Provisionnement de fabric SD-Access

Guide de déploiement normatif

Juillet 2019

Sommaire

Définition et conception : SD-Access

L'accès défini par logiciel (SD-Access) Cisco® est l'évolution des conceptions de réseaux locaux classiques vers des réseaux qui mettent directement en œuvre l'intention d'une entreprise. SD-Access est activé avec un package d'applications qui s'exécute dans le cadre du logiciel Cisco DNA Center pour la conception, le provisionnement, l'application de la politique et la création d'un réseau local intelligent câblé et d'un réseau sans fil en toute sécurité.

Ce guide est utilisé pour déployer l'infrastructure de gestion, y compris Cisco DNA Center, Cisco Identity Services Engine (ISE) et les contrôleurs LAN sans fil Cisco, décrits dans le Guide de conception de solutions SD-Access associé. Le déploiement décrit dans ce guide est utilisé avant le déploiement d'une fabric SD-Access Cisco, comme décrit dans le document associé Guide de déploiement de la fabric SD-Access.

Si vous n'avez pas téléchargé ce guide à partir de la communauté Cisco ou de la zone de conception, vous pouvez en rechercher la dernière version.

Trouver les documents Guide de conception de solutions SD-Access, Guide normatif de déploiement d'infrastructure de gestion SD-Access, Guide normatif de déploiement de SD-Access pour le réseau local distribué, les guides de déploiement connexes, les guides de conception et les livres blancs dans les pages suivantes :

- https://www.cisco.com/go/designzone
- https://cs.co/en-cvds

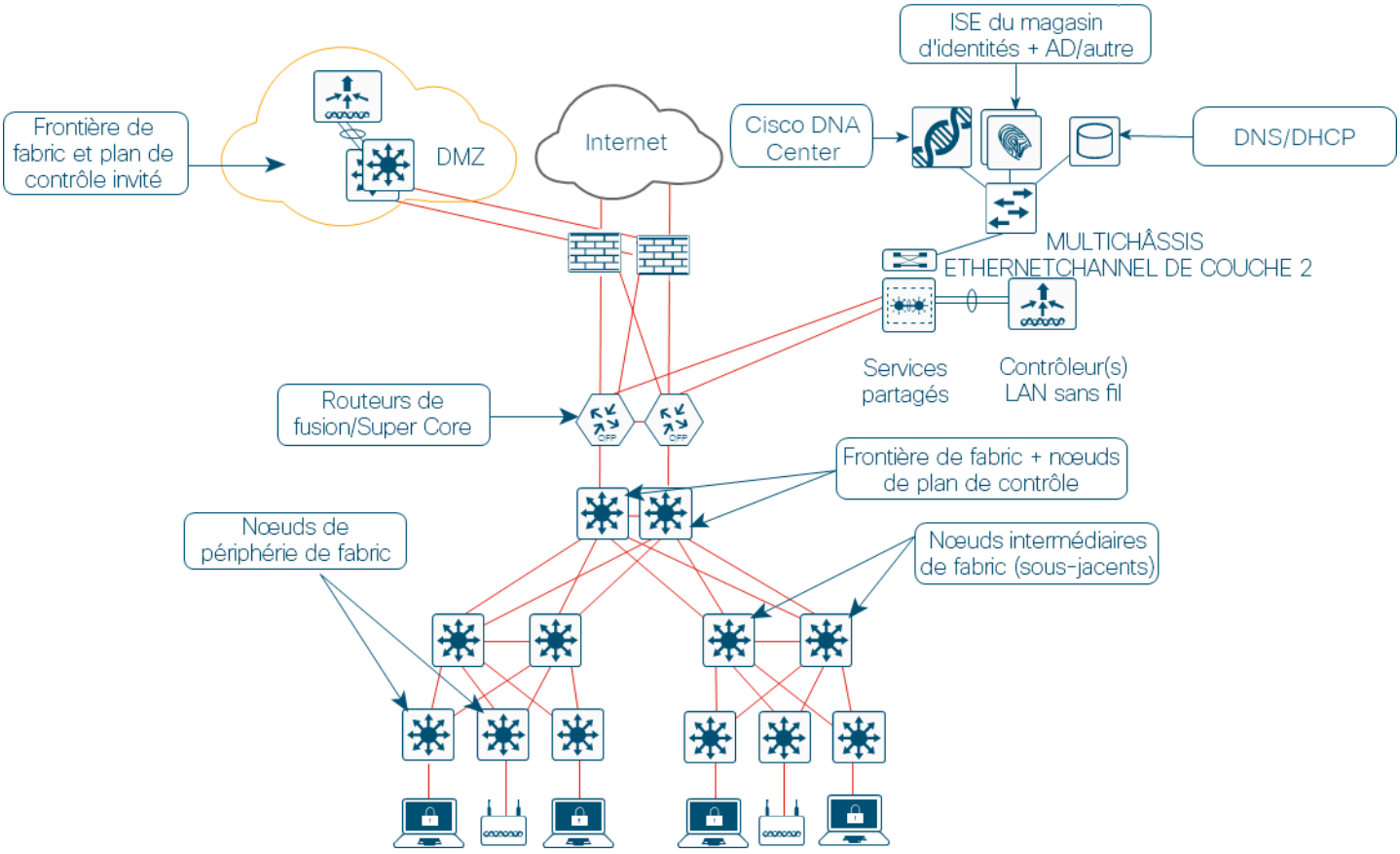
Déploiement : fabric SD-Access

Comment lire les commandes de déploiement

Ce guide utilise les conventions suivantes pour les commandes que vous saisissez au niveau de l'interface de ligne de commande (CLI).
Commandes à saisir à l'invite de la CLI :
`configure terminal`
Commandes qui spécifient une valeur pour une variable (la variable est en gras et en italique) :
`ntp server` ***`10.4.0.1`***
Commandes avec des variables que vous devez définir (la définition est mise entre parenthèses en gras et en italique) :
`class-map` ***`[highest class name]`***
Commandes à l'invite de la CLI ou d'un script (les commandes saisies sont en gras) :
`Router#` **`enable`**
Longues commandes qui reviennent à la ligne sur une page imprimée (le texte souligné est saisi comme une seule commande) :
`police rate` ***`1000`*** `pps burst` ***`10000`*** `packets conform-action`

Les composants de gestion SD-Access sont déployés dans la topologie décrite dans le document associé Guide de conception de solutions SD-Access, comme illustré dans le schéma de topologie. Ce guide suppose que Cisco DNA Center, Cisco Identity Services Engine (ISE) et l'infrastructure de gestion du contrôleur LAN sans fil Cisco sont déjà installés et disponibles, comme décrit dans le document Guide de déploiement de l'infrastructure de gestion SD-Access.

Figure 1. Topologie de validation



Le réseau d'entreprise intégré au déploiement de la fabric du réseau local décrit n'est pas virtualisé et exécute EIGRP (Enhanced Interior Gateway Routing Protocol) en tant que protocole de routage. Les préfixes IP du réseau local, y compris les services partagés, doivent être disponibles pour les réseaux sous-jacents et de superposition de la fabric tout en préservant l'isolation entre les réseaux superposés. Pour maintenir l'isolement, VRF-Lite s'étend des nœuds de frontière de la fabric à un ensemble de routeurs de fusion. Les routeurs de fusion mettent en œuvre la fuite de routes VRF à l'aide d'une configuration d'importation et d'exportation cible de routes BGP et effectuent une redistribution mutuelle avec EIGRP dans le réseau de l'entreprise et avec BGP sur la fabric du réseau local. Une configuration de mappage de route pour l'étiquetage et le filtrage dynamiques des routes redistribuées offre un moyen simple et dynamique d'empêcher les boucles de routage tout en accueillant plusieurs points de redistribution dans la conception haute disponibilité.

Processus : utilisation de Cisco DNA Center pour la conception et la découverte initiales du réseau

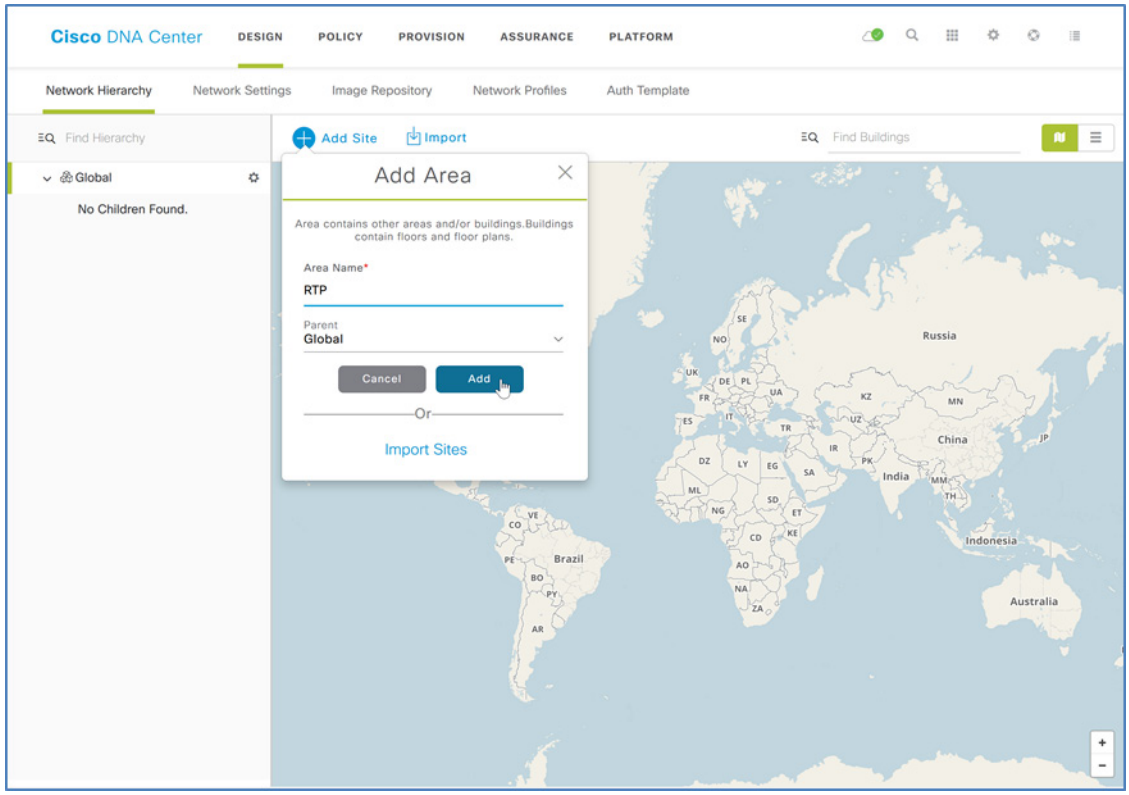
Cisco DNA Center offre une application de conception robuste qui permet aux clients de différentes tailles et échelles de définir facilement leurs sites physiques et leurs ressources communes. À l'aide d'un format hiérarchique intuitif, l'application de conception évite de redéfinir les mêmes ressources, telles que les serveurs DHCP, DNS et AAA, à plusieurs emplacements, lors du provisionnement des périphériques. La hiérarchie de réseau créée dans l'application de conception doit imiter la hiérarchie de réseau physique réelle de votre déploiement.

Grâce à Cisco DNA Center, vous créez une hiérarchie réseau composée de zones qui peuvent contenir des zones supplémentaires ou des bâtiments et des étages dans ces zones. Les périphériques sont mappés aux bâtiments et aux étages pour le provisionnement des services.

Procédure 1. Créer des sites réseau

Étape 1. Connectez-vous à Cisco DNA Center. Dans le tableau de bord principal de Cisco DNA Center, accédez à Design (Conception) > Network Hierarchy (Hiérarchie du réseau).

Étape 2. Cliquez sur **Add Site (Ajouter un site)**, dans le menu déroulant, sélectionnez **Add Area (Ajouter une zone)**, indiquez un **Area Name (Nom de zone)** approprié, puis cliquez sur **Add (Ajouter)**.



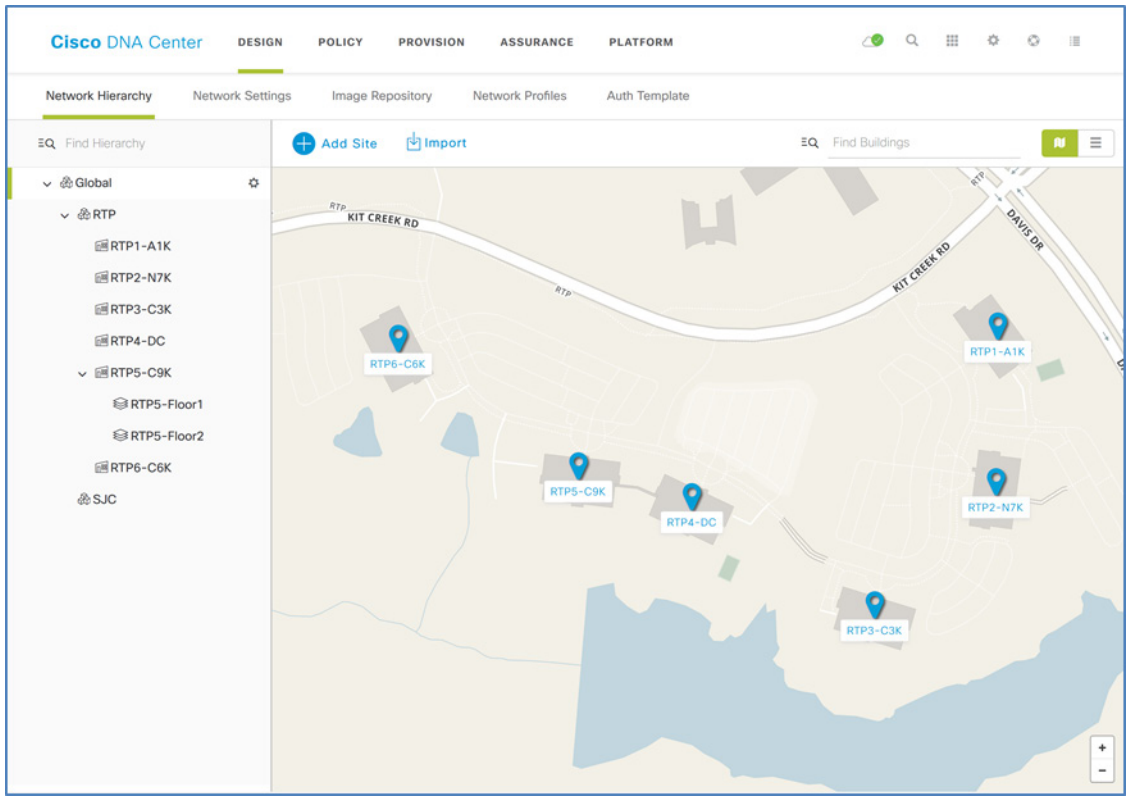
Étape 3. Cliquez sur **Add Site (Ajouter un site)**, dans le menu déroulant, sélectionnez le bouton **Add Building (Ajouter un bâtiment)**, indiquez un **Building Name (Nom de bâtiment)** approprié, sélectionnez le site créé à l'étape précédente comme **Parent**, complétez l'Assistant pour affecter un emplacement, puis cliquez sur **Add (Ajouter)**.

Pour ajouter un bâtiment, vous pouvez utiliser une adresse de rue approximative à proximité du bâtiment dans l'Assistant et, si vous le souhaitez, affiner la position du bâtiment sur la carte en cliquant sur l'emplacement cible.

Étape 4. Répétez l'étape précédente autant de fois que nécessaire pour ajouter des sites et des bâtiments, de manière à créer une hiérarchie pertinente pour votre entreprise.

Étape 5. Si vous intégrez un réseau sans fil à un bâtiment ou si vous avez besoin de plus de précision pour les choix de réseau au sein d'un bâtiment, sélectionnez le bâtiment sur la carte (ou sélectionnez l'icône représentant un engrenage à côté d'un bâtiment dans la hiérarchie), choisissez **Add Floor (Ajouter un étage)**, puis indiquez les informations dans l'Assistant.

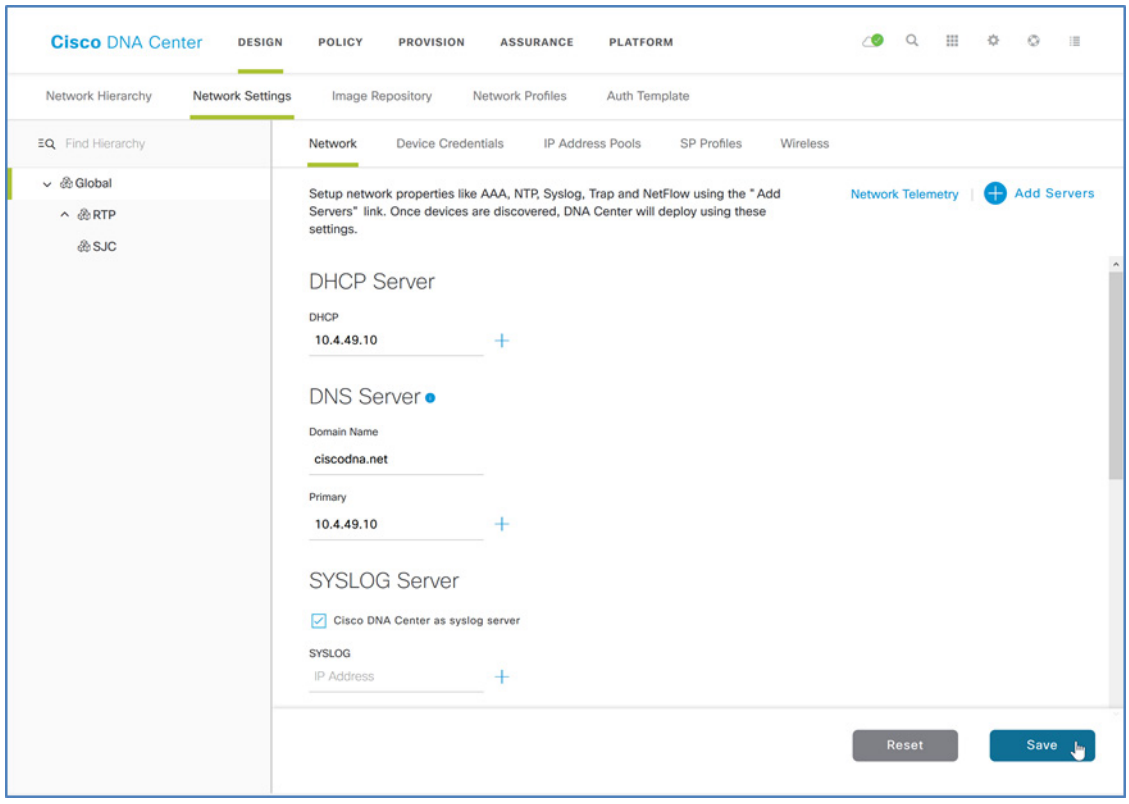
Les étages sont référencés lors du provisionnement sans fil. Si vous avez des schémas de plans d'étage au format DXF, DWG, JPG, GIF ou PNG, ajoutez-les à tout étage défini ; cela constituera un élément utile pour montrer les emplacements et la couverture des points d'accès lors des déploiements sans fil. Vous pouvez ajouter des centaines de sites jusqu'aux limites décrites dans le document Guide de conception de solutions SD-Access.



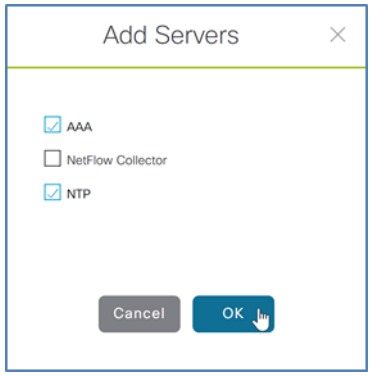
Procédure 2. Configurez les services réseau pour les sites

Configurez des services AAA, DHCP et DNS alignés sur la hiérarchie de Cisco DNA Center. Si les services utilisent les mêmes serveurs dans l'ensemble de la hiérarchie, vous pouvez les configurer globalement et les propriétés d'héritage de la hiérarchie appliquent les paramètres globaux à tous les sites. Les différences pour les sites individuels peuvent ensuite être appliquées site par site. Cette procédure montre la configuration de manière globale.

Étape 1. Dans Cisco DNA Center, accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > Network (Réseau)**. Dans le volet de gauche de la hiérarchie du site, sélectionnez le niveau approprié (par exemple : Global), indiquez l'adresse IP du **DHCP Server (Serveur DHCP)** (par exemple : 10.4.49.10), sous DNS Server (Serveur DNS) indiquez le nom de domaine (par exemple : ciscodna.net) et l'adresse IP **Primary (Principale)** du serveur (par exemple : 10.4.49.10), ajoutez les serveurs redondants ou supplémentaires (vous pouvez laisser les sélections par défaut pour utiliser Cisco DNA Center pour le serveur SYSLOG et le serveur SNMP), puis cliquez sur **Save (Enregistrer)**.



Étape 2. Dans la partie supérieure, en regard de **Network Telemetry (Télémétrie réseau)**, cliquez sur le bouton **+ Add Servers (Ajouter des serveurs)**, cochez les cases **AAA** et **NTP**, puis cliquez sur **OK**.



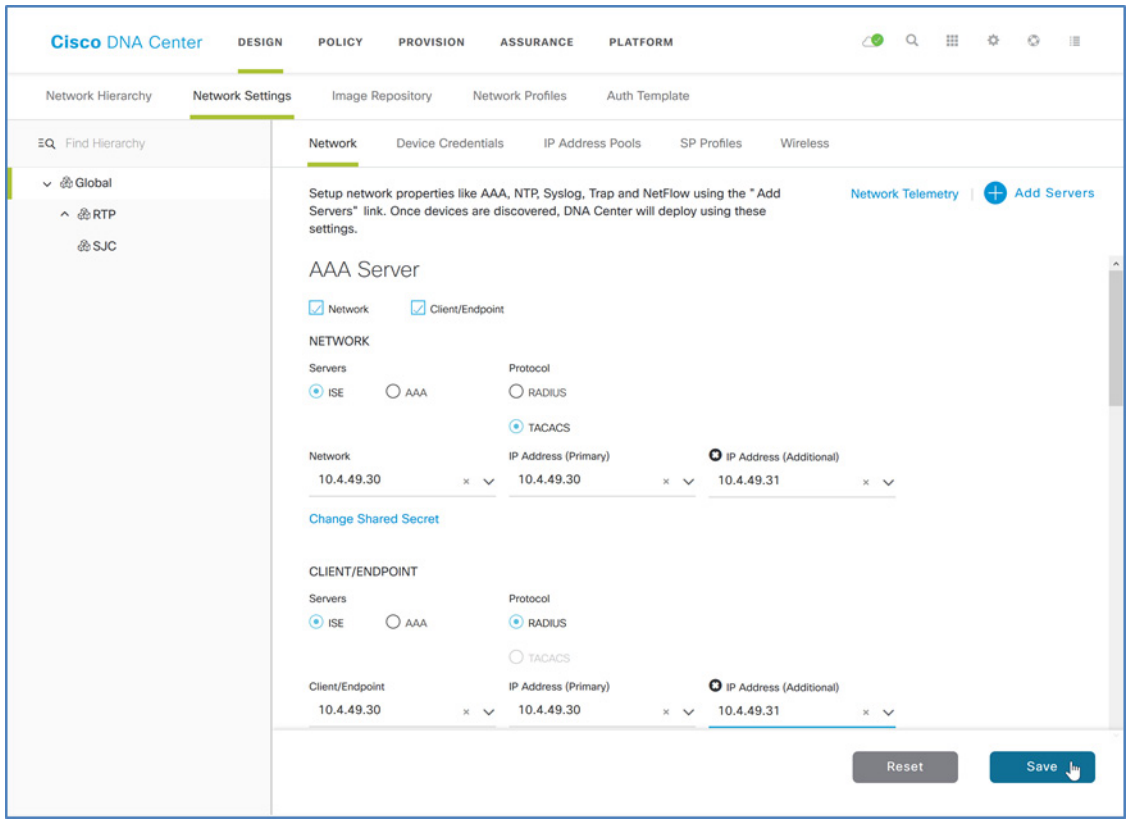
Le volet de configuration est mis à jour avec **AAA Server (Serveur AAA)** et **NTP Server (Serveur NTP)** comme sections de configuration disponibles. Vous configurez les services AAA pour l'administration du périphérique d'infrastructure réseau et pour les terminaux clients qui se connectent à l'infrastructure. Dans cet exemple, les nœuds ISE autonomes haute disponibilité sont utilisés.

Conseil technique
De nombreuses entreprises utilisent TACACS pour la prise en charge de l'administration des périphériques d'infrastructure. Si vous avez l'intention d'activer TACACS sur le serveur ISE utilisé pour l'authentification client RADIUS, vous devez également l'intégrer à Cisco DNA Center au cours de cette étape, en utilisant le menu déroulant **View Advanced Settings (Afficher les paramètres avancés)**. Vous trouverez des informations de configuration ISE pour activer l'intégration TACACS en accédant dans ISE à **Work Centers (Centres de travail) > Device Administration (Administration des périphériques) > Overview (Présentation)**.

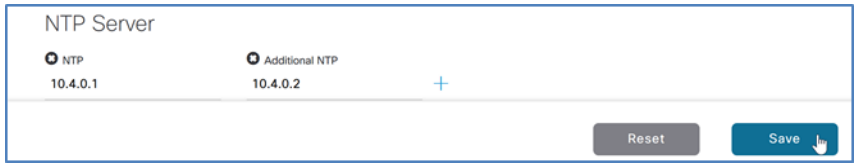
Étape 3. Sous **AAA Server (Serveur AAA)**, cochez les cases **Network (Réseau)** et **Client/Endpoint (Client/Terminal)**, sous **NETWORK (RÉSEAU)**, sélectionnez le bouton radio **ISE**, sous **Network (Réseau)**, utilisez le menu déroulant pour sélectionner le serveur ISE prérempli (par exemple : 10.4.49.30), sous **Protocol (Protocole)**, sélectionnez le bouton radio **TACACS**, sous **IP Address (Primary) (Adresse IP [principale])**, utilisez le deuxième menu déroulant pour sélectionner le serveur ISE principal (par exemple : 10.4.49.30), cliquez sur le bouton plus (**+**), puis dans la liste déroulante **IP Address (Additional) (Adresse IP [Supplémentaire])**, sélectionnez le nœud du serveur ISE redondant (par exemple : 10.4.49.31).

