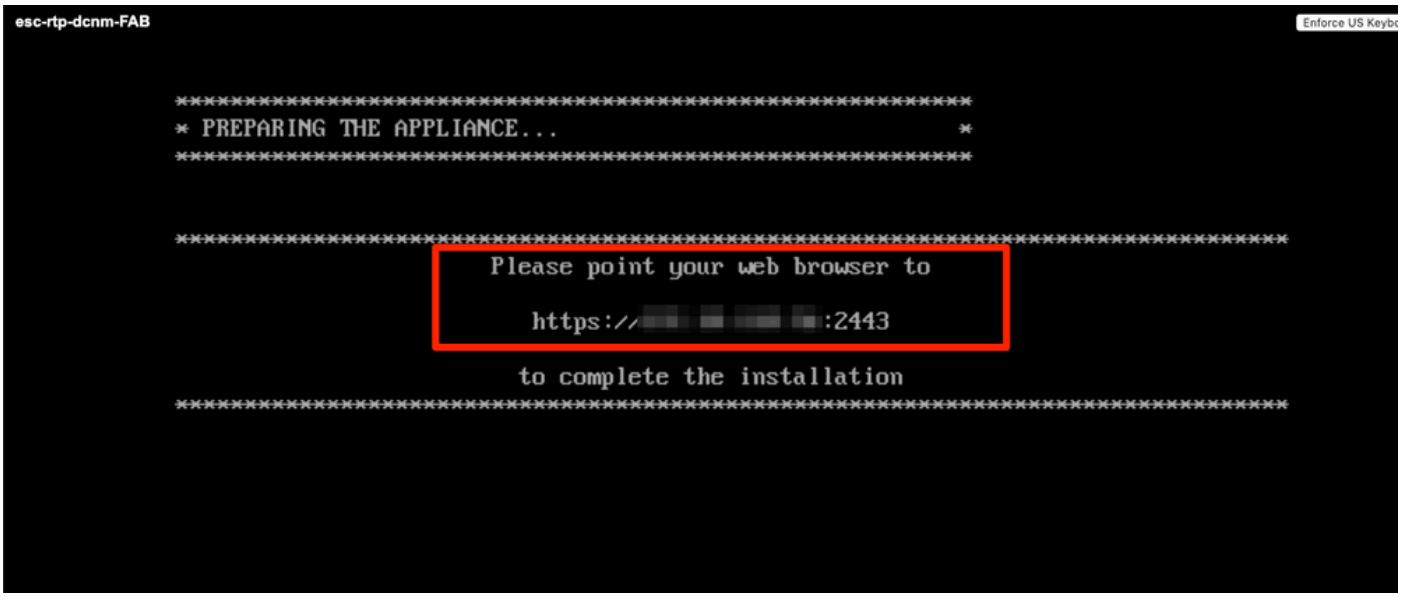


Étape 2. Une fois terminé, démarrez votre machine virtuelle DCNM, comme indiqué ici.





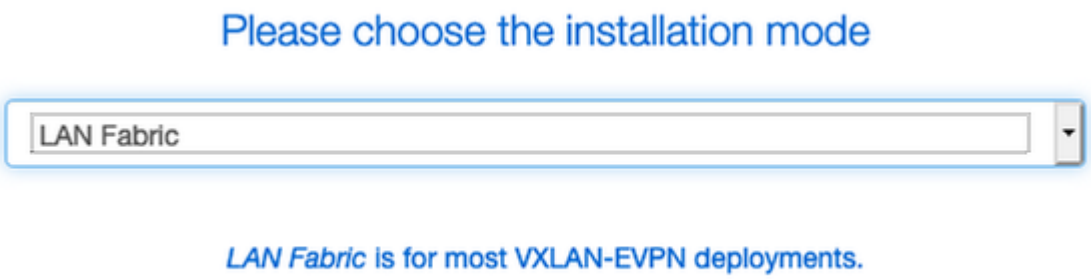
Étape 3. Lancez la console Web, une fois dans la console, vous devriez voir ces invites (IP diffère car il est spécifique à votre environnement et à votre configuration) :



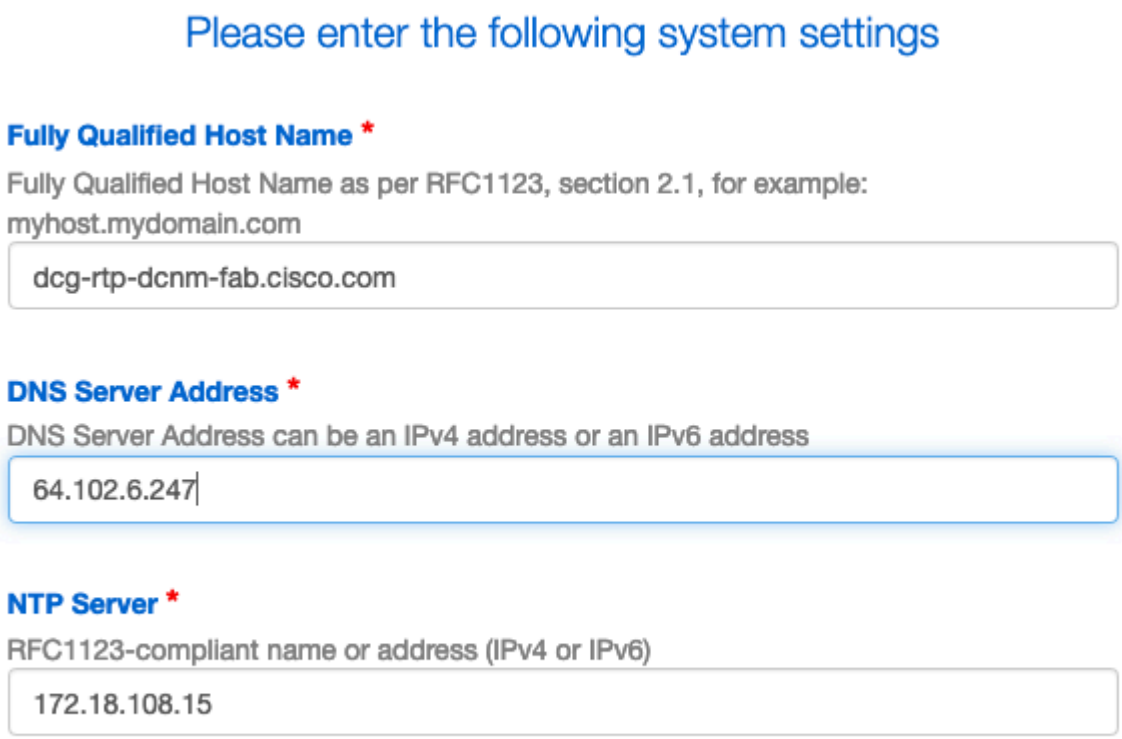
Étape 4. Accédez à https://<votre adresse IP>:2443 (il s'agit de l'adresse IP que vous avez configurée précédemment lors du déploiement OVA) et cliquez sur Get Started. Dans cet exemple, une nouvelle installation est traitée.



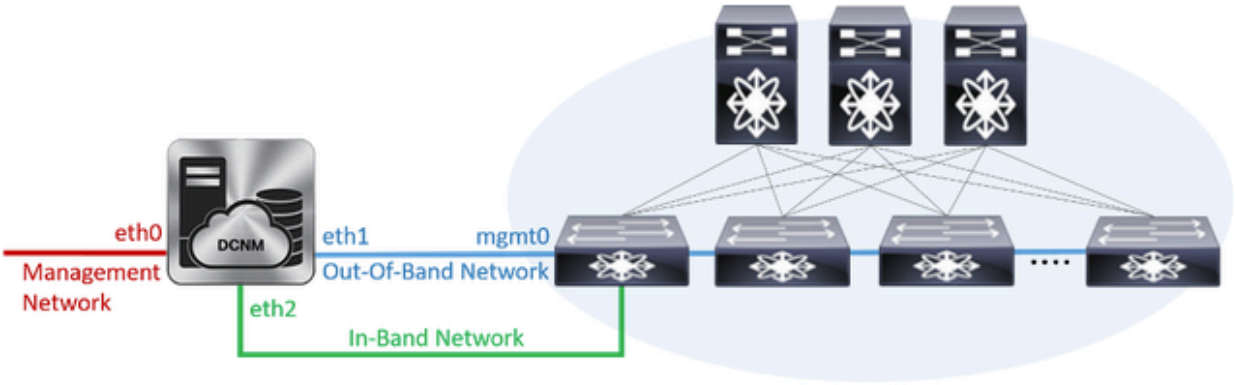
Étape 5. Après avoir configuré le mot de passe admin, vous devez sélectionner le type de fabric que vous souhaitez installer. Choisissez entre LAN ou FAB car chaque type a une fonction différente. Assurez-vous donc de bien comprendre et de choisir correctement. Pour cet exemple, le fabric LAN est utilisé, il est utilisé pour la plupart des déploiements VXLAN-EVPN.



Étape 6. Suivez les instructions du programme d'installation avec le DNS de votre réseau, le serveur NTP (Network Time Protocol), le nom d'hôte DCNM, etc.



Étape 7 : configuration de l’adresse IP de gestion et de la passerelle de gestion Le réseau de gestion fournit la connectivité (SSH, SCP, HTTP, HTTPS) au serveur DCNM. Il s'agit également de l'adresse IP que vous utilisez pour accéder à l'interface utilisateur graphique. L'adresse IP doit être préconfigurée à partir de l'installation OVA effectuée précédemment.



Management Network

The Management Network is the main network connection used for reaching the DCNM web user interface. When High Availability is enabled, 3 IP addresses are required on this network.

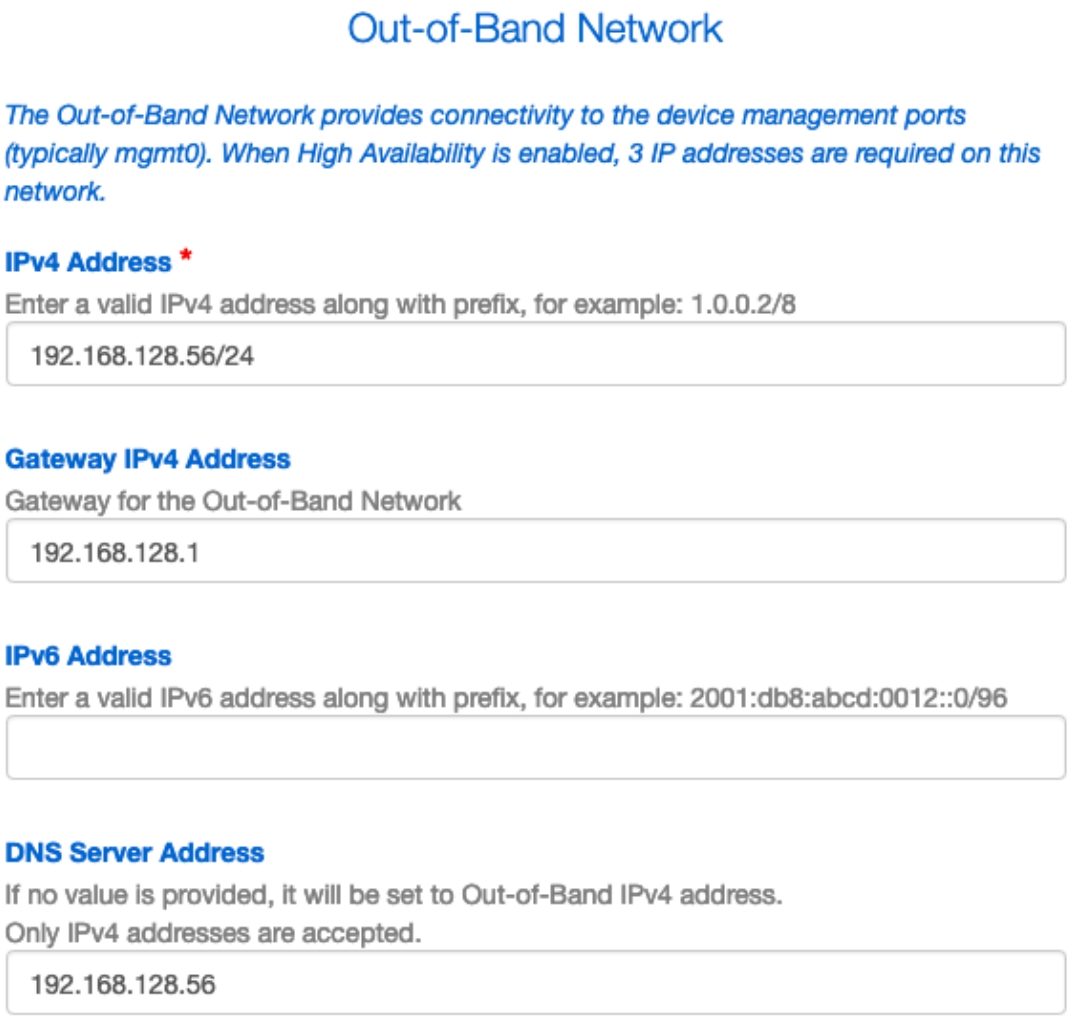
Management IPv4 Address *

Enter a valid IPv4 address along with prefix, for example: 10.10.10.2/24

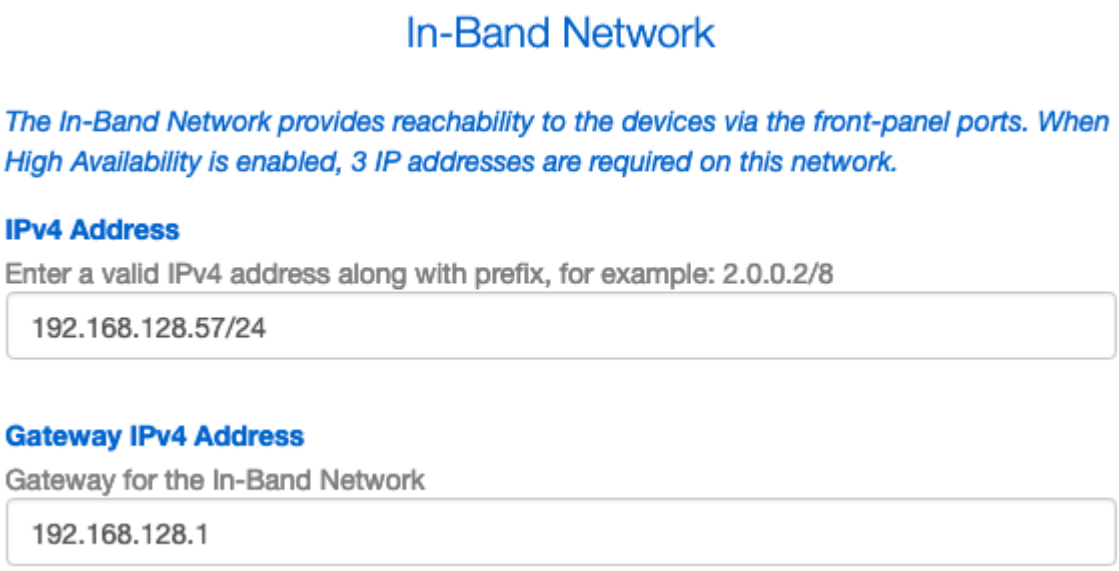
172.18.118.56/24

Management Network Default IPv4 Gateway *

172.18.118.1



Étape 8. Configuration du réseau intrabande Le réseau intrabande est utilisé pour des applications telles que Endpoint Locator qui nécessite une connectivité de port de façade aux 9 Ko du fabric pour fonctionner lorsqu'une session BGP (Border Gateway Protocol) est établie entre DCNM et les 9 Ko.

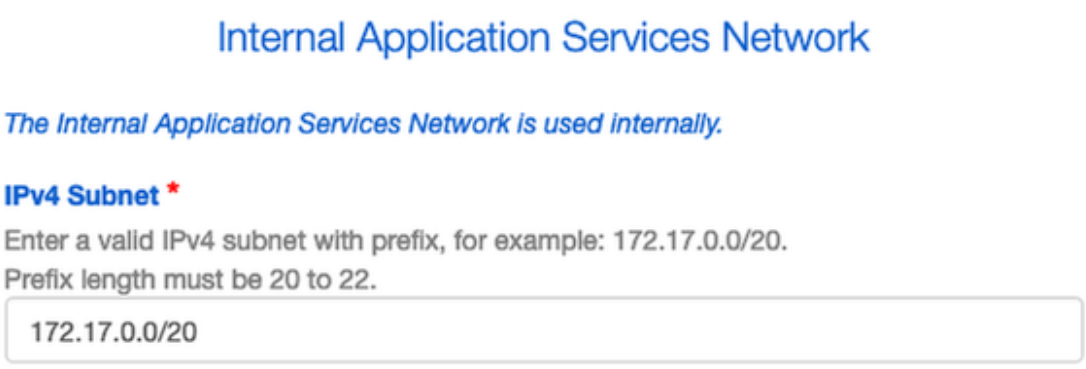


Étape 9. Configuration du réseau interne des services d'applications —

Pour commencer avec la version 11.0 de DCNM, DCNM prend en charge le cadre d'application (AFW) avec l'installation LAN OVA/ISO de DCNM. Cette structure utilise Docker pour orchestrer les applications en tant que microservices dans des environnements en cluster et non en cluster afin de réaliser une architecture évolutive.

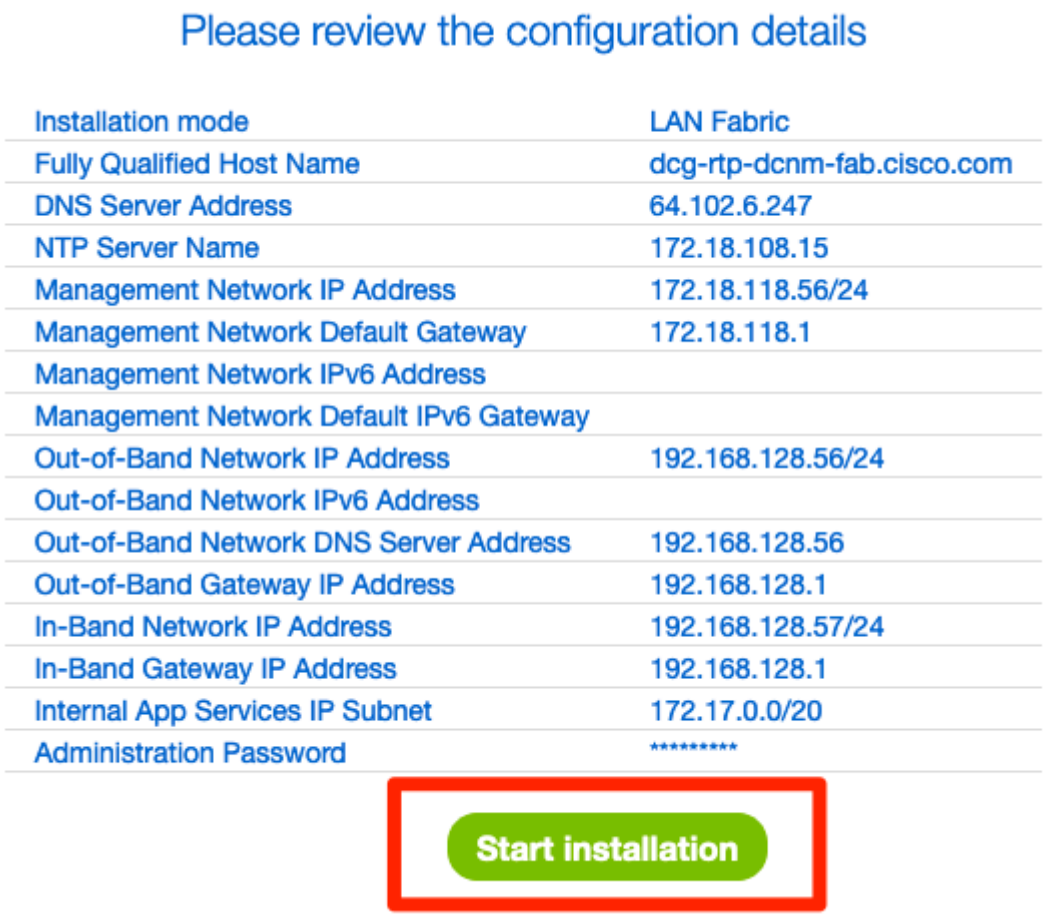
Les autres applications fournies par défaut avec le DCNM sont Endpoint Locator, Watch Tower, Virtual Machine Manager plugin, Config Compliance, etc. AFW s'occupe de la gestion du cycle de vie de ces applications, notamment de la mise en réseau, du stockage, de l'authentification, de la sécurité, etc. AFW gère également le déploiement et le cycle de vie des applications Network Insights, à savoir NIR et NIA. Ce sous-réseau est destiné aux services Docker lorsque NIA/NIR est activé.

La procédure d'installation de NIA/NIR est décrite dans la section Opérations du jour 2.



Remarque : Ce sous-réseau ne doit pas chevaucher les réseaux affectés aux interfaces eth0/eth1/eth2 affectées au DCNM et aux noeuds de calcul. En outre, ce sous-réseau ne doit pas chevaucher les adresses IP allouées aux commutateurs ou autres périphériques gérés par DCNM. Le sous-réseau choisi doit rester cohérent lors de l'installation des noeuds DCNM principal et secondaire (dans le cas d'un déploiement haute disponibilité natif).

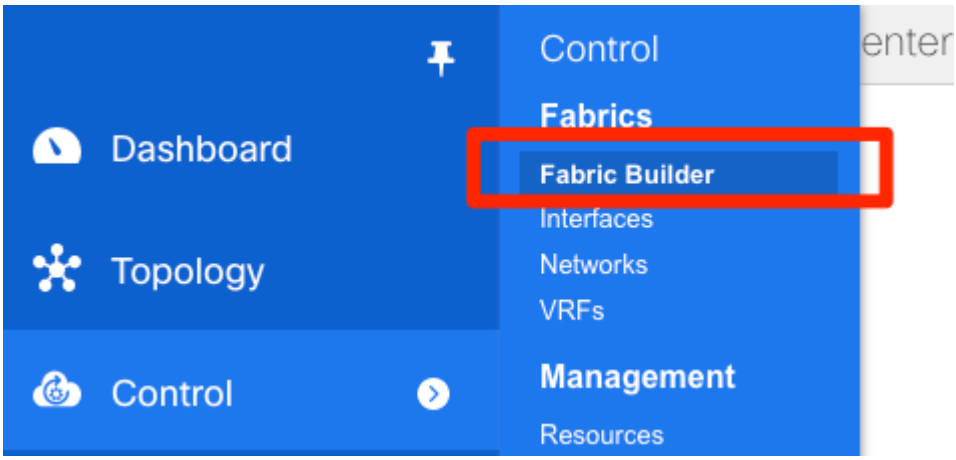
Étape 10. Vérifiez et confirmez tous les détails de configuration et démarrez l'installation.



Étape 11. Une fois DCNM entièrement installé, connectez-vous à l'interface utilisateur graphique (adresse IP ou nom d'hôte que vous avez précédemment configuré).

Déploiement du premier fabric : fabric RTP

Étape 1. Une fois dans l'interface graphique utilisateur de DCNM, accédez à Fabric Builder. Control > Fabrics > Fabric Builder afin de créer votre premier fabric.