Pour garantir que la redondance du serveur ISE est correctement activée, vérifiez que les adresses IP principale et supplémentaire sont affichées avec l'adresse réseau sélectionnée avant de continuer.

Étape 4. Sous **CLIENT/ENDPOINT (CLIENT/TERMINAL)** et **Servers (Serveurs)**, sélectionnez le bouton radio **ISE**, sous **Client/Endpoint (Client/Terminal)**, utilisez la liste déroulante pour sélectionner le serveur ISE prérempli. Sous **Protocol (Protocole)**, sélectionnez le bouton radio **RADIUS**, sous **IP Address (Primary) (Adresse IP [Principale])**, utilisez la liste déroulante pour sélectionner le serveur ISE principal, cliquez sur le bouton de signe plus (**+**), puis sous **IP Address (Additional) (Adresse IP [Supplémentaire])**, utilisez la liste déroulante pour sélectionner le nœud de serveur ISE redondant, puis cliquez sur **Save (Enregistrer)**.



Étape 5. Dans le même écran, faites défiler l'écran jusqu'à **NTP Server (Serveur NTP)**, ajoutez la **IP Address (Adresse IP)** du serveur NTP (par exemple : 10.4.0.1), si vous avez un ou plusieurs serveurs NTP supplémentaires, cliquez sur le bouton de signe plus (**+**), puis dans **Additional NTP (NTP supplémentaire)**, ajoutez l'adresse IP des serveurs NTP redondants (par exemple : 10.4.0.2), puis cliquez sur **Save (Enregistrer)**.



Les serveurs ISE pour AAA et les serveurs pour DHCP, DNS et NTP pour le niveau sélectionné dans la hiérarchie du site sont tous enregistrés pour être utilisés lors du provisionnement de la fabric.

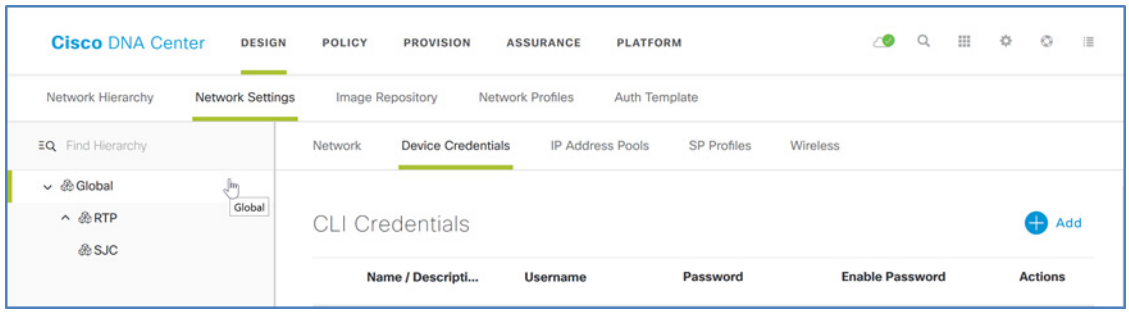
Procédure 3. Ajoutez des informations d'identification des périphériques pour la détection et la gestion

Lorsque vous déployez le SD-Access sous-jacent à l'aide de périphériques déjà configurés et qui sont accessibles à Cisco DNA Center via le réseau, vous pouvez détecter et gérer les périphériques en fournissant les informations d'identification de l'interface CLI et du protocole SNMP (Simple Network Management Protocol).

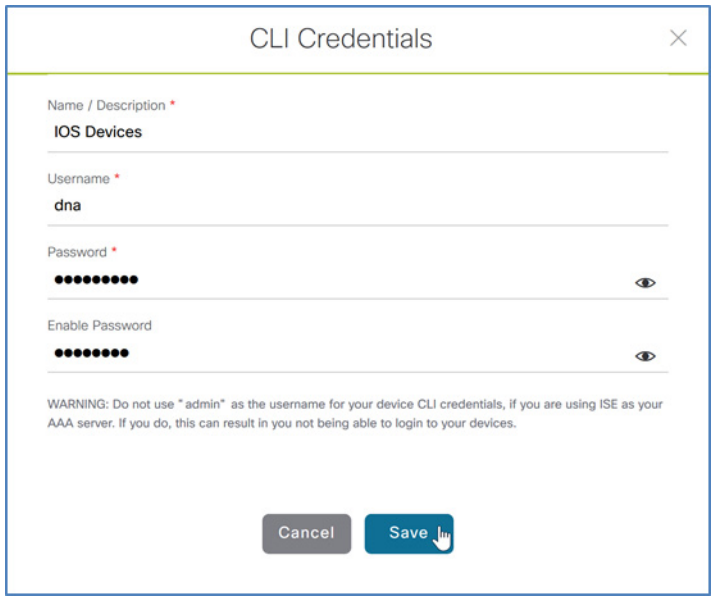
Vous pouvez également déployer des commutateurs LAN sans configurations existantes dans la sous-couche à l'aide des fonctionnalités d'automatisation du LAN de Cisco DNA Center. Cisco Network Plug and Play (PnP) est le mécanisme permettant la connectivité et la configuration initiale des commutateurs pris en charge. Pour les déploiements d'automatisation du LAN, vous pouvez également fournir des informations d'identification de l'interface de ligne de commande et SNMP pour accéder à et préparer un ou plusieurs périphériques PnP de départ pris en charge, tels que les commutateurs de la série Cisco Catalyst 9500, dans une distribution ou un cœur. L'automatisation du LAN permet de détecter les commutateurs directement connectés aux interfaces de périphériques de départ sélectionnées et leurs commutateurs voisins immédiats à l'aide de Cisco Discovery Protocol ; ils doivent tous exécuter l'agent PnP et ne pas avoir déjà été configurés. Les informations d'identification fournies permettent à Cisco DNA Center et aux périphériques de départ de fonctionner ensemble pour configurer les périphériques détectés et les ajouter à l'inventaire géré.

Ajoutez les informations d'identification de périphérique pour gérer les étendues de la hiérarchie de site créée dans la conception. Ces informations d'identification permettent de détecter et de gérer le réseau.

Étape 1. Dans Cisco DNA Center, accédez à **Design (Conception) > Network Settings (Paramètres réseau) > Device Credentials (Identifiants du périphérique)** et sélectionnez un niveau approprié de la hiérarchie du site dans le volet de gauche (par exemple : Global, pour les informations d'identification communes à toute la hiérarchie).



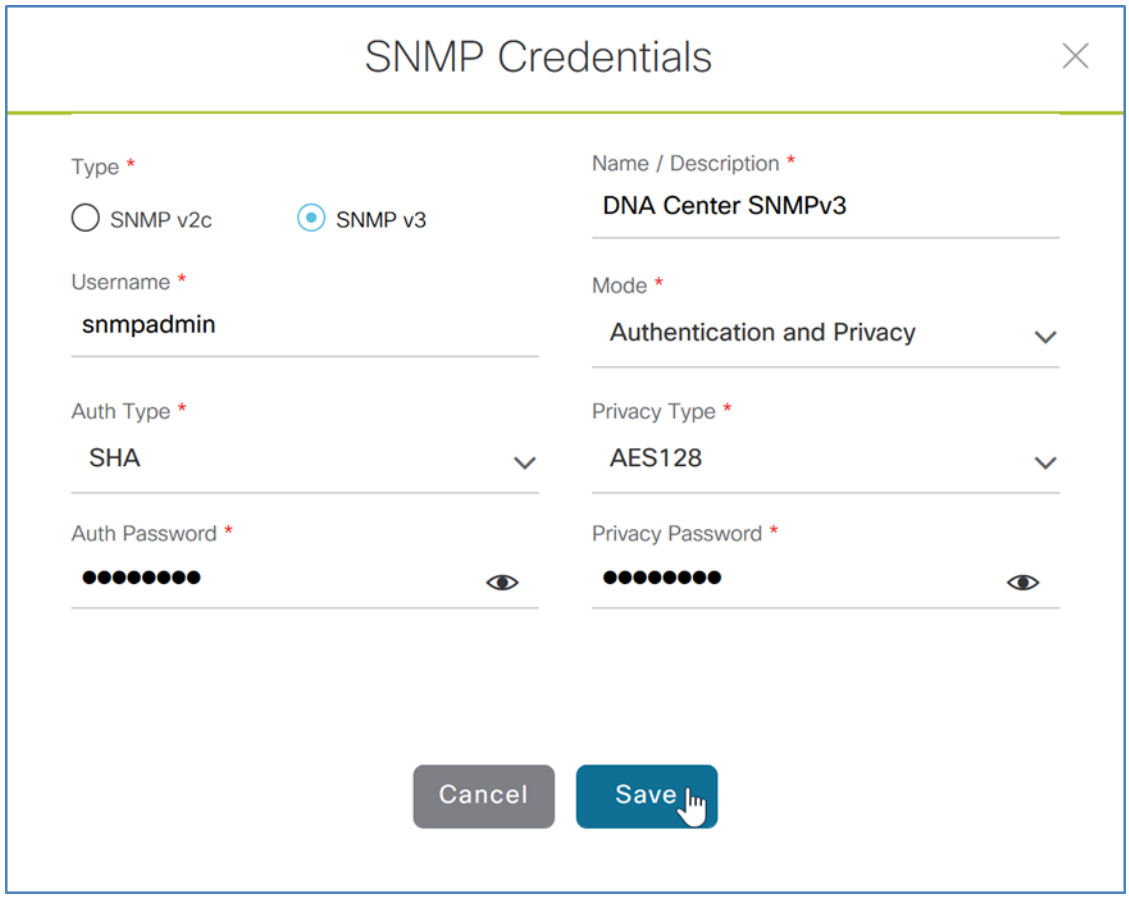
Étape 2. En haut de la section **CLI Credentials (Informations d'identification CLI)**, cliquez sur **Add (Ajouter)**, renseignez les champs **Name / Description (Nom / Description)** (par exemple : IOS Devices [Périphériques iOS]), **Username (Nom d'utilisateur)**, **Password (Mot de passe)** et **Enable Password (Activer le mot de passe)**, puis cliquez sur **Save (Enregistrer)**.



Avertissement

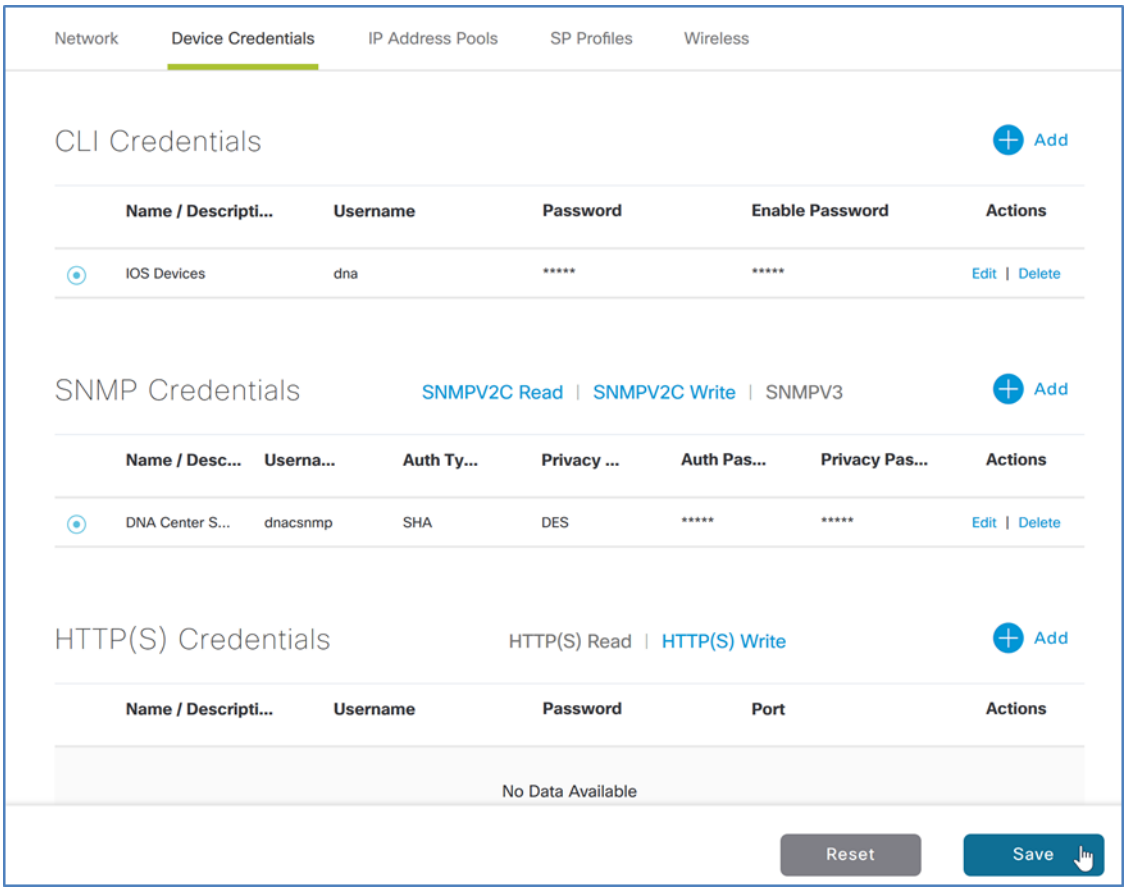
Si vous utilisez ISE en tant que serveur AAA, évitez d'utiliser **admin** comme nom d'utilisateur pour les informations d'identification de l'interface de ligne de commande du périphérique, car il risque d'entrer en conflit avec le nom d'utilisateur de l'administrateur ISE lorsque celui-ci est connecté, vous empêchant ainsi de vous connecter aux périphériques.

Étape 3. En haut de la section **SNMP Credentials (Informations d'identification SNMP)**, sélectionnez un type d'information d'identification SNMP à mettre à jour (par exemple : SNMPV3). Cliquez sur **Add (Ajouter)**, sélectionnez le bouton radio dans la ligne en regard des informations d'identification à mettre à jour (une seule information par ligne à la fois), complétez les informations d'identification (les mots de passe de 12 caractères sont recommandés pour la compatibilité avec les contrôleurs LAN sans fil Cisco), puis cliquez sur **Save (Enregistrer)**.



Étape 4. Répétez les étapes 2 et 3 pour toutes les informations d'identification supplémentaires requises dans la hiérarchie. Les **CLI Credentials (Informations d'identification de l'interface de ligne de commande)** et soit **SNMPV3**, soit **SNMPV2C Read (Lecture SNMPV2C)** et **SNMPV2C Write (Écriture SNMPV2C)** sont les exigences les plus courantes.

Étape 5. Pour chacun des identifiants de l'interface de ligne de commande et du protocole SNMP affectés, cliquez sur tous les boutons radio en regard de chaque affectation créée. Après chaque sélection, en bas de l'écran Device Credentials (Informations d'identification du périphérique), cliquez sur **Save (Enregistrer)**. Si vous avez utilisé plusieurs types d'informations d'identification SNMP, répétez cette étape en basculant chacune des options d'informations d'identification SNMP, en cliquant sur le bouton radio en regard de l'option, puis en cliquant sur **Save (Enregistrer)**.



Une confirmation Created Common Settings Successfully (Paramètres communs créés) s'affiche. Les informations d'identification du périphérique à utiliser pour la détection et la gestion du réseau sont désormais disponibles dans Cisco DNA Center.

Procédure 4. Définissez des pools d'adresses IP globales

Définissez les adresses IP de vos réseaux en les affectant manuellement dans Cisco DNA Center. Vous pouvez, si vous le souhaitez, envoyer les affectations d'adresses IP à un gestionnaire d'adresses IP (IPAM) (par exemple : Infoblox, BlueCat) en intégrant l'IPAM via les API. Vous pouvez effectuer l'intégration avec un IPAM en accédant à **System Settings (Paramètres système) > Settings (Paramètres) > IP Address Manager (Gestionnaire d'adresses IP)** et en remplissant le formulaire avec les caractéristiques de votre fournisseur IPAM. Dans cet exemple, où l'intégration IPAM n'est pas utilisée, vous configurez manuellement l'adressage IP et les étendues DHCP sur vos serveurs IPAM pour qu'ils correspondent aux affectations dans Cisco DNA Center.

Les étendues DHCP configurées sur le serveur DHCP doivent prendre en charge les allocations d'adresses et toutes les options DHCP supplémentaires requises pour faire fonctionner un périphérique. Par exemple, certains fournisseurs de téléphonie IP requièrent des options DHCP spécifiques pour permettre à leurs périphériques de fonctionner correctement (par exemple : l'option DHCP 150 pour la configuration par serveur TFTP). Consultez la documentation du produit pour répondre aux exigences de votre déploiement.

Cette procédure explique comment définir manuellement les pools d'adresses IP utilisés pendant le processus de réservation de pool. Ces pools sont affectés aux sites de votre réseau et les étapes d'affectation sont nécessaires pour les déploiements IPAM manuels et intégrés. Vous avez la possibilité de créer un pool global plus grand, puis de réserver un sous-ensemble du pool à des niveaux inférieurs dans la hiérarchie du site. Les pools d'adresses IP sont uniquement créés au niveau global et vous réservez des adresses des pools uniquement à des niveaux autres que le niveau global.

Le déploiement décrit dans ce guide utilise les pools d'adresses globaux répertoriés dans le tableau. Pour faciliter la compréhension, des espaces d'adressage plus petits sont utilisés pour la majeure partie du pool d'adresses global, par rapport à ce qu'une entreprise peut généralement déployer, par exemple un espace d'adressage /16 ou plus grand. Des pools d'adresses globaux plus importants prennent en charge de nombreuses réservations d'espace d'adressage plus petites dans la hiérarchie du site, comme illustré dans l'exemple EMPLOYEE. Bien que l'affectation de l'adresse d'une passerelle IP dans chaque pool soit requise, SD-Access utilise uniquement la passerelle lors de la création d'un réseau superposé. Le tableau contient également des exemples de pools disponibles pour une sous-couche LAN manuelle et une sous-couche LAN automatisée séparée, ainsi que pour l'appairage de multidiffusion.

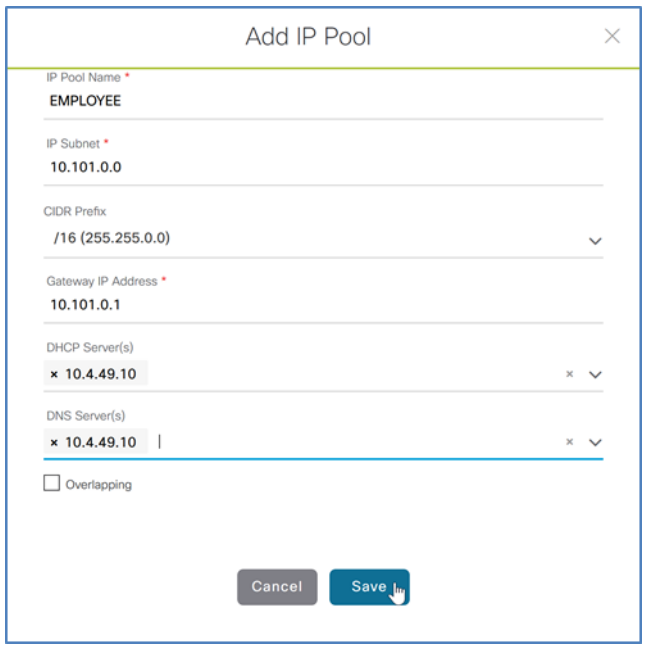
Tableau 1. Exemples de pools d'adresses globaux

Nom du pool	Réseau/masque	Passerelle IP	Dans le serveur DHCP	Dans le serveur DNS
EMPLOYEE	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
GUEST	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10
LAN_UNDERLAY	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10
LAN_AUTOMATION	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10
BORDER_HANDOFF	172.16.172.0/24	172.16.172.1	–	–
MULTICAST_PEER	172.16.173.0/24	172.16.174.1	–	–
ACCESS_POINT	172.16.174.0/24	172.16.173.1	10.4.49.10	10.4.49.10

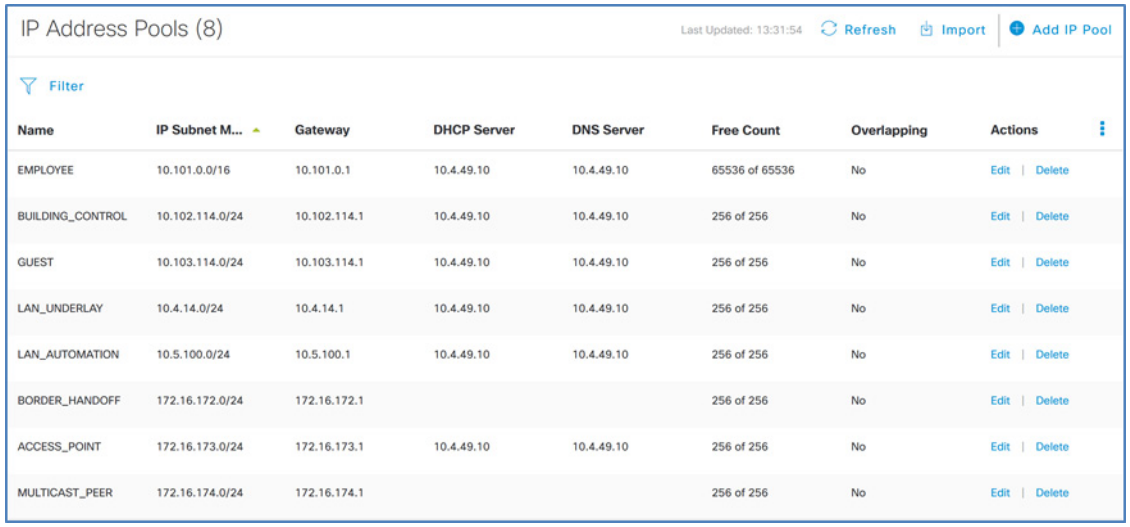
Tableau 2. Exemples de réservations de pools d'adresses du pool global EMPLOYEE

Nom du pool	Réseau/masque	Passerelle IP	Dans le serveur DHCP	Dans le serveur DNS
EMPLOYEE-DATA-RTP5	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
EMPLOYEE-PHONE-RTP5	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10

Étape 1. Ajoutez un pool global dans Cisco DNA Center dédié au provisionnement de la connectivité du nœud de frontière de fabric SD-Access. Dans Cisco DNA Center, accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > IP Address Pools (Pools d'adresses IP)**. Dans la hiérarchie du site à gauche, sélectionnez **Global**, puis cliquez sur **+ Add IP Pool (Ajouter un pool d'adresses IP)**. Renseignez **IP Pool Name (Nom du pool d'adresses IP)**, **IP Subnet (Sous-réseau IP)**, **CIDR Prefix (Préfixe CIDR)** et **Gateway IP Address (Adresse IP de la passerelle)**. Si le pool dispose de clients terminaux, utilisez les menus déroulants pour affecter le ou les **DHCP Server(s) (Serveur[s] DHCP)** et le ou les **DNS Server(s) (Serveur[s] DNS)**. Ne sélectionnez pas **Overlapping (Chevauchement)**. Une fois que vous avez terminé, cliquez sur **Save (Enregistrer)**.



Étape 2. Répétez l'étape précédente pour tout pool d'adresses IP global supplémentaire incluant des sous-réseaux au niveau du site et du bâtiment. Les pools sont ajoutés à la liste des pools globaux.

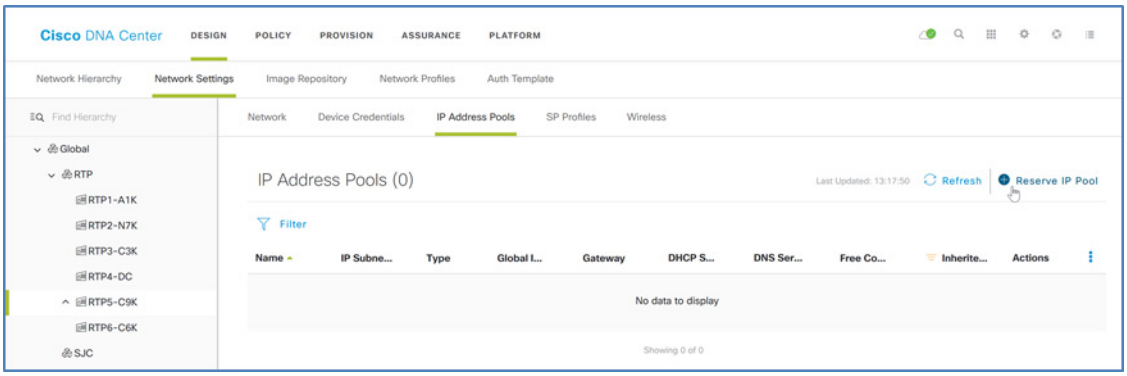


Name	IP Subnet M...	Gateway	DHCP Server	DNS Server	Free Count	Overlapping	Actions
EMPLOYEE	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10	65536 of 65536	No	Edit | Delete
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
GUEST	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
LAN_UNDERLAY	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
LAN_AUTOMATION	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
BORDER_HANDOFF	172.16.172.0/24	172.16.172.1			256 of 256	No	Edit | Delete
ACCESS_POINT	172.16.173.0/24	172.16.173.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
MULTICAST_PEER	172.16.174.0/24	172.16.174.1			256 of 256	No	Edit | Delete

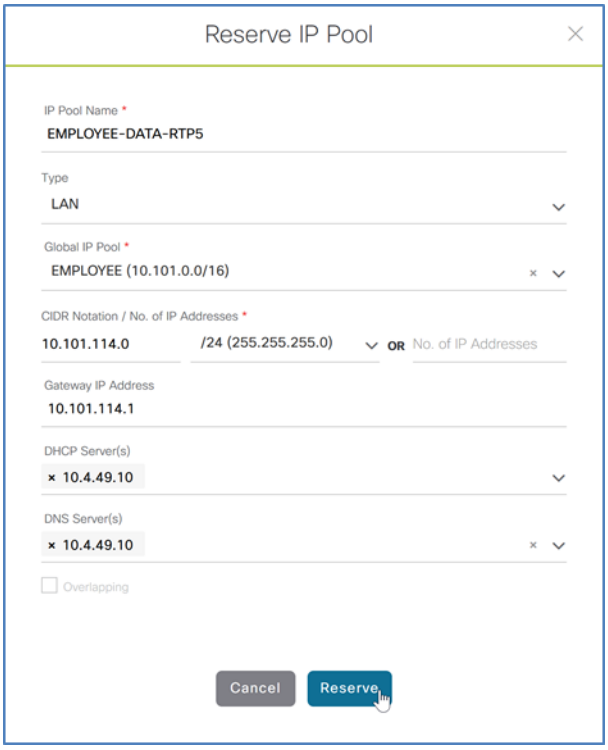
Procédure 5. Réserver des pools d'adresses IP

Utilisez les pools d'adresses IP globaux définis pour réserver des adresses IP aux sites de votre conception à l'aide de la hiérarchie de réseau. Pour les déploiements à site unique, il est possible de réserver l'ensemble des pools d'adresses IP globaux pour le site en question. Lorsque vous réservez des adresses à partir des pools d'adresses IP globaux définis, les serveurs DNS et DHCP peuvent être utilisés dans ces réservations, ou ils peuvent être remplacés.