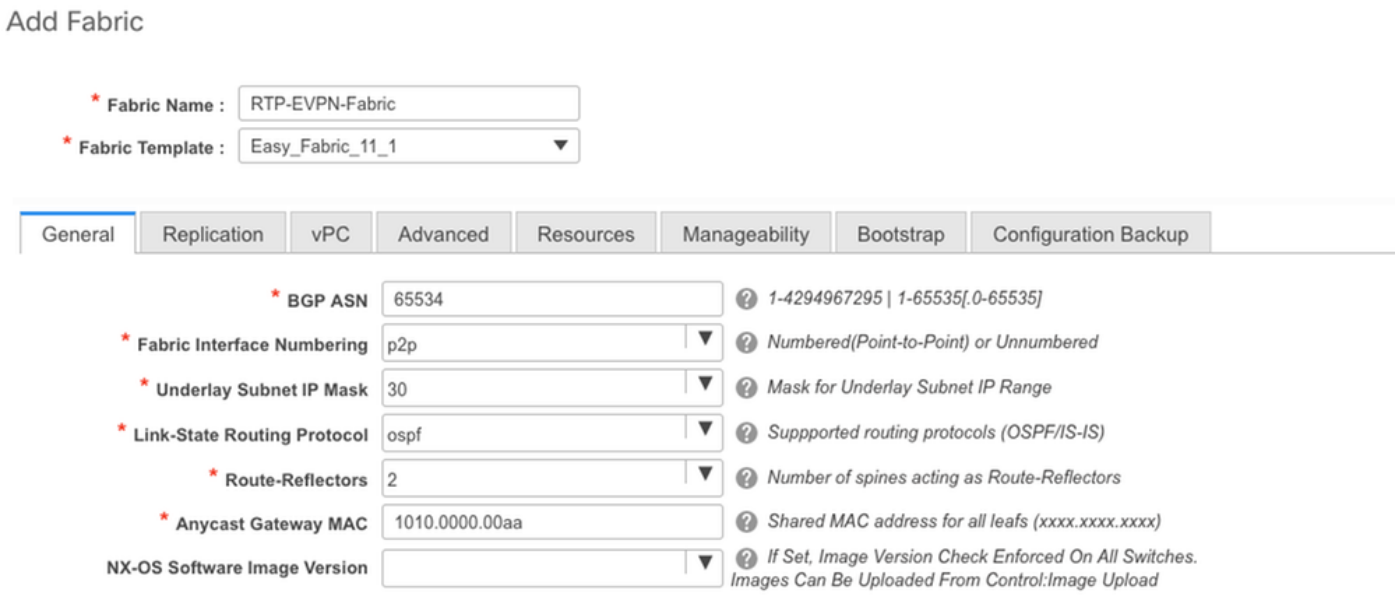


Étape 2. Cliquez sur Create Fabric et remplissez les formulaires nécessaires pour votre réseau. Easy Fabric est le modèle correct pour le déploiement local d'EVPN VXLAN :

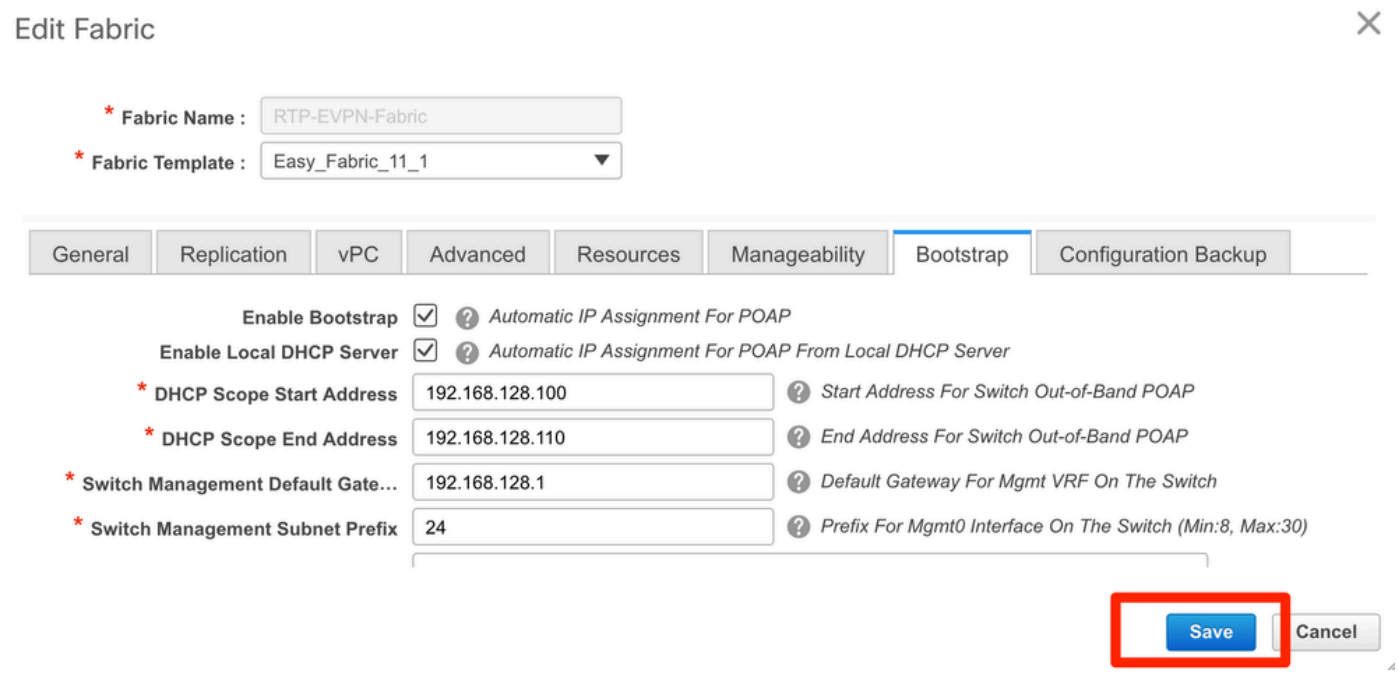


Étape 3. Remplir les conditions requises pour la sous-couche, la superposition, le vPC, la réplication, les ressources, etc. du fabric

Cette section couvre tous les paramètres de sous-couche, de superposition, vPC, de réplication, etc. requis via DCNM. Cela dépend du schéma d'adressage réseau, des exigences, etc. Dans cet exemple, la plupart des champs sont conservés par défaut. Les protocoles L2VNI et L3VNI ont été modifiés de sorte que les protocoles L2VNI commencent par 2 et les protocoles L3VNI par 3 pour faciliter le dépannage ultérieur. La détection de transfert bidirectionnel (BFD) est également activée avec d'autres fonctionnalités.

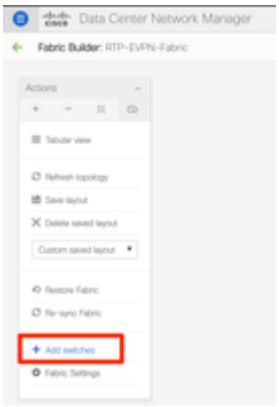


Étape 4. Dans la configuration Bootstrap, configurez la plage d'adresses DHCP que DCNM doit distribuer aux commutateurs du fabric pendant le processus POAP. Configurez également une passerelle par défaut appropriée (existante). Cliquez sur Save une fois que vous avez terminé et vous pouvez maintenant passer à l'ajout de commutateurs dans le fabric.



Ajout de commutateurs dans le fabric

Étape 1. Accédez à Control > Fabrics > Fabric Builder, puis sélectionnez votre Fabric. Dans le panneau de gauche, cliquez sur Add Switches, comme illustré dans l'image.



Vous pouvez détecter des commutateurs en utilisant une adresse IP de départ (ce qui signifie que l'adresse IP mgmt0 de chaque commutateur doit être configurée manuellement) ou vous pouvez détecter les commutateurs via POAP et demander à DCNM de configurer toutes les adresses IP mgmt0, la gestion VRF, etc. pour vous. Dans cet exemple, nous allons utiliser le protocole POAP.

Étape 2. Une fois que vous voyez le(s) commutateur(s) de votre intérêt, entrez l'adresse IP et le nom d'hôte souhaités que DCNM doit utiliser, entrez Admin PW, puis cliquez sur Bootstrap, comme indiqué dans l'image.



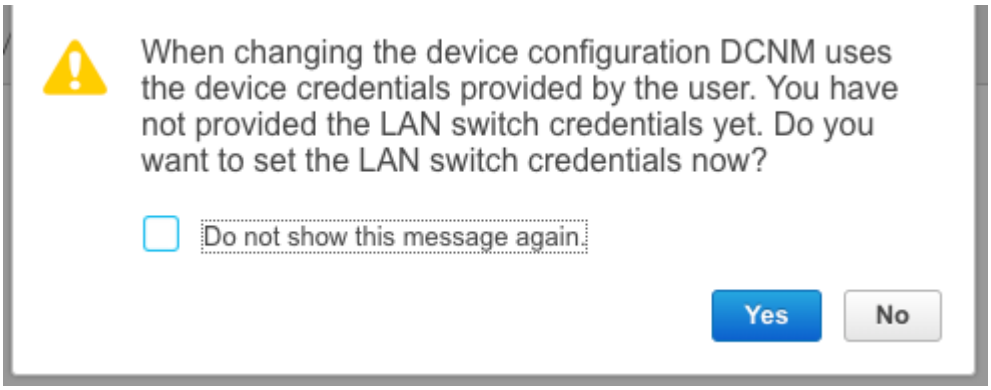
Un journal de démarrage réussi doit apparaître comme illustré dans l'image ci-contre à partir de la console du commutateur.

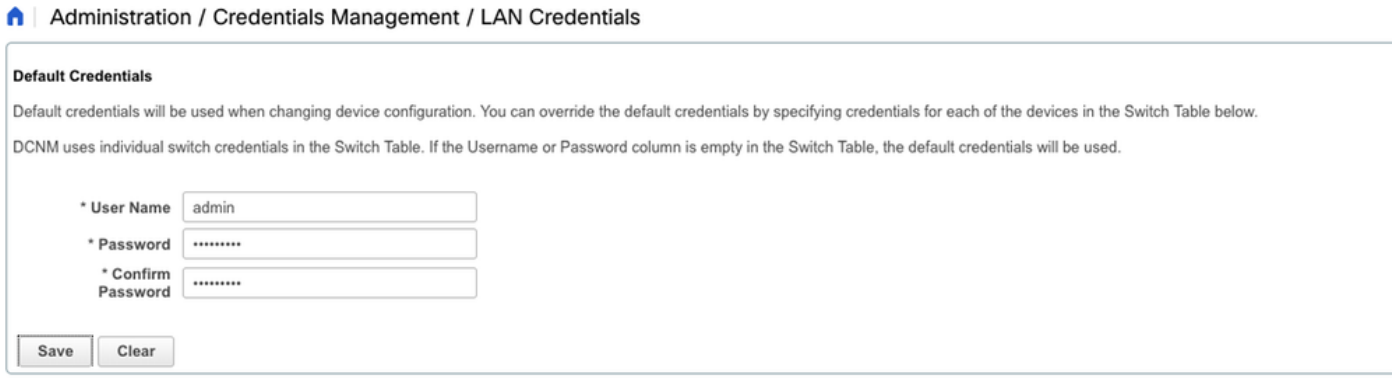
```
2019 Jun 19 14:58:51 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: [FDO21331SLK-70:7D:B9:4A:72:21] - POAP DHCP Discover
phase started
2019 Jun 19 14:59:12 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Start DHCP v4 session
2019 Jun 19 14:59:12 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: [FDO21331SLK-70:7D:B9:4A:72:21] - POAP DHCP Discover
phase started
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Using DHCP, information received over
mgmt0 from 192.168.128.57
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Assigned IP address: 192.168.128.102
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Netmask: 255.255.255.0
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - DNS Server: 64.102.6.247
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Default Gateway: 192.168.128.1
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Script Server: 192.168.128.56
2019 Jun 19 14:59:37 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Script Name: poap_dcnm.py
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Using DHCP, information received over
mgmt0 from 192.168.128.56
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Assigned IP address: 192.168.128.102
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Netmask: 255.255.255.0
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - DNS Server: 64.102.6.247
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Default Gateway: 192.168.128.1
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Script Server: 192.168.128.56
2019 Jun 19 14:59:38 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Script Name: poap_dcnm.py
2019 Jun 19 14:59:48 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - The POAP Script download has started
2019 Jun 19 14:59:48 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - The POAP Script is being downloaded
from [copy tftp://192.168.128.56/poap_dcnm.py bootflash:scripts/script.sh vrf management ]
2019 Jun 19 14:59:49 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_DOWNLOADED: [FDO21331SLK-70:7D:B9:4A:72:21] - Successfully downloaded
POAP script file
2019 Jun 19 14:59:49 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - Script file size 100623, MD5 checksum
d44d85cd6433a6efb6467faa17396933
2019 Jun 19 14:59:49 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO21331SLK-70:7D:B9:4A:72:21] - MD5 checksum received from the script
file is d44d85cd6433a6efb6467faa17396933
2019 Jun 19 14:59:49 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_STARTED_MD5_VALIDATED: [FDO21331SLK-70:7D:B9:4A:72:21] - POAP script
execution started(MD5 validated)
2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG:   - CLI : show license host-id - script.sh
2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG:   - INFO: Get serial number: FDO21331SLK - script.sh
2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO:device type is n9k - script.sh

2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO:device type is n9k - script.sh
2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO:device os version is  - script.sh
2019 Jun 19 14:59:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO: check free space - script.sh
2019 Jun 19 14:59:57 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO: free space is 34643592 kB - script.sh
2019 Jun 19 14:59:57 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - Get and set interface default  - script.sh
2019 Jun 19 14:59:57 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - CLI : show run | inc breakout - script.sh
2019 Jun 19 14:59:58 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - CLI : show run int | inc Ethernet - script.sh
2019 Jun 19 14:59:59 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO: Ready to copy protocol scp, host
192.168.128.56, source /var/lib/dcnm/dcnm-server-list.cfg vrf management user poap password ***** - script.sh
2019 Jun 19 14:59:59 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - CLI : terminal dont-ask ; terminal password ***** ;
copy scp://poap@192.168.128.56/var/lib/dcnm/dcnm-server-list.cfg dcnm-server-list.cfg vrf management - script.sh
2019 Jun 19 15:00:00 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO21331SLK] - INFO: Get Device Image Config File - script.sh
```

Étape 3. Avant de déployer la configuration pour l'ensemble du fabric, assurez-vous que vous avez préalablement configuré DCNM avec les informations d'identification du périphérique. Une fenêtre contextuelle aurait dû apparaître dans l'interface utilisateur graphique lorsque vous vous connectez. Dans le cas contraire, vous pouvez toujours y accéder via Administration > Credentials Management > LAN Credentials.

Remarque : Si les informations d'identification du périphérique sont manquantes, DCNM ne parvient pas à transmettre la configuration aux commutateurs.



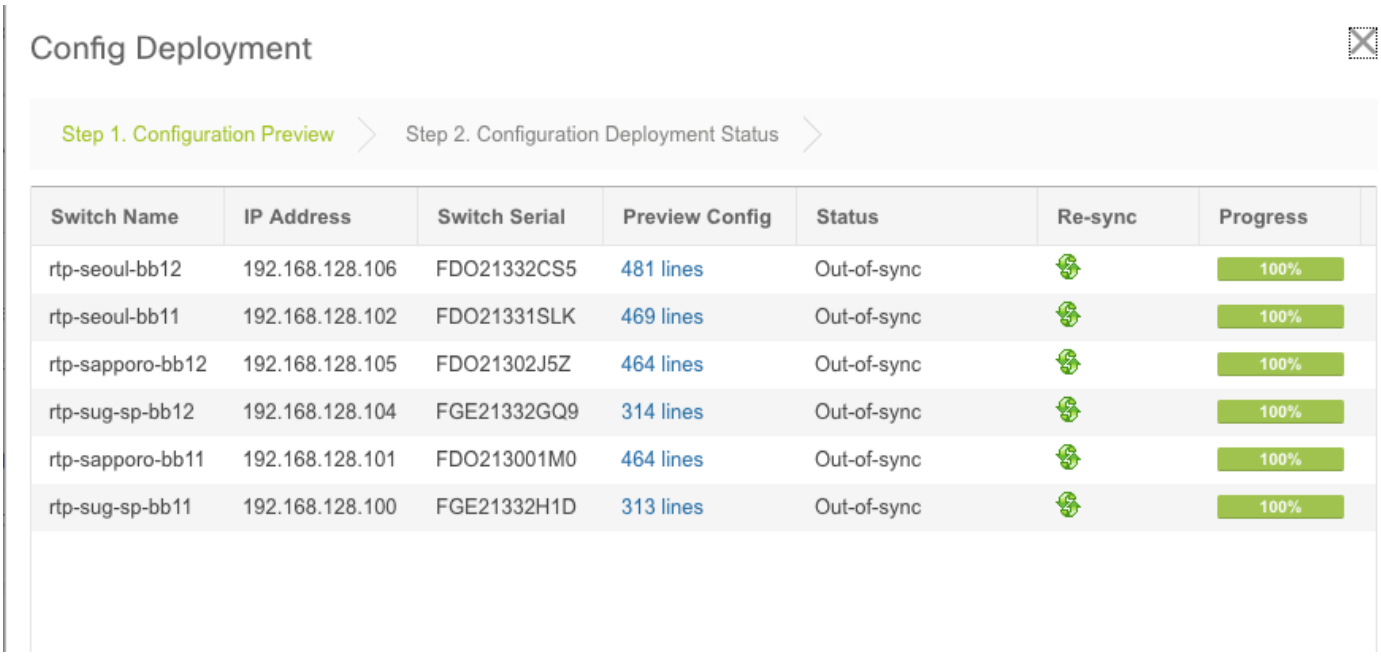


Déploiement de la configuration du fabric

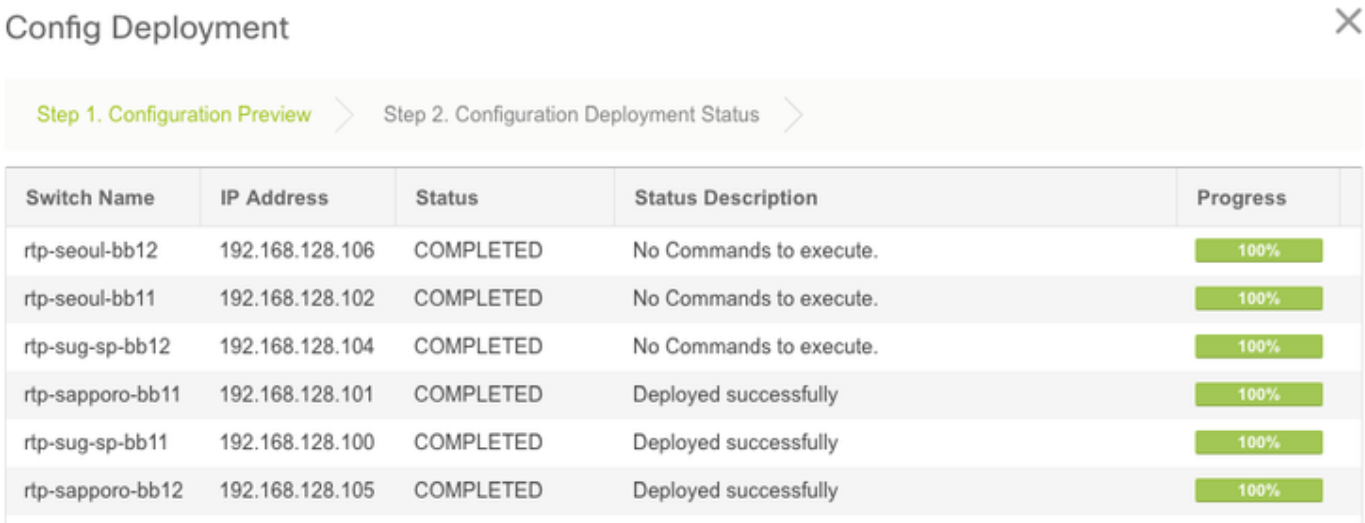
Étape 1. Une fois que vous avez découvert tous les commutateurs pour le fabric donné en suivant les mêmes étapes, accédez à Control > Fabrics > Fabric Builder > <votre fabric sélectionné>. Vous devriez voir vos commutateurs avec toutes leurs liaisons ici. Cliquez sur Enregistrer et déployer.



Étape 2. Dans la fenêtre Config Deployment, vous voyez combien de lignes de configuration pour chaque commutateur DCNM envoie. Vous pouvez également prévisualiser la configuration si vous le souhaitez et comparer les éléments avant et après :



Assurez-vous que tous les commutateurs sont à l'état TERMINÉ et 100 % exempts d'erreurs. En cas d'erreurs, veillez à les résoudre une par une (voir la section Problèmes rencontrés pendant ce déploiement pour obtenir des exemples)



Étape 3. (Facultatif) Vous pouvez vous connecter aux périphériques à ce stade et émettre n'importe quelle commande show run CLIs pour vérifier que la configuration a été correctement poussée par DCNM.

Exemple :

```
rtp-sug-sp-bb11# show run bgp


!Command: show running-config bgp
!Time: Wed Jun 19 17:28:37 2019


version 7.0(3)I7(5) Bios:version 08.34
feature bgp


router bgp 65534
  router-id 10.1.0.11
  neighbor 10.1.0.7
    remote-as 65534
    update-source loopback0
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
  neighbor 10.1.0.8
    remote-as 65534
    update-source loopback0
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
  neighbor 10.1.0.9
    remote-as 65534
    update-source loopback0
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
  neighbor 10.1.0.10
    remote-as 65534
    update-source loopback0
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
```

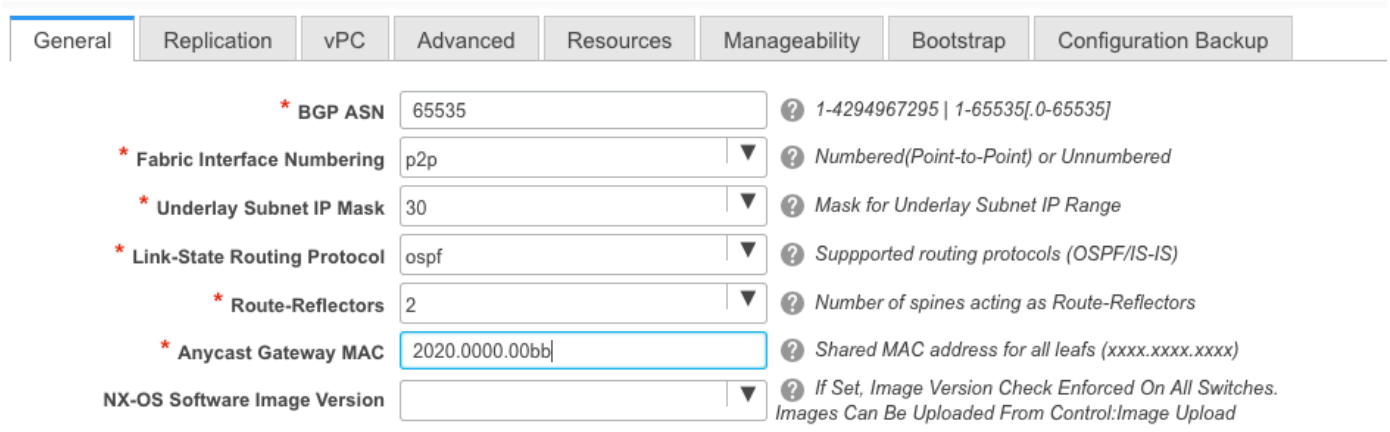
Déployer le deuxième fabric : SJ

Effectuez les mêmes étapes que précédemment avec le fabric RTP en utilisant des valeurs différentes pour BGP AS, etc.