Étape 1. Dans Cisco DNA Center, accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > IP Address Pools (Pools d'adresses IP)**, à gauche dans la hiérarchie du site, sélectionnez un site ou un niveau inférieur pour la réservation d'un pool d'adresses IP (par exemple : RTP5-C9K), puis, dans le coin supérieur droit, cliquez sur **Reserve IP Pool (Réserver un pool d'adresses IP)**.



Étape 2. Renseignez **IP Pool Name (Nom du pool d'adresses IP)** (par exemple : EMPLOYEE-DATA-RTP5), sous **Type**, sélectionnez **LAN**, sélectionnez la source du **Global IP Pool (Pool d'adresses IP global)** pour la réservation (par exemple : EMPLOYEE), sous **CIDR Notation / No. of IP Addresses (Notation CIDR/No. des adresses IP)**, sélectionnez la partie de l'espace d'adressage à utiliser (par exemple : 10.101.114.0/24), affectez une **Gateway IP Address (Adresse IP de passerelle)** (par exemple : 10.101.114.1), utilisez le menu déroulant pour affecter le ou les **DHCP Server(s) (Serveur[s] DHCP)** et le ou les **DNS Servers(s) (Serveur[s] DNS)**, puis cliquez sur **Reserve (Réserver)**.



Étape 3. Répétez l'étape précédente pour tous les blocs d'adresses de pools globaux qui doivent être réservés dans la hiérarchie pour chaque site.

La hiérarchie présente les pools d'adresses affectés. Cet exemple présente les réservations de pools dans le site RTP, au niveau du bâtiment RTP5-C9K.

Processus : création de la segmentation et de la politique pour le réseau SD-Access

Dans le cadre des décisions de conception à prendre pour préparer votre déploiement de réseau SD-Access, vous choisissez des stratégies de segmentation du réseau pour l'entreprise. La macrosegmentation utilise des réseaux superposés (VN) supplémentaires dans la fabric, et la microsegmentation utilise des balises de groupe dimensionnables pour appliquer la politique à des groupes d'utilisateurs ou des profils de périphériques.

Utilisez des stratégies de groupe pour obtenir facilement les résultats souhaités à l'aide de la segmentation. Par exemple dans une université, les machines des étudiants et des enseignants peuvent être autorisées à accéder aux ressources d'impression, mais les machines des étudiants ne doivent pas communiquer directement avec les machines du corps enseignant, et les périphériques d'impression ne doivent pas communiquer les uns avec les autres.

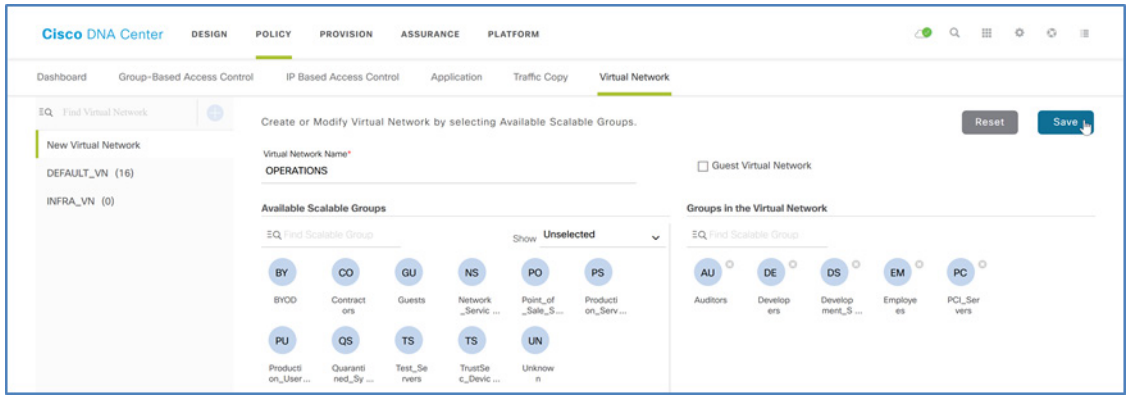
Dans d'autres cas, un meilleur isolement est nécessaire. Par exemple, dans un magasin, les machines de point de vente ne doivent jamais communiquer avec l'infrastructure réseau de surveillance vidéo, qui elle-même ne doit jamais communiquer avec le système de chauffage, de ventilation et de climatisation du bâtiment. Dans les cas où les besoins d'isolation vont de la périphérie du réseau jusqu'au cœur du réseau pour accéder aux services centralisés, la macrosegmentation à l'aide de réseaux de superposition (VN) est le meilleur choix. Les exigences en matière de conformité gouvernementale et industrielle, ainsi que les politiques en matière de risque de l'entreprise, conduisent souvent à utiliser la macrosegmentation.

Pour une exploration plus approfondie de la conception de la segmentation pour SD-Access, avec des exemples d'utilisation, consultez le document Guide de conception de la segmentation SD-Access sur Cisco.com.

Utilisez ces procédures comme exemples de déploiement de vos politiques de macrosegmentation et de microsegmentation.

Procédure 1. Ajoutez une liaison VN superposée au réseau SD-Access

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **POLICY (POLITIQUE) > Virtual Network (Réseau virtuel)**, cliquez sur le signe plus (**+**) pour créer un nouveau réseau virtuel, saisissez un **Virtual Network Name (Nom de réseau virtuel)** (par exemple : OPERATIONS), faites glisser les groupes évolutifs depuis le pool **Available Scalable Groups (Groupes évolutifs disponibles)** vers le pool **Groups in the Virtual Network (Groupes du réseau virtuel)** (par exemple : Auditors, Developers, Development_Servers, Employees, et PCI_Servers), puis cliquez sur **Save (Enregistrer)**.



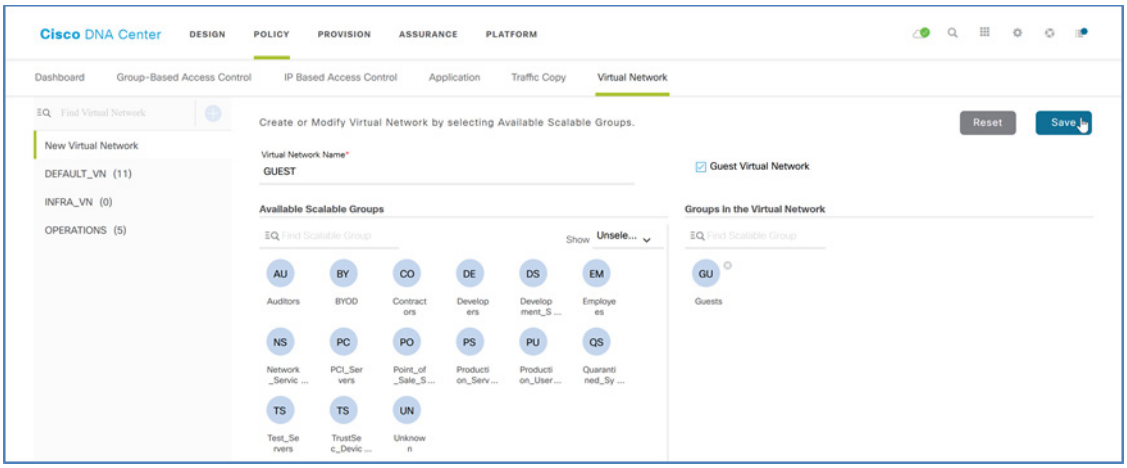
Le VN avec les groupes associés est défini et apparaît dans la liste des réseaux virtuels définis. Ces définitions de réseau virtuel sont disponibles pour le provisionnement des fabrics.

Conseil technique
Si vous ne voyez aucun groupe, il est probable que la connectivité pxGrid entre Cisco DNA Center et ISE n'est pas entièrement opérationnelle. Dans ce cas, passez en revue les procédures d'intégration d'ISE avec Cisco DNA Center et veillez à approuver la demande de connexion pxGrid dans ISE depuis Cisco DNA Center.

Étape 2. Si votre entreprise exige des groupes différents des groupes par défaut, créez des groupes personnalisés en accédant à **POLICY (POLITIQUE) > Group-Based Access Control (Contrôle d'accès basé sur des groupes) > Scalable Groups (Groupes évolutifs)**, puis cliquez sur **Add Groups (Ajouter des groupes)** pour créer un nouveau groupe et une nouvelle balise SGT.

Étape 3. Répétez les deux premières étapes pour chaque réseau superposé. Vous pouvez également revenir à ces étapes après le provisionnement de la fabric afin de créer d'autres réseaux superposés.

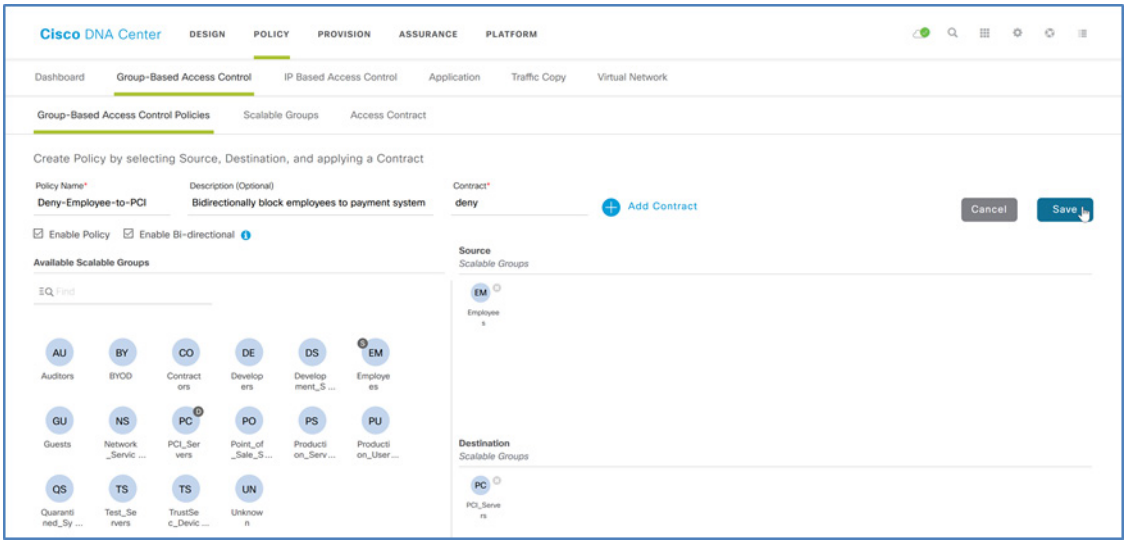
Étape 4. De nombreux réseaux nécessitent un service invité pour les utilisateurs sans fil : créez un VN invité pour prendre en charge cette fonctionnalité. Dans le tableau de bord principal de Cisco DNA Center, accédez à **POLICY (POLITIQUE) > Virtual Network (Réseau virtuel)**, cliquez sur le signe plus (**+**) pour créer un nouveau réseau virtuel, saisissez un **Virtual Network Name (Nom de réseau virtuel)** (par exemple : GUEST), cochez la case en regard de **Guest Virtual Network (Réseau virtuel invité)**, faites glisser les groupes évolutifs **Guests (Invités)** du pool **Available Scalable Groups (Groupes évolutifs disponibles)** vers le pool **Groups in the Virtual Network (Groupes du réseau virtuel)**, puis cliquez sur **Save (Enregistrer)**.



Procédure 2. Créez une politique de microsegmentation à l'aide de balises de groupe de sécurité (SGT)

Les politiques de microsegmentation sont personnalisées pour le déploiement d'une entreprise. Cet exemple simple montre une politique de base qui peut être utilisée pour empêcher les utilisateurs du groupe Employee de communiquer avec le groupe PCI_Servers. Lorsque les profils d'authentification affectent de manière appropriée une balise SGT à un terminal ou à un utilisateur, ISE capture l'objectif de cette politique et la restitue dans le réseau.

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **POLICY (POLITIQUE) > Group-Based Access Control (Contrôle d'accès basé sur les groupes) > Group-Based Access Control Policies (Politiques de contrôle d'accès basé sur les groupes)**, cliquez sur **+ Add Policy (Ajouter une politique)**, dans le volet **Available Scalable Groups (Groupes évolutifs disponibles)**, faites glisser le groupe **Employees** et déposez-le dans le volet **Source**, faites glisser le groupe **PCI_Servers** dans le volet **Destination**, saisissez un **Policy Name (Nom de politique)** (par exemple : Deny-Employee-to-PCI), saisissez une **Description**, sélectionnez **Enable Policy (Activer la politique)**, sélectionnez **Enable Bi-directional (Activer bidirectionnel)**, cliquez sur **+ Add Contract (Ajouter un contrat)**, sélectionnez **deny (refuser)**, cliquez sur **OK**, puis cliquez sur **Save (Enregistrer)**.



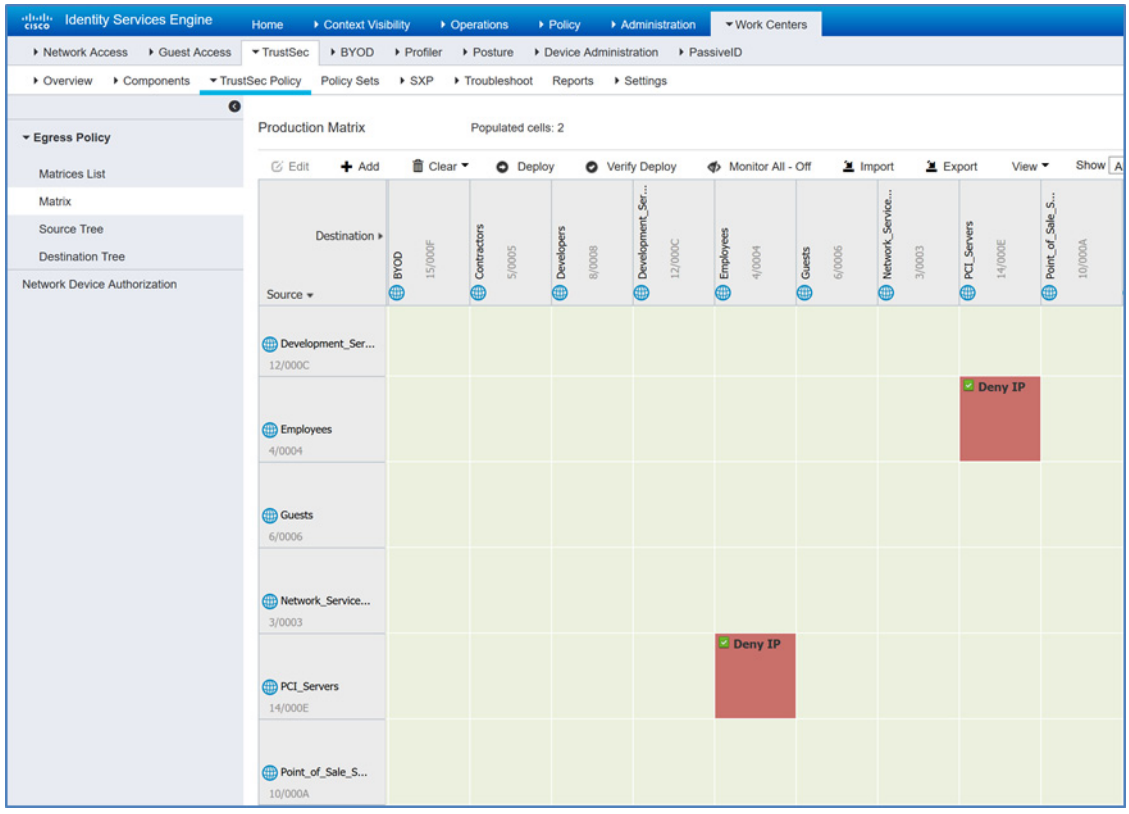
La politique est créée et est répertoriée avec l'état **CREATED (CRÉÉE)**. En raison de la sélection de l'option bidirectionnelle, la politique inverse est également créée.

Étape 2. Sélectionnez les politiques créées, puis cliquez sur **Deploy (Déployer)**.

L'état passe à **DEPLOYED (DÉPLOYÉ)** et les politiques sont disponibles pour être appliquées aux fabrics SD-Access que Cisco DNA Center crée et sont également disponibles dans ISE, affichables à l'aide de la matrice de politiques Cisco TrustSec.

Étape 3. En haut à droite, cliquez sur **Advanced Options (Options avancées)**. Le lien est un raccourci pour se connecter à ISE, accéder aux **Work Centers (Centres de travail) > TrustSec > TrustSec Policy (Politique TrustSec)**, puis sur le côté gauche, sélectionner **Matrix (Matrice)**. Vous êtes redirigé pour vous connecter à ISE, qui redirige le navigateur et affiche la matrice de politique TrustSec.

Vérifiez que la politique a été mise à jour vers ISE pour être restituée dans le réseau.



Processus : préparation pour l'automatisation de la gestion du réseau

Préparez-vous à déployer les conceptions et les politiques de réseau en créant une sous-couche réseau opérationnelle comprenant la connectivité de gestion des périphériques. Dans le cadre de l'intégration d'ISE avec Cisco DNA Center illustrée dans le document Guide normatif de déploiement de SD-Access pour les réseaux locaux distribués, l'ISE est configuré avec la prise en charge de l'administration des périphériques d'infrastructure TACACS. Pour les configurations TACACS, Cisco DNA Center modifie les périphériques détectés afin qu'ils utilisent les services d'authentification et de gestion des comptes de l'ISE et les serveurs de basculement locaux par défaut. L'ISE doit être préparé pour prendre en charge les configurations d'administration des périphériques envoyées aux périphériques pendant le processus de détection.

Procédure 1. Configuration de la gestion des périphériques réseau sous-jacents à l'aide de l'interface de ligne de commande Cisco IOS-XE

Pour une résilience et une bande passante maximales, utilisez une interface de bouclage sur chaque périphérique et activez la connectivité de couche 3 pour la découverte et la gestion intrabande de Cisco DNA Center. Les étapes suivantes configurent la connectivité Ethernet point à point entre des périphériques qui utilisent IS-IS comme protocole de routage et SSHv2 pour la configuration du périphérique à l'aide des interfaces de bouclage de ce dernier. La configuration SNMP est repoussée à une procédure ultérieure dans le cadre de la détection de périphériques.

N'ajoutez pas de configuration aux périphériques que vous avez l'intention de détecter et de configurer à l'aide de l'automatisation LAN dans le cadre d'une procédure ultérieure. Les périphériques ayant des configurations existantes ne peuvent pas être configurés à l'aide de l'automatisation LAN. Cet exemple présente une configuration utilisant Cisco IOS XE sur un commutateur Cisco Catalyst.

Étape 1. Utilisez l'interface de ligne de commande du périphérique pour configurer le nom d'hôte afin d'en faciliter l'identification et de désactiver les services inutilisés.

```
hostname [hostname]
no service config
```

Étape 2. Configurez la connexion et le mot de passe locaux.

```
username dna privilege 15 algorithm-type scrypt secret [password]
! older software versions may not support scrypt (type 9)
! username dna privilege 15 secret [password]
enable secret [enable password]
service password-encryption
```

Étape 3. Configurez le protocole SSH (Secure Shell) comme méthode d'accès à la gestion sur la ligne de commande.

```
ip domain-name ciscodna.net
! generate key with choice of modulus, required by some switches
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 15
  login local
  transport input ssh
  transport preferred none
```

Étape 4. Configurez le commutateur de façon qu'il prenne en charge les trames Ethernet Jumbo. L'unité de transmission maximale (MTU) choisie autorise les en-têtes de fabric supplémentaires et permet la compatibilité avec la valeur commune la plus élevée sur la plupart des commutateurs, et le nombre arrondi doit être facile à retenir lors de la configuration et du dépannage.

```
system mtu 9100
```

Conseil technique

La connectivité sous-jacente à l'aide de Cisco IOS XE sur les routeurs nécessite l'utilisation d'une commande **mtu** au niveau de la configuration de l'interface, et les commutateurs Cisco Catalyst et Cisco Nexus® qui n'utilisent pas Cisco IOS XE utilisent une commande **system jumbo mtu** au niveau de configuration global.

Étape 5. Configurez l'adresse de bouclage du commutateur et affectez la gestion SSH pour l'utiliser.

interface Loopback***0***

ip address ***[Device loopback IP address]*** 255.255.255.255

ip ssh source-interface Loopback***0***

Procédure 2. Configurez les liaisons réseau sous-jacentes pour la connectivité d'accès routée

Si votre réseau sous-jacent est déjà configuré à l'aide d'un modèle de déploiement de réseau à accès routé, ignorez cette procédure. Les déploiements de couche 2 standard nécessitent cette procédure.

N'ajoutez pas de configuration aux périphériques que vous avez l'intention de détecter et de configurer à l'aide de la fonctionnalité d'automatisation LAN. Il n'est pas possible de configurer les périphériques dotés de configurations existantes à l'aide de l'intégration de l'automatisation LAN sans les réinitialiser aux configurations par défaut d'origine.

Étape 1. Configurez les connexions de commutateur dans l'infrastructure de réseau sous-jacente. Répétez cette étape pour chaque liaison à un commutateur voisin dans la fabric sous-jacente. Si le périphérique sous-jacent est provisionné en tant que nœud de frontière de fabric et que la connexion doit être utilisée en tant que transfert de la fabric vers l'infrastructure externe, utilisez plutôt la procédure suivante.

```
interface TenGigabitEthernet1/0/1
 no switchport
 ip address [Point-to-point IP address] [netmask]
```

Étape 2. Activez le routage IP et activez le protocole de routage IS-IS sur le commutateur.

```
! ip routing is not enabled by default on some switches
ip routing
ip multicast-routing
ip pim register-source Loopback0
ip pim ssm default
router isis
 net 49.0000.0100.0400.0001.00
 domain-password [domain password]
 metric-style wide
 nsf ietf
 log-adjacency-changes
 bfd all-interfaces
```

Conseil technique

Une convention courante dans IS-IS consiste à intégrer l'adresse IP de bouclage dans le réseau unique ou l'ID système. Par exemple, une adresse IP de bouclage ***10.4.32.1*** (***010.004.032.001***) est regroupée pour devenir ***0100.0403.2001***, la valeur ***.00*** lui est ajoutée et elle est précédée d'un ID de zone, tel que ***49.0000***, ce qui se traduit par NET ***49.0000.0100.0403.2001.00***.

Étape 3. Activez le routage IS-IS sur toutes les interfaces d'infrastructure configurées dans la sous-couche, à l'exception des interfaces de transfert de frontière, qui sont configurées dans la procédure suivante. L'interface de bouclage est activée pour partager l'adresse IP de gestion et les interfaces physiques sont activées pour partager les informations de routage avec l'infrastructure connectée.

```
interface Loopback0
! ip address assigned in earlier step
 ip router isis
 ip pim sparse-mode
interface range TenGigabitEthernet1/0/1-2,  TenGigabitEthernet2/0/1-2
! routed ports with ip addresses assigned via earlier steps
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 dampening
```

Procédure 3. Activer la connectivité de routage à la frontière avec le routeur externe voisin

Si votre réseau sous-jacent est déjà configuré en tant que réseau d'accès routé et intégré au reste de votre réseau à l'aide de BGP avec un transfert 802.1Q, ignorez cette procédure. La plupart des déploiements nécessitent cette procédure.

Pour connecter des périphériques de nœuds de frontière à votre réseau, vous devez établir une connectivité entre les interfaces configurées à l'aide de VRF-Lite, qui utilise le balisage VLAN 802.1Q pour séparer les VRF. Connectez les services réseau communs disponibles en dehors des nœuds de frontière tels que DNS, DHCP, les contrôleurs LAN sans fil et la gestion Cisco DNA Center lorsqu'ils ne sont pas directement connectés aux nœuds de réseau SD-Access, en étendant votre réseau d'entreprise existant à la sous-couche située à la frontière. La connectivité à Cisco DNA Center est nécessaire pour effectuer un provisionnement supplémentaire.

Le périphérique externe qui gère le routage entre plusieurs réseaux virtuels et une instance de routage globale fait office de routeur de fusion pour ces réseaux. La séparation de la connectivité est assurée à l'aide de VRF connectés par des interfaces balisées 802.1Q avec la frontière, également appelés VRF-Lite. L'établissement de la connectivité sous-jacente à l'aide du protocole BGP permet à Cisco DNA Center de gérer la détection et la configuration initiales à l'aide de la liaison, puis d'utiliser la même liaison augmentée de balises et de sessions BGP supplémentaires si nécessaire pour la connectivité VN de superposition.

Étape 1. Pour chaque nœud de frontière, si vous configurez un commutateur prenant en charge les interfaces trunk de VLAN, comme les commutateurs de la série Cisco Catalyst 9000, 3800 ou 6800, vous devez configurer un trunk sur l'interface connectée avec un VLAN dédié pour établir la connectivité sous-jacente pour l'appairage de route vers le routeur de fusion.

```
vlan 100
interface vlan100
```

```
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
interface FortyGigabitEthernet1/0/24
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 100
 no shutdown
```

Étape 2. Pour chaque nœud de frontière, si vous configurez un périphérique tel qu'un routeur ASR ou ISR qui prend en charge le balisage VLAN 802.1Q, utilisez une autre configuration de sous-interface au lieu d'une interface trunk de commutateur pour établir la connectivité sous-jacente au routeur de fusion.

```
interface TenGigabitEthernet0/1/0
 no shutdown
!
interface TenGigabitEthernet0/1/0.100
 encapsulation dot1Q 100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
```

Étape 3. Connectez les nœuds de frontière redondants avec au moins une interface routée pour la communication sous-jacente et l'appairage BGP ultérieur. La configuration pour l'intégration au protocole IS-IS est indiquée. Répétez cette étape pour chaque interface reliant des nœuds de frontière.

```
interface FortyGigabitEthernet1/0/23
 no switchport
 ip address [Point-to-point IP address] [netmask]
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
no shutdown
```

Étape 4. Activez le routage BGP vers le routeur de fusion pour la connectivité aux réseaux externes à la fabric et activez BGP sur les interfaces de connexion. Configurez le protocole BGP pour autoriser l'accès de gestion de Cisco DNA Center aux périphériques réseau sous-jacents, tout en autorisant le provisionnement des réseaux virtuels sur les interfaces et en limitant les interruptions de la connectivité réseau. Répétez cette étape pour chaque nœud de frontière.

```
router bgp [underlay AS number]
 bgp router-id [loopback 0 IP address]
 bgp log-neighbor-changes
! fusion router is an eBGP neighbor
 neighbor [fusion interface IP address] remote-as [external AS number]
! redundant border is an iBGP neighbor
 neighbor [redundant border Lo0 address] remote-as [underlay AS number]
```

```
neighbor [redundant border Lo0 address] update-source Loopback0
!
address-family ipv4
 network [Lo0 IP address] mask 255.255.255.255
! advertise underlay IP network summary in global routing table
 aggregate-address [underlay IP network summary] [netmask] summary-only
 redistribute isis level-2
 neighbor [fusion interface IP address] activate
 neighbor [redundant border Lo0 address] activate
 maximum-paths 2
exit-address-family
```

Procédure 4. Redistribuer les sous-réseaux de services partagés dans l'IGP sous-jacent

Une route par défaut dans la sous-couche ne peut pas être utilisée par les points d'accès pour atteindre le contrôleur LAN sans fil. Une route plus spécifique (telle qu'une route de sous-réseau /24 ou d'hôte /32) vers l'adresse IP du contrôleur LAN sans fil doit exister dans la table de routage globale sur chaque nœud où les points d'accès se connectent pour établir la connectivité. Autorisez les routes plus spécifiques pour les services partagés de contrôleur LAN sans fil et DHCP requis de BGP (par exemple : 10.4.174.0/24 et 10.4.48.0/21) dans le réseau sous-jacent en redistribuant la route des services partagés à la frontière dans le processus de routage IGP sous-jacent à l'aide de cette procédure. Avec ce processus, les préfixes utilisés correspondent aux préfixes dans la table de routage BGP.

Étape 1. Connectez-vous à chaque nœud de frontière et ajoutez une liste de préfixes et une table de routage pour les sous-réseaux utilisés pour les services partagés.

```
ip prefix-list SHARED_SERVICES_NETS seq 5 permit 10.4.48.0/21
ip prefix-list SHARED_SERVICES_NETS seq 10 permit 10.4.174.0/24
route-map GLOBAL_SHARED_SERVICES_NETS permit 10
 match ip address prefix-list SHARED_SERVICES_NETS
```

Étape 2. À chaque nœud de frontière, redistribuez les préfixes dans votre protocole de routage sous-jacent. Cet exemple suppose l'utilisation d'ISIS.

```
router isis
 redistribute bgp [underlay AS number] route-map GLOBAL_SHARED_SERVICES_NETS metric-type external
```

Procédure 5. Activer la connectivité au niveau du routeur de fusion externe vers le voisin de frontière

Les routeurs de fusion connectés à vos routeurs de frontière de fabric nécessitent une configuration CLI pour une connectivité sous-jacente cohérente avec les procédures précédentes. Procédez comme suit pour chaque routeur de fusion externe connecté à une frontière.

Le routeur de fusion exemple est configuré avec l'appairage de route entre un VRF contenant les routes globales à l'échelle de l'entreprise et la table de routage globale à la frontière pour l'accessibilité de la fabric sous-jacente, sans utiliser la table de routage globale du routeur de fusion.

Il est également possible d'effectuer un appairage entre la table de routage globale à l'échelle de l'entreprise du routeur de fusion et la table de routage globale sur la frontière, sans utiliser de VRF.

Étape 1. Sur chaque routeur de fusion externe, créez le VRF, le différentiateur de route et les cibles de route pour la connectivité de gestion initiale à la frontière.

```
vrf definition VRF-GLOBAL_ROUTES
 rd 100:100
 !
 address-family ipv4
  route-target export 100:100
  route-target import 100:100
exit-address-family
```

Étape 2. Pour chaque connexion entre le routeur fusion externe et la frontière de fabric SD-Access, activez l'interface, la sous-interface avec balisage VLAN et l'adressage IP. Cet exemple utilise le balisage VLAN 802.1Q sur un routeur avec des sous-interfaces. Pour les commutateurs nécessitant des configurations de ports trunk, associez l'autre côté précédemment configuré.

```
interface TenGigabitEthernet0/1/7
 description to Border
 mtu 9100
 no ip address
 no shutdown
interface TenGigabitEthernet0/1/7.100
 encapsulation dot1Q 100
 vrf forwarding VRF-GLOBAL_ROUTES
 ip address [IP network] [netmask]
```

La connectivité IP est maintenant activée pour le VLAN (par exemple : 100) sur la connexion avec balises 802.1Q entre le routeur de fusion et le nœud de frontière.

Étape 3. Créez des mappages de route pour baliser les routes et éviter les boucles de routage lors de la redistribution entre le protocole IGP utilisé dans le reste du réseau et le protocole BGP lors de la connexion à l'aide de plusieurs liaisons. Les protocoles IGP peuvent varier : l'exemple donné est pour EIGRP, qui complète la connectivité de routage de IS-IS à BGP et à EIGRP.

```
route-map RM-BGP-TO-EIGRP permit 10
 set tag 100
!
route-map RM-EIGRP-TO-BGP deny 10
 match tag 100
route-map RM-EIGRP-TO-BGP permit 20
```

Étape 4. Activez l'appairage BGP depuis les routeurs de fusion redondants vers les nœuds de frontière et redistribuez l'IGP utilisé pour atteindre les réseaux au-delà des routeurs de fusion.

```
router bgp [external AS number]
 bgp router-id [loopback IP address]
 bgp log-neighbor-changes
 !
address-family ipv4 vrf VRF-GLOBAL_ROUTES
  redistribute eigrp 100 route-map RM-EIGRP-TO-BGP
  neighbor [redundant fusion IP] remote-as [external AS number]
  neighbor [redundant fusion IP] activate
```

```
 neighbor [border IP address] remote-as [underlay AS number]
 neighbor [border IP address] activate
 maximum-paths 2
 default-information originate
exit-address-family
```

Étape 5. Redistribuez BGP dans IGP pour permettre l'accessibilité. Les protocoles IGP peuvent varier : l'exemple illustré est pour l'EIGRP en mode nommé.

```
router eigrp LAN
 !
 address-family ipv4 unicast vrf VRF-GLOBAL_ROUTES autonomous-system 100
  topology base
   redistribute bgp [external AS number] metric 1000000 1 255 1 9100 route-map RM-BGP-
TO-EIGRP
  exit-af-topology
  network [external IP network address] [netmask]
  eigrp router-id [loopback IP address]
 exit-address-family
```

Procédure 6. Configuration de la MTU sur les périphériques intermédiaires non gérés

En option

Il est avantageux de faire en sorte que Cisco DNA Center gère tous les périphériques d'un domaine de fabric. Cisco DNA Center gère déjà les nœuds de périphérie de la fabric et les nœuds de frontière ; toutefois, si vous avez des périphériques intermédiaires dans la fabric qui ne seront pas gérés par Cisco DNA Center (par exemple : l'assistance matériel ou logiciel n'est pas disponible dans Cisco DNA Center), les périphériques doivent toujours satisfaire aux exigences de transport du trafic SD-Access via ces nœuds intermédiaires de fabric de transit. Les principales exigences sont les suivantes :

- Il doit s'agir de périphériques de couche 3 qui participent activement à la topologie de routage dans les autres périphériques sous-jacents de fabric.
- Ils doivent être capables de transporter les trames jumbo que permettent les techniques d'encapsulation de fabric.

Pour les nœuds intermédiaires non gérés de la fabric, vous devez définir une MTU appropriée (par exemple : 9100) et configurer manuellement le routage avec les autres périphériques de la sous-couche. Les instructions de configuration dans cette situation sont spécifiques au périphérique et ne sont pas traitées plus en détail dans ce guide.

N'ajoutez pas de configuration aux périphériques que vous avez l'intention de détecter et de configurer à l'aide de l'automatisation LAN dans le cadre d'une procédure ultérieure. Les périphériques ayant des configurations existantes ne peuvent pas être configurés à l'aide de l'automatisation LAN.

Procédure 7. Détecter et gérer les périphériques réseau

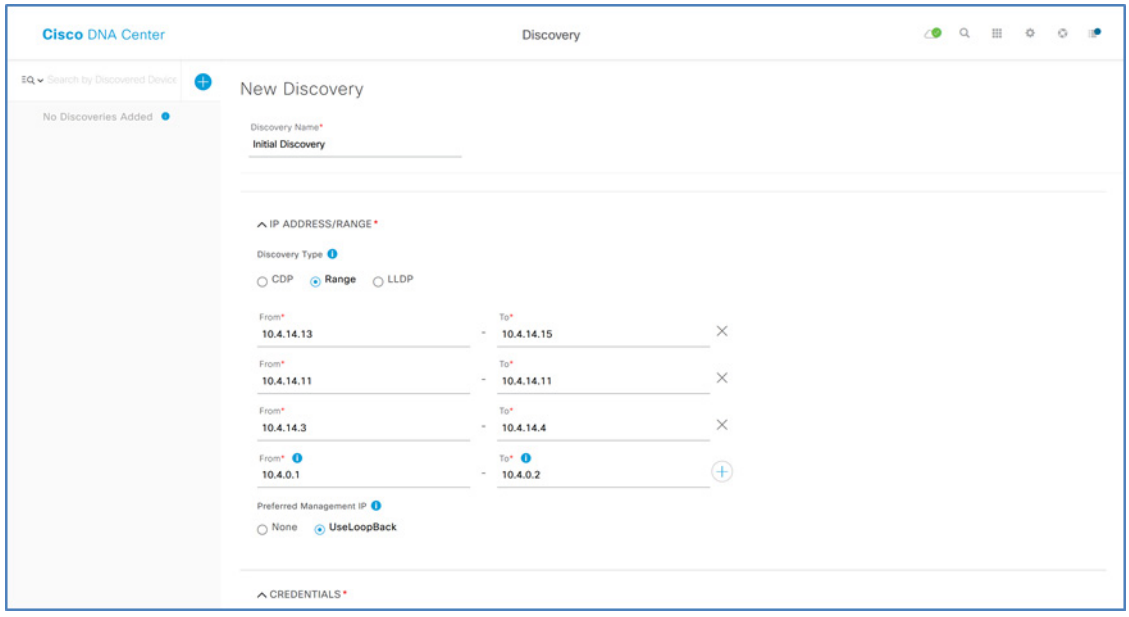
Vous utilisez Cisco DNA Center pour détecter et gérer les périphériques réseau sous-jacents pour SD-Access en autorisant la connectivité IP aux périphériques et en fournissant à Cisco DNA Center les informations d'identification pour la gestion. Suivez cette procédure pour tous les périphériques de départ pour l'automatisation LAN et tous les autres périphériques que vous ne prévoyez pas de détecter et de gérer à l'aide de l'automatisation LAN dans la procédure suivante.

Ces étapes expliquent comment lancer la détection en fournissant une plage d'adresses IP ou plusieurs plages pour l'analyse des périphériques réseau, ce qui limite la détection et permet de gagner du temps. Sinon, pour les périphériques qui n'utilisent pas l'intégration d'automatisation LAN, vous pouvez fournir un périphérique initial pour la détection et demander à Cisco DNA Center d'utiliser Cisco Discovery Protocol pour rechercher des voisins connectés. Lorsque vous utilisez Cisco Discovery Protocol, réduisez le nombre de sauts par défaut à un nombre raisonnable pour accélérer la détection.

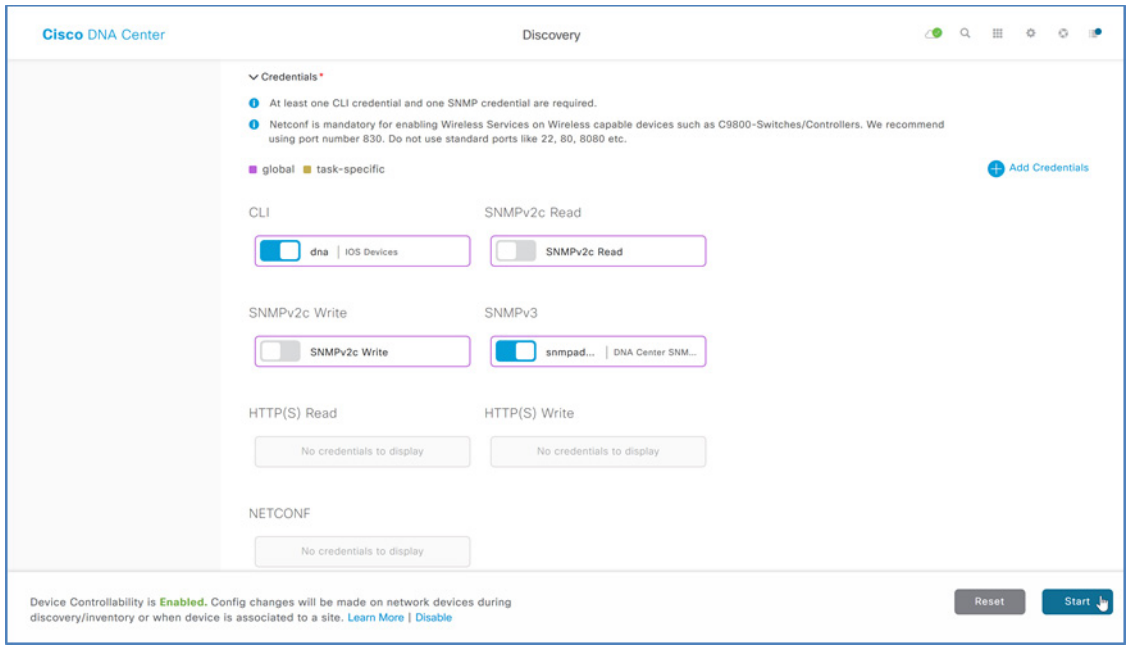
Étape 1. Accédez au tableau de bord principal de Cisco DNA Center, faites défiler l'écran jusqu'à la section **Tools (Outils)**, cliquez sur **Discovery (Détection)** et indiquez un **Discovery Name (Nom de détection)**. Sélectionnez **Range (Plage)** et saisissez une adresse IP de bouclage de début et de fin pour **IP Ranges (Plages d'adresses IP)** (pour couvrir une seule adresse, saisissez cette adresse pour le début et la fin de la plage). Pour **Preferred Management IP (Adresse IP de gestion préférée)**, si un périphérique dispose d'une interface de bouclage utilisée pour la gestion, sélectionnez **UseLoopBack**.

Conseil technique
Si vous utilisez un commutateur de la série Cisco Catalyst 6800 avec une très grande configuration, vous pouvez éviter les expirations de délai de détection en ajoutant la commande suivante à ce commutateur en mode de configuration : `snmp mib flash cache`

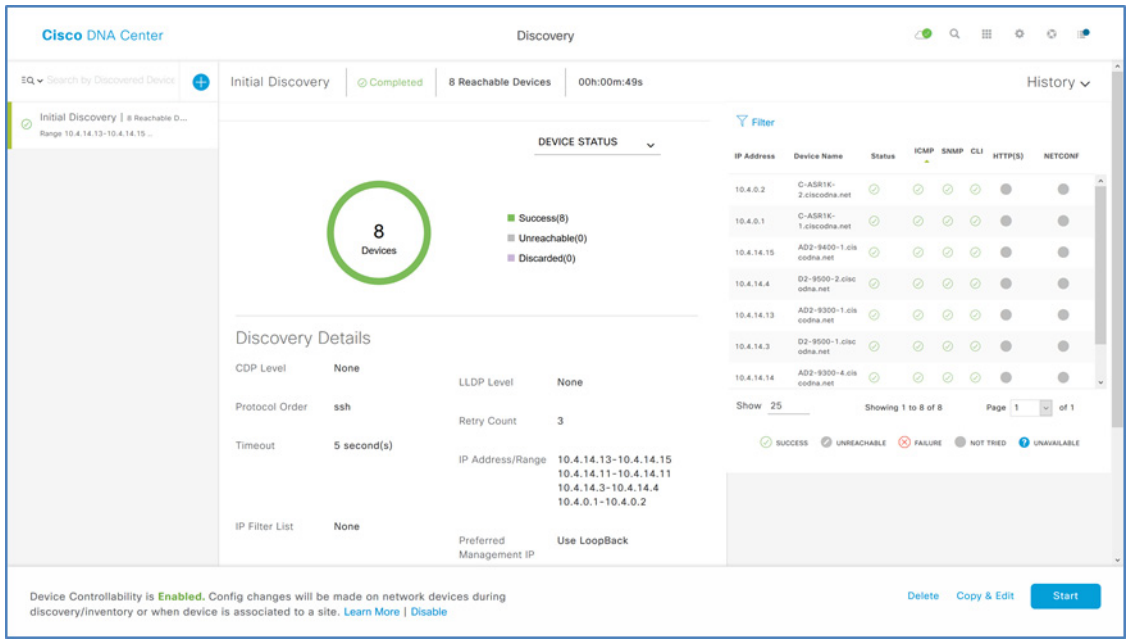
Étape 2. Si vous avez des plages supplémentaires, à côté de la première plage, cliquez sur **+** (signe plus), saisissez la plage supplémentaire et répétez l'opération pour toutes les plages restantes.



Étape 3. Faites défiler l'écran pour vérifier les informations d'identification de l'interface de ligne de commande utilisées pour la détection et les configurations d'informations d'identification SNMP envoyées au périphérique par la fonction de contrôle de périphérique de Cisco DNA Center, puis cliquez sur **Start (Démarrer)** en bas.



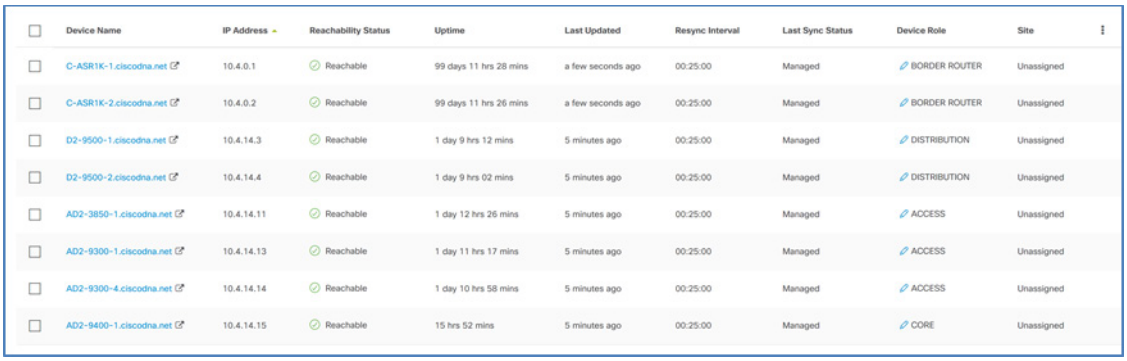
Les informations de détection sont affichées pendant que la détection est exécutée.



À la fin de la détection d'un périphérique avec la fonction de contrôle de périphérique activée, les informations d'identification affectées à l'aide de l'interface de ligne de commande et stockées localement sur le périphérique sont utilisées comme sauvegarde. Les informations d'identification locales sont utilisées uniquement en cas de perte de la connexion à ISE, qui est utilisé pour accéder aux informations d'identification centralisées principales.

Étape 4. S'il y a des défaillances de détection, examinez la liste des périphériques, résolvez le problème et redémarrez la détection pour ces périphériques, ainsi que les périphériques supplémentaires à ajouter à l'inventaire.

Étape 5. Après avoir terminé toutes les tâches de détection, accédez au tableau de bord principal de Cisco DNA Center, puis, sous la section **Tools (Outils)**, cliquez sur **Inventory (Inventaire)**. Les périphériques détectés s'affichent. Une fois la collecte d'inventaire terminée, chaque périphérique affiche un état de synchronisation **Managed (Géré)**, ce qui signifie que Cisco DNA Center tient à jour un modèle interne qui reflète le déploiement physique du périphérique.



Cisco DNA Center peut désormais accéder aux périphériques, synchroniser l'inventaire de configuration et apporter des modifications de configuration aux périphériques.

Conseil technique

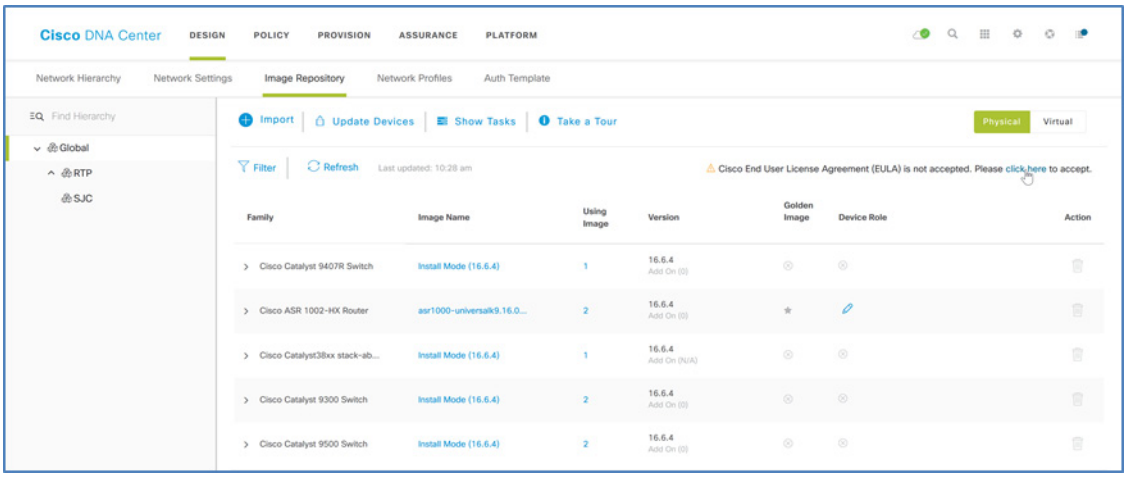
Sur le côté droit de la ligne de titre de la table d'inventaire, vous pouvez modifier les colonnes affichées. Utilisez la colonne **Device Role (Rôle du périphérique)** pour voir le rôle de périphérique affecté par la détection en fonction du type de périphérique et pour ajuster ce rôle de manière à mieux refléter le déploiement réel d'un périphérique, tel que routeur d'accès, de distribution, central ou de frontière, où routeur de frontière dans cet écran est un rôle de périphérique générique n'appartenant pas à la fabric. Le réglage du rôle à ce stade, plutôt que dans les procédures ultérieures, permet d'améliorer l'apparence des cartes topologiques initiales.

Procédure 8. Gérer les images logicielles des périphériques de l'inventaire

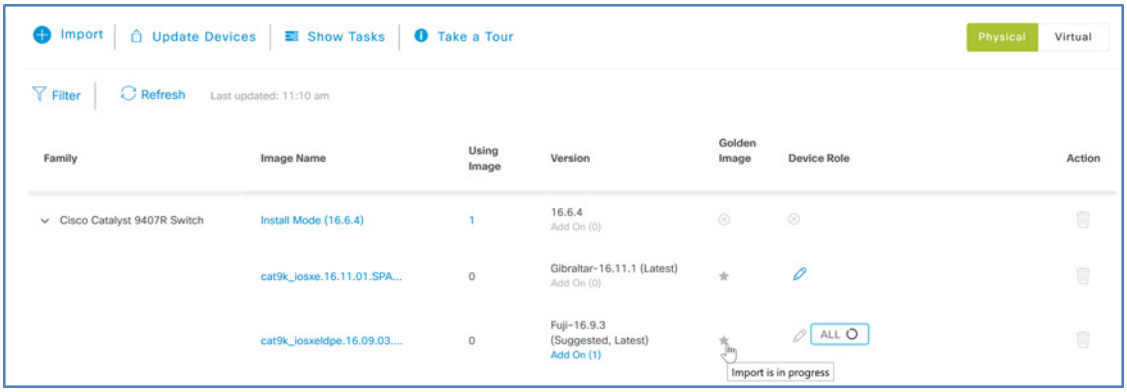
Pour tirer pleinement parti des fonctionnalités de SD-Access, le package SD-Access dans Cisco DNA Center comporte des exigences de version logicielle minimale requise pour les périphériques qu'il provisionne. La fonction de gestion d'images logicielles intégrée à Cisco DNA Center permet de mettre à niveau les périphériques qui n'exécutent pas une version d'image recommandée. Vous trouverez des images recommandées pour SD-Access en utilisant la matrice de compatibilité matérielle et logicielle SD-Access sur Cisco.com. Les images utilisées pour la validation sont répertoriées dans l'Annexe A : Liste des produits.

Procédez comme indiqué dans les étapes suivantes pour mettre en œuvre les mises à jour logicielles des images et les mises à jour de maintenance logicielle (SMU) sur les périphériques, en important les images requises, en les marquant comme Golden et en les appliquant aux périphériques.

Étape 1. Accédez au tableau de bord principal de Cisco DNA Center, cliquez sur **Design (Conception)**, puis cliquez sur **Image Repository (Référentiel d'images)**. Si vous utilisez le logiciel pour la première fois, dans la notification en haut à droite du **Contrat de licence de l'utilisateur final Cisco**, sélectionnez **click here (cliquer ici)**, puis cliquez sur **Accept License Agreement (Accepter la licence d'utilisation)**.