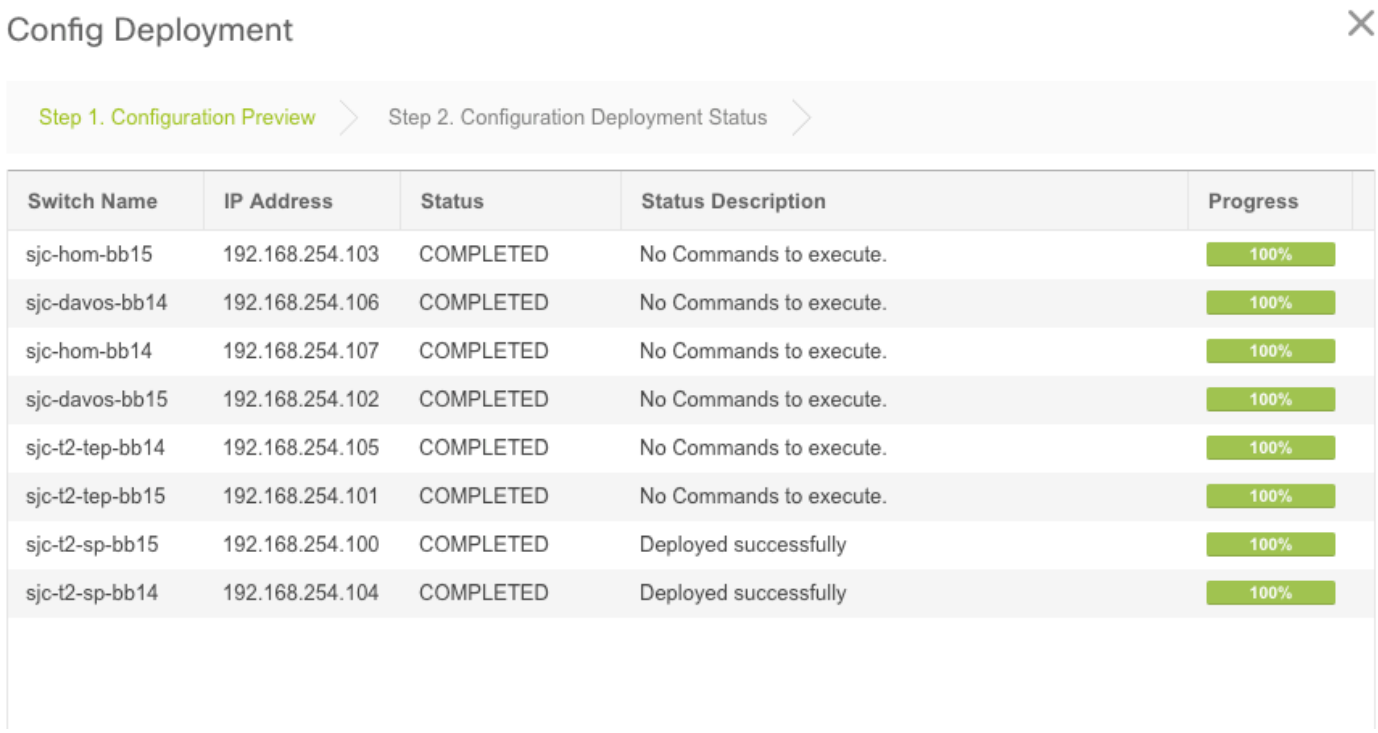
Étape 1. Accédez à Control > Fabrics > Fabric Builder > Create Fabric > Name it !

Cette section couvre tous les paramètres de sous-couche, de superposition, vPC, de réplication, etc. requis. Cela dépend du schéma d'adressage réseau, des exigences, etc.

Remarque : L'adresse MAC Anycast Gateway ici doit correspondre à celle de l'autre fabric si Multi-Site est utilisé. Par la suite, des adresses MAC Anycast Gateway différentes ne sont pas prises en charge. Cette erreur a été corrigée ultérieurement dans la section Déploiement multisite (non indiquée dans l'article pour des raisons de concision).

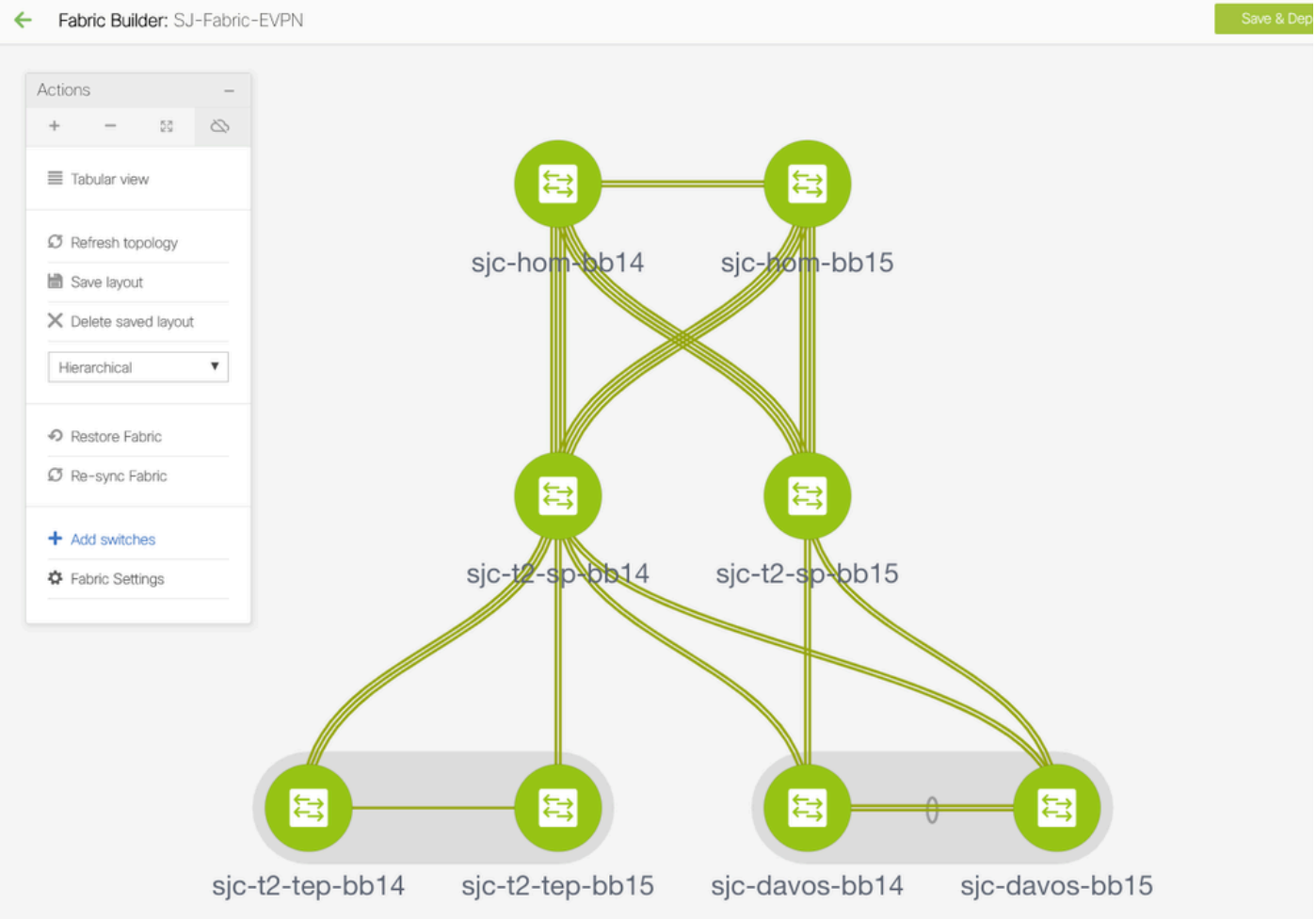


Étape 2. Configurez la section Bootstrap comme indiqué précédemment. Naviguez à nouveau dans Ajouter des commutateurs. Une fois tous les éléments détectés, cliquez sur Save & Deploy pour déployer la configuration. Tout ceci a été traité dans la section RTP Fabric Deployment (omission ici pour des raisons de concision).

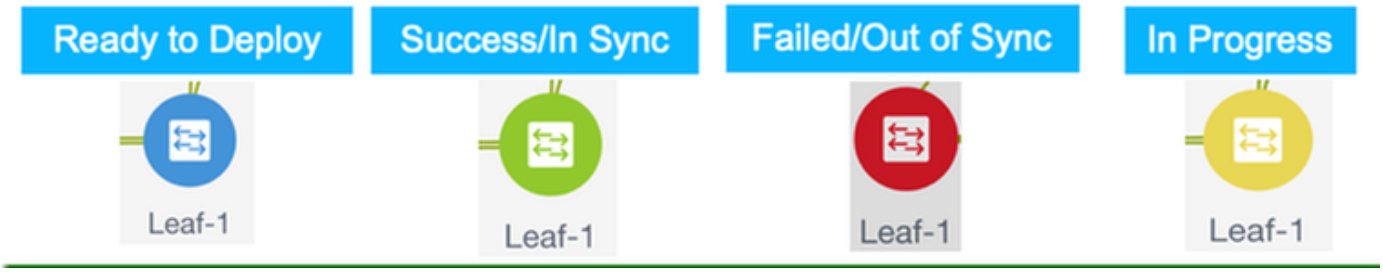


Switch Name	IP Address	Status	Status Description	Progress
sjc-hom-bb15	192.168.254.103	COMPLETED	No Commands to execute.	100%
sjc-davos-bb14	192.168.254.106	COMPLETED	No Commands to execute.	100%
sjc-hom-bb14	192.168.254.107	COMPLETED	No Commands to execute.	100%
sjc-davos-bb15	192.168.254.102	COMPLETED	No Commands to execute.	100%
sjc-t2-tep-bb14	192.168.254.105	COMPLETED	No Commands to execute.	100%
sjc-t2-tep-bb15	192.168.254.101	COMPLETED	No Commands to execute.	100%
sjc-t2-sp-bb15	192.168.254.100	COMPLETED	Deployed successfully	100%
sjc-t2-sp-bb14	192.168.254.104	COMPLETED	Deployed successfully	100%

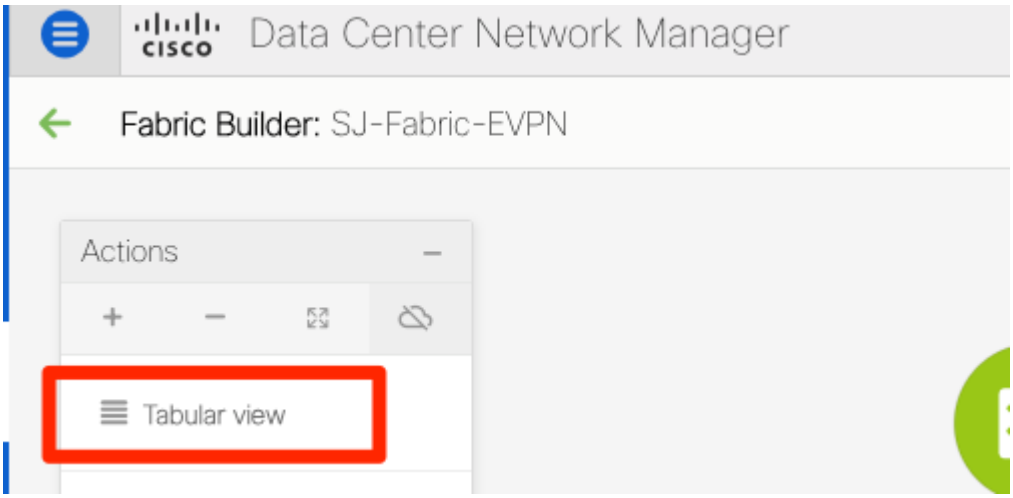
Topologie du point de vue de Fabric Builder à la fin.



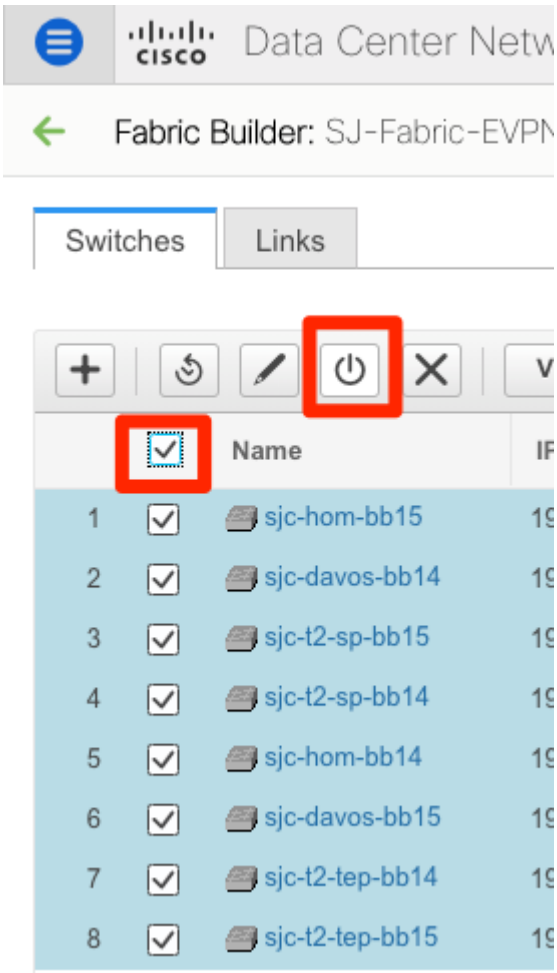
Idéalement, tous les commutateurs doivent apparaître en vert avec leurs liaisons. Cette image montre les différentes couleurs d'état dans la moyenne DCNM.



Étape 3. Une fois les deux fabrics configurés et déployés, veillez à enregistrer la configuration et le rechargement pour que les modifications TCAM prennent effet. Accédez à Contrôles > Fabrics > Fabric Builder > <votre Fabric>, accédez à Vue tabulaire, comme illustré dans l'image.

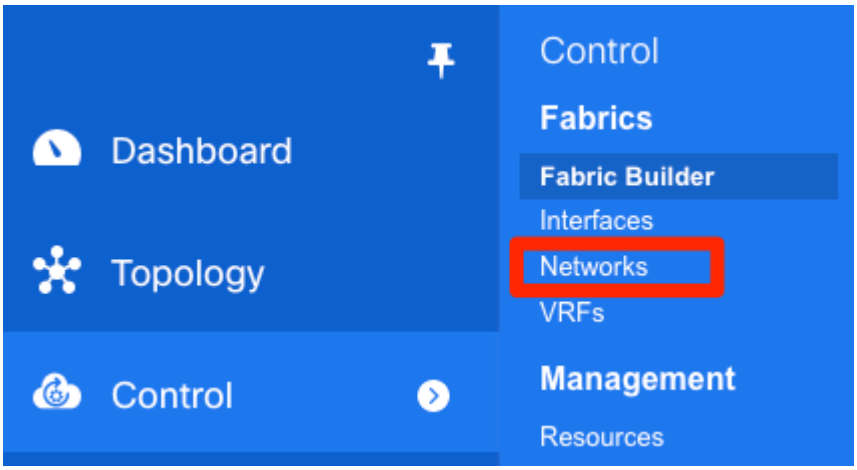


Étape 4. Cliquez ensuite sur le bouton d'alimentation (cela recharge tous vos commutateurs simultanément) :

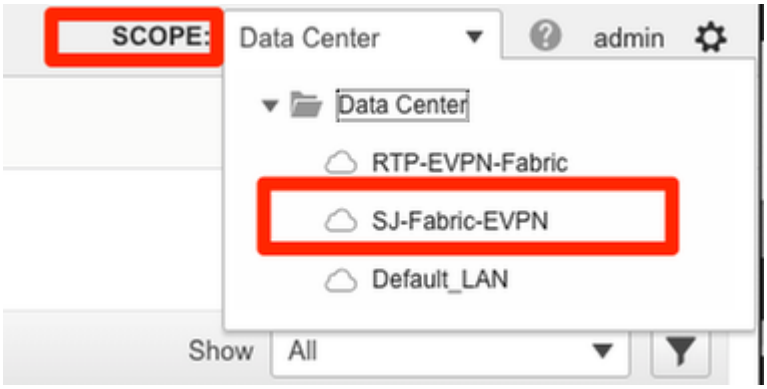


Créer un réseau (VLAN/L2VNI) et des VRF (L3VNI)

Étape 1. Accédez à Control > Fabrics > Networks, comme indiqué dans l'image.



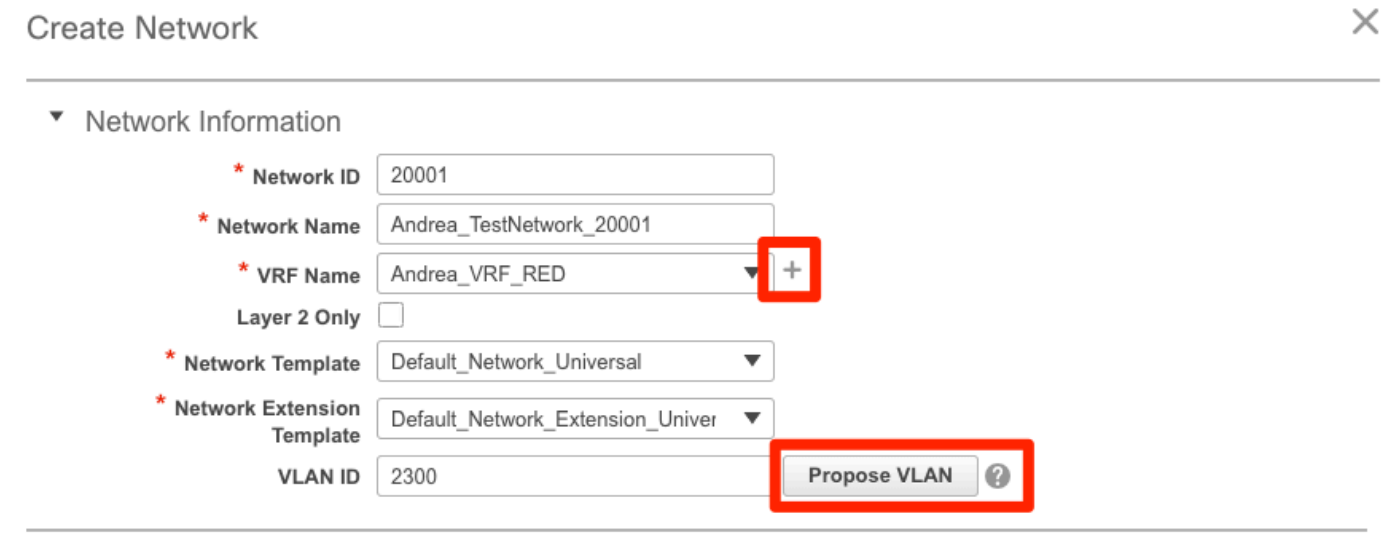
Étape 2. Comme le montre l'image, sélectionnez l'étendue de la modification. À quel fabric cette configuration doit-elle être appliquée ?

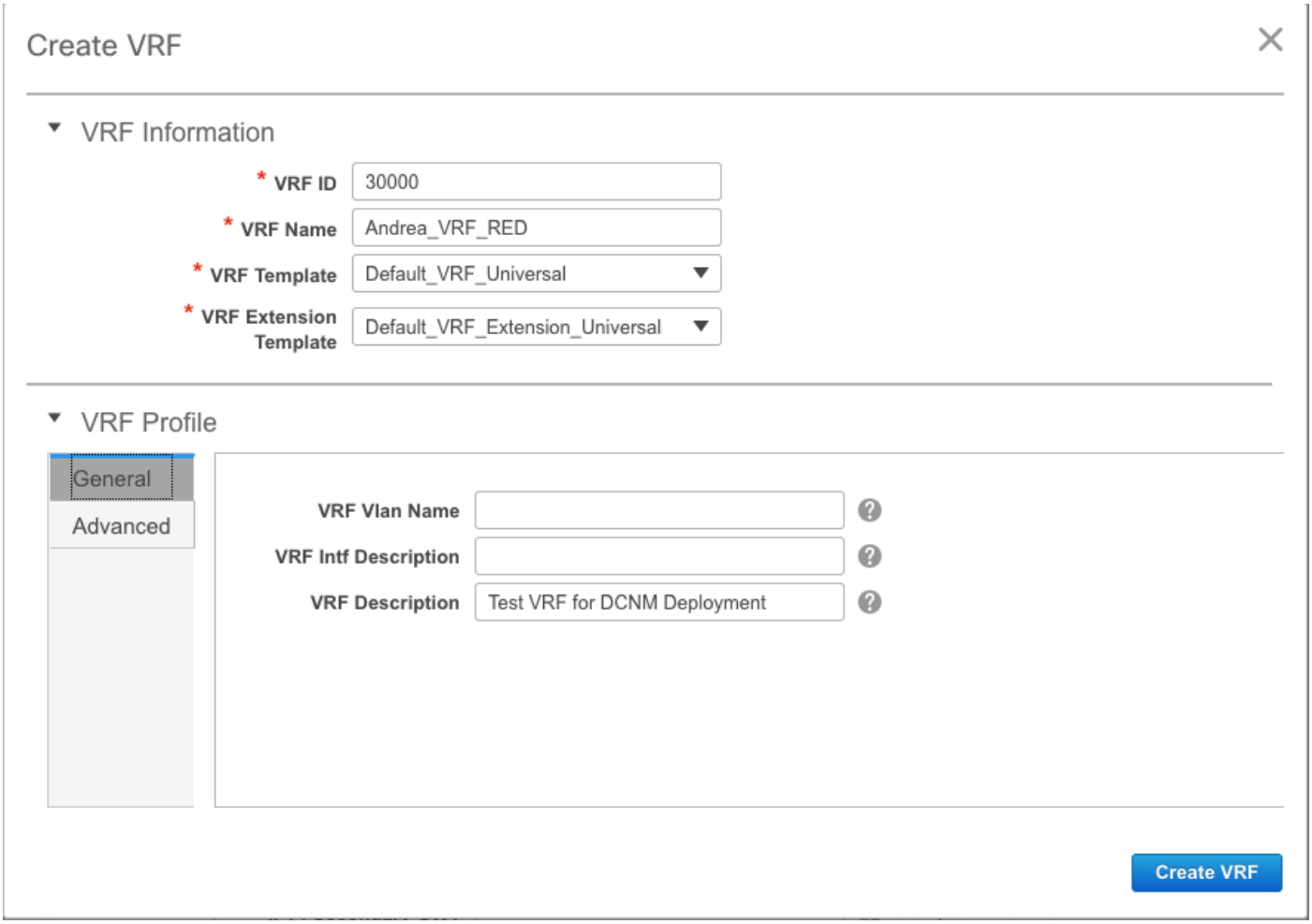


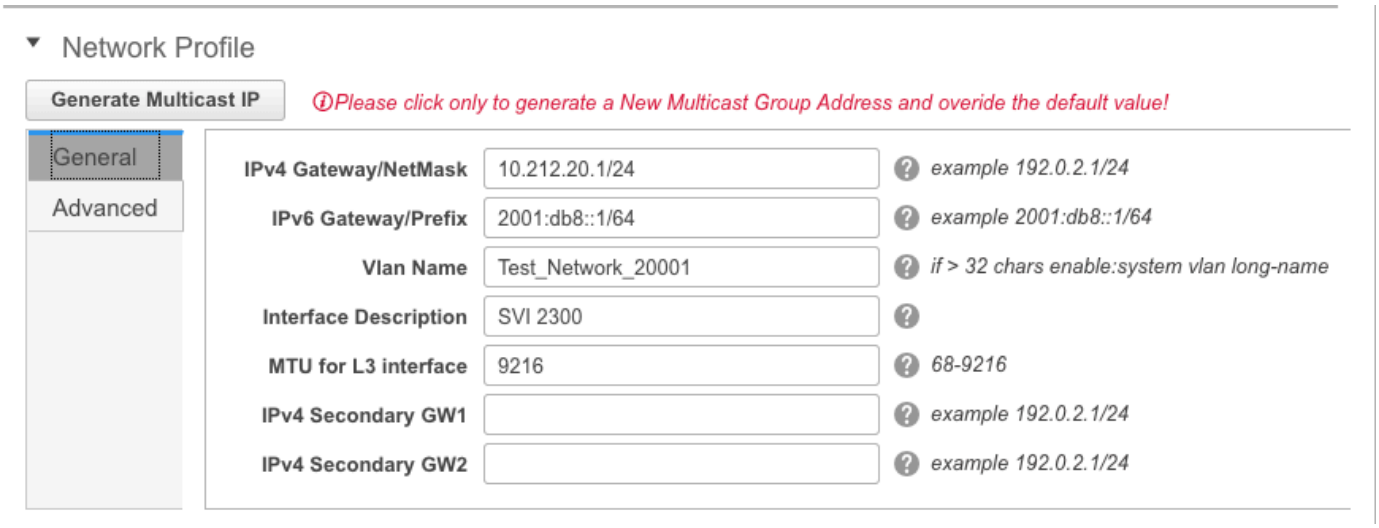
Étape 3. Cliquez sur le signe +, comme illustré dans l'image.



Étape 4. DCNM vous guide tout au long du processus de création de l'interface virtuelle de commutateur (SVI) (ou VLAN L2 pur). Si aucun VRF n'est créé à ce stade, cliquez à nouveau sur le bouton + et cela vous amène temporairement à la visite des VRF avant d'aller de l'avant avec les paramètres SVI.


Create Network
Network Information
* Network ID
20001
* Network Name
Andrea_TestNetwork_20001
* VRF Name
Andrea_VRF_RED
Layer 2 Only
* Network Template
Default_Network_Universal
* Network Extension Template
Default_Network_Extension_Univer
VLAN ID
2300
Propose VLAN


Create VRF
VRF Information
* VRF ID
30000
* VRF Name
Andrea_VRF_RED
* VRF Template
Default_VRF_Universal
* VRF Extension Template
Default_VRF_Extension_Universal
VRF Profile
General
Advanced
VRF Vlan Name
VRF Intf Description
VRF Description
Test VRF for DCNM Deployment
Create VRF



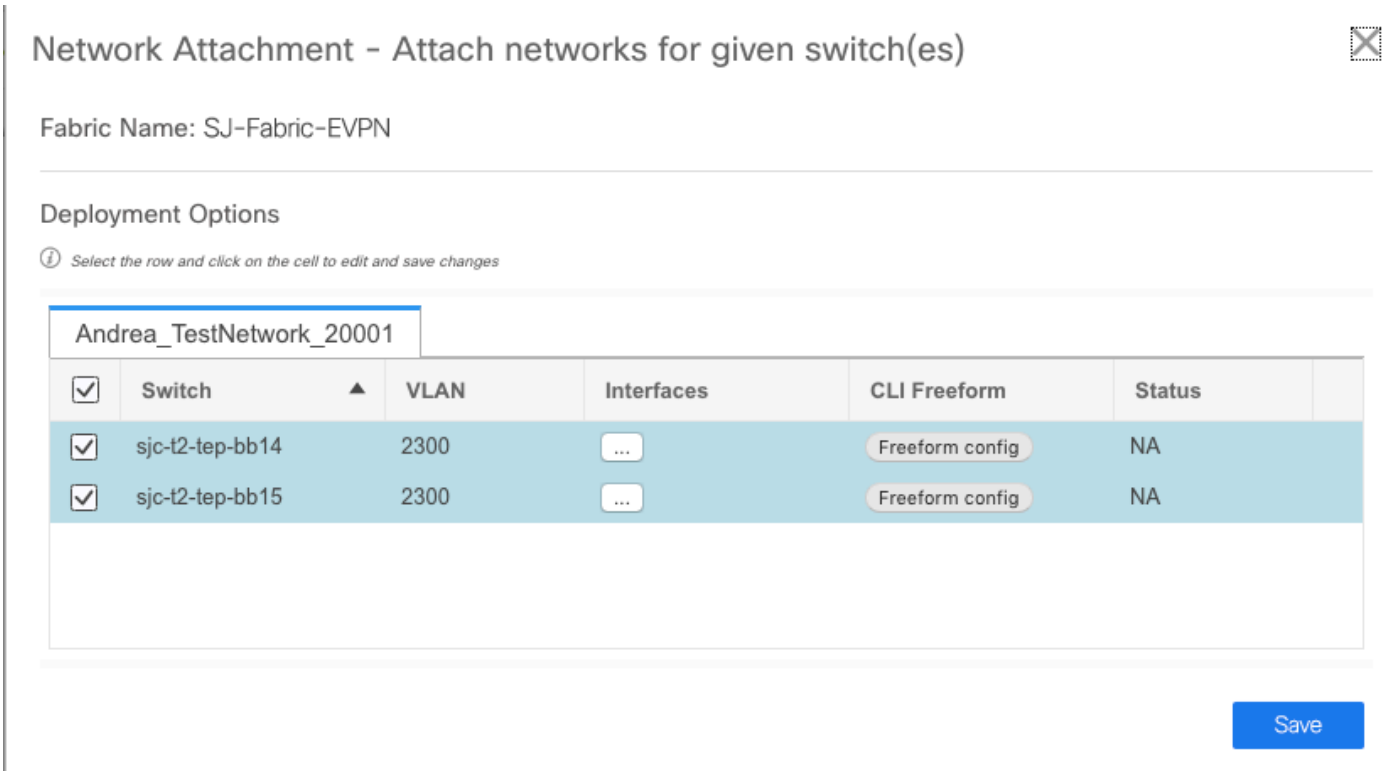
Ces fonctionnalités peuvent être configurées sous l'onglet Advanced :

- Suppression ARP
- Réplication entrante
- Groupe multidiffusion
- DCHP
- Balises de routage
- TRM
- VNI L2 Route-Target
- Activer la passerelle L3 en limite

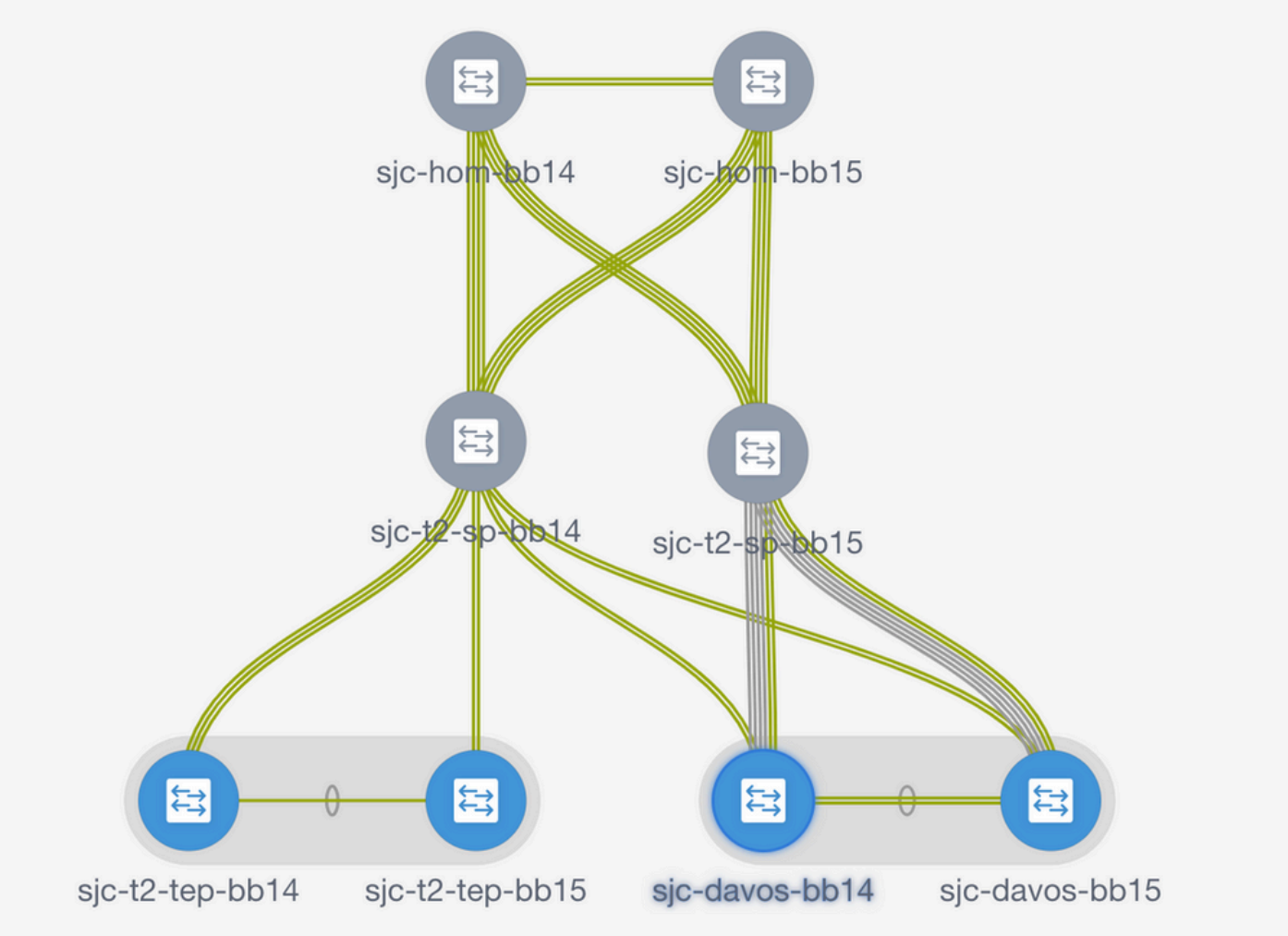
Étape 5. Cliquez sur Continue pour déployer la configuration Network/VRF.

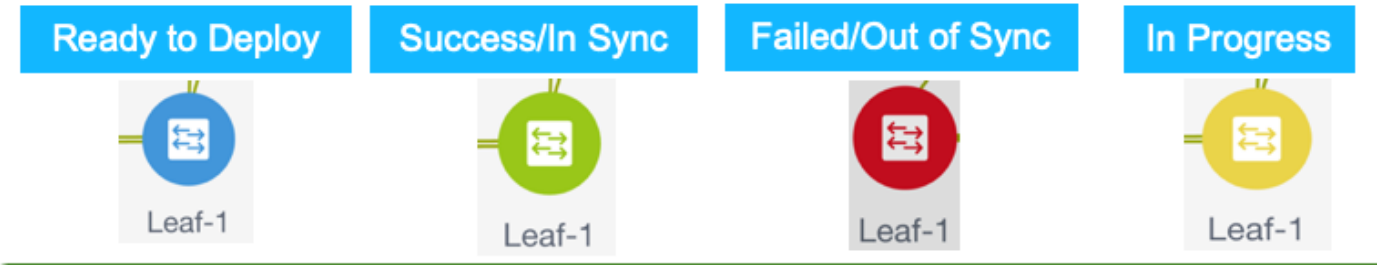


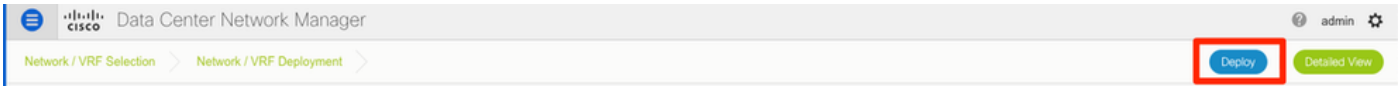
Étape 6. Double-cliquez sur un ou plusieurs périphériques dans la vue topologique (DCNM vous y emmène automatiquement) pour les sélectionner en fonction de la configuration applicable. Cliquez sur Save, comme le montre l'image.



Étape 7. Une fois sélectionnés, les commutateurs doivent apparaître en bleu (prêts à être déployés), comme illustré dans cette image.







Remarque : si vous souhaitez vérifier la configuration de l'interface de ligne de commande avant le déploiement, vous pouvez cliquer sur Vue détaillée au lieu de Déployer et cliquer sur Aperçu sur l'écran suivant.

Les commutateurs deviennent jaunes lorsque la configuration est appliquée et redeviennent verts une fois qu'elle est terminée.

Étape 8. (Facultatif) Vous pouvez vous connecter à l'interface de ligne de commande pour vérifier la configuration si nécessaire (n'oubliez pas d'utiliser l'option expand-port-profile) :

```
sjc-davos-bb14# show nve peers
Interface Peer-IP          State LearnType Uptime   Router-Mac
--------- ---------------  ----- --------- -------- -----------------
nve1      10.2.0.16        Up    CP        00:00:34 00f6.638e.4fd5

sjc-davos-bb14# show nve vni
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured         SA - Suppress ARP
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication
Interface VNI      Multicast-group   State Mode Type [BD/VRF]      Flags
--------- -------- ----------------- ----- ---- ------------------ -----
nve1      20001    239.2.2.0         Up    CP   L2 [2300]
nve1      30000    n/a               Up    CP   L3 [andrea_vrf_red]

sjc-davos-bb14# show nve vrf andrea_vrf_red
VRF-Name     VNI        Interface Gateway-MAC
------------ ---------- --------- -----------------
andrea_vrf_red 30000      nve1      707d.b987.11a3

sjc-davos-bb14# show run int vlan 2300 expand-port-profile


!Command: show running-config interface Vlan2300 expand-port-profile
!Running configuration last done at: Mon Jun 24 15:07:05 2019
!Time: Mon Jun 24 15:08:13 2019


version 9.2(3) Bios:version 07.61

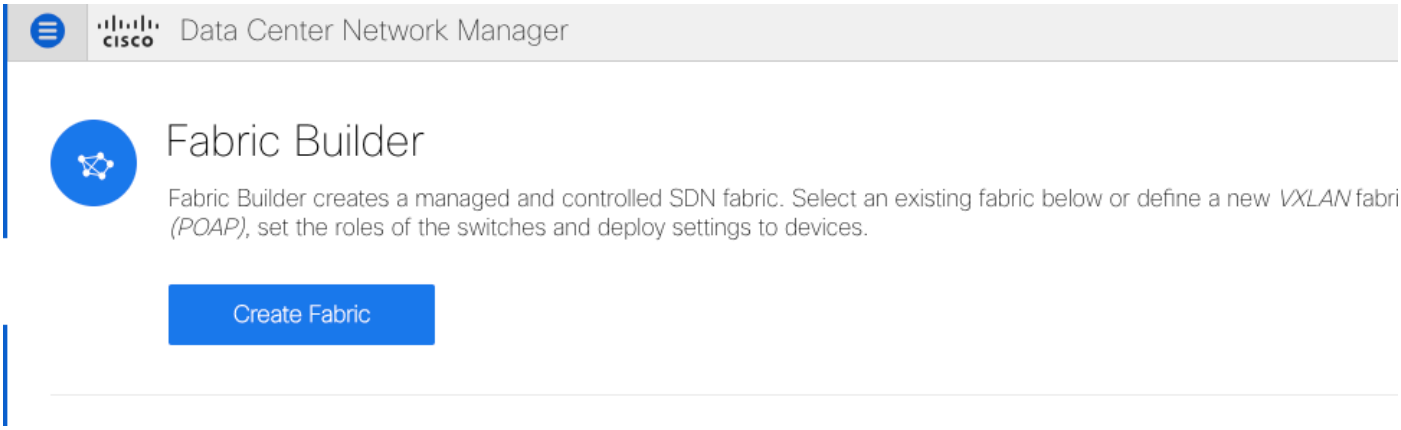

interface Vlan2300
  description SVI 2300
  no shutdown
  mtu 9216
  vrf member andrea_vrf_red
  no ip redirects
  ip address 10.212.20.1/24 tag 12345
  ipv6 address 2001:db8::1/64 tag 12345
  no ipv6 redirects
  fabric forwarding mode anycast-gateway

sjc-davos-bb14# show nve interface nve 1 detail
Interface: nve1, State: Up, encapsulation: VXLAN
VPC Capability: VPC-VIP-Only [notified]
Local Router MAC: 707d.b987.11a3
Host Learning Mode: Control-Plane
Source-Interface: loopback1 (primary: 10.2.0.14, secondary: 10.2.0.15)
Source Interface State: Up
Virtual RMAC Advertisement: No
NVE Flags:
Interface Handle: 0x49000001
Source Interface hold-down-time: 180
Source Interface hold-up-time: 30
Remaining hold-down time: 0 seconds
Virtual Router MAC: 0200.0a02.000f
Interface state: nve-intf-add-complete
```

Configuration multisite

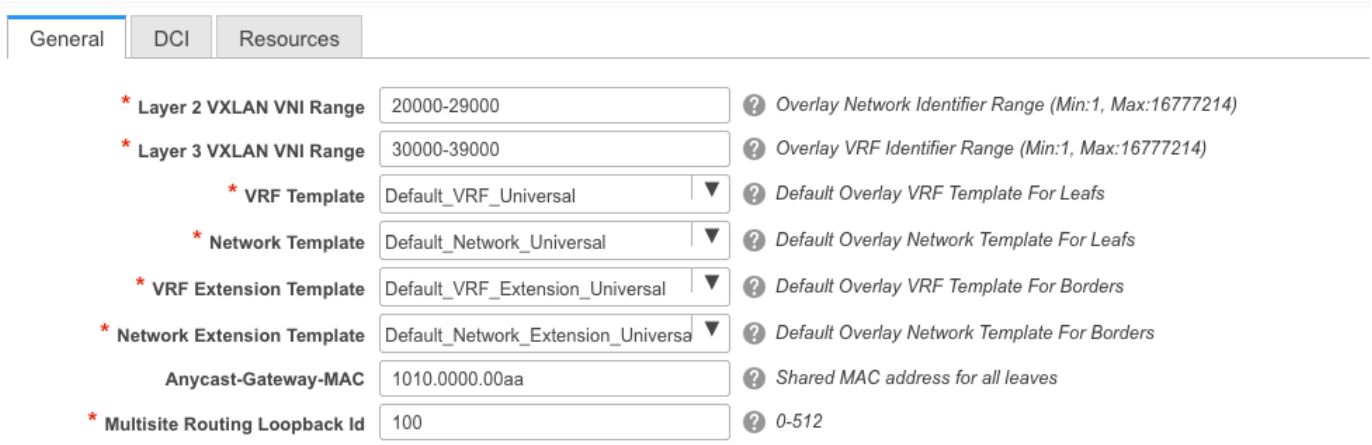
Pour ce déploiement Greenfield, le fabric MSD est déployé via l'appairage direct entre les passerelles de périphérie (BGW). Une alternative consiste à utiliser un serveur de routage centralisé, non traité dans ce document.

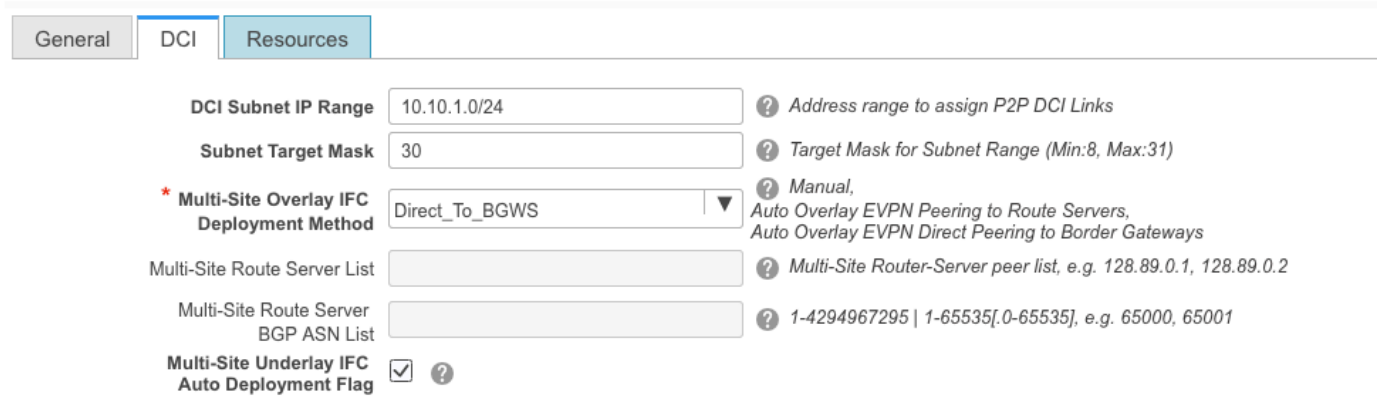
Étape 1. Accédez à Control > Fabric Builder > Create Fabric, comme indiqué dans l'image.



Étape 2. Attribuez un nom à votre fabric multisite et choisissez MSD_Fabric_11_1 dans la liste déroulante Modèle de fabric.

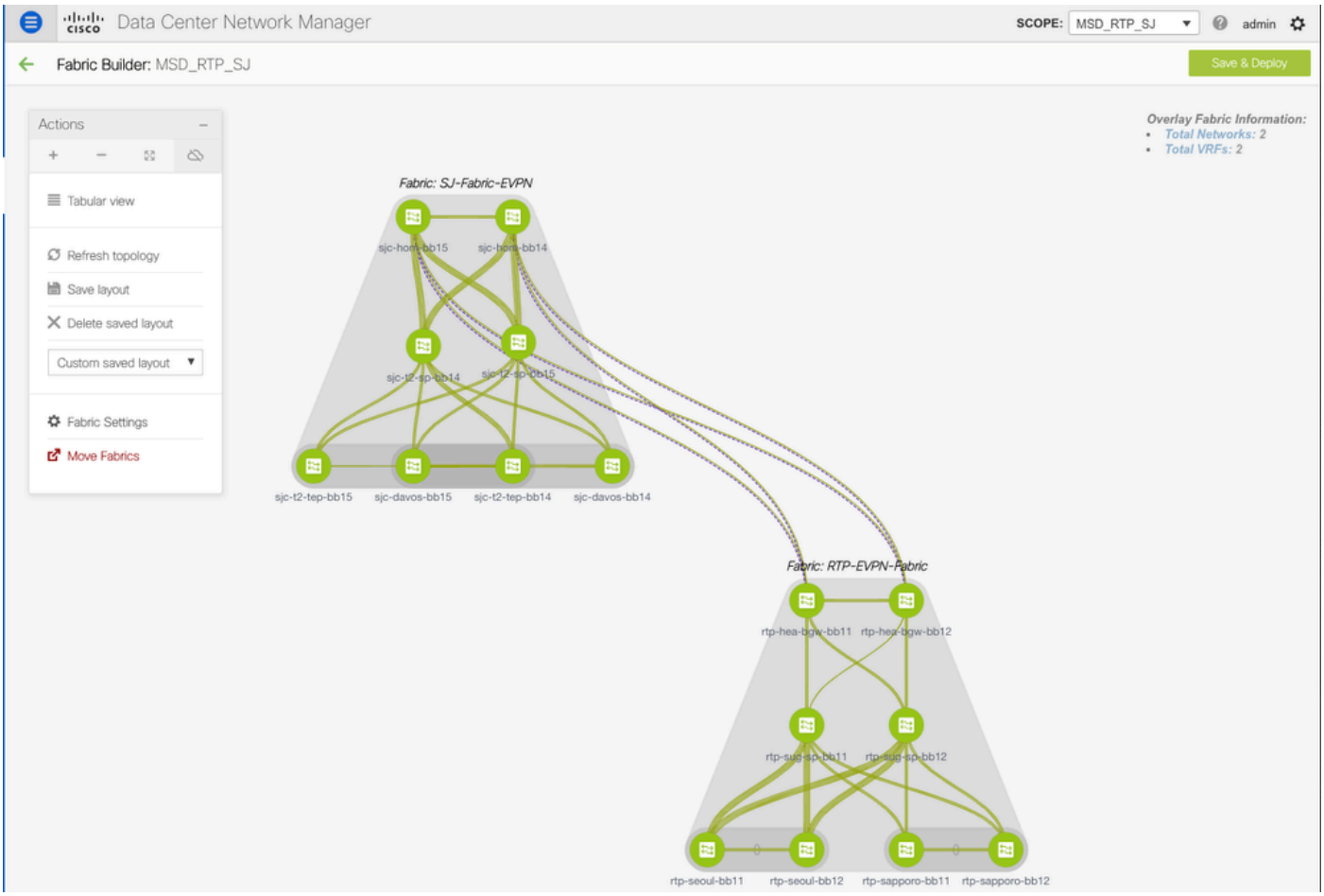
Étape 3. Sous Général, vérifiez que votre gamme VNI L2 et L3 correspond à ce que vos fabrics individuels utilisent. En outre, l'adresse MAC de la passerelle Anycast doit correspondre sur les deux fabrics (RTP/SJ dans cet exemple). DCNM vous signale une erreur si les adresses MAC de la passerelle ne correspondent pas et qu'il est nécessaire de la corriger avant de poursuivre le déploiement de MSD.