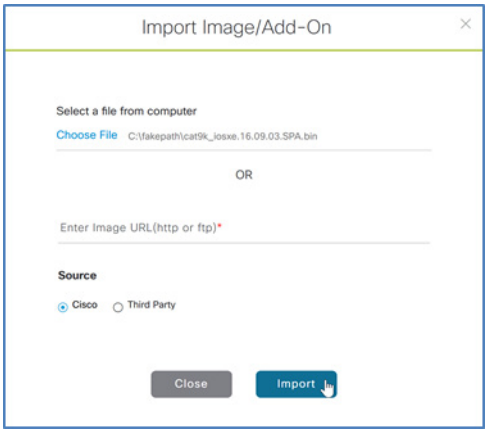
Étape 2. Si vous choisissez de demander à Cisco DNA Center de télécharger une nouvelle image à appliquer à un périphérique, sous la colonne **Image Name (Nom de l'image)**, cliquez sur la flèche vers le bas en regard de l'image répertoriée pour une famille de périphériques, puis cliquez sur l'étoile **Golden Image (Image Golden)** pour marquer l'image appropriée comme préférée pour la plate-forme.



Les images qui n'ont pas encore été importées sont automatiquement importées à l'aide des informations d'identification Cisco.com. Vous pouvez mettre à jour les informations d'identification Cisco.com à l'aide de **Settings (Paramètres)** (engrenage) **> System Settings (Paramètres système) > Settings (Paramètres) > Cisco Credentials (Informations d'identification Cisco)**.

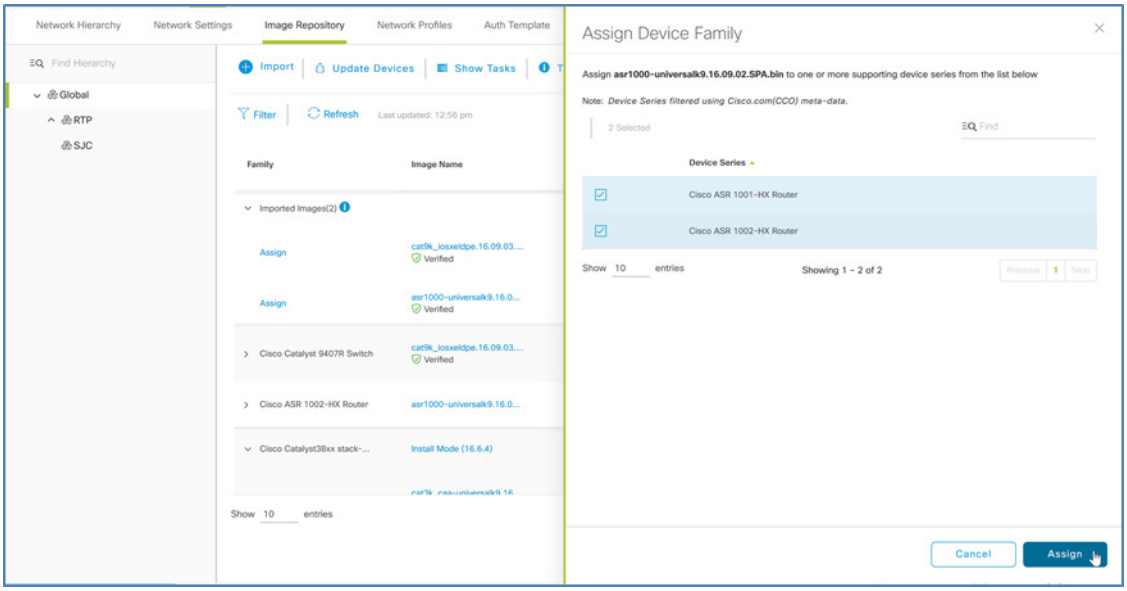
Étape 3. Répétez l'importation et le balisage des images comme Golden jusqu'à ce que tous les périphériques soient marqués d'une image appropriée.

Étape 4. Si vous choisissez d'importer une image depuis votre ordinateur local, cliquez sur **+ Import (Importer)**, dans la boîte de dialogue Import Image/Add-On (Importer une image/un module complémentaire), choisissez un emplacement de fichier, puis cliquez sur **Import (Importer)**.



L'importation de l'image dans Cisco DNA Center démarre.

Étape 5. Une fois l'importation terminée, affectez l'image importée aux périphériques. À côté de l'image importée, cliquez sur **Assign (Affecter)**, sélectionnez les périphériques devant utiliser l'image, puis dans le menu contextuel, cliquez sur **Assign (Affecter)**.



L'image se trouve dans le référentiel et est disponible pour être marquée comme Golden pour ces périphériques.

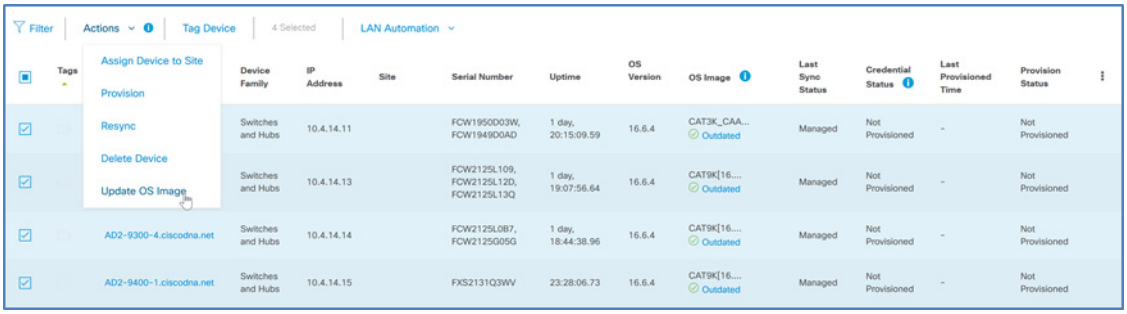
Étape 6. Pour chaque périphérique auquel une image vient d'être affectée, cliquez sur l'étoile **Golden Image (Image Golden)** pour marquer l'image appropriée comme préférée pour la plate-forme.

Étape 7. Répétez ces étapes pour toutes les images que vous souhaitez déployer à l'aide de Cisco DNA Center. Tous les types de périphériques auxquels une image Golden a été affectée sont prêts pour la distribution de l'image logicielle.

Procédure 9. Utiliser la gestion des images logicielles pour mettre à jour les logiciels des périphériques

Cisco DNA Center exécute une vérification de conformité des périphériques dans l'inventaire par rapport aux images marquées comme Golden. Les périphériques qui ne sont pas conformes à l'image Golden sont signalés comme **Outdated (Obsolètes)** dans l'inventaire. Mettez à jour les images avec la version marquée Golden. La collecte d'inventaire doit s'être terminée avec succès et les périphériques doivent être à l'état **Managed (Géré)** avant de continuer. Vous devez d'abord distribuer les images logicielles et planifier ou activer manuellement les périphériques avec les images distribuées.

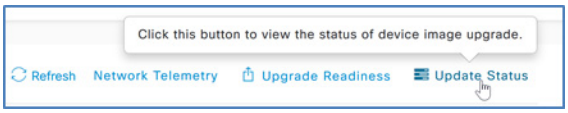
Étape 1. Accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, sélectionnez tous les périphériques marqués comme **Outdated (Obsolètes)**, puis dans le menu **Actions**, cliquez sur **Update OS Image (Mettre à jour l'image du système d'exploitation)**. Pour mieux les contrôler, démarrez les mises à jour du système d'exploitation sur les périphériques qui peuvent redémarrer sans affecter la connectivité aux autres périphériques que vous mettez à jour.



Étape 2. Dans la fenêtre qui s'affiche, sous **Distribute (Distribuer)> When (Quand)**, sélectionnez **Now (Maintenant)**, cliquez sur **Next (Suivant)**, sous **Activate (Activer)**, sélectionnez **Schedule Activation after Distribution is completed (Planifier l'activation une fois la distribution terminée)**, cliquez sur **Next (Suivant)**, puis sous **Confirm (Confirmer)**, cliquez sur le bouton **Confirm (Confirmer)**.

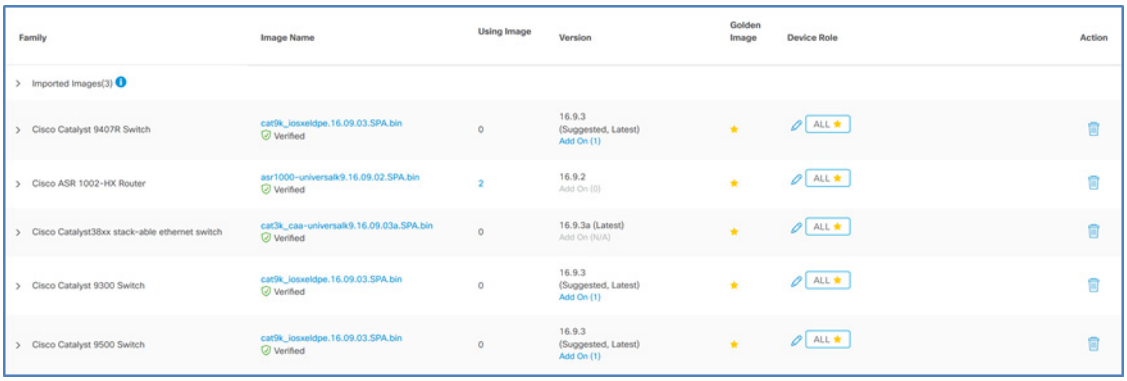
Les images sont distribuées aux périphériques sélectionnés.

Étape 3. En haut à droite, cliquez sur **Update Status (Mettre à jour l'état)**.



L'écran d'état fournit plus d'informations que l'écran principal et notamment des explications sur les éventuelles défaillances. Utilisez le bouton **Refresh (Actualiser)** pour observer à quel moment l'état **In Progress (En cours)** passe à **Successful (Réussi)**.

Étape 4. Répétez cette procédure autant de fois que nécessaire pour mettre à jour les logiciels des périphériques vers les versions requises pour le déploiement réseau. À l'issue de l'opération, tous les périphériques du déploiement sont associés à une image Golden qui est installée sur ceux-ci.



Processus : provisionnement du réseau sous-jacent pour SD-Access

Une fois que Cisco DNA Center détecte les périphériques qui exécutent les versions logicielles appropriées pour SD-Access et dispose d'un contrôle de gestion sur ceux-ci, utilisez Cisco DNA Center pour provisionner les périphériques dans le réseau sous-jacent.

Procédure 1. Provisionner les commutateurs sous-jacents à l'aide de la fonction d'automatisation LAN

En option

Suivez cette procédure si vous déployez de nouveaux commutateurs LAN non configurés dans la sous-couche à l'aide des fonctionnalités d'automatisation LAN de Cisco DNA Center. Utilisez les procédures précédentes pour configurer un ou plusieurs périphériques de départ (les périphériques gérés où se connecte le nouveau réseau non géré), les informations d'identification de l'interface de ligne de commande et SNMP du périphérique à envoyer par PnP, ainsi que le pool d'adresses IP accessible via le réseau utilisé pour la connectivité. Bien que cela ne soit pas obligatoire, chaque périphérique de départ est généralement un commutateur affecté dans les procédures ultérieures en tant que frontière et doit disposer d'un mode VTP et d'une configuration MTU appropriés (exemples : vtp mode transparent, system mtu 9100). Les ports sur le périphérique de départ connecté aux périphériques à détecter doivent être en mode de couche 2 (port d'accès et non port routé), et ne peuvent pas être des ports de gestion hors bande (OOB) dédiés.

Conseil technique

L'automatisation LAN permet de détecter les commutateurs pris en charge à partir des périphériques de départ pris en charge (les commutateurs utilisés dans cette validation sont répertoriés dans l'annexe). Les commutateurs détectés sont directement connectés aux interfaces du périphérique de départ choisi (les ports de gestion hors bande [OOB] ne peuvent pas être connectés pendant l'intégration des périphériques par l'automatisation LAN, car ils bloquent l'automatisation LAN sur les ports non OOB) et jusqu'à un tronçon supplémentaire de commutateurs connectés, pour une distance totale de deux tronçons du périphérique de départ. Les informations d'identification fournies permettent à Cisco DNA Center et aux périphériques de départ de fonctionner ensemble pour configurer les périphériques détectés et les ajouter à l'inventaire géré. Étant donné que les périphériques détectés doivent exécuter l'agent PnP sans configuration précédente, tous les commutateurs précédemment configurés doivent être restaurés dans un état dans lequel l'agent PnP s'exécute, ce qui est réalisé à l'aide du mode de configuration et des commandes du mode d'exécution suivants :

```
(config)#config-register 0x2102
(config)#crypto key zeroize
(config)#no crypto pki certificate pool
delete /force vlan.dat
delete /force nvram:*.cer
delete /force nvram:pnp*
delete /force flash:pnp*
delete /force stby-nvram:*.cer
delete /force stby-nvram:*.pnp*
! previous two lines only for HA systems
write erase
reload
```

N'enregistrez pas les configurations pour le processus de rechargement. Pour préparer les piles de commutateurs pour l'automatisation LAN, utilisez les mêmes commandes de restauration pour chaque commutateur d'une pile.

Les exigences d'empilage des commutateurs ne changent pas pour l'automatisation LAN : tous les commutateurs d'une pile doivent exécuter la même licence logicielle et la même version prenant en charge les fonctionnalités de routage IP, et être en mode installation (pas en mode Bundle). Si vous souhaitez contrôler au mieux le comportement de la pile et de la numérotation des ports, avant de démarrer le processus d'automatisation LAN, vous pouvez ajuster la numérotation de la pile de commutateurs et intervenir également sur un commutateur pour qu'il prenne le rôle ACTIVE (ACTIF) au sein d'une pile, en augmentant la priorité à l'aide des commandes suivantes en mode d'exécution :

```
switch [switch stack number] renumber [new stack number]
switch [switch stack number] priority 15
```

Identifiez un ou deux périphériques qui sont dans l'inventaire et gérés par Cisco DNA Center pour les affecter au rôle de périphérique de départ sur un site. Les mêmes périphériques de départ peuvent être utilisés pour plusieurs exécutions de la fonction d'automatisation LAN, ce qui permet d'affecter les périphériques détectés à différents bâtiments ou étages à chaque exécution.

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**. Sélectionnez jusqu'à deux périphériques de départ, dans la liste déroulante **Actions**, cliquez sur **Assign Device to Site (Affecter un périphérique au site)**, dans l'écran **Assign Device to Site (Affecter un périphérique au site)**, sélectionnez les affectations de sites aux périphériques, puis cliquez sur **Apply (Appliquer)**.

Étape 2. Si vous utilisez un périphérique de départ de la série Catalyst 6800, utilisez la commande de mode de configuration d'interface pour modifier les ports vers les périphériques détectés en ports de couche 2.

```
switchport
```

Après avoir enregistré le changement de configuration, resynchronisez le périphérique en accédant au tableau de bord principal de Cisco DNA Center ; sous **Tools (Outils)**, sélectionnez **Inventory (Inventaire)**, sélectionnez le commutateur Catalyst 6800 modifié, puis, en haut, dans le menu déroulant **Actions**, sélectionnez **Resync (Resynchroniser)**.

Conseil technique

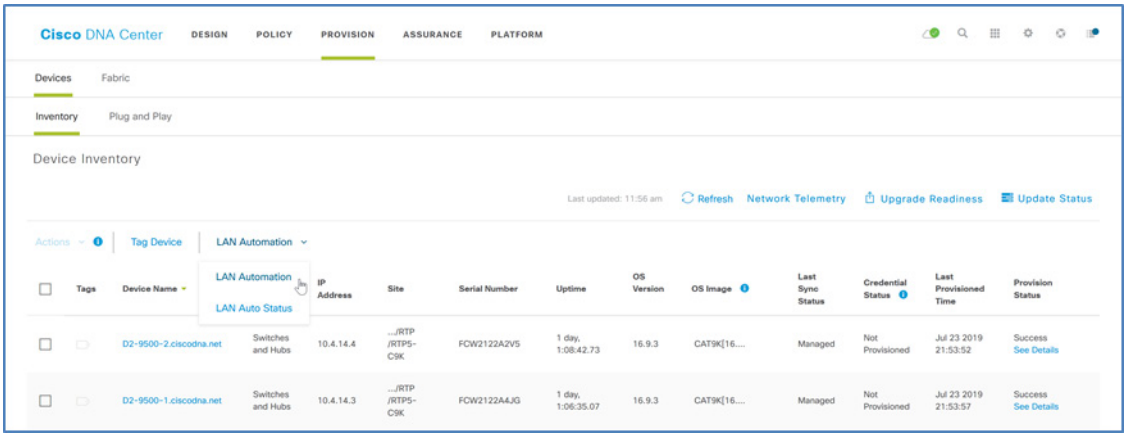
Le pool d'adresses IP utilisé pour l'automatisation LAN doit être beaucoup plus grand que le nombre de périphériques à découvrir. Le pool est divisé en deux, dont une moitié est utilisée pour les services DHCP du VLAN 1 fournis par les périphériques de départ. La deuxième moitié du pool est divisée en deux à nouveau, ce qui laisse un quart de l'espace d'adressage total pour l'adressage de la liaison point à point et un quart pour l'adressage de bouclage. Les terminaux ne doivent pas être branchés sur les commutateurs, car ils peuvent épuiser le pool d'adresses IP utilisé par DHCP pour le provisionnement PnP.

Les adresses du pool d'automatisation LAN doivent être accessibles à Cisco DNA Center pour que le provisionnement réussisse, et ne doivent pas être utilisées ailleurs dans le réseau. Si votre Cisco DNA Center utilise le réseau de gestion dédié en option pour le port d'accès au web au lieu d'un port unique avec une route par défaut, vous devez vous assurer que la route vers le pool d'adresses IP d'automatisation LAN est disponible via le port d'infrastructure du réseau d'entreprise. Si le pool d'adresses IP n'est pas inclus dans les routes configurées sur Cisco DNA Center, connectez-vous à Cisco DNA Center en utilisant le port SSH 2222, puis connectez-vous en tant que maglev et exécutez la commande suivante :

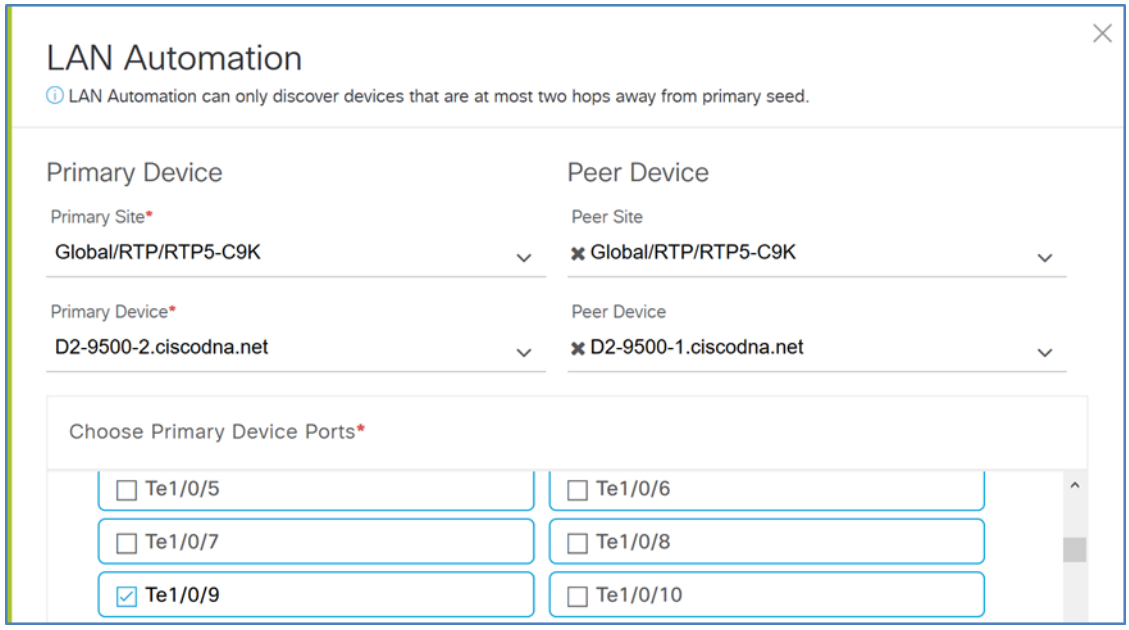
```
sudo maglev-config update
```

Utilisez l'Assistant de configuration pour configurer les routes statiques afin d'inclure le pool d'adresses IP sur la carte réseau appropriée avant de démarrer l'automatisation du réseau local.

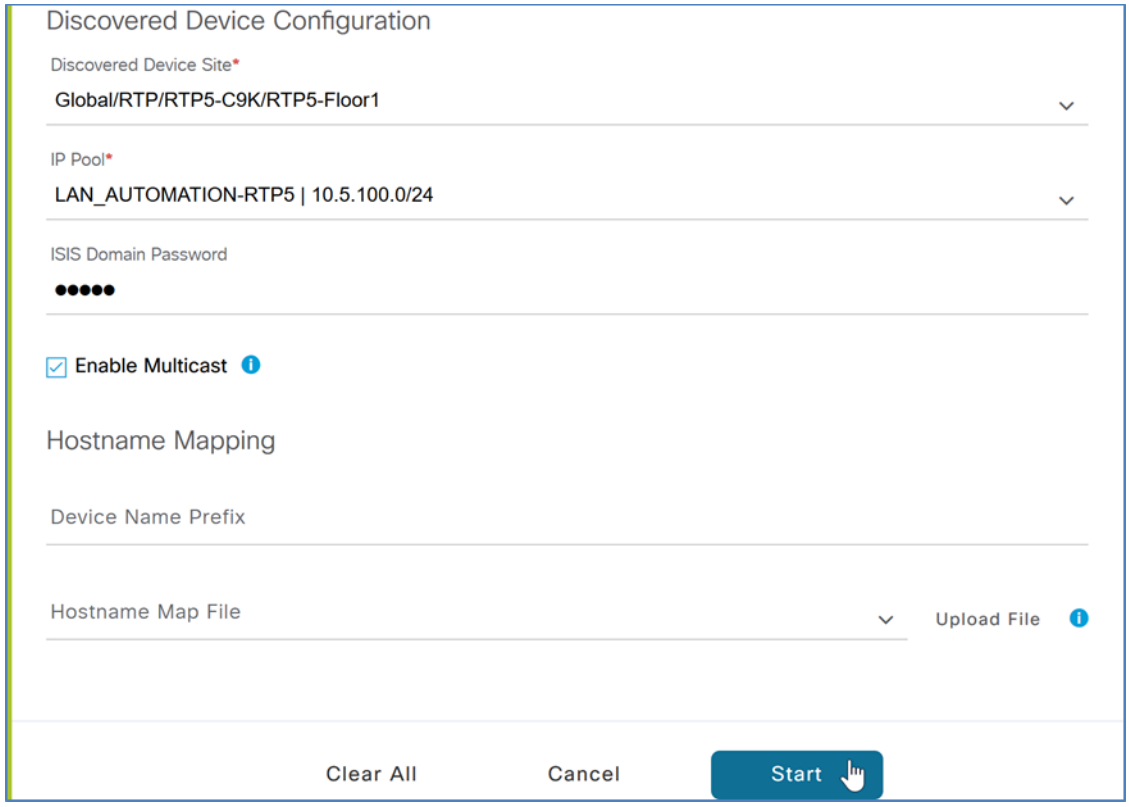
Étape 3. Accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**. En haut de l'écran, cliquez sur le menu déroulant **LAN Automation (Automatisation LAN)**, puis cliquez sur **LAN Automation (Automatisation LAN)**.



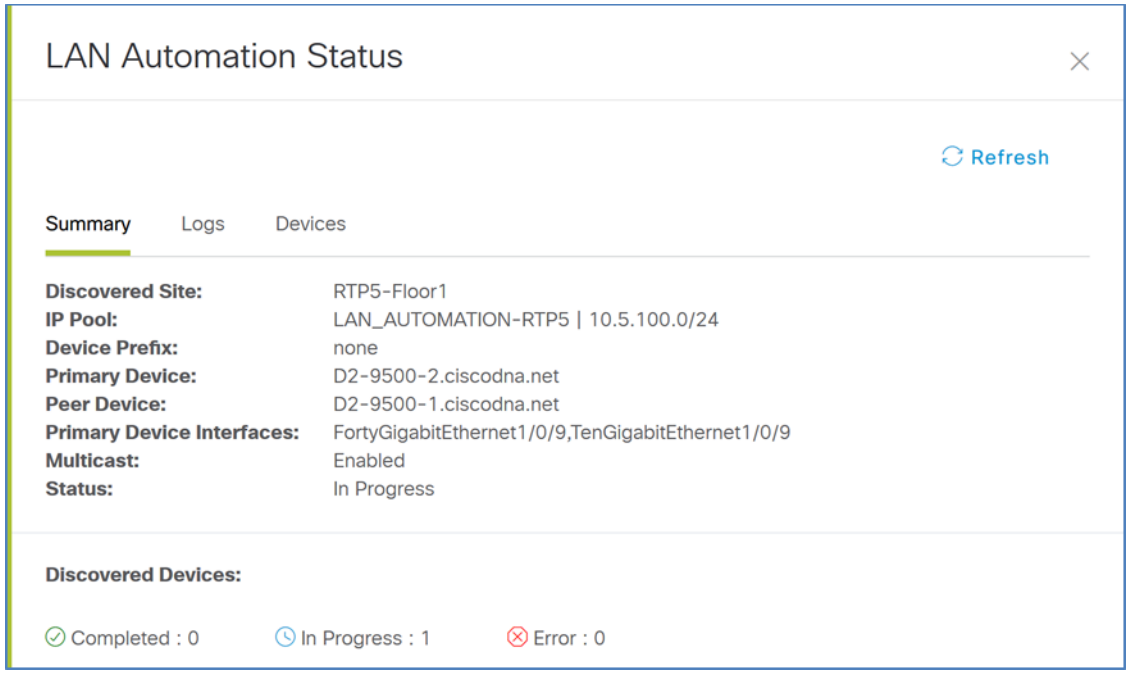
Étape 4. À droite dans la fenêtre coulissante LAN Automation (Automatisation LAN), complétez les paramètres de la détection. Sous **Primary Device (Périphérique principal)**, renseignez **Primary Site* (Site principal)**, **Primary Device* (Périphérique principal)**, **Choose Primary Device Ports* (Choisir les ports du périphérique principal)**, sous **Peer Device (Périphérique homologue)**, indiquez **Peer Site (Site homologue)** et **Peer Device (Périphérique homologue)**.