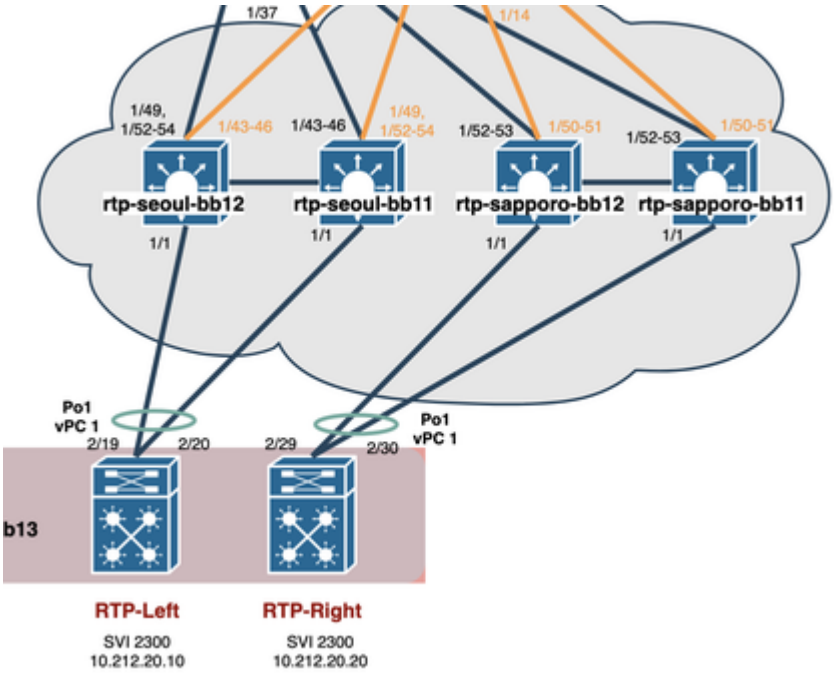
Étape 4. Cliquez sur Save, puis accédez à MSD Fabric et cliquez sur Save & Deploy. Votre topologie devrait ressembler à celles-ci (tous les commutateurs + liaisons en vert) une fois terminée :



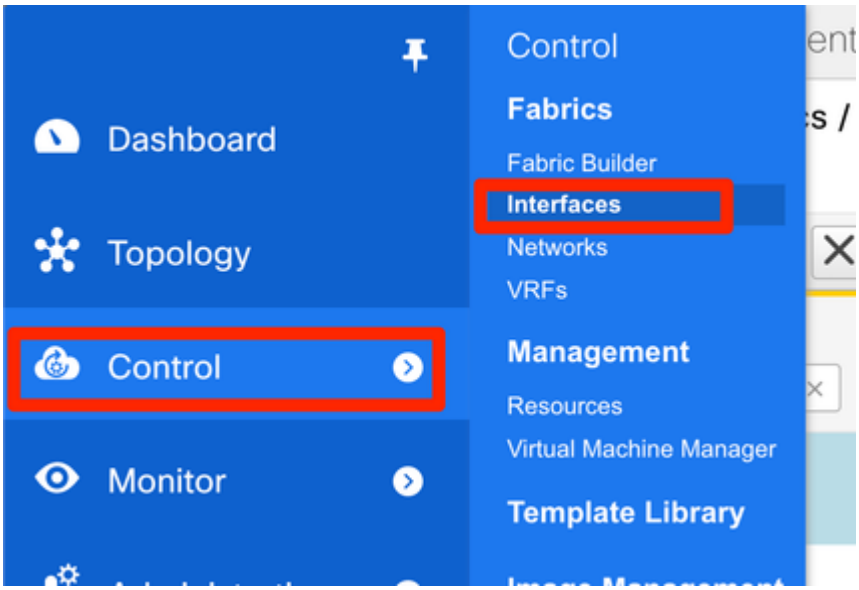
Do not forget to re-deploy any Networks/VRFs across both fabrics + the MSD Fabric!

Déployer des politiques d'accès/trunk hôte

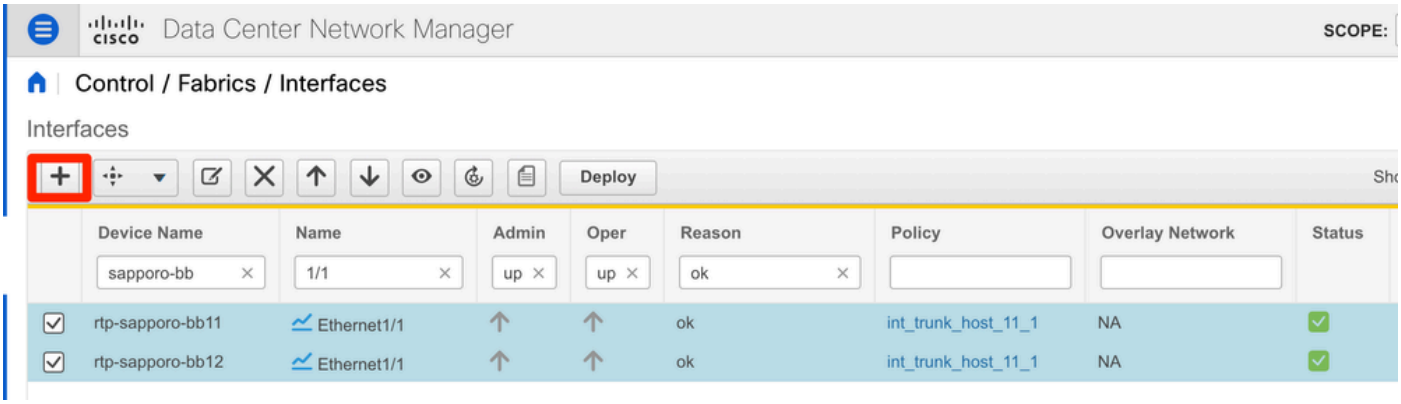
Dans cet exemple, les agrégations vPC de deux paires VTEP différentes sont configurées et testent la connectivité au sein du fabric RTP local. Topologie appropriée, comme illustré dans l'image :



Étape 1. Accédez à Control > Fabrics > Interfaces, comme indiqué dans l'image.

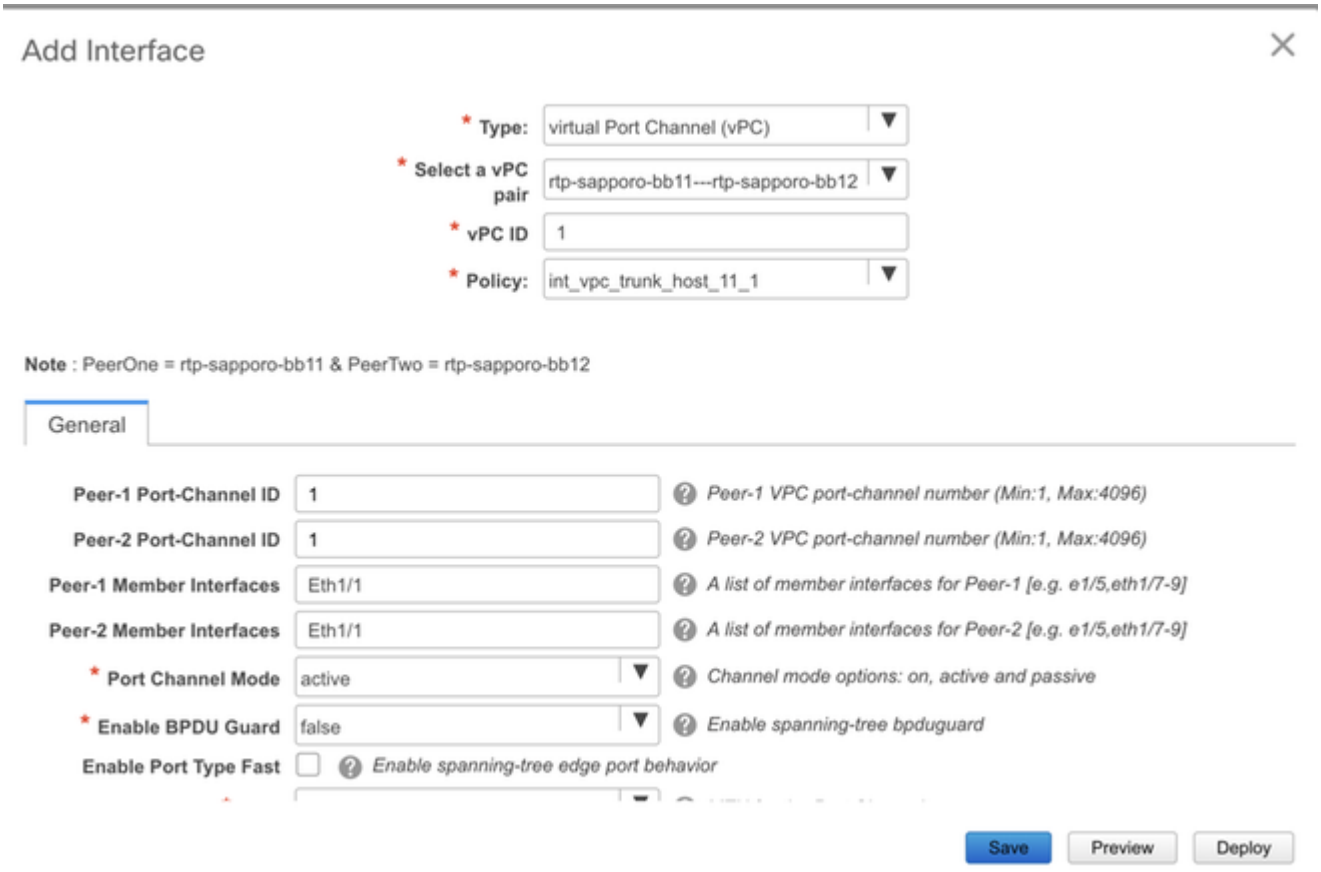


Étape 2. Cliquez sur le signe + pour accéder à l'Assistant Ajout d'une interface, comme illustré dans l'image.



Dans cet exemple, une agrégation vPC est créée en aval du N7K qui est utilisé pour envoyer une requête ping aux tests de cette procédure pas à pas.

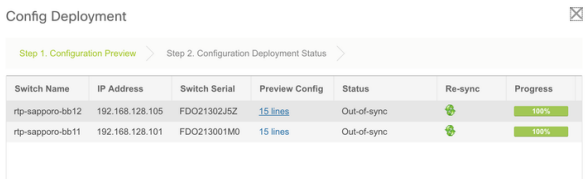
Étape 3. Sélectionnez la paire vPC appropriée, les interfaces physiques, l'activation/désactivation LACP, BPDUGuard, etc.



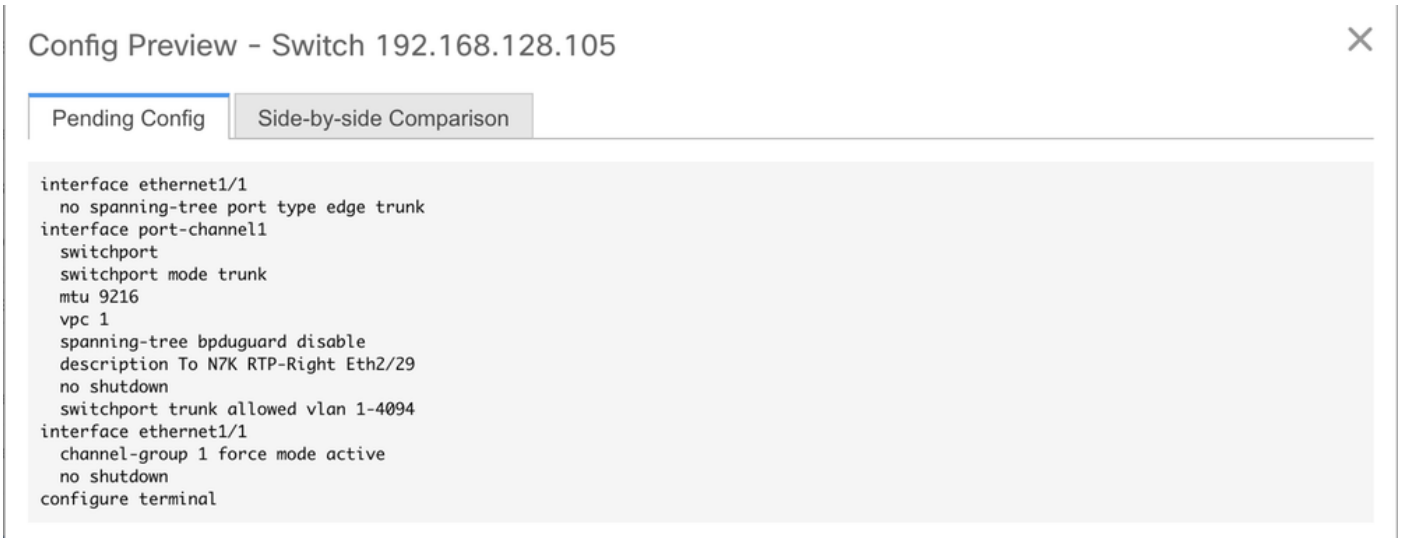


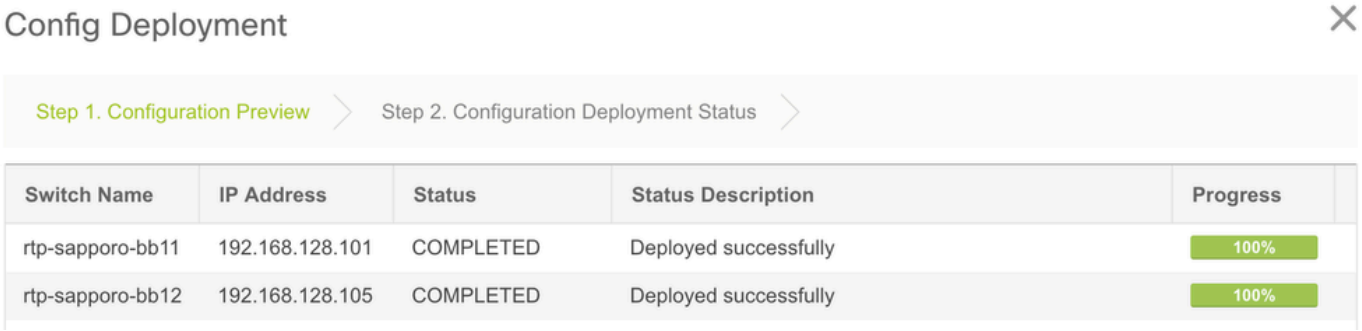
Étape 4. Cliquez sur Save lorsque vous avez terminé. Vous pouvez également effectuer un déploiement direct, comme illustré dans l'image.





Étape 5. (Facultatif) Vérifiez la configuration à appliquer.





Étape 6. (Facultatif) Configuration manuelle sur 7K :

```
RTP-Right# show run interface port-channel 1 membership


!Command: show running-config interface port-channel1 membership
!Running configuration last done at: Mon Sep  9 17:29:39 2019
!Time: Mon Sep  9 17:33:01 2019


version 8.2(4)


interface port-channel1
  switchport
  switchport mode trunk


interface Ethernet2/29
  description vPC from sapporo-bb11/12 eth1/1
  switchport
  switchport mode trunk
  channel-group 1 mode active
  no shutdown


interface Ethernet2/30
  description vPC from sapporo-bb11/12 eth1/1
  switchport
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

RTP-Right# show port-channel summary interface po1
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth2/29(P)   Eth2/30(P)
```

Étape 7.(Facultatif) Création d'une interface SVI de test sur N7K pour envoyer une requête ping aux VTEP dans RTP (les VTEP ont Anycast Gateway de 10.212.20.1 dans VRF andrea_red) :

```
RTP-Right# show run interface vlan 2300


!Command: show running-config interface Vlan2300
!Running configuration last done at: Mon Sep  9 17:41:10 2019
!Time: Mon Sep  9 17:44:30 2019


version 8.2(4)


interface Vlan2300
  description VRF Andrea_Red in TEPs
  no shutdown
  no ip redirects
  ip address 10.212.20.20/24
  no ipv6 redirects


RTP-Right# ping 10.212.20.1
PING 10.212.20.1 (10.212.20.1): 56 data bytes
64 bytes from 10.212.20.1: icmp_seq=0 ttl=254 time=1.235 ms
64 bytes from 10.212.20.1: icmp_seq=1 ttl=254 time=0.832 ms
64 bytes from 10.212.20.1: icmp_seq=2 ttl=254 time=0.819 ms
64 bytes from 10.212.20.1: icmp_seq=3 ttl=254 time=0.81 ms
64 bytes from 10.212.20.1: icmp_seq=4 ttl=254 time=0.828 ms


--- 10.212.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.81/0.904/1.235 ms
```

Étape 8. (Facultatif) Vérifiez que les autres VTEP du protocole RTP voient cet hôte via EVPN/HMM :

```
rtp-seoul-bb12# show bgp l2vpn evpn 10.212.20.20 vrf andrea_vrf_red
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 10.1.0.10:35067    (L2VNI 20001)
BGP routing table entry for [2]:[0]:[0]:[48]:[002a.6a5c.6045]:[32]:[10.212.20.20]/272, version 168
Paths: (2 available, best #1)
Flags: (0x000212) (high32 00000000) on xmit-list, is in l2rib/evpn, is not in HW


  Advertised path-id 1
  Path type: internal, path is valid, is best path, in rib
            Imported from 10.1.0.13:35067:[2]:[0]:[0]:[48]:[002a.6a5c.6045]:[32]:[10.212.20.20]/272
  AS-Path: NONE, path sourced internal to AS
    10.1.0.1 (metric 6) from 10.1.0.11 (10.1.0.11)
      Origin IGP, MED not set, localpref 100, weight 0
      Received label 20001 30000
      Extcommunity: RT:65534:20001 RT:65534:30000 SOO:10.1.0.1:0 ENCAP:8
          Router MAC:3890.a5eb.05cf
      Originator: 10.1.0.13 Cluster list: 10.1.0.11
```

Étape 9.(Facultatif) Répétez la même procédure pour seoul-bb11/12 (create vPC port-channel, create SVI 2300). Envoi d'une requête ping de RTP-Left à RTP-Right pour confirmer la connectivité de couche 2 sur EVPN dans le fabric RTP :

```
RTP-Left# ping 10.212.20.20
PING 10.212.20.20 (10.212.20.20): 56 data bytes
64 bytes from 10.212.20.20: icmp_seq=0 ttl=254 time=1.385 ms
64 bytes from 10.212.20.20: icmp_seq=1 ttl=254 time=1.03 ms
64 bytes from 10.212.20.20: icmp_seq=2 ttl=254 time=0.98 ms
64 bytes from 10.212.20.20: icmp_seq=3 ttl=254 time=0.997 ms
64 bytes from 10.212.20.20: icmp_seq=4 ttl=254 time=0.974 ms

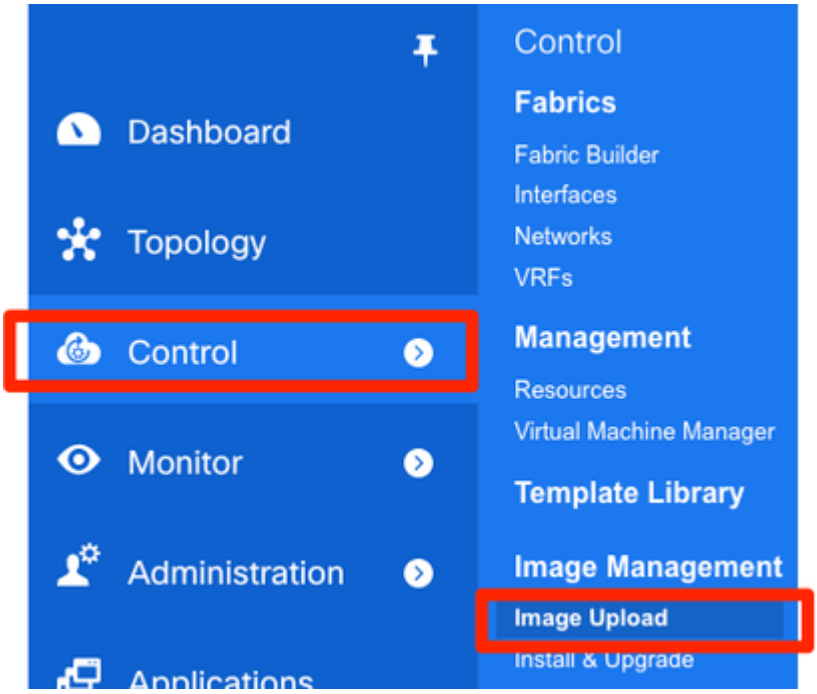

--- 10.212.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.974/1.073/1.385 ms
```

Des étapes similaires peuvent être suivies pour créer des canaux de port non-vPC, des interfaces d'accès, etc. dans le contexte Ajouter des interfaces.

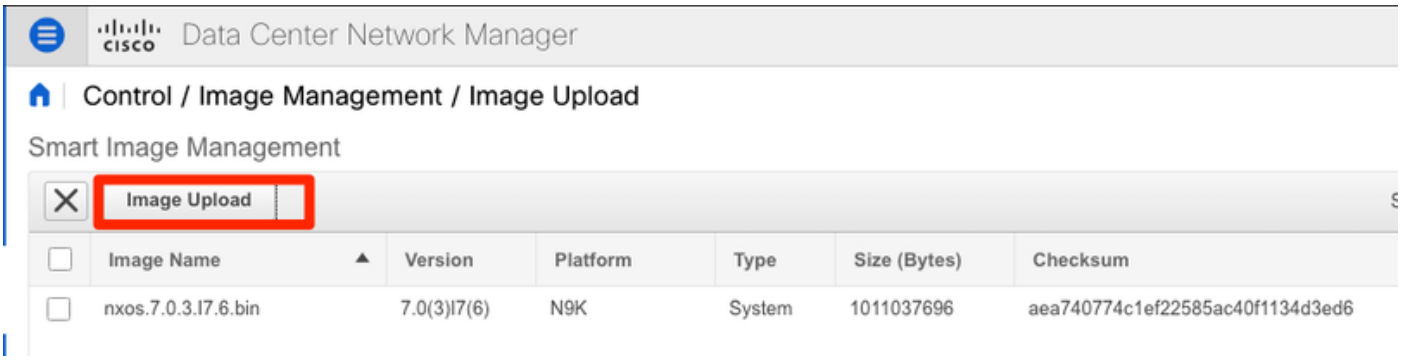
Opérations du jour 2

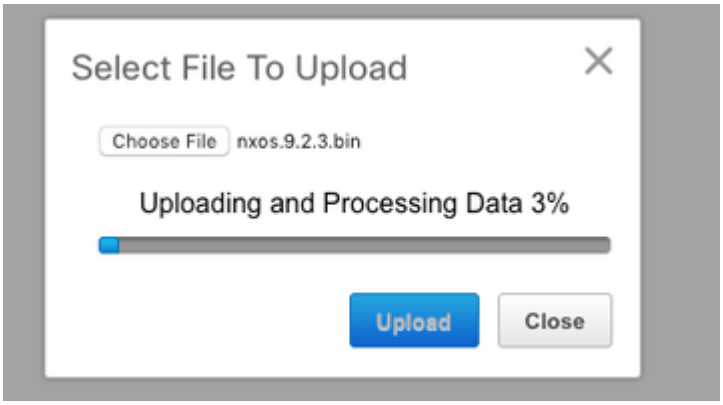
Mise à niveau du logiciel NX-OS via DCNM

Étape 1. Téléchargez une image (ou un ensemble d'images sur le serveur de DCNM), puis accédez à Control > Image Management > Image Upload, comme indiqué dans l'image.

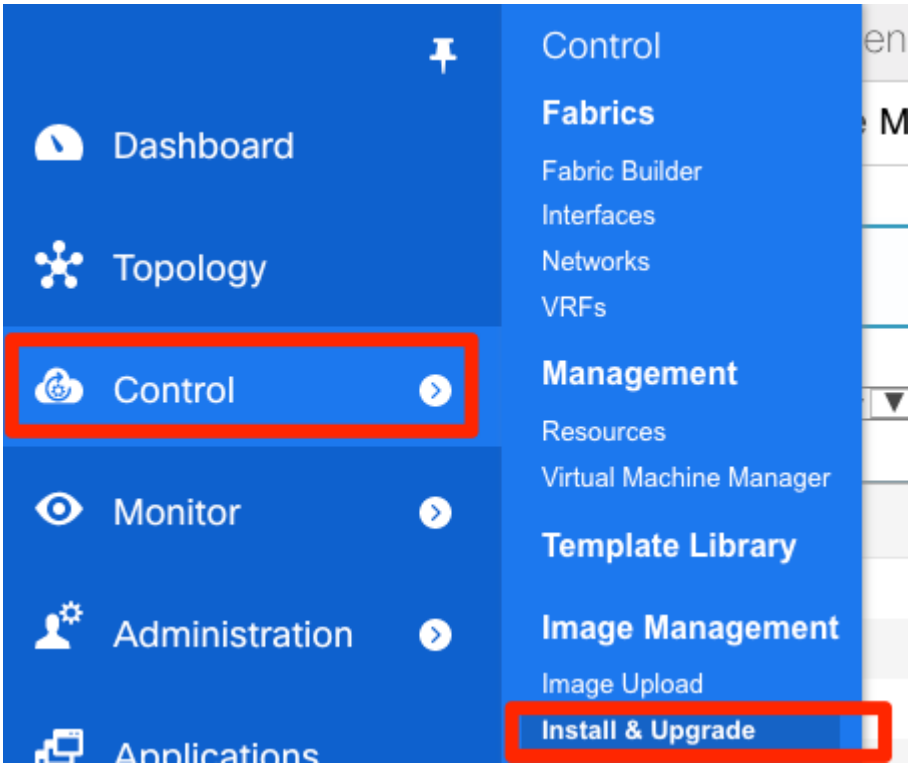


Étape 2. Suivez les invites pour un téléchargement local, puis le ou les fichiers doivent apparaître comme illustré dans cette image :



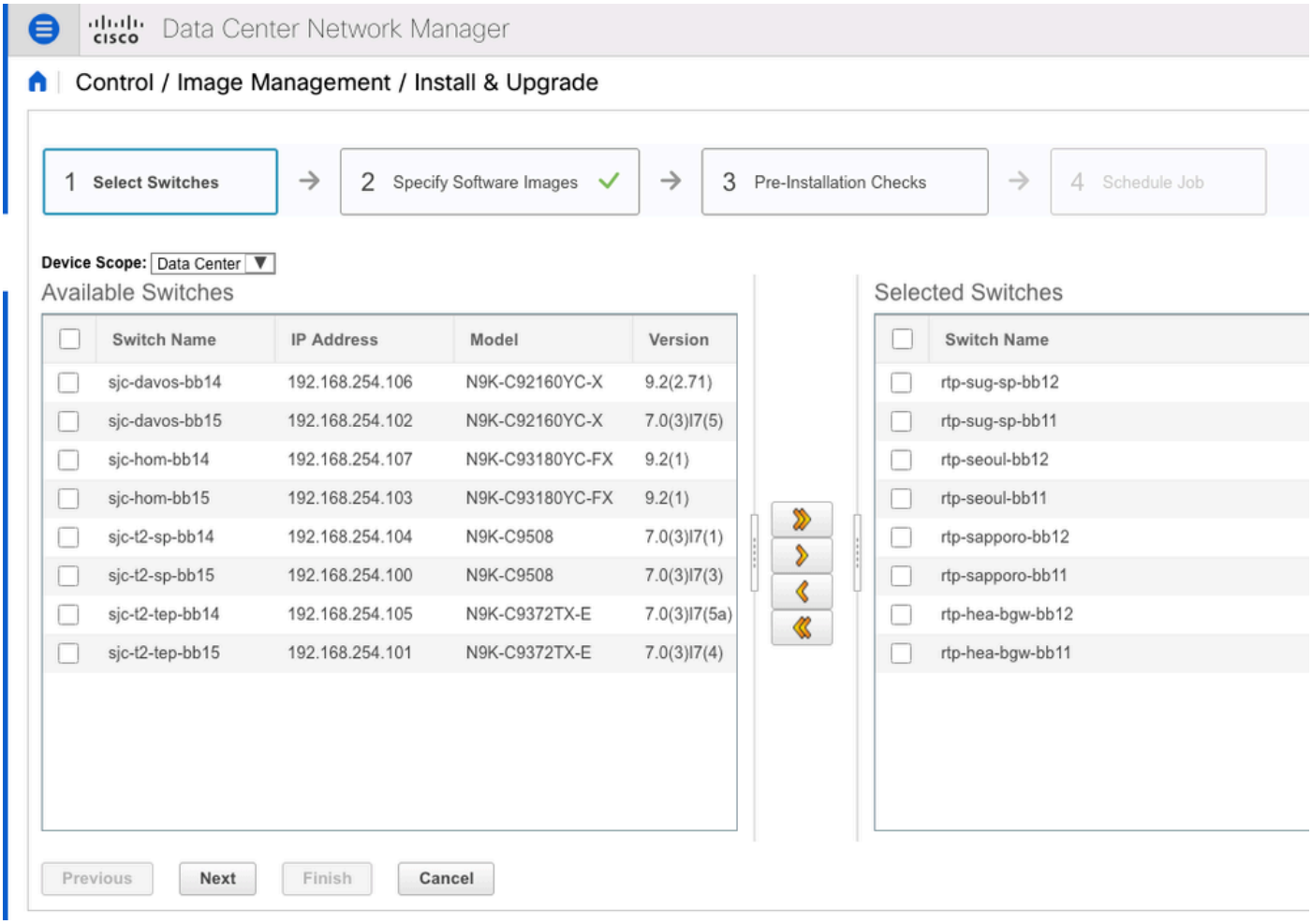


Étape 3. Une fois le ou les fichiers téléchargés, vous pouvez passer à Installer et mettre à niveau si les commutateurs nécessitent une mise à niveau. Accédez à Control > Image Management > Install & Upgrade, comme indiqué dans l'image.

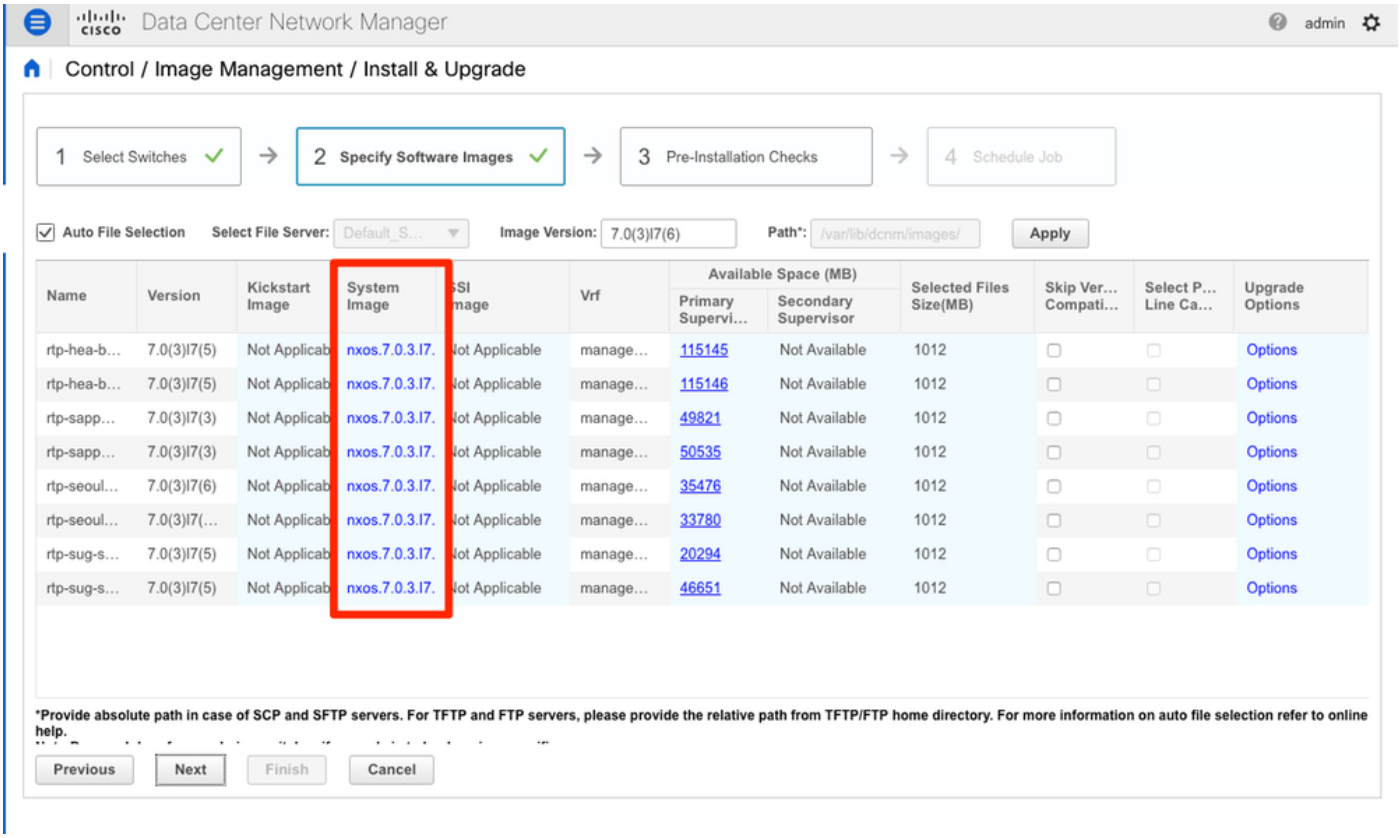


Étape 4. Sélectionnez les commutateurs à mettre à niveau. Dans cet exemple, l'ensemble du

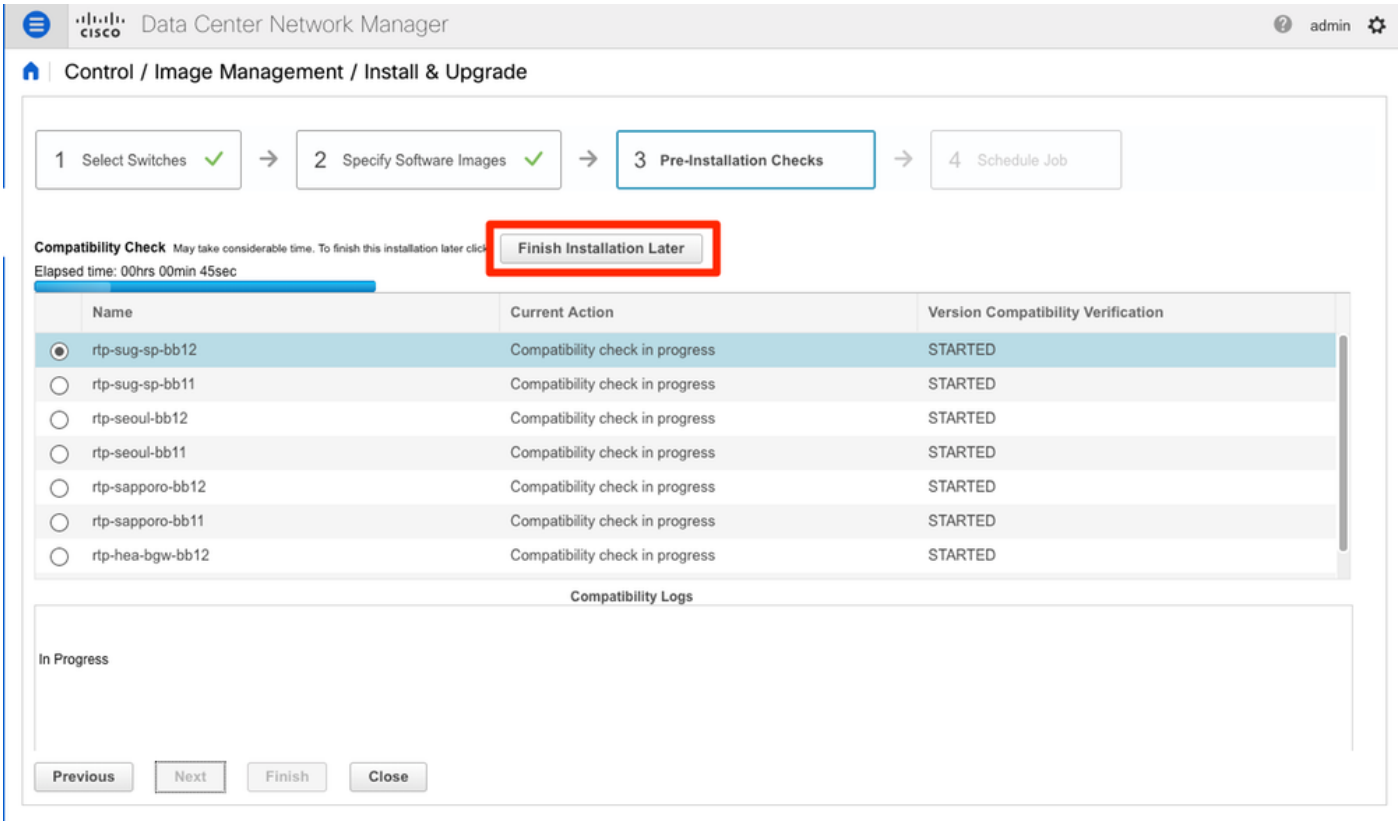
fabric RTP est mis à niveau.



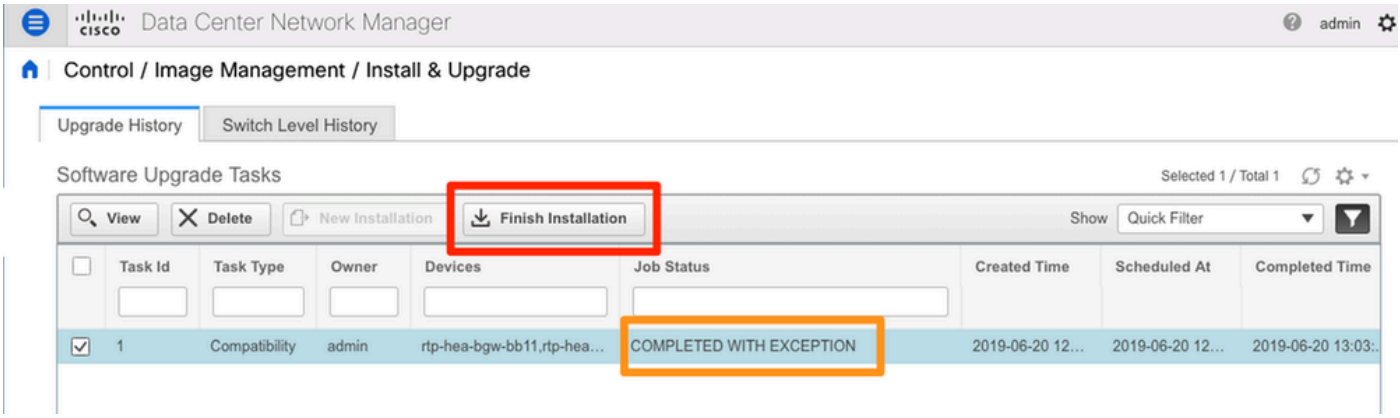
Étape 5. Sélectionnez la version de NX-OS vers laquelle vous souhaitez mettre à niveau les commutateurs (comme pratique recommandée, mettez à niveau tous les commutateurs vers la même version de NX-OS) :



Étape 6. Cliquez sur Next et DCNM exécute les commutateurs via des vérifications de pré-installation. Cette fenêtre peut prendre un certain temps. Vous pouvez donc sélectionner Finish Installation Later et programmer la mise à niveau pendant que vous êtes absent.



Cette opération met la tâche en file d'attente et est similaire à celle illustrée dans l'image ci-contre, une fois terminée.

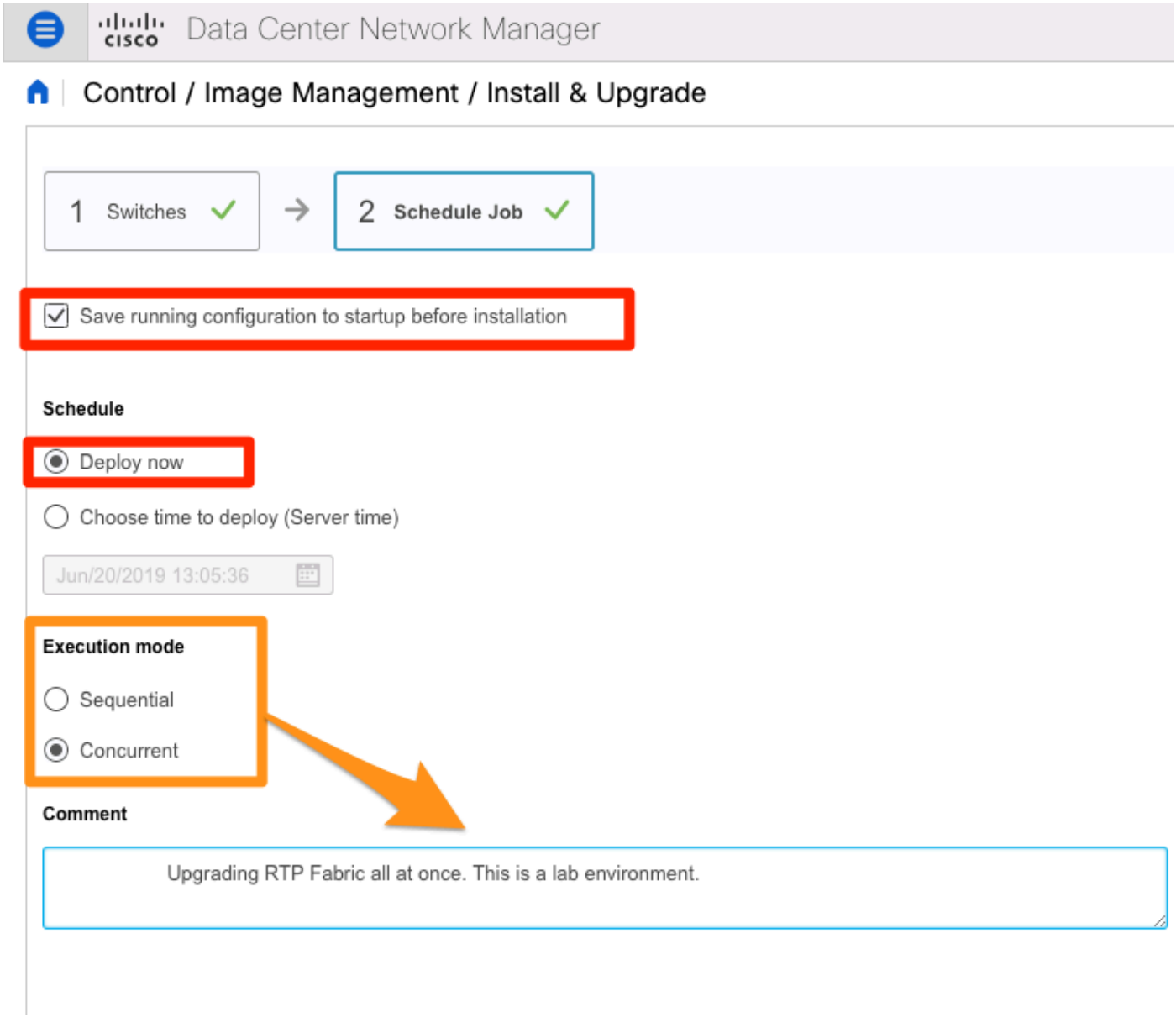


Remarque : l'exception dans le cas ci-dessus était que l'un des commutateurs RTP ne disposait pas de suffisamment d'espace pour l'image NX-OS.

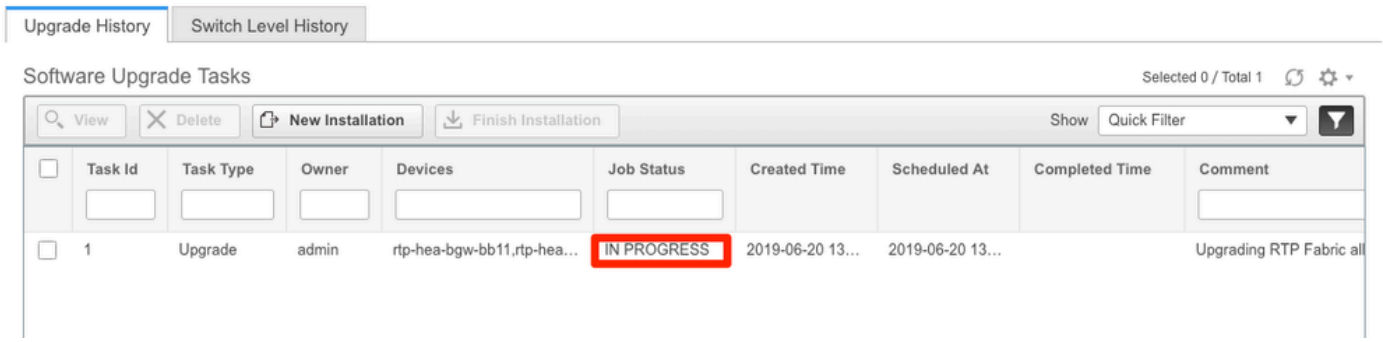
Étape 7. Une fois la compatibilité terminée, cliquez sur Finish Installation dans la même fenêtre, comme indiqué dans l'image.

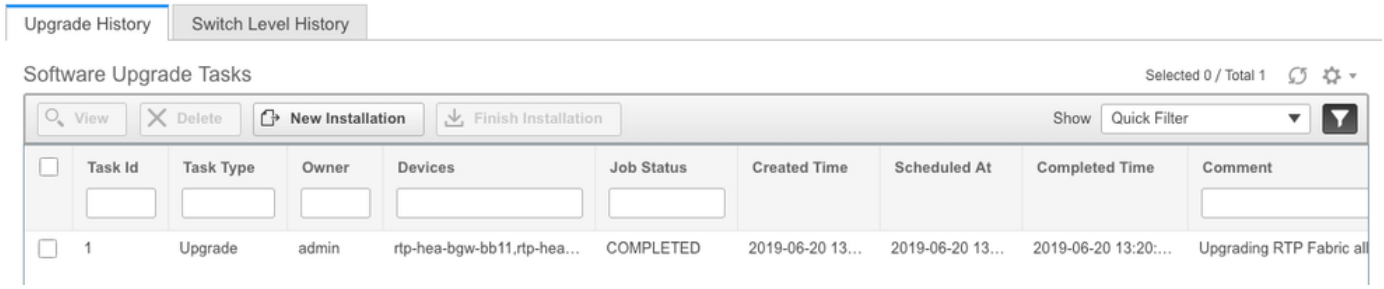


Étape 8. Vous pouvez sélectionner les mises à niveau à effectuer simultanément (toutes en même temps) ou séquentielles (une par une). Comme il s'agit d'un environnement de travaux pratiques, l'option sélectionnée est simultanée.