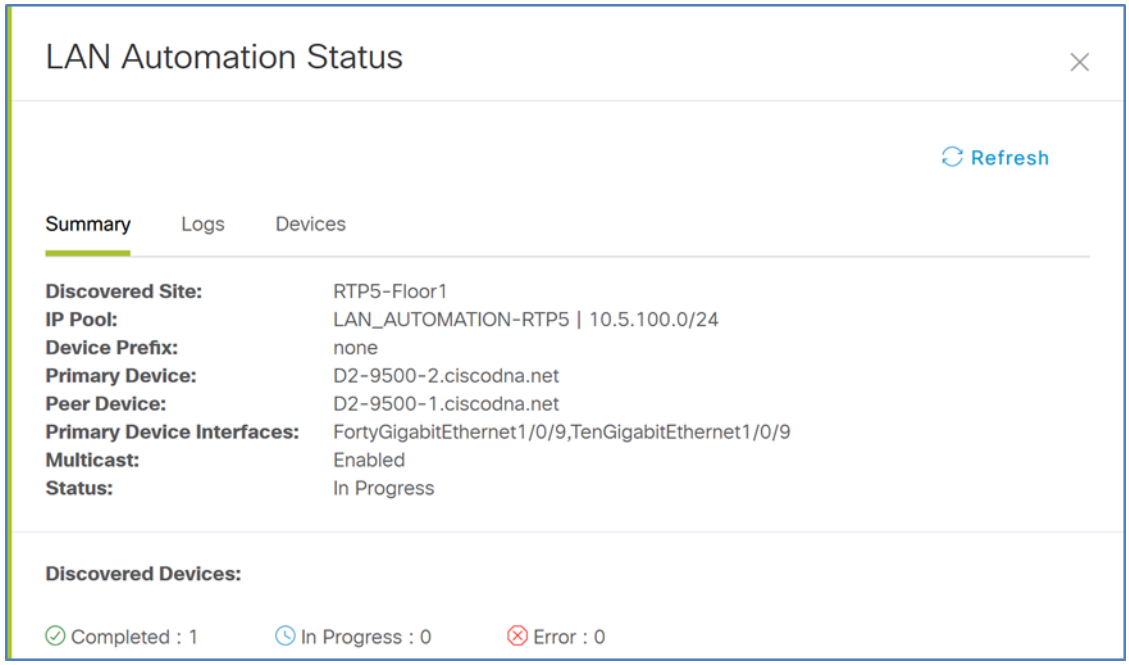
Étape 5. À droite dans la fenêtre coulissante LAN Automation (Automatisation LAN), continuez à renseigner les paramètres de détection. Sous **Discovered Device Configuration (Configuration du périphérique détecté)**, indiquez le **Discovered Device Site* (Site du périphérique détecté)**, le **IP Pool* (Pool d'adresses IP)**, s'il est utilisé, indiquez le **ISIS Domain Password (Mot de passe du domaine ISIS)**, sélectionnez **Enable Multicast (Activer la multidiffusion)**, puis cliquez sur **Start (Démarrer)**.



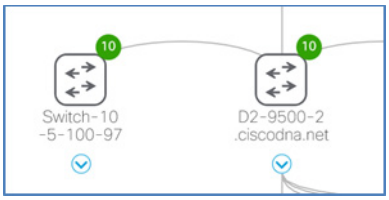
Étape 6. En haut de l'écran, cliquez sur la liste déroulante **LAN Automation (Automatisation LAN)**, puis cliquez sur **LAN Auto Status (État auto LAN)** pour afficher la progression.



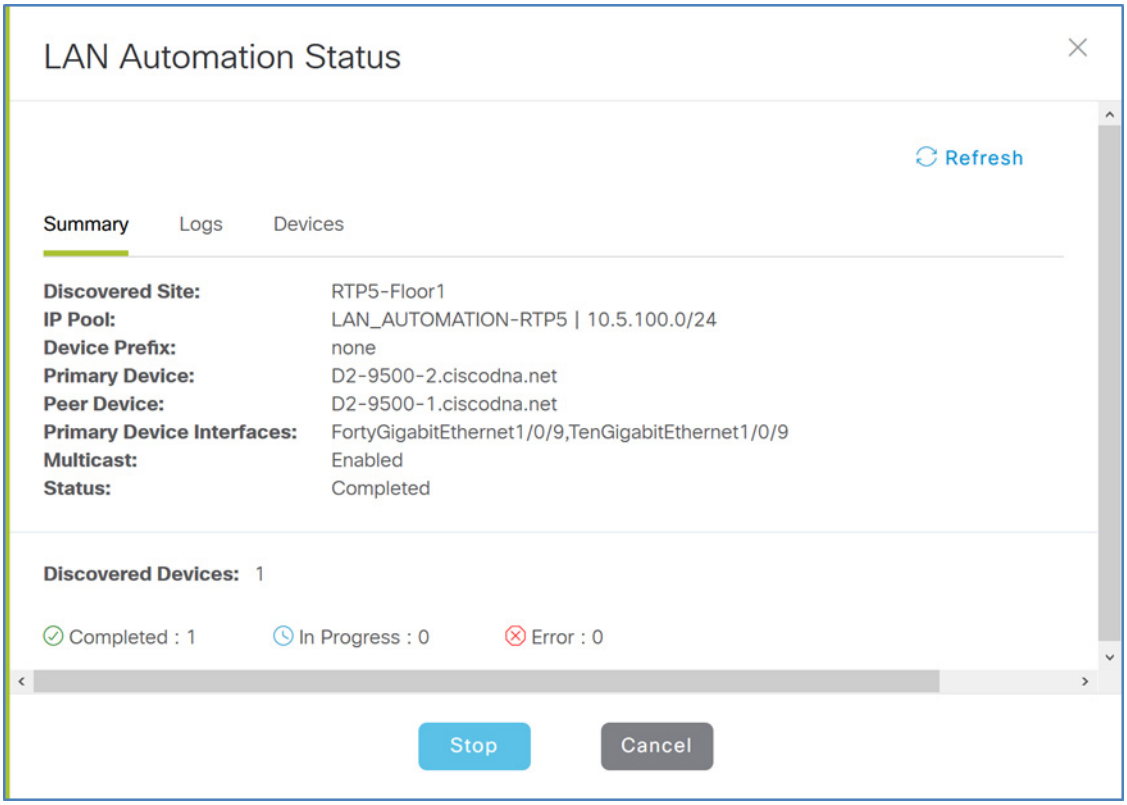
Ne cliquez pas sur **Stop (Arrêter)** au cours de cette étape. Attendez que tous les périphériques affichent l'état **Completed (Terminé)**, puis passez à l'étape de vérification suivante. L'arrêt prématuré du processus PnP laisse la détection dans un état dont le rétablissement implique une intervention manuelle. La détection des périphériques situés à un tronçon supplémentaire du périphérique de départ peut nécessiter beaucoup plus de temps.



Étape 7. Accédez au tableau de bord principal de Cisco DNA Center et sous **Tools (Outils)**, sélectionnez **Topology (Topologie)**. Tous les liens doivent être détectés. S'il manque des liens dans la topologie, vérifiez la connectivité physique.



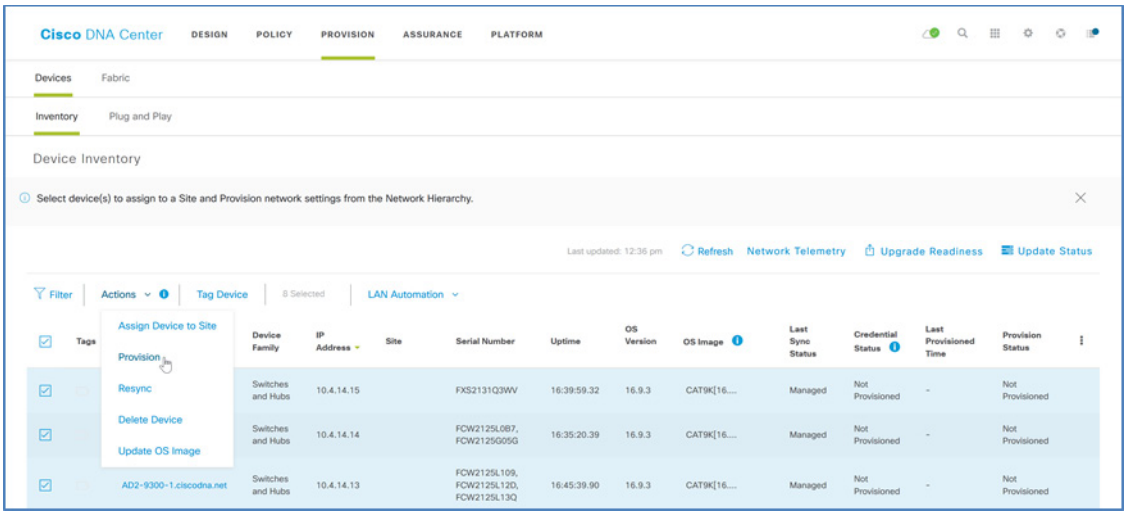
Étape 8. Accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**. En haut de l'écran, cliquez sur la liste déroulante **LAN Automation (Automatisation LAN)**, puis sur **LAN Auto Status (État auto LAN)**. Une fois que tous les périphériques détectés atteignent l'état **Completed (Terminé)**, cliquez sur **Stop (Arrêter)**. L'automatisation LAN détruit toutes les connexions de couche 2 sur le VLAN 1 et le processus de routage IS-IS sous-jacent est utilisé pour l'accessibilité au réseau routé, et les périphériques sont gérés dans l'inventaire.



Procédure 2. Provisionner des périphériques et les affecter aux sites pour préparer SD-Access

Provisionnez les périphériques réseau, puis affectez-les à un site en vue de leur intégration dans un réseau SD-Access.

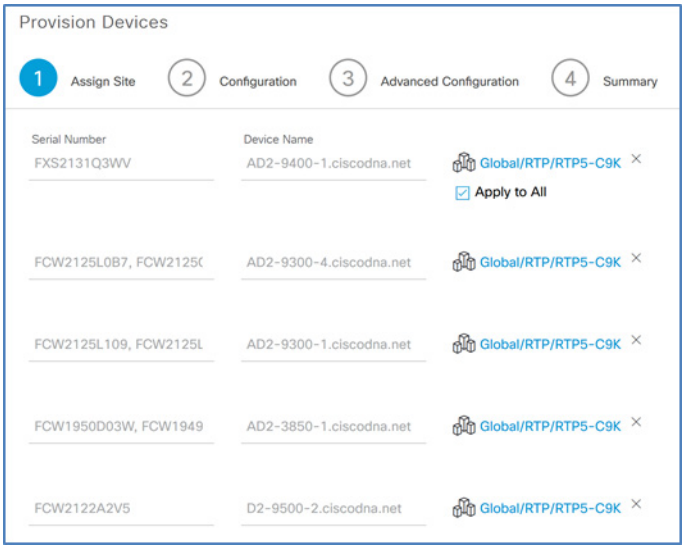
Étape 1. Dans Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, sélectionnez les périphériques du même type (exemple : tous les commutateurs) à provisionner sur le réseau, cliquez sur **Actions**, puis sur **Provision (Provisionner)**.



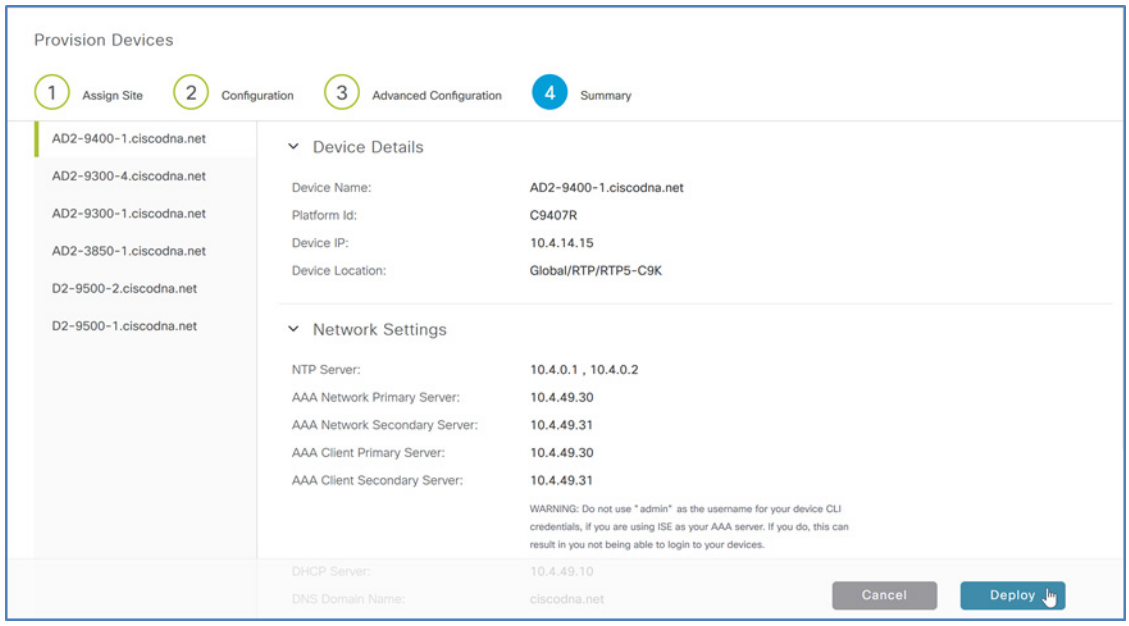
L'écran de l'Assistant **Provision Devices (Provisionnement des périphériques)** apparaît.

Conseil technique
Les périphériques doivent être de même type (par exemple : tous les routeurs) pour pouvoir les provisionner en même temps. Vous pouvez regrouper les opérations de provisionnement en plusieurs petits lots pour les affectations de site communes, le cas échéant.

Étape 2. Dans le premier écran de l'Assistant, sélectionnez les affectations de site pour les périphériques, puis cliquez sur **Next (Suivant)** en bas de l'écran.



Étape 3. Cliquez deux fois de suite sur **Next (Suivant)** pour ignorer les écrans **Configuration** et **Advanced Configuration (Configuration avancée)**, dans l'écran **Summary (Résumé)**, examinez les informations relatives à chaque périphérique, puis cliquez sur **Deploy (Déployer)**.

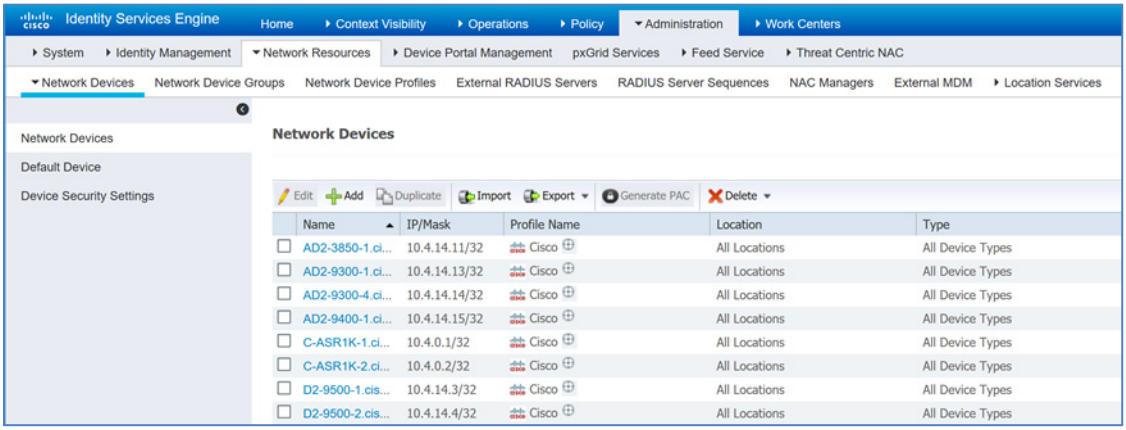


Étape 4. Dans l'écran contextuel, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

La configuration de chaque périphérique commence, et des messages d'état apparaissent au fur et à mesure qu'il est provisionné avec succès. L'écran Device Inventory (Inventaire des périphériques) est mis à jour avec le **Provision Status (État de provisionnement)** et le **Sync Status (État de synchronisation)**. Utilisez le bouton **Refresh (Actualiser)** pour mettre à jour l'état final.

Étape 5. Répétez les étapes de provisionnement de Cisco DNA Center pour chaque lot de périphériques ajouté. L'intégration pxGrid Cisco DNA Center met à jour les périphériques dans ISE.

Étape 6. Vérifiez la fonction d'intégration ISE en vous connectant à ISE et en accédant à **Administration > Network Resources (Ressources réseau) > Network Devices (Périphériques réseau)**. Les périphériques provisionnés s'affichent.



Processus : provisionnement du réseau superposé SD-Access

Un réseau superposé de fabric est créé dans Cisco DNA Center à l'aide des périphériques détectés qui ont été ajoutés à l'inventaire et provisionnés sur un site. Cisco DNA Center automatise la configuration supplémentaire des périphériques prenant en charge les réseaux superposés SD-Access.

La solution SD-Access prend en charge le provisionnement des constructions de fabric suivantes :

- Site de fabric : fabric indépendante, comprenant les fonctions de nœud de plan de contrôle et de nœud de périphérie, qui utilise un nœud de frontière de fabric pour la sortie du site de fabric et qui comprend généralement un nœud de commutation de paquets (PSN) ISE et un contrôleur LAN sans fil (WLC) en mode fabric
- Site de transit : également connu sous le nom de réseau de transit, connecte un site de fabric à un réseau externe (transit basé sur IP) ou à un ou plusieurs sites de fabric en préservant la segmentation de manière native (transit SD-Access)
- Domaine de fabric : englobe un ou plusieurs sites de fabric et les sites de transit correspondants

Les réseaux de transit basés sur IP connectent la fabric aux réseaux externes, utilisant généralement VRF-Lite pour la connectivité IP. Les transits SD-Access transportent des informations de balise SGT et VN, qui transportent intrinsèquement la politique et la segmentation entre les sites de fabric, créant ainsi un réseau local distribué.

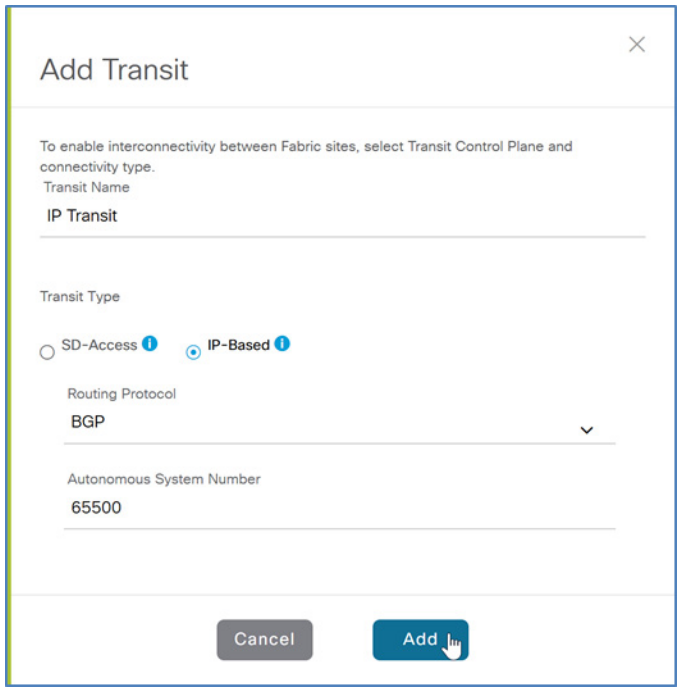
Conseil technique
Le logiciel Cisco DNA Center et le logiciel Cisco IOS répertoriés dans l'annexe ne comportent pas de validation du transit SD-Access, traitée dans le document Guide de déploiement normatif de SD-Access pour le réseau local distribué. Vous trouverez des versions de logiciel alternatives qui peuvent prendre en charge des options supplémentaires en recherchant sur Cisco.com la Matrice de compatibilité matérielle et logicielle SD-Access.

Le logiciel Cisco DNA Center et le logiciel Cisco IOS répertoriés dans l'annexe ne comportent pas de validation du transit SD-Access, traitée dans le document Guide de déploiement normatif de SD-Access pour le réseau local distribué. Vous trouverez des versions de logiciel alternatives qui peuvent prendre en charge des options supplémentaires en recherchant sur Cisco.com la Matrice de compatibilité matérielle et logicielle SD-Access.

Procédure 1. Créer un site de transit basé sur IP, un domaine de fabric et des sites de fabric

Le site de transit basé sur IP représente le système autonome (AS) distant BGP. Le système autonome BGP local est configuré dans le cadre du provisionnement de la frontière de fabric au cours d'une procédure ultérieure.

Étape 1. À l'aide de Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, en haut à droite cliquez sur **+ Add Fabric or Transit (Ajouter une fabric ou un transit)**, cliquez sur **Add Transit (Ajouter un transit)**, dans la fenêtre coulissante indiquez un **Transit Name (Nom de transit)** (exemple : IP_Transit), sélectionnez **IP-Based (Basé sur IP)**, pour **Routing Protocol (Protocole de routage)** sélectionnez **BGP**, saisissez un **Autonomous System Number (Numéro de système autonome)** pour le système autonome BGP distant (exemple : 65500), puis cliquez sur **Add (Ajouter)**.

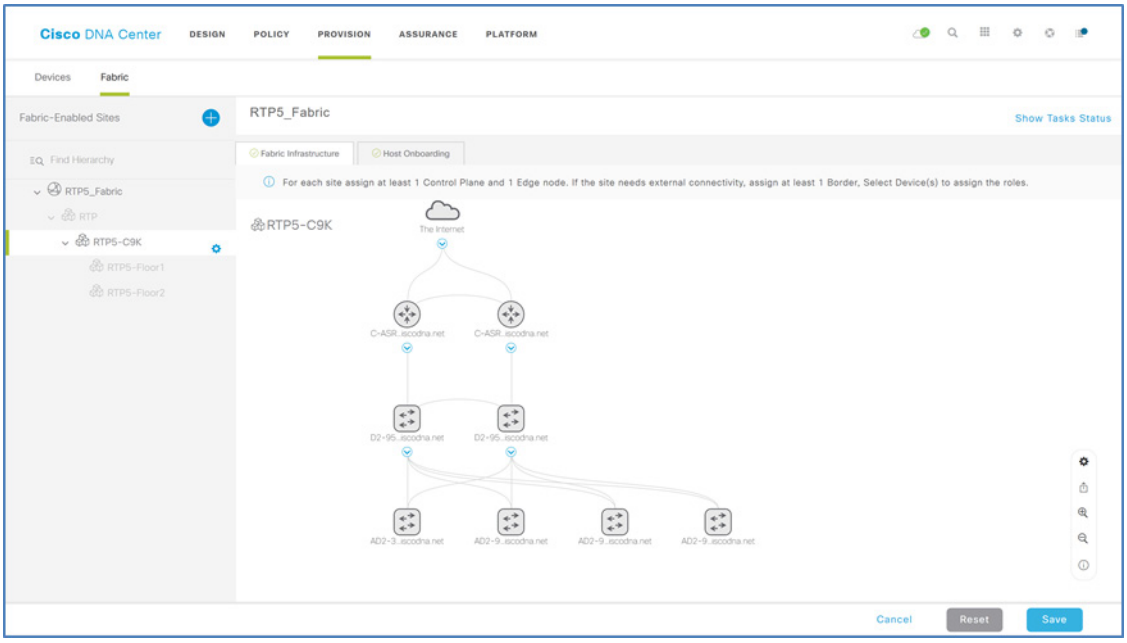


Un message d'état s'affiche et le transit est créé.

Étape 2. Accédez à **PROVISION (PROVISIONNER) > Fabric**, en haut à droite cliquez sur **+ Add Fabric or Transit (Ajouter une fabric ou un transit)**, cliquez sur **Add Fabric (Ajouter une fabric)**, dans la fenêtre coulissante indiquez un **Fabric Name (Nom de fabric)** (exemple : RTP5_Fabric), utilisez la hiérarchie du site pour sélectionner un emplacement comprenant les sites pour l'activation de la fabric (exemple : RTP5-C9K), puis cliquez sur **Add (Ajouter)**.

La nouvelle fabric de réseau local est créée.

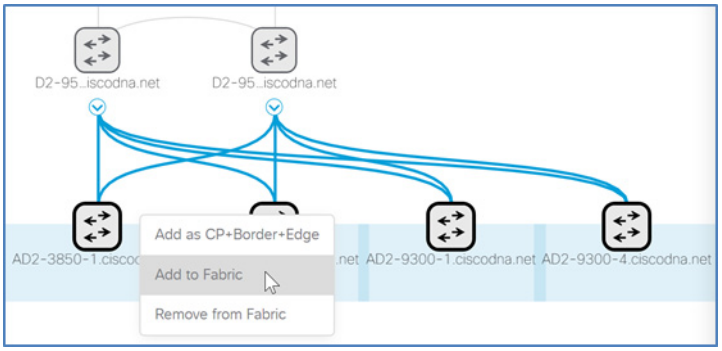
Étape 3. Cliquez sur le nom de domaine de la fabric que vous venez de créer (exemple : RTP5_Fabric) et, dans la hiérarchie **Fabric-Enabled Sites (Sites compatibles fabric)** sur la gauche, sélectionnez le site ajouté à l'étape précédente (exemple : RTP5-C9K). Une vue de la fabric et des sites associés s'affiche.



Si le schéma de topologie de fabric affiché ne reproduit pas la topologie à deux niveaux (distribution/accès) ou à trois niveaux (cœur/distribution/accès) qui est déployée, corrigez la topologie en accédant à **Tools (Outils) > Inventory (Inventaire)**, à droite de la ligne de titre de la table d'inventaire, ajustez les colonnes affichées pour inclure **Device Role (Rôle du périphérique)**, puis paramétrez le rôle de manière à refléter au mieux le déploiement réel d'un périphérique. Revenez à la vue topologique du domaine de fabric après avoir modifié les rôles de périphériques pour obtenir une vue mise à jour.