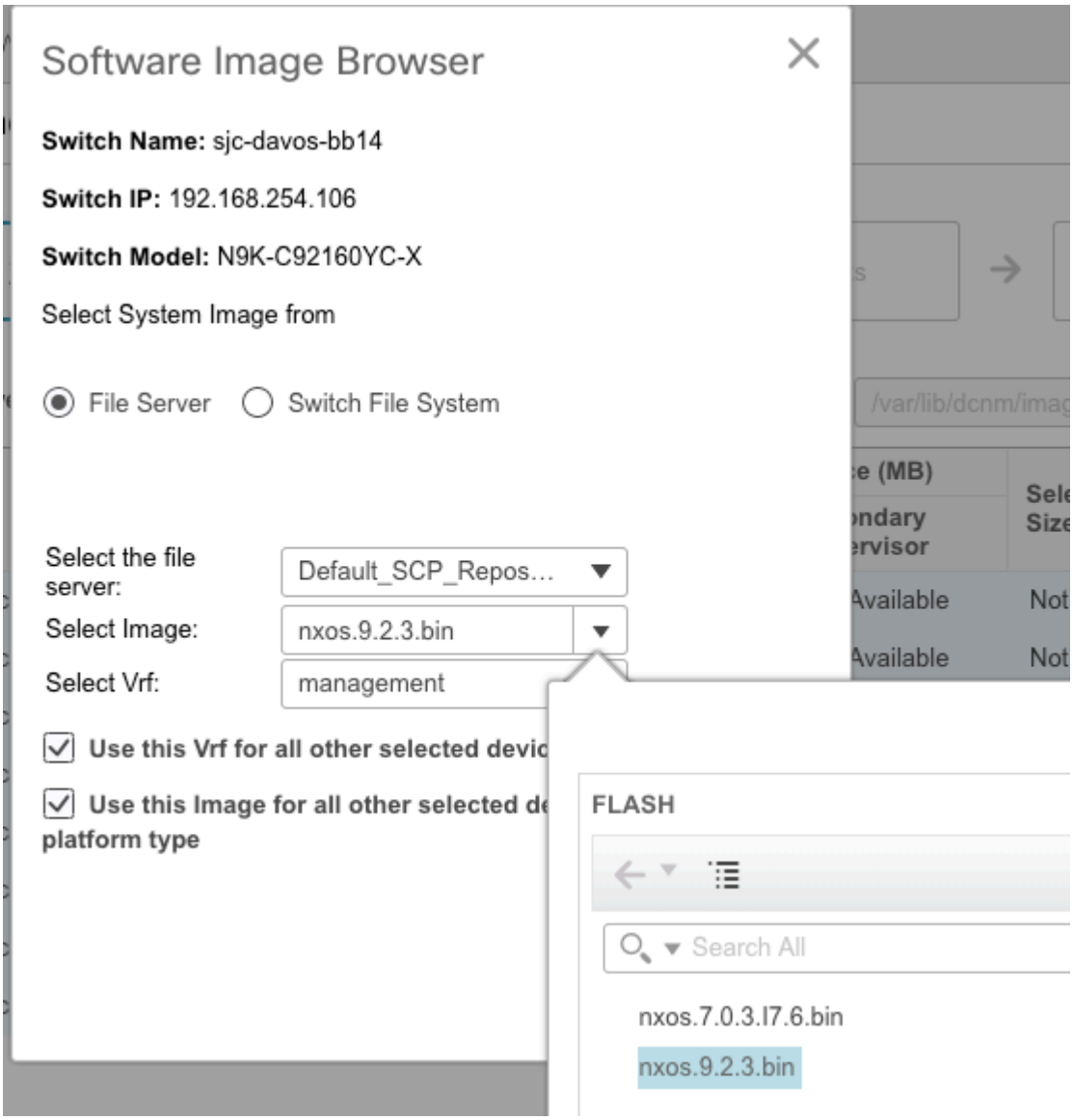
La tâche est créée et apparaît EN COURS, comme illustré dans l'image.





Une autre méthode de sélection de l'image s'affiche ici.





Installer Endpoint Locator

Pour que les applications DCNM fonctionnent correctement, vous devez disposer d'une connectivité intrabande entre le serveur DCNM et un port du panneau avant vers l'un des Nexus 9000 du fabric. Dans cet exemple, le serveur DCNM est connecté à Ethernet1/5 de l'un des Spines du fabric RTP.

Étape 1. Cette CLI est ajoutée manuellement au Nexus 9000 :

```
rtp-sug-sp-bb12# show run interface ethernet1/5


!Command: show running-config interface Ethernet1/5
!Running configuration last done at: Wed Sep 11 14:41:05 2019
!Time: Wed Sep 11 14:53:25 2019

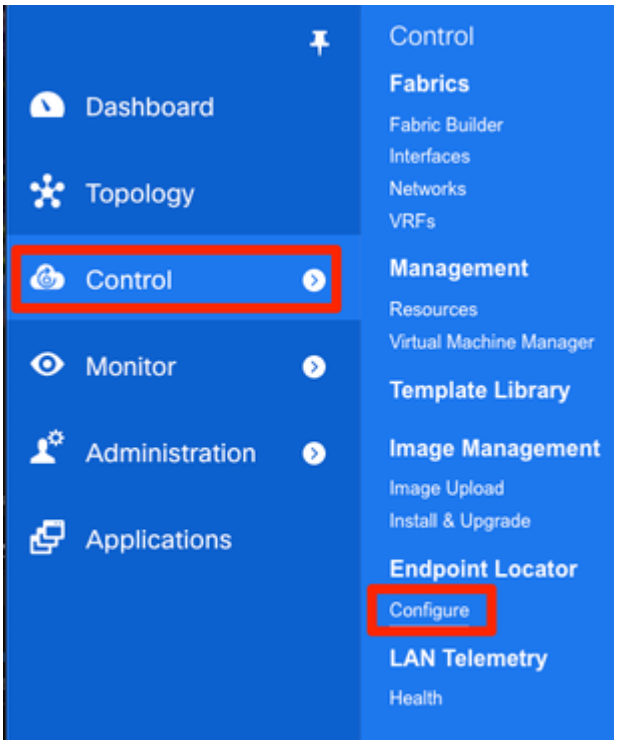

version 7.0(3)I7(7) Bios:version 08.36


interface Ethernet1/5
  description To DCNM Server for Endpoint Locator & Apps
  mtu 9216
  no ip redirects
  ip address 99.99.99.2/30
  no ipv6 redirects
  no shutdown
```

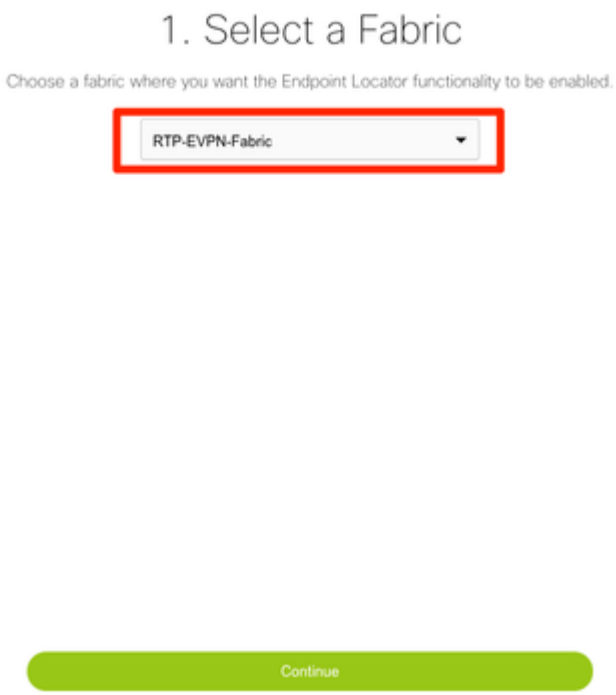
Étape 2. Assurez-vous que vous pouvez envoyer une requête ping au serveur DCNM et vice-versa sur cette connexion point à point.

```
[root@dcg-rtp-dcnm-fab ~]# ping 99.99.99.2
PING 99.99.99.2 (99.99.99.2) 56(84) bytes of data.
64 bytes from 99.99.99.2: icmp_seq=1 ttl=255 time=0.780 ms
64 bytes from 99.99.99.2: icmp_seq=2 ttl=255 time=0.802 ms
64 bytes from 99.99.99.2: icmp_seq=3 ttl=255 time=0.772 ms
^C
--- 99.99.99.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.772/0.784/0.802/0.034 ms
```

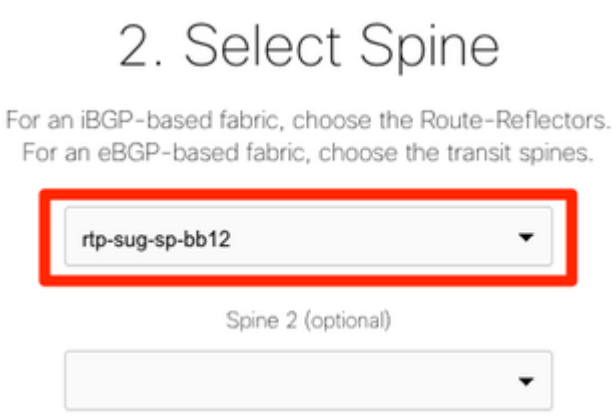
Étape 3. Accédez à l’interface graphique utilisateur de DCNM > Control > Endpoint Locator > Configure, comme indiqué dans l’image.



Étape 4. Sélectionnez le fabric sur lequel vous souhaitez activer Endpoint Locator, comme illustré dans l'image.



Étape 5. Comme l'illustre l'image, sélectionnez une colonne vertébrale.



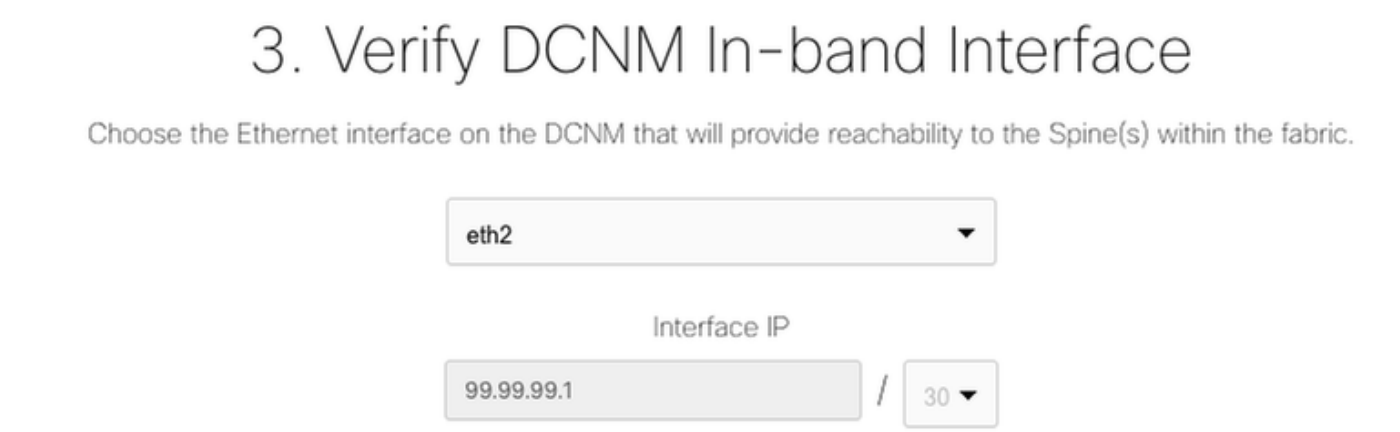
Étape 6. (Facultatif) Avant de passer à l'étape suivante, l'adresse IP de eth2 a été modifiée à partir du déploiement d'origine via cette interface de ligne de commande sur le serveur DCNM (cette étape n'est pas nécessaire si l'adresse IP d'origine configurée lors de la nouvelle installation du serveur DCNM reste correcte) :

```
[root@dcg-rtp-dcnm-fab ~]# ifconfig eth2 0.0.0.0
[root@dcg-rtp-dcnm-fab ~]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 99.99.99.1
InBand Network Mask [e.g. 255.255.255.0]: 255.255.255.252
InBand Gateway [e.g. 2.2.2.1]: 99.99.99.2
Validating Inputs ...
You have entered these values..
PIP=99.99.99.1
NETMASK=255.255.255.252
GATEWAY=99.99.99.2

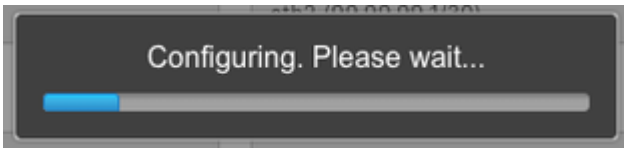

Press 'y' to continue configuration, 'n' to discontinue [y] y
{"ResponseType":0,"Response":"Refreshed"}
Done.

[root@dcg-rtp-dcnm-fab ~]# ifconfig eth2
eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 99.99.99.1  netmask 255.255.255.252  broadcast 99.99.99.3
        inet6 fe80::250:56ff:fe9e:23f5  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:9e:23:f5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 698 (698.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

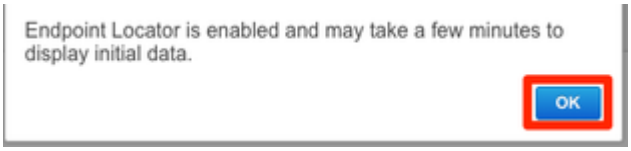
Étape 7. Vérification de la configuration de l’interface intrabande Cela devrait correspondre à ce qui a été configuré à l'étape précédente.



Étape 8. Après avoir vérifié la configuration, cliquez sur Configure. Cette étape peut prendre quelques minutes :



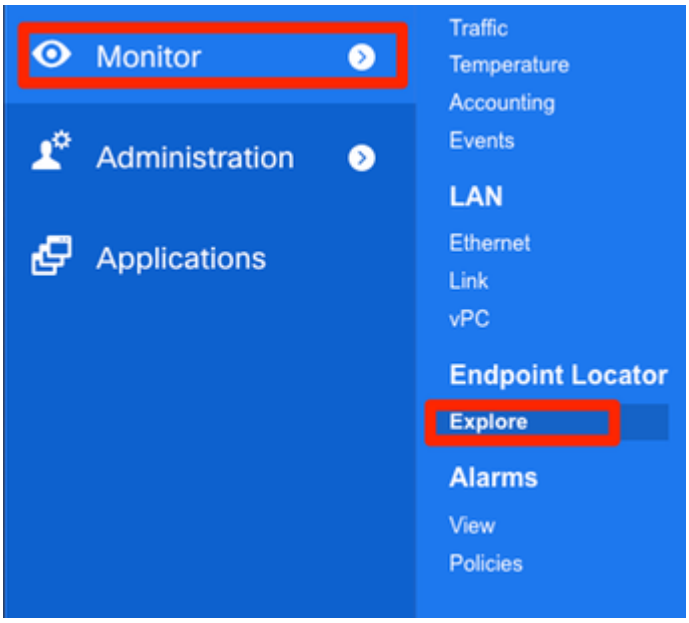
Une fois terminé, la notification, telle qu'elle apparaît dans l'image, apparaît.



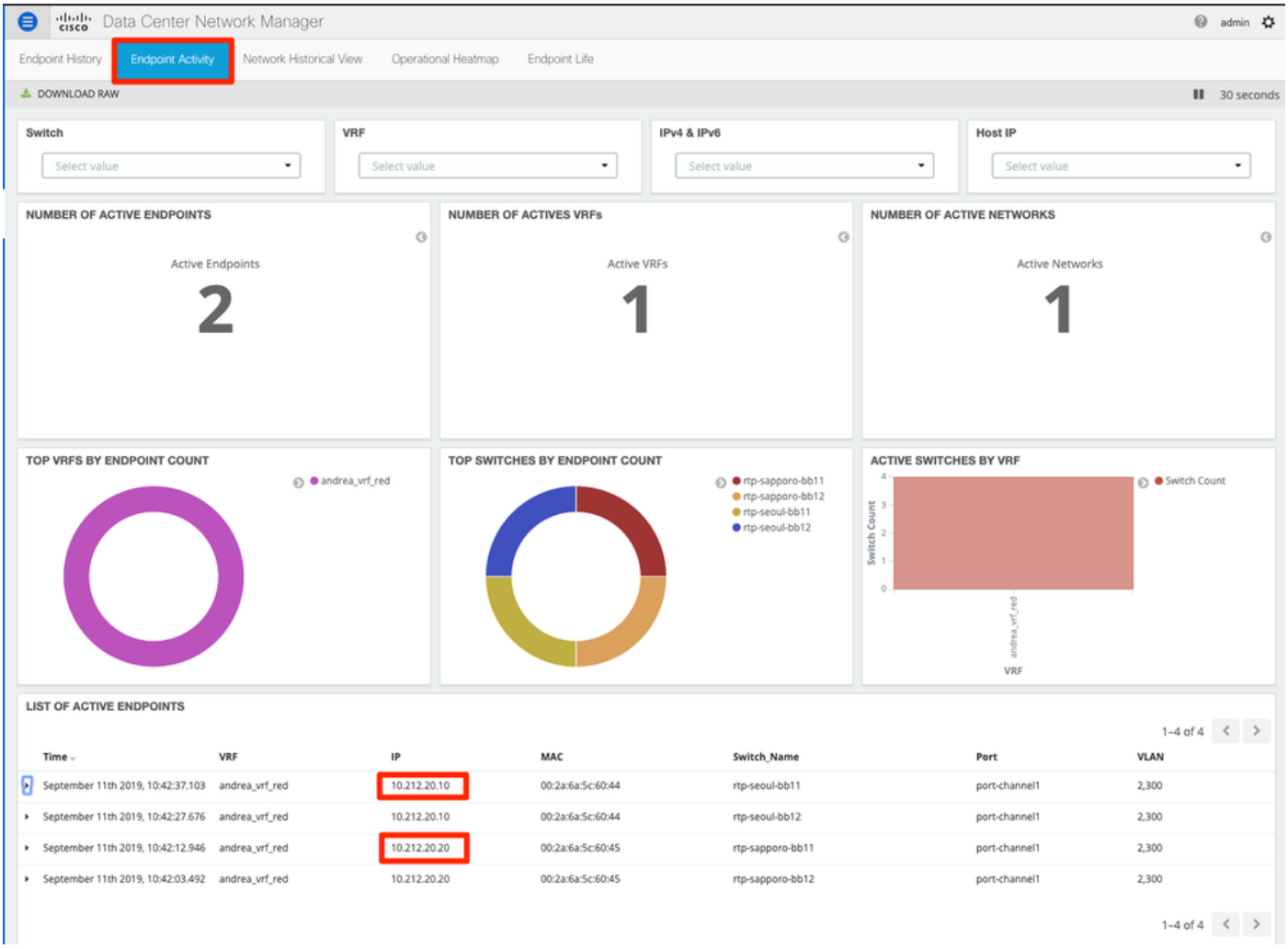
Notez que DCNM a configuré un voisin BGP sur le Spine sélectionné dans la famille L2VPN EVPN.