Procédure 2. Créer une superposition de fabric

Étape 1. Dans la vue topologique du domaine de fabric, maintenez la touche Maj enfoncée, cliquez sur tous les nœuds qui sont des nœuds de périphérie de fabric, puis dans la zone contextuelle, cliquez sur **Add to Fabric (Ajouter à la fabric)**.



Des bordures d'icônes bleues et des symboles de rôle de fabric apparaissent, indiquant le comportement cible prévu pour les périphériques.

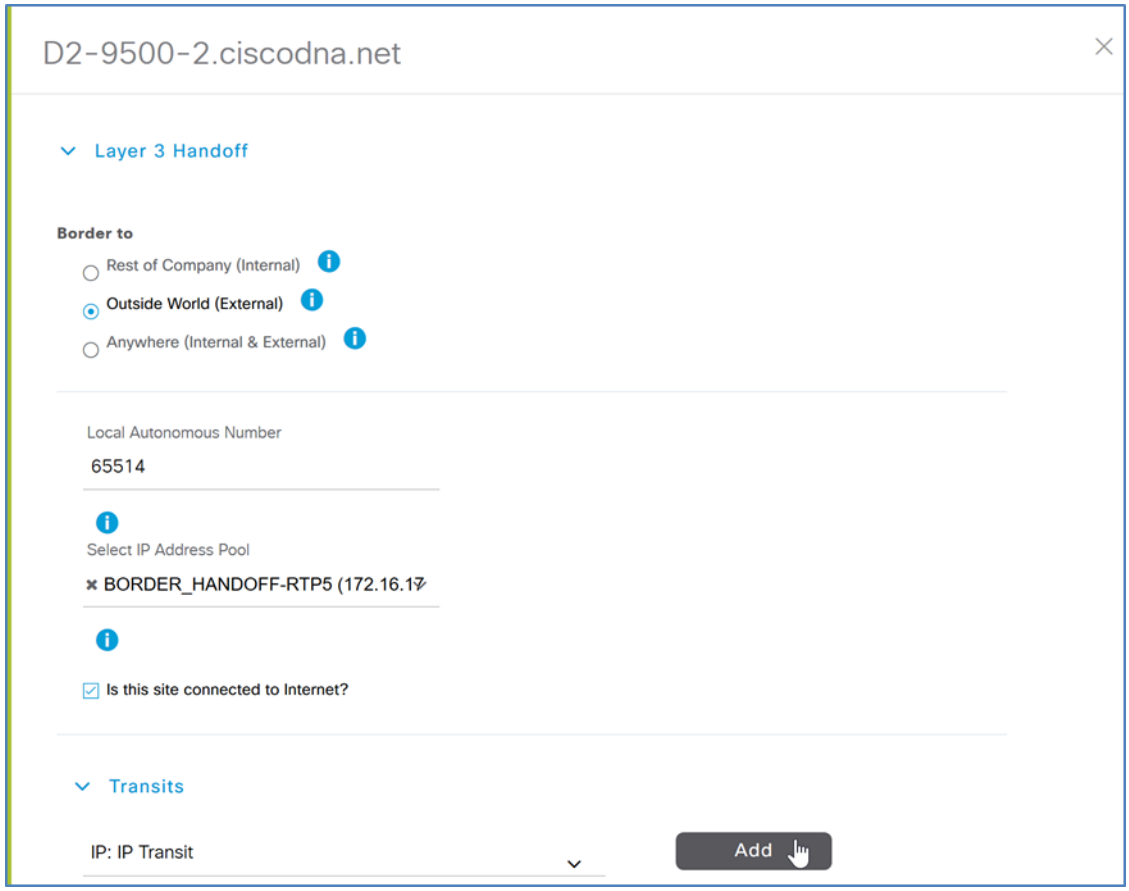
Étape 2. Si vous disposez d'un nœud pour la fabric dédié au rôle de nœud de plan de contrôle sans fonctionnalité de frontière, cliquez dessus, puis dans la zone contextuelle, cliquez sur **Add as CP (Ajouter en tant que plan de contrôle)**.

Répétez cette étape pour un nœud de plan de contrôle dédié redondant sans fonctionnalité de frontière.

Conseil technique

Si les nœuds de frontière sont des commutateurs de la gamme Cisco Nexus 7700 utilisant le logiciel répertorié dans l'Annexe A : liste des produits, utilisez des nœuds de plan de contrôle dédiés et connectez-les directement aux commutateurs de la série 7700, configurés en tant que nœuds de frontière externes. Si votre version du système d'exploitation NX-OS l'exige, activez la licence MPLS. Configurez MPLS LDP sur les liaisons physiques vers les nœuds du plan de contrôle pour prendre en charge la connectivité de ce dernier.

Étape 3. Cliquez sur un périphérique devant tenir le rôle de frontière de fabric, dans la zone contextuelle, cliquez sur **Add as Border (Ajouter en tant que frontière)** ou sur **Add as CP+Border (Ajouter en tant que plan de contrôle+frontière)** (si vous ignorez l'étape précédente) et renseignez la boîte de dialogue coulissante supplémentaire. Sous **Layer 3 Handoff (Transfert de couche 3)**, sélectionnez **Border (Frontière)** vers (par exemple : Outside World [External] [Monde extérieur [externe]]), spécifiez le **BGP Local Autonomous Number (Numéro autonome local BGP)** (par exemple : 65514), sous **Select IP Address Pool (Sélectionner le pool d'adresses IP)**, sélectionnez le pool global configuré précédemment pour la fonctionnalité de connectivité de frontière (par exemple : BORDER_HANDOFF-RTP5), pour les frontières externes, sélectionnez **Is this site connected to the Internet? (Ce site est-il connecté à Internet ?)**, dans le menu **Transit**, sélectionnez le transit (par exemple : IP : IP Transit [Transit IP]), puis, en regard du transit, cliquez sur le bouton gris **Add (Ajouter)**.

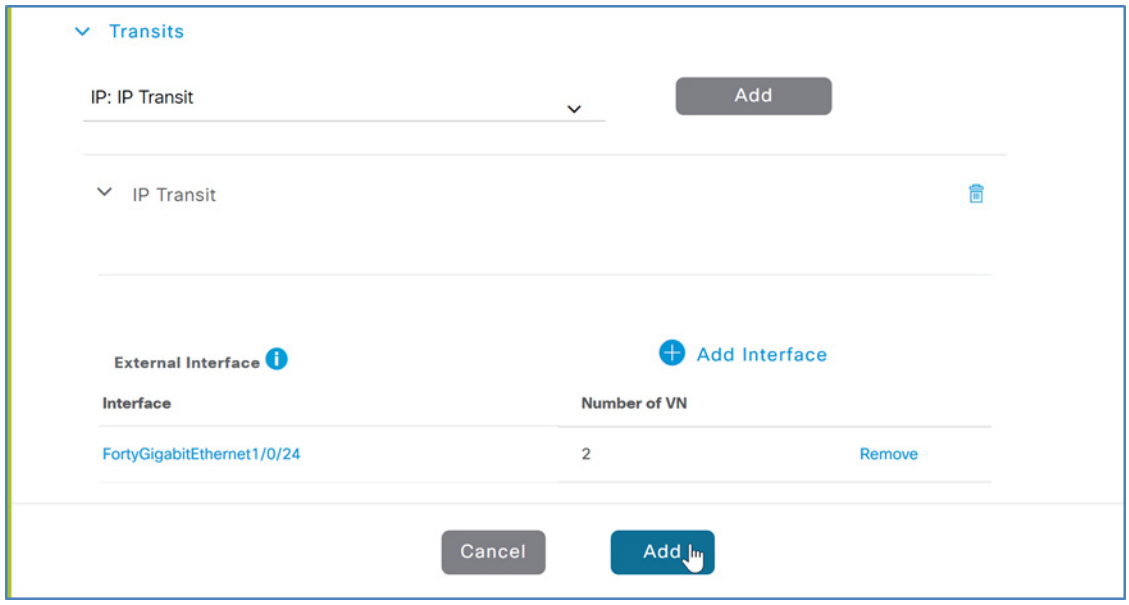


Une section supplémentaire **IP Transit (Transit IP)** apparaît.

Conseil technique

Si la frontière est le seul chemin pour sortir de la fabric vers le reste du réseau, vous devez choisir une frontière externe. Si vous disposez d'une fonction combinée de plan de contrôle et de nœud de frontière et que le nœud utilise des fonctionnalités de frontière interne, il peut être nécessaire de filtrer davantage le plan de contrôle lors de l'utilisation des versions validées indiquées dans l'Annexe A : liste des produits.

Étape 4. Cliquez sur le texte **IP Transit (Transit IP)**, cliquez sur **+ Add Interface (Ajouter une interface)** qui apparaît, dans la zone coulissante, sélectionnez l'interface de connexion au routeur de fusion à l'extérieur de la fabric, sous le **Remote AS Number (Numéro AS distant)** BGP du périphérique en dehors de la fabric qui s'affiche, développez le panneau de sélection **Virtual Network (Réseau virtuel)**, sélectionnez chaque VN utilisé dans la fabric à inclure dans le transfert de couche 3 en dehors de la fabric (par exemple : INVRA_VN, OPERATIONS), cliquez sur **Save (Enregistrer)**, puis sur **Add (Ajouter)**.

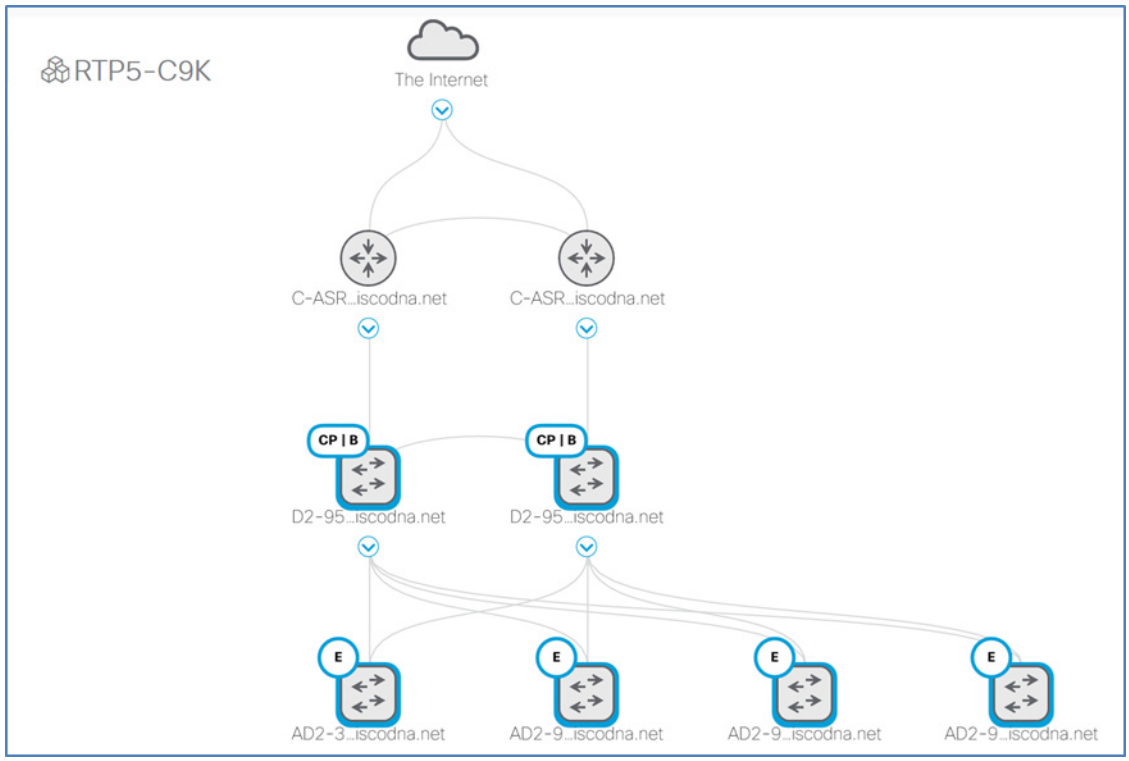


Validez les éventuelles fenêtres contextuelles supplémentaires d'information.

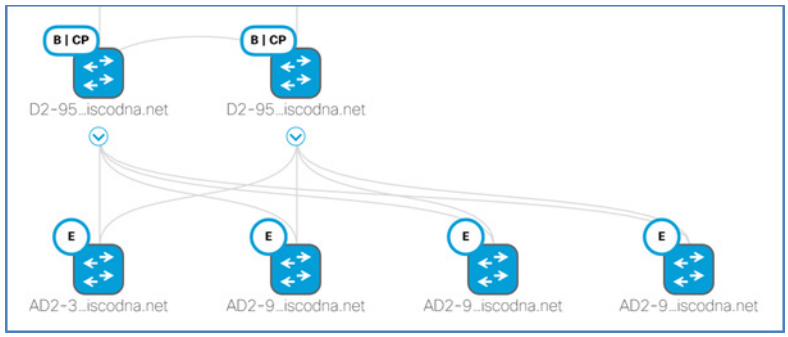
Étape 5. Si vous disposez d'un nœud de frontière de fabric supplémentaire, répétez les deux étapes précédentes pour ce dernier.

Conseil technique
Pour configurer une interface de transfert VRF-Lite de la frontière au reste du réseau, vous devez disposer d'une interface avec balises 802.1Q. Si vous gérez la frontière à l'aide de la connectivité intrabande sur les liaisons redondantes à convertir, vous devez d'abord établir la connexion sur une interface balisée, comme décrit dans les processus de configuration de la gestion sur un périphérique de frontière pour la découverte de réseau. Lors de l'utilisation de la version de SD-Access validée dans ce guide, le provisionnement échoue si l'interface inclut déjà une configuration non balisée.

Étape 6. Une fois que tous les rôles requis ont été affectés aux nœuds de la fabric, en bas, cliquez sur **Save (Enregistrer)**, utilisez le choix par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**. Votre domaine de fabric de réseau local est créé.



Les icônes de fabric deviennent bleues, ce qui indique votre intention de créer la fabric. Le provisionnement réel des périphériques peut prendre plus de temps.



Procédure 3. Activer la multidiffusion pour la fabric

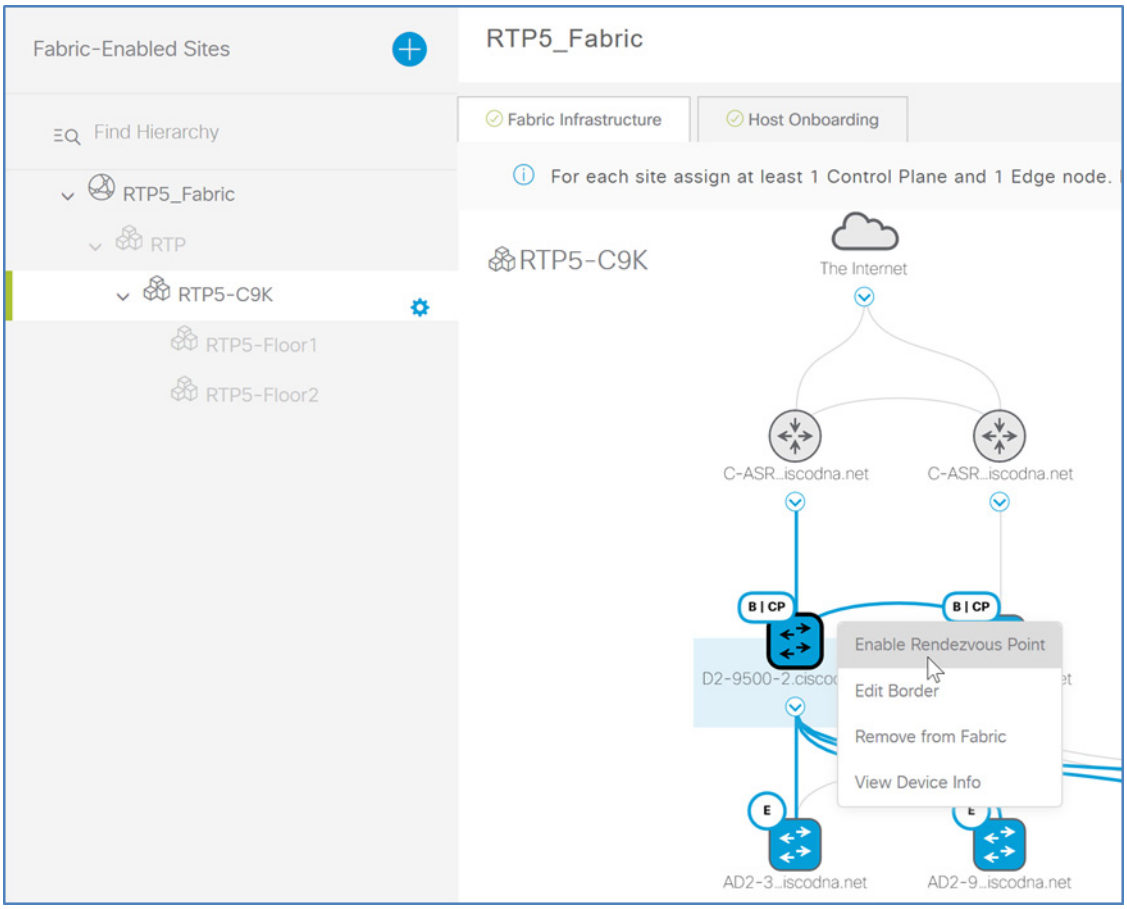
Suivez cette procédure pour configurer la prise en charge de la multidiffusion dans la superposition de fabric.

Les fabrics SD-Access peuvent prendre en charge la multidiffusion, quelle que soit la source (ASM, Any Source Multicast) et la multidiffusion d'une source spécifique (SSM, Source Specific Multicast). Les sources peuvent se trouver dans la fabric ou en dehors de celle-ci, et la configuration Rendezvous Point n'est disponible que sur les nœuds frontière de la fabric. Les messages PIM sont transmis en monodiffusion entre les nœuds de frontière et la périphérie de la fabric, et les paquets de multidiffusion sont répliqués sur les périphériques de frontière de fabric de tête de réseau vers les nœuds de périphérie de la fabric.

Étape 1. Un pool global dans Cisco DNA Center dédié aux interfaces IP de monodiffusion est utilisé pour configurer la multidiffusion pour chaque VN où elle est activée. S'il n'y en a pas, reportez-vous à la procédure « Définir des pools d'adresses IP globales » pour en créer un.

Étape 2. Dans le tableau de bord Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabrics**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de fabric (par exemple : RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Fabric**

Infrastructure (Infrastructure de fabric), cliquez sur un nœud de frontière de fabric, puis sélectionnez **Enable Rendezvous Point (Activer le point de rendez-vous)**.



Étape 3. Dans la fenêtre contextuelle **Associate Multicast Pools to VNs (Associer des pools de multidiffusion à des VN)** à droite, sous Associate Virtual Networks (Associer des réseaux virtuels), sélectionnez le VN (par exemple : OPERATIONS), sous **Select IP Pools (Sélectionner des pools d'adresses IP)**, sélectionnez le pool créé pour la multidiffusion (par exemple : MULTICAST_PEER-RTP5), cliquez sur **Next (Suivant)**, sélectionnez un VN (par exemple : OPERATIONS), puis cliquez sur **Enable (Activer)**.

Étape 4. Répétez l'étape précédente pour tous les nœuds de frontière de fabric supplémentaires. En bas de l'écran, cliquez sur **Save (Enregistrer)**, puis sur **Apply (Appliquer)**.

Cisco DNA Center envoie les configurations de multidiffusion vers les nœuds de la fabric et crée les appairages de bouclage et MSDP (Multicast Source Discovery Protocol) pour la communication de l'état du point de rendez-vous (RP) entre les nœuds de frontière.

Étape 5. Si la communication de multidiffusion est requise en dehors de la frontière vers le routeur de fusion, activez les commandes suivantes sur chaque périphérique.

Global:

```
ip multicast-routing
ip pim rp address [RP Address]
ip pim register-source Loopback0
ip pim ssm default
```

Interface or subinterface (for each virtual network):

```
ip pim sparse-mode
```

Étape 6. Dans le volet de navigation de gauche, sur le site configuré avec la fabric, à côté du nom du site, cliquez sur l'icône d'engrenage, cliquez sur **Enable Native Multicast for IPv4 (Activer la multidiffusion native pour IPv4)**, en bas, cliquez sur **Save (Enregistrer)**, et dans la fenêtre coulissante, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

La configuration de multidiffusion de superposition est déployée pour utiliser la multidiffusion sous-jacente pour une communication d'infrastructure efficace.

Procédure 4. Activer la connectivité eBGP pour le VN au niveau du voisin (fusion) vers le routeur de frontière

L'application SD-Access dans Cisco DNA Center configure le transfert BGP du nœud de frontière de fabric vers les réseaux externes. Dans la version SD-Access décrite, vous configurez manuellement les homologues de réseau externe des périphériques de frontière avec les informations d'appairage VRF-Lite et BGP compatibles.

Étape 1. Utilisez l'interface de ligne de commande pour vous connecter aux périphériques de frontière afin d'observer les configurations automatisées pour la connectivité IP hors de la frontière créées par l'application SD-Access de Cisco DNA Center. Certaines des commandes suivantes peuvent être utiles.

```
show running-config brief
show running-config | section vrf definition
show running-config | section interface Vlan
show running-config | section router bgp
```

Conseil technique

Pour assurer la protection contre les échecs de connectivité entre les nœuds de frontière et les routeurs de fusion, vous devez déployer une paire résiliente de nœuds de frontière avec une connexion directe entre eux. Pour activer la redirection automatique du trafic, créez une relation de voisinage iBGP entre les nœuds de frontière pour chaque VN configuré. Prenez en charge plusieurs connexions logiques à l'aide du balisage 802.1Q en utilisant des configurations de ports trunk sur les commutateurs et les sous-interfaces des routeurs.

Étape 2. Connectez-vous à chaque périphérique de fusion externe à la fabric connectée à la frontière, en vous servant de la configuration des frontières comme guide, et configurez les VRF comme requis par les réseaux virtuels créés sur la frontière. Les VRF séparent la communication entre les groupes d'interfaces et les contextes de réseau virtuel dans la fabric.

```
vrf definition [VRF name]
 rd [Route Distinguisher]
 address-family ipv4
  route-target export [Route Target]
  route-target import [Route Target]
 exit-address-family
```

Par exemple, si la configuration suivante est provisionnée à la frontière :

```
vrf definition OPERATIONS
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

Effectuez la même configuration pour le routeur de fusion.

Répétez cette étape pour chaque contexte de réseau virtuel (y compris le GUEST VRF, si vous en avez configuré un), en restant cohérent avec la configuration du nœud de frontière.

Conseil technique
Le nom du VRF, le différentiateur de route et la cible de routage que vous configurez sur le routeur de fusion doivent correspondre à la configuration du nœud de frontière.

Étape 3. Configurez chaque interface avec le voisin. Certains périphériques prennent en charge la configuration de la sous-interface VLAN directement sur les trunks, et d'autres périphériques nécessitent que des interfaces VLAN soient créées et associées à un trunk. Répétez la configuration de l'interface du voisin pour chaque voisin de chaque homologue à la frontière.

```
interface [Peer physical interface]
 switchport mode trunk
interface [VLAN interface]
 vrf forwarding [VN/VRF name]
 ip address [Peer point-to-point IP address]
```

Par exemple, si la configuration suivante est provisionnée à la frontière :

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/24
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.9 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.13 255.255.255.252
```

Configurez la connectivité et l'adressage compatibles pour le routeur de fusion. Une interface VLAN sans instruction de transfert VRF associée est utilisée pour la communication INFRA_VN avec la table de routage globale.

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/7
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.10 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.14 255.255.255.252
```

Étape 4. Configurez le routage de monodiffusion IPv4 BGP vers la frontière pour prendre en charge la connectivité de chaque VRF associé à chaque VN dans la fabric.

```
router bgp [Local BGP AS]
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
 neighbor [Border VLAN IP Address] update-source [VLAN interface]
 ! repeat for any additional neighbors
address-family ipv4
  network [Loopback IP Address] mask 255.255.255.255
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
  maximum-paths 2
 exit-address-family
 address-family ipv4 vrf [VN/VRF name]
  neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
  neighbor [Border VLAN IP Address] update-source [VLAN interface]
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
 exit-address-family
```

Par exemple, si la configuration suivante est provisionnée à la frontière :

```
router bgp 65514
 bgp router-id interface Loopback0
 neighbor 172.16.172.14 remote-as 65500
 neighbor 172.16.172.14 update-source Vlan3004
 !
 address-family ipv4
  network 172.16.173.1 mask 255.255.255.255
  aggregate-address 172.16.173.0 255.255.255.0 summary-only
  neighbor 172.16.172.14 activate
exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.10 remote-as 65500
  neighbor 172.16.172.10 update-source Vlan3003
  neighbor 172.16.172.10 activate
exit-address-family
```

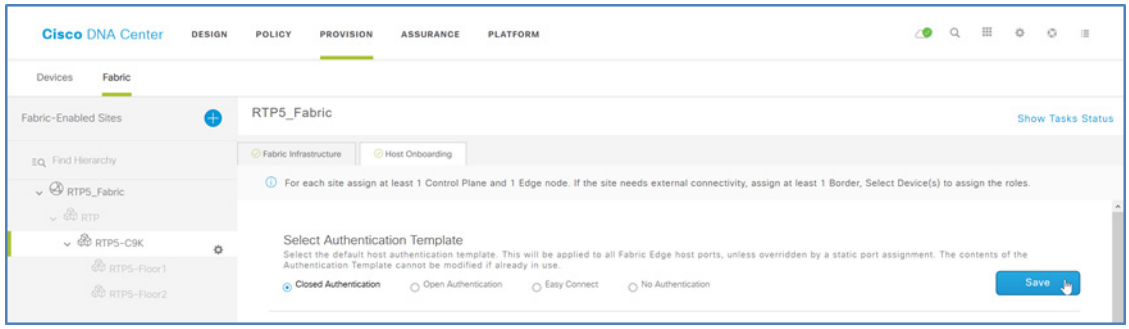
Configurez les éléments suivants sur le routeur de fusion :

```
router bgp 65500
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
```

```
 neighbor 172.16.172.13 remote-as 65514
 neighbor 172.16.172.13 update-source Vlan3004
 !
 address-family ipv4
  neighbor 172.16.172.13 activate
 exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.9 remote-as 65500
  neighbor 172.16.172.9 update-source Vlan3003
  neighbor 172.16.172.9 activate
exit-address-family
```

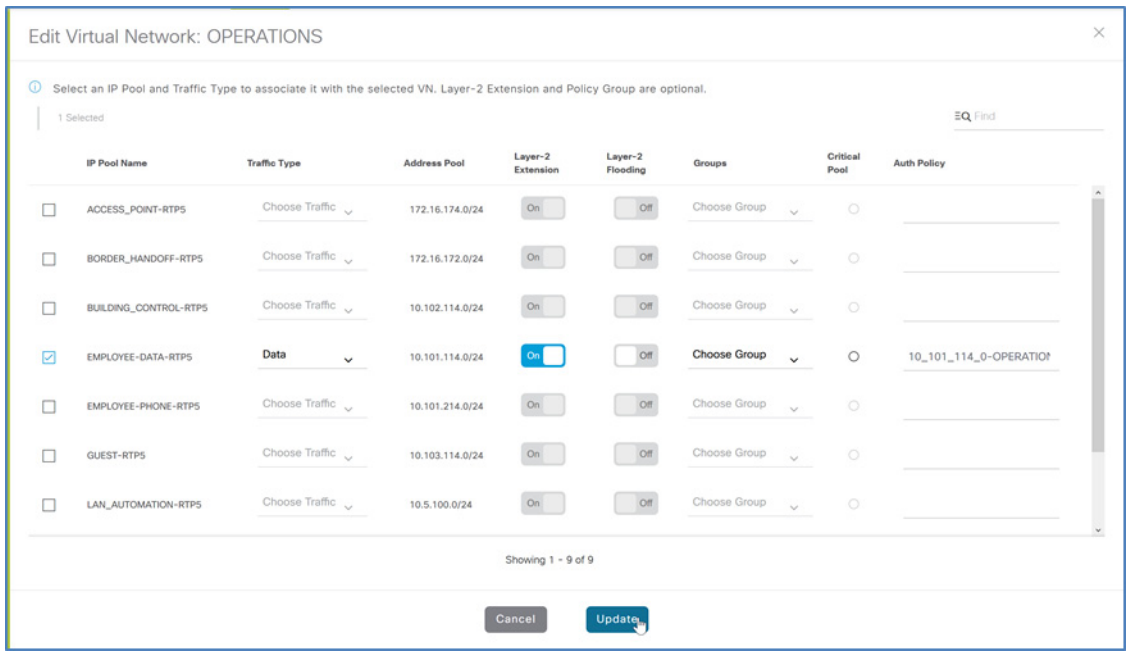
Procédure 5. Affecter des clients filaires à un VN et activer la connectivité

Étape 1. Dans le tableau de bord Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabrics**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de fabric (par exemple : RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Host Onboarding (Intégration de l'hôte)**, sous **Select Authentication template (Sélectionner un modèle d'authentification)**, sélectionnez **Closed Authentication (Authentification fermée)**, en haut de la section, cliquez sur **Save (Enregistrer)**, puis cliquez sur **Apply (Appliquer)**.



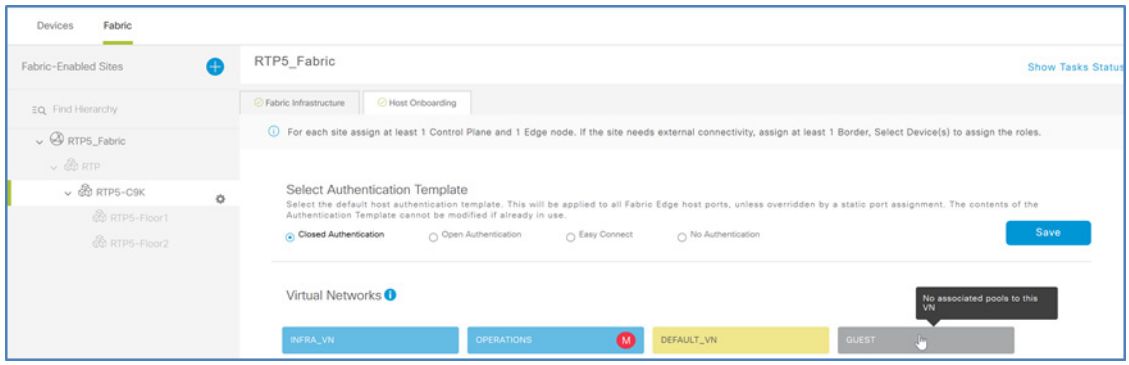
L'authentification fermée est définie comme valeur par défaut pour les ports hôtes, ce qui nécessite une authentification 802.1x pour qu'un terminal se connecte à la fabric ; ce paramètre peut être remplacé par port à d'autres fins, par exemple pour les ports de point d'accès.

Étape 2. Sous **Virtual Networks (Réseaux virtuels)**, sélectionnez un VN à utiliser pour les clients filaires (par exemple : OPERATIONS), dans le volet **Edit Virtual Network (Modifier le réseau virtuel) : *OPERATIONS***, sélectionnez les noms des **IP Pools (Pools d'adresses IP)** à ajouter au VN (par exemple : EMPLOYEE-DATA-RTP5), sélectionnez un **Traffic Type (Type de trafic)** de **Data (Données)**, assurez-vous que la **Layer 2 Extension (Extension de couche 2)** est **On (Activée)**, modifiez éventuellement le nom de la **Auth Policy (Politique d'authentification)** pour qu'il soit significatif pour le site, cliquez sur **Update (Mettre à jour)**, puis cliquez sur **Apply (Appliquer)**.

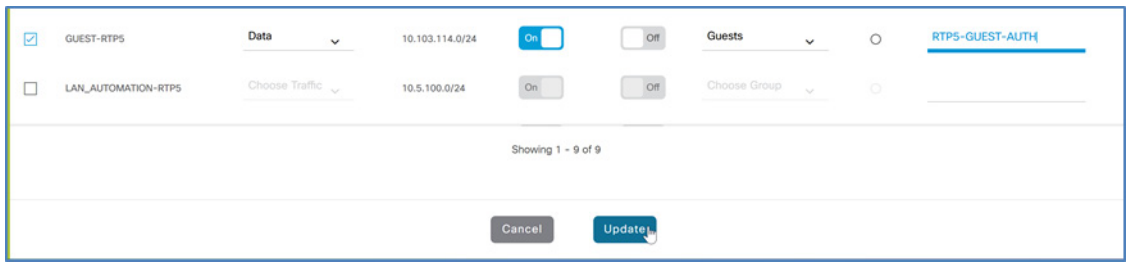


Un message d'état s'affiche, puis l'écran **Host Onboarding (Intégration d'hôte)** s'affiche.

Étape 3. Si vous avez créé un réseau virtuel invité, associez un pool d'adresses IP pour les services invité. Sous **Virtual Networks (Réseaux virtuels)**, sélectionnez un VN à utiliser pour les clients sans fil invités (par exemple : GUEST).



Étape 4. Dans le volet **Edit Virtual Network (Modifier le réseau virtuel) : *GUEST (Invité)***, sélectionnez les noms des **IP Pools (Pools d'adresses IP)** à ajouter au VN (par exemple : EMPLOYEE-DATA-RTP5), sélectionnez un **Traffic Type (Type de trafic)** de **Data (Données)**, vérifiez que **Layer 2 Extension (Extension de couche 2)** est **On (Activée)**, modifiez éventuellement le nom de la **Auth Policy (Politique d'authentification)** pour qu'il soit significatif pour le site, cliquez sur **Update (Mettre à jour)**, puis cliquez sur **Apply (Appliquer)**.



Un message d'état s'affiche, puis l'écran **Host Onboarding (Intégration d'hôte)** s'affiche.

Procédure 6. Activer les ports de périphérie de fabric pour l'intégration des clients

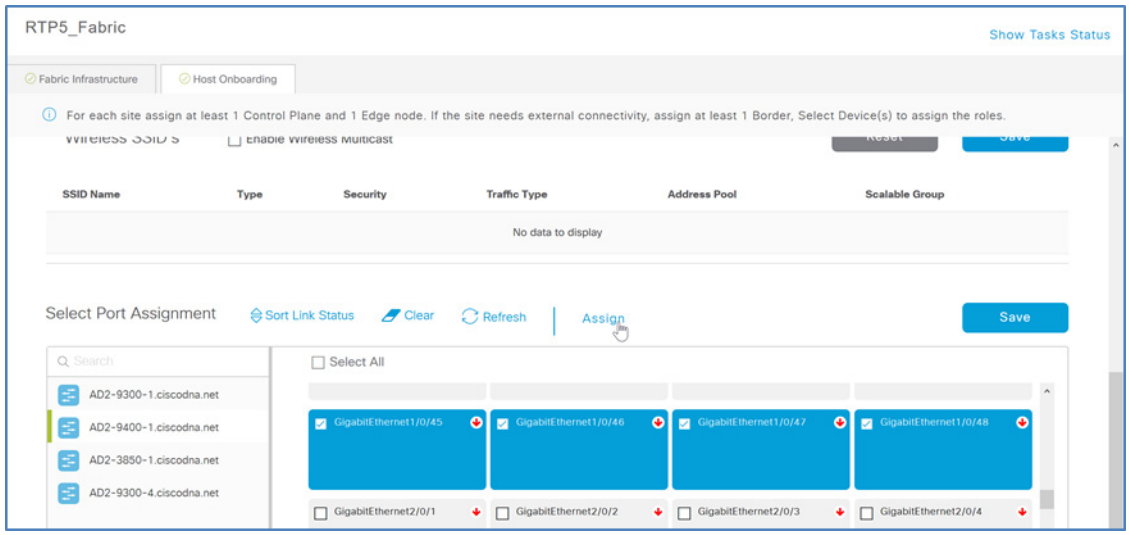
En option

Remplacez le modèle d'authentification par défaut (authentification fermée) affecté lors de la procédure précédente, lorsque des périphériques connectés ne prennent pas en charge 802.1x, ou lorsque vous utilisez d'autres méthodes d'authentification, telles que l'authentification MAB pour les objets connectés, ou lors de l'affectation manuelle d'un pool d'adresses à un port.

Répétez cette procédure pour chaque commutateur de périphérie de fabric avec des clients qui se connectent aux ports de périphérie de fabric exigeant un remplacement du modèle d'authentification par défaut.

Étape 1. Accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabrics**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de fabric (par exemple : RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Host Onboarding (Intégration de l'hôte)**, puis sous la section **Select Port Assignment (Sélectionner l'affectation de port)**, dans la colonne de gauche, sélectionnez un commutateur.

Étape 2. Dans la liste des ports de commutateur, sélectionnez un ensemble de ports de périphérie de fabric filaires devant participer à un VN de fabric, puis cliquez sur **Assign (Affecter)**.



Étape 3. Dans la fenêtre coulissante, sélectionnez le **Connected Device Type (Type de périphérique connecté)** approprié (par exemple : User Devices [Périphériques utilisateur] [téléphone IP, ordinateur, ordinateur portable]), sélectionnez le **Address Pool (Pool d'adresses)** (par exemple : 10_101_114_0 [EMPLOYEE-DATA-RTP5]), sélectionnez le **Group (Groupe)** (par exemple : Employees), sélectionnez un **Voice Pool (Pool de voix)** si nécessaire, sélectionnez un **Auth Template (Modèle d'authentification)** (par exemple : No Authentication [Aucune authentification]), puis cliquez sur **Update (Mettre à jour)**.

Étape 4. À droite de la section **Select Port Assignment (Sélectionner l'affectation des ports)**, sélectionnez **Save (Enregistrer)**, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

Étape 5. Répétez les étapes précédentes pour chaque commutateur supplémentaire ajouté.

Les périphériques peuvent désormais se connecter aux ports de périphérie de fabric à l'aide de la superposition de réseau filaire et de la méthode d'authentification créée.

Conseil technique
L'affectation de groupe est utilisée pour affecter un groupe de manière statique si le port de périphérie de la fabric ne reçoit pas son affectation dynamiquement au moyen d'un serveur d'authentification, ce qui est utile pour certains types de périphériques utilisés dans une entreprise. Si l'option « No Authentication (Aucune authentification) » est sélectionnée comme méthode d'authentification, Cisco DNA Center envoie le modèle d'authentification global par défaut sélectionné dans la section « Select Authentication template (Sélectionner le modèle d'authentification) » en haut de l'écran. Cisco DNA Center envoie une configuration de port lorsque vous sélectionnez « Closed Authentication (Authentification fermée) », mais aussi lorsque vous sélectionnez « Open Authentication (Authentification ouverte) ».

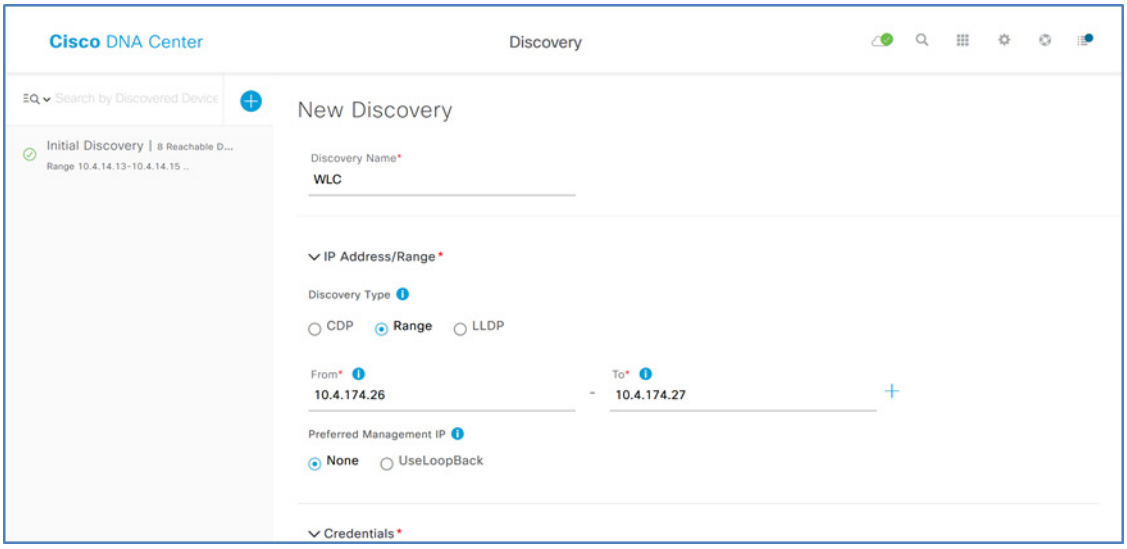
Processus : intégration de SD-Access sans fil dans la fabric

Le processus d'installation des contrôleurs LAN sans fil pour SD-Access est décrit dans le document Guide de déploiement normatif de SD-Access pour le réseau local distribué. Ce processus d'intégration sans fil suppose que des contrôleurs sont disponibles pour s'intégrer dans la fabric à l'aide de Cisco DNA Center.

Procédure 1. Ajouter les contrôleurs sans fil dans l'inventaire et créer une paire SSO haute disponibilité

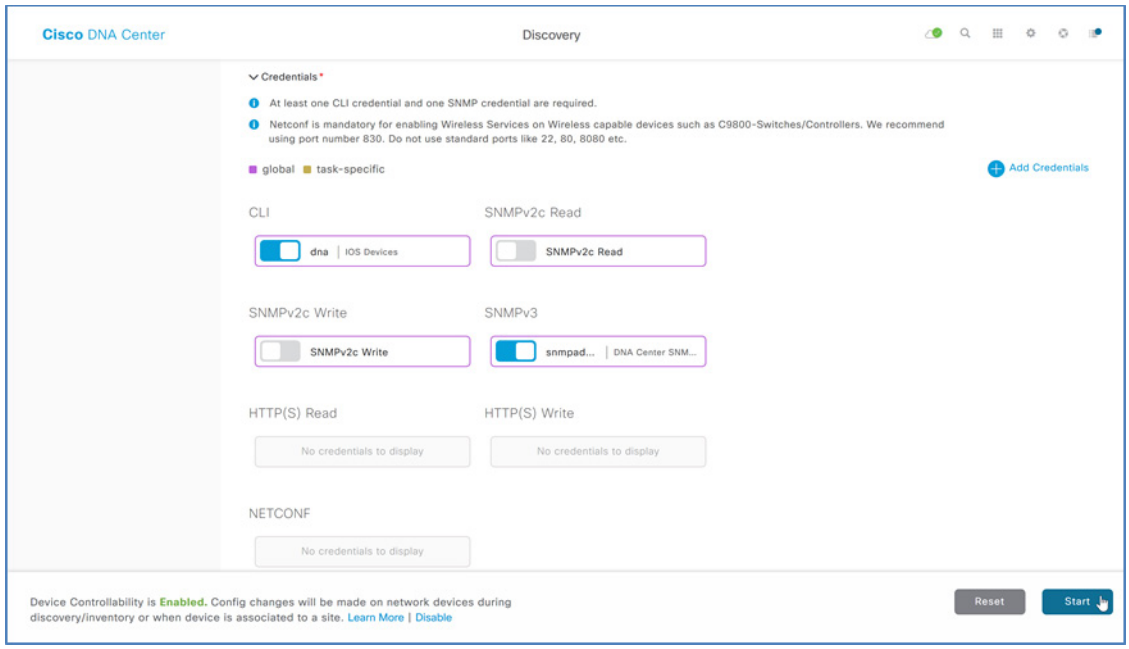
Si les contrôleurs LAN sans fil ne se trouvent pas dans l'inventaire Cisco DNA Center, vous devez les ajouter avant l'intégration sans fil. Pour la résilience, vous devez également utiliser deux contrôleurs LAN sans fil de même type pour créer une paire SSO haute disponibilité.

Étape 1. Accédez au tableau de bord principal de Cisco DNA Center, faites défiler l'écran jusqu'à la section **Tools (Outils)**, cliquez sur **Discovery (Détection)** et indiquez un **Discovery Name (Nom de détection)**. Sélectionnez **Range (Plage)** et saisissez une adresse IP de bouclage de début et de fin pour **IP Ranges (Plages d'adresses IP)** (pour couvrir une seule adresse, saisissez cette adresse pour le début et la fin de la plage). Pour **Preferred Management IP (Adresse IP de gestion préférée)**, utilisez **None (Aucune)**.

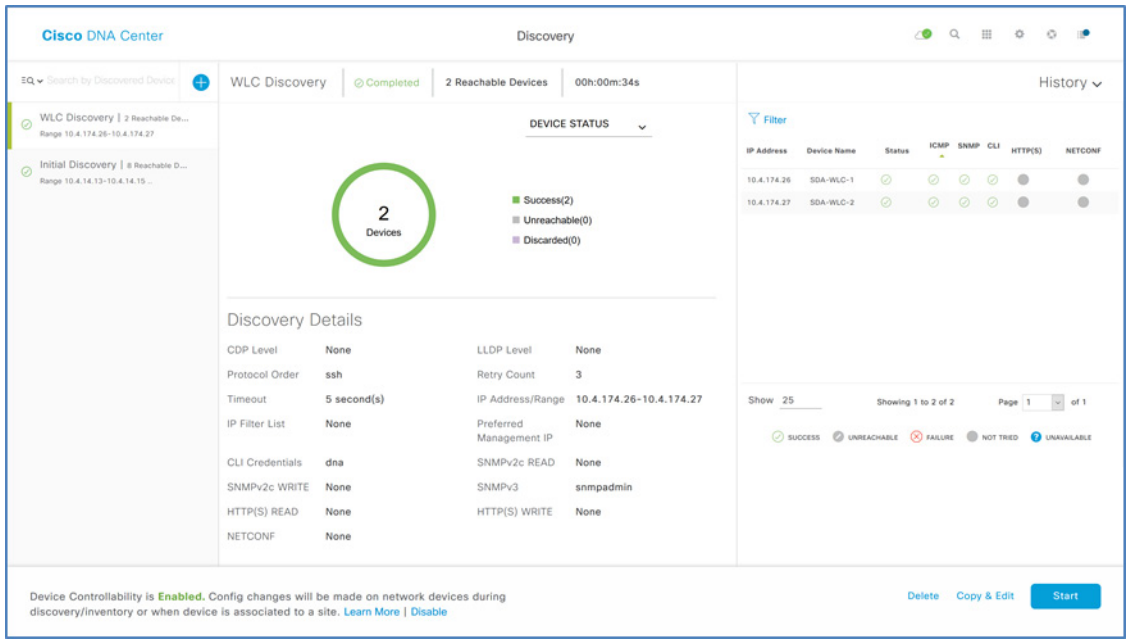


Étape 2. Si vous avez des plages supplémentaires, à côté de la première plage, cliquez sur **+** (signe plus), saisissez la plage supplémentaire et répétez l'opération pour toutes les plages restantes.

Étape 3. Faites défiler l'écran pour vérifier les informations d'identification de l'interface de ligne de commande utilisées pour la détection et les configurations d'informations d'identification SNMP envoyées au périphérique par la fonction de contrôle des périphériques Cisco DNA Center. Si vous avez des informations d'identification propres à la détection pour le périphérique, cliquez sur **+ Add Credentials (Ajouter des informations d'identification)**, ajoutez chaque nouvelle information d'identification, enregistrez-la, puis en bas cliquez sur **Start (Démarrer)**.



Les informations de détection sont affichées pendant que la détection est exécutée.



Étape 4. S'il y a des défaillances de détection, examinez la liste des périphériques, résolvez le problème et redémarrez la détection pour ces périphériques, ainsi que les périphériques supplémentaires à ajouter à l'inventaire.

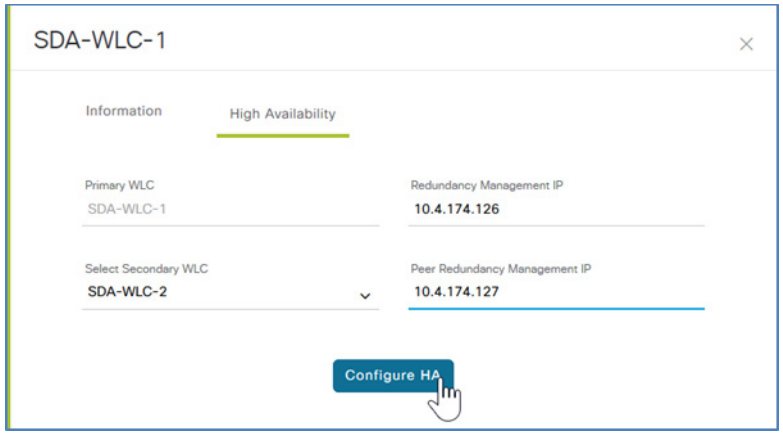
Étape 5. Après avoir terminé toutes les tâches de détection, accédez au tableau de bord principal de Cisco DNA Center, puis, sous la section **Tools (Outils)**, cliquez sur **Inventory (Inventaire)**. Les périphériques détectés s'affichent. Une fois la collecte d'inventaire terminée, chaque périphérique affiche un état de synchronisation **Managed (Géré)**, ce qui signifie que Cisco DNA Center tient à jour un modèle interne qui reflète le déploiement physique du périphérique.

Cisco DNA Center peut désormais accéder aux périphériques, synchroniser l'inventaire de configuration et apporter des modifications de configuration aux périphériques.

Conseil technique
Sur le côté droit de la ligne de titre de la table d'inventaire, vous pouvez modifier les colonnes affichées. Utilisez la colonne **Device Role (Rôle du périphérique)** pour voir le rôle de périphérique affecté par la détection en fonction du type de périphérique et pour ajuster ce rôle de manière à mieux refléter le déploiement réel d'un périphérique, tel que routeur d'accès, de distribution, central ou de frontière, où routeur de frontière dans cet écran est un rôle de périphérique générique n'appartenant pas à la fabric. Le réglage du rôle à ce stade, plutôt que dans les procédures ultérieures, permet d'améliorer l'apparence des cartes topologiques initiales. Pour les contrôleurs LAN sans fil, l'affectation au rôle central permet de rapprocher le périphérique de son emplacement type.

Avant de continuer, utilisez le bouton **Refresh (Actualiser)** pour mettre à jour le **Last Inventory Collection Status (État de la dernière collecte d'inventaire)** jusqu'à ce qu'il soit à l'état **Managed (Géré)**.

Étape 6. Si vous créez une paire SSO à haute disponibilité avec un ensemble de contrôleurs qui ne sont pas actuellement appairés, accédez au tableau de bord principal Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, cliquez sur le texte **Device Name (Nom du périphérique)** du contrôleur LAN sans fil principal (par exemple : SDA-WLC1), en haut et à droite de la fenêtre contextuelle, sélectionnez **High Availability (Haute disponibilité**), sous **Select Secondary WLC (Sélectionner le contrôleur LAN sans fil secondaire)**, sélectionnez le deuxième contrôleur LAN sans fil dans la paire SSO haute disponibilité (par exemple : SDA-WLC-2), fournissez la **Redundancy Management IP (Adresse IP de gestion de la redondance)** et la **Peer Redundancy Management IP (Adresse IP de gestion de la redondance des homologues)** (par exemple : 10.4.174.126, 10.4.174.127), cliquez sur **Configure HA (Configurer la haute disponibilité)**, puis cliquez sur **OK** dans la fenêtre contextuelle d'avertissement de redémarrage.



Dans le navigateur, des messages d'avertissement s'affichent.

```
Configuring HA for Primary. Please do not Refresh the page..
Configuring HA for Secondary...
```

La reconfiguration et le redémarrage peuvent prendre plusieurs minutes.

Étape 7. Utilisez le bouton d'actualisation en haut de l'écran pour actualiser l'affichage jusqu'à ce que les contrôleurs LAN sans fil en mode haute disponibilité s'affichent comme un seul périphérique. Vérifiez l'état de la haute disponibilité en cliquant sur le texte **Device Name (Nom du périphérique)** du contrôleur LAN sans fil