```
rtp-sug-sp-bb12# show run bgp | sec "neighbor 99"
  neighbor 99.99.99.1
    remote-as 65534
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
```

Étape 9. Vous pouvez maintenant utiliser Endpoint Locator. Accédez à Monitor > Endpoint Locator > Explore.



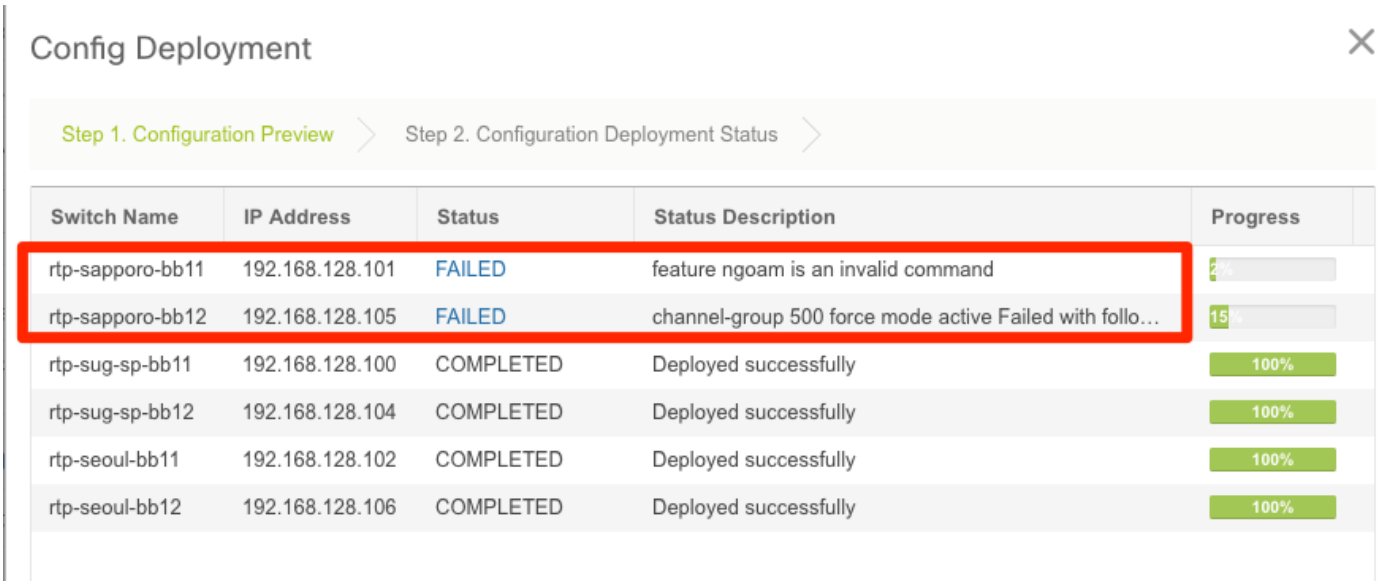
Dans cet exemple, vous pouvez voir les deux hôtes qui ont été configurés pour les tests ping locaux dans le fabric RTP :



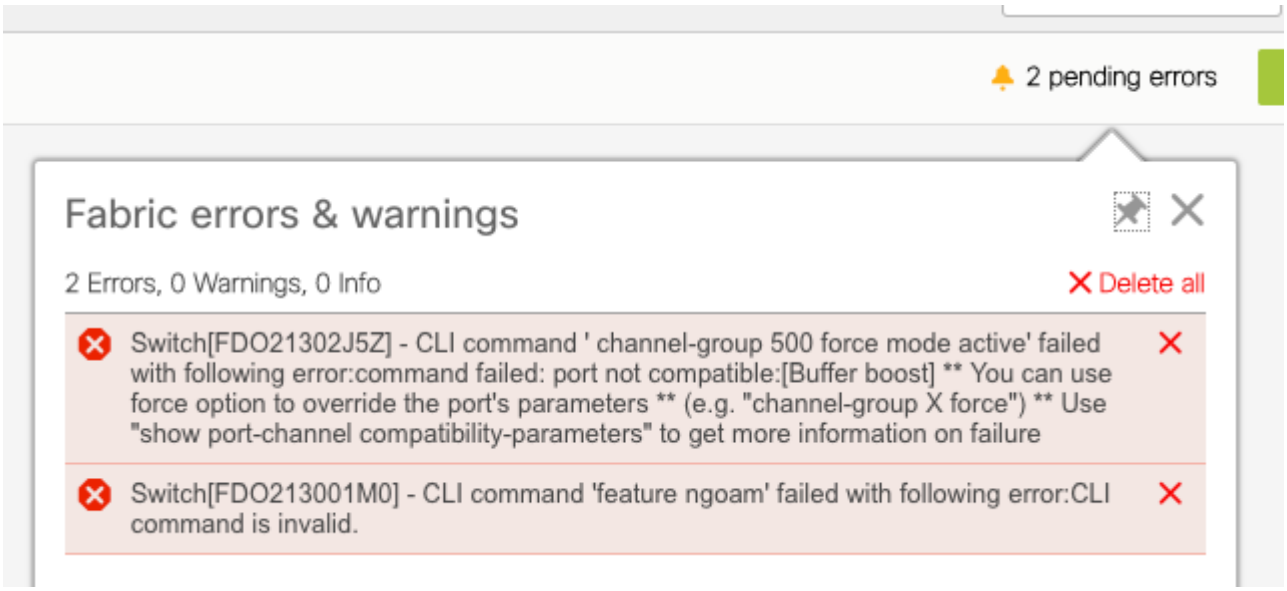
Problèmes Rencontrés Lors De Ce Déploiement

Câblage incorrect

Un câblage incorrect a été installé sur une paire de commutateurs, ce qui a provoqué une erreur de groupement pour le port-channel500 de liaison entre homologues vPC. Exemple :

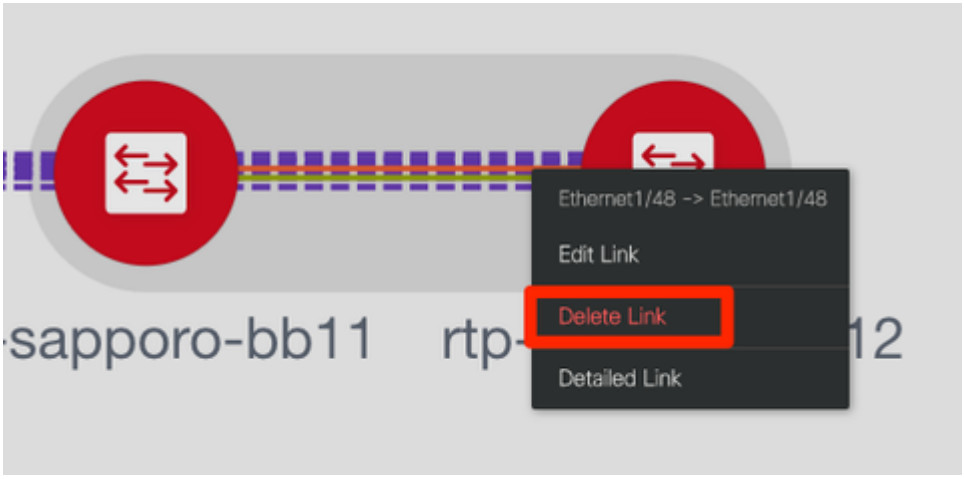


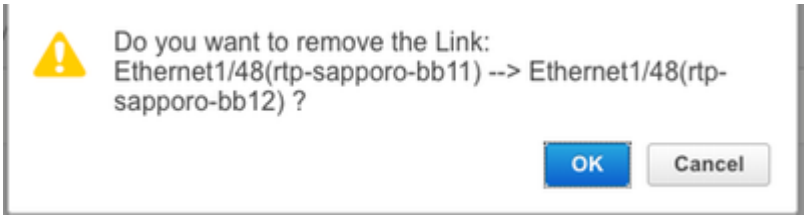
Étape 1. Revenez à Control > Fabric Builder et vérifiez les erreurs :



Étape 2. Pour la première erreur concernant l'échec de la commande port-channel500 — Vérifiez via show cdp neighbors que la connexion à l'homologue vPC se trouvait sur un port 10G et un port 40G (non compatible). Retirez physiquement le port 10G et supprimez également la liaison de

DCNM :



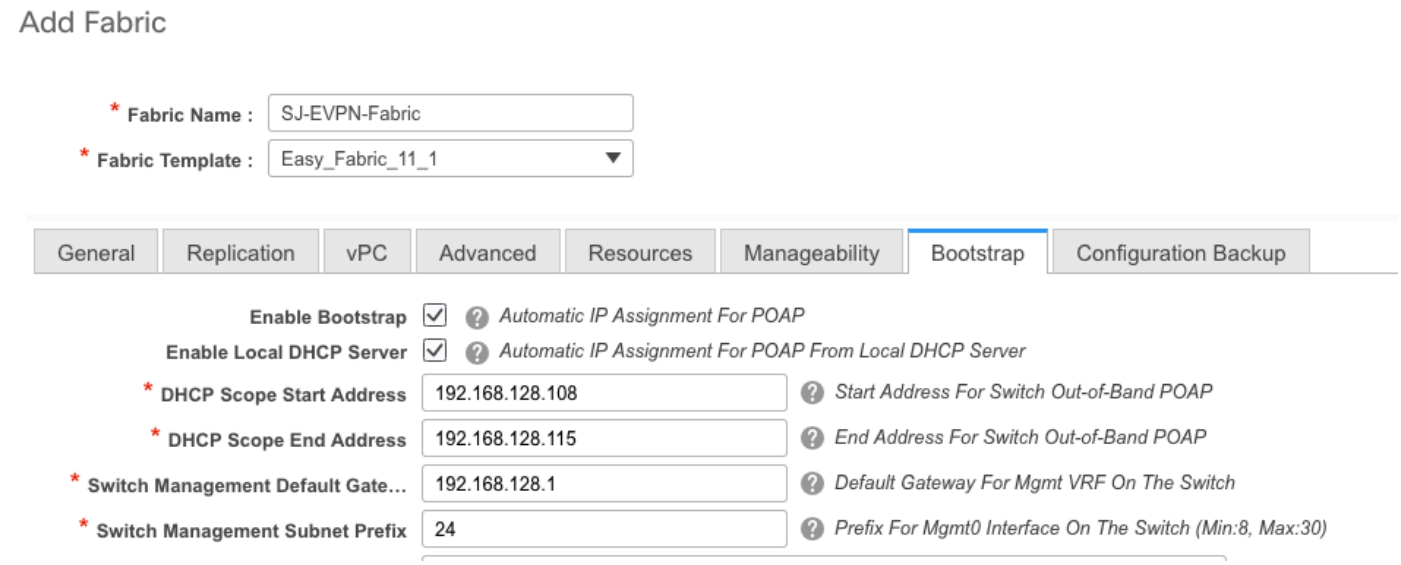


Échec de la configuration d'une fonctionnalité

Pour la deuxième erreur concernant l'échec de la configuration de « feature ngoam » — Le commutateur a été mis à niveau vers une version plus récente de NX-OS où « feature ngoam » est pris en charge et cliquez à nouveau sur Save & Deploy. Les deux questions ont été résolues.

Chevaucher les sous-réseaux de gestion de différents fabrics

Pendant le déploiement du second fabric, SJ, le même sous-réseau a été utilisé (s'il est physiquement séparé, cela devrait être correct) ; Cependant, DCNM consigne un conflit et le POAP échoue. Ceci est résolu lorsque le fabric SJ est placé dans un VLAN de gestion différent et que la plage des adresses DHCP est modifiée.



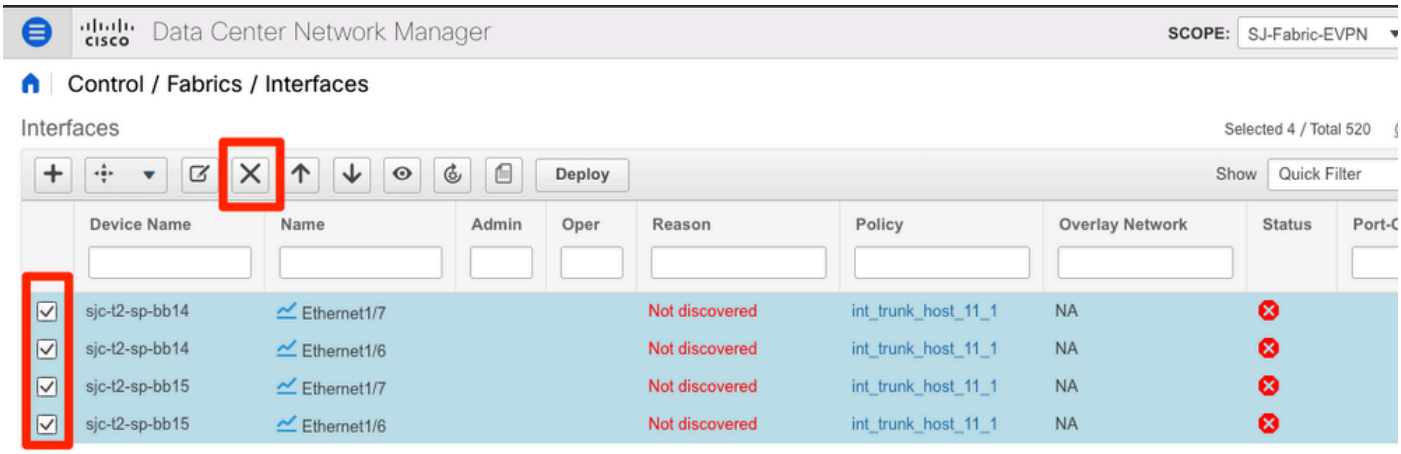


Interfaces de répartition

Étape 1. Pour les interfaces de dérivation de certains commutateurs (reportez-vous à la topologie), cette interface de ligne de commande a été ajoutée manuellement pour les spines T2 :

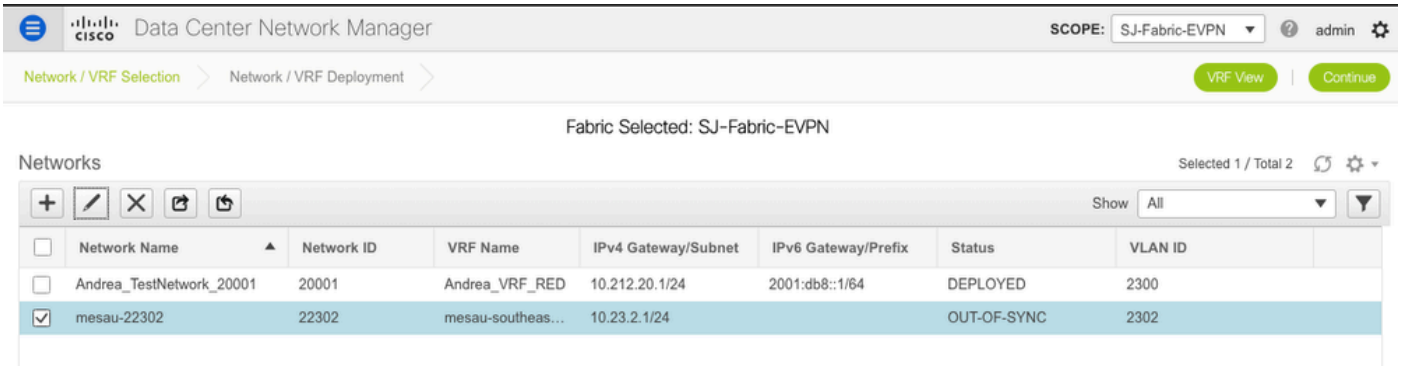
```
sjc-t2-sp-bb14# show run | i i breakout
interface breakout module 1 port 6-7 map 10g-4x
```

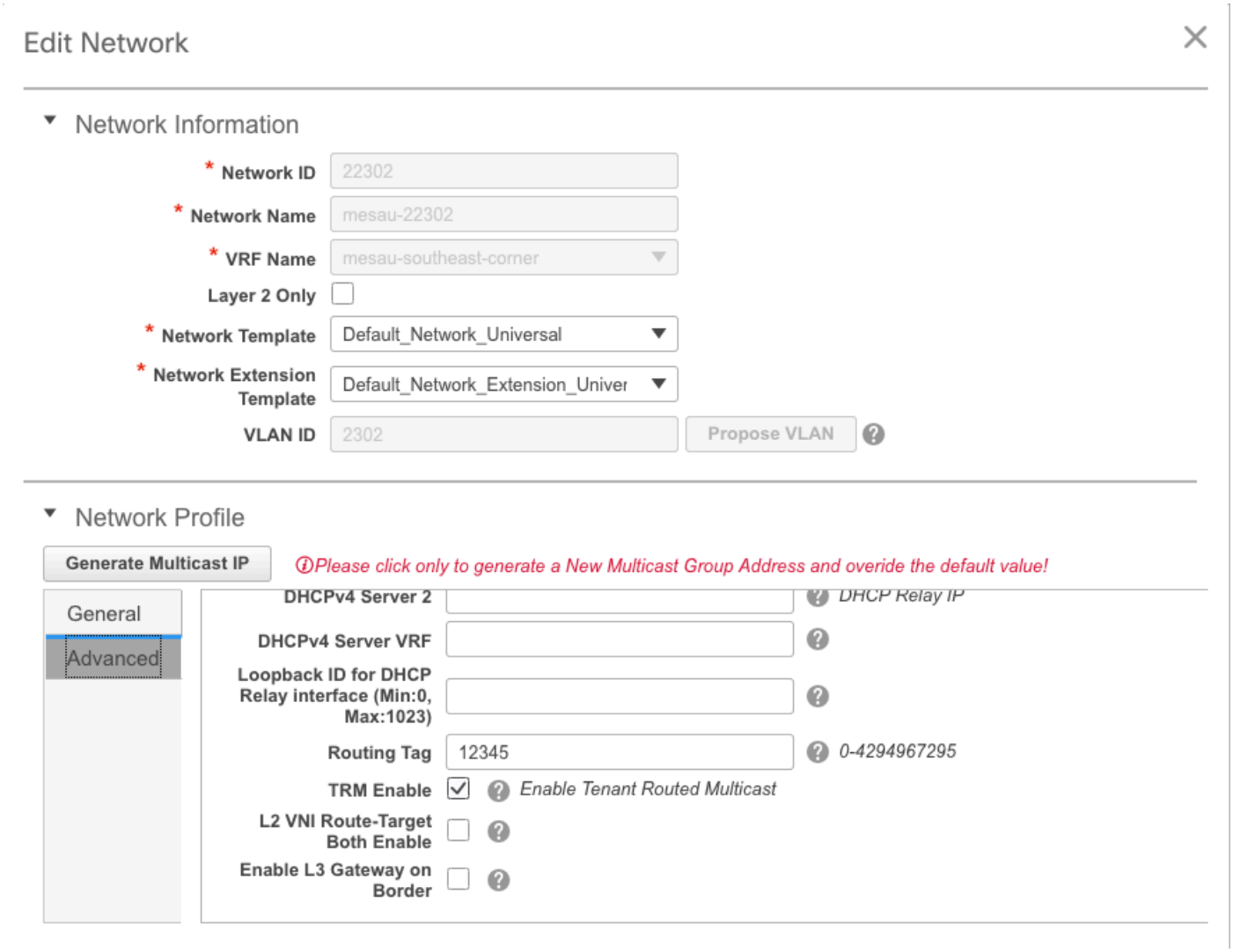
Étape 2. Accédez à Control > Interfaces et supprimez les interfaces parent :



Les interfaces réellement utilisées sont Eth1/6/1-4 et Eth1/7/1-4. Si vous ne corrigez pas ce problème, la commande Enregistrer et déployer échouera ultérieurement. Il y a un moyen de faire la cassure à travers DCNM lui-même (bouton à côté du signe + ; toutefois, non couvert dans cet article)

Erreur de fabric lors du déploiement vers une fonctionnalité non prise en charge

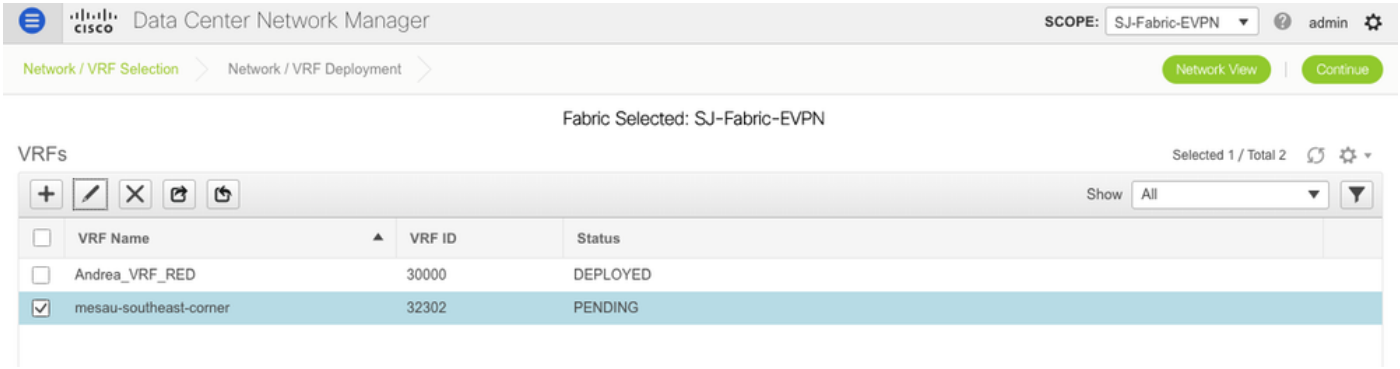


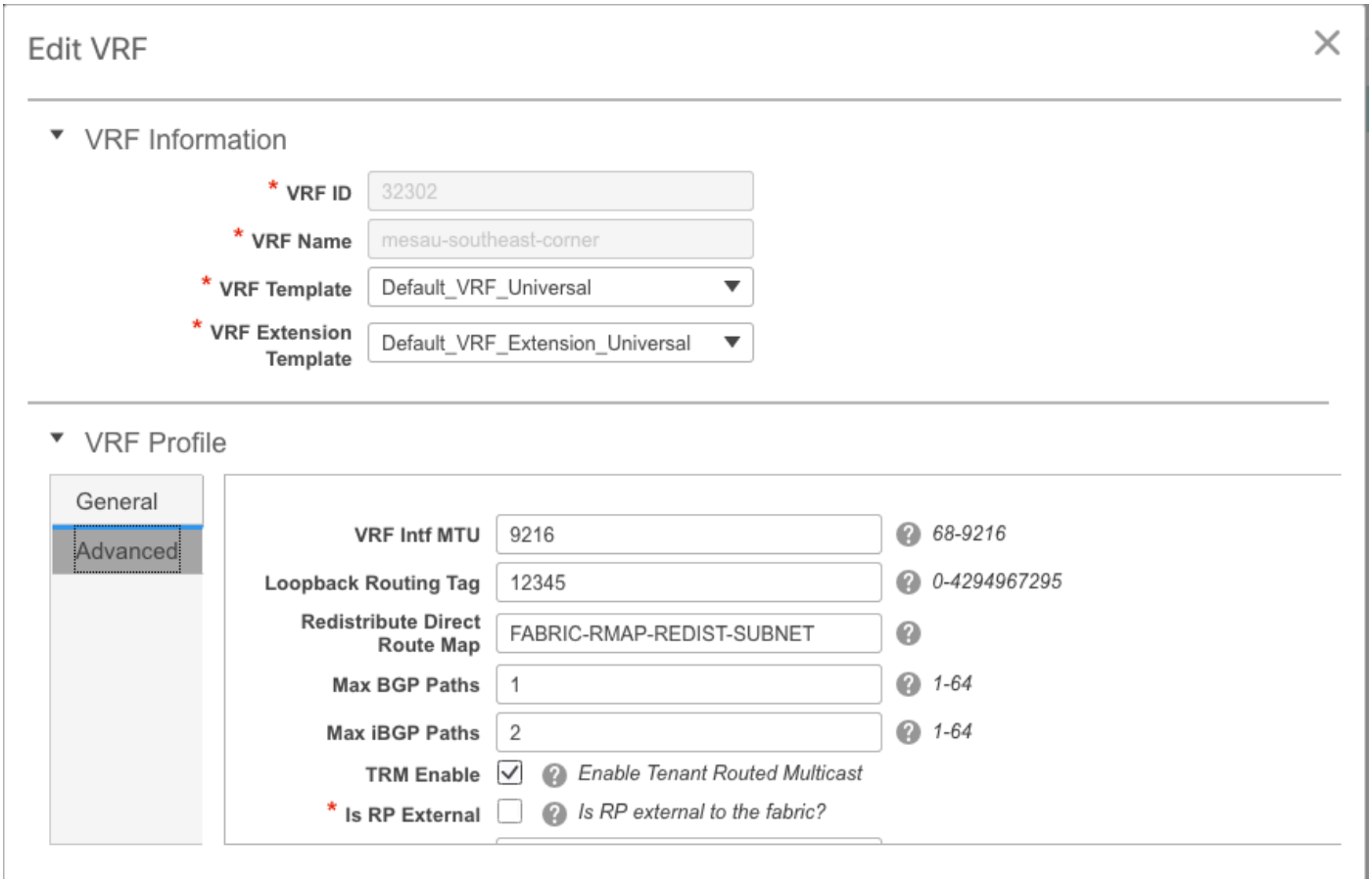


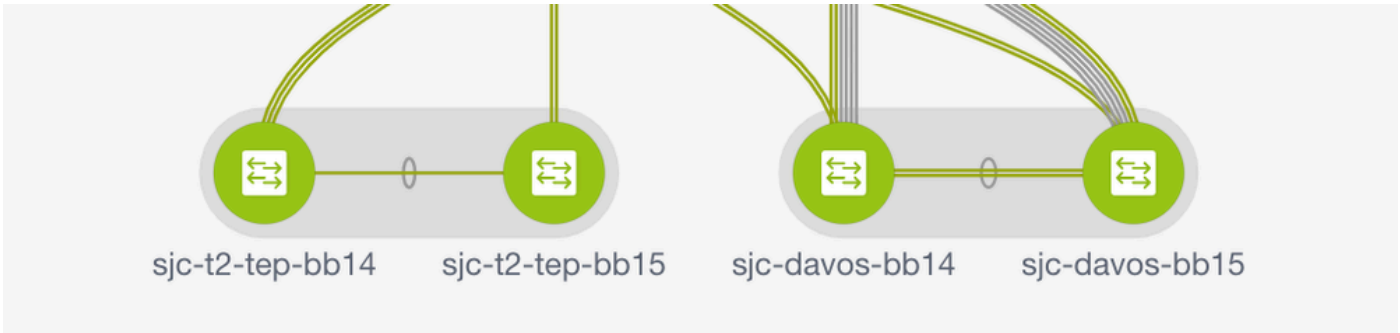
Certains des châssis (T2) de SJ Fabric ne prennent pas en charge TRM. Par conséquent, lorsque DCNM a tenté d'appliquer cette configuration, il n'a pas pu avancer. Assistance TRM ici : https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/vxlan-92x/configuration/guide/b-cisco-nexus-9000-series-nx-os-vxlan-configuration-guide-92x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_9x_chapter_01001.html#concept_vw1_syb_zfb

Décochez la case Activer TRM sous les fenêtres Network et VRF Edit qui s'affiche dans l'image.

Répétez le même processus sous Control > Fabric Builder > VRF.







Cliquez sur Continue, puis sur Deploy, comme indiqué précédemment.

Quelles sont les nouveautés de DCNM 11.2 ?

- Appairage de structure vPC
- Fabrics routés basés sur eBGP
    - Activer EVPN au-dessus
- Améliorations apportées au champ primaire Easy Fabric
    - Spine frontière/Spine GW frontière
    - Bidir PIM
    - Multidiffusion routée par le locataire
- Day-0/Bootstrap avec serveur DHCP externe

Opérations du jour 2 :

- Ressources Network Insights
- Network Insights Advisor
- Prise en charge IPv6 pour l'accès externe (eth0)
- Visibilité informatique VMM avec UCS-FI
- Améliorations de la vue topologique
- Mise à niveau en ligne depuis 11.0/11.1

Passage du vPC traditionnel au vPC sans MCT à l'aide de DCNM :

Avantages du vPC sans MCT :

- Solution de double hébergement améliorée sans perte de ports physiques
- Préserve les caractéristiques vPC traditionnelles
- Routage optimisé pour les terminaux à hébergement unique avec PIP

Informations connexes

- Guide de configuration du fabric LAN Cisco DCNM, version 11.2(1)
  https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/series.html

- Chapitre : Cas d'utilisation du provisionnement en limite dans les fabrics EVPN BGP VXLAN - Multisite
  https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/series.html
- Livre blanc sur le DCI de nouvelle génération avec VXLAN EVPN multisite utilisant les passerelles de périphérie vPC
  https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/whitepaper-c11-742114.html#_Toc5275096

- Chapitre : Applications DCNM
  https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/series.html

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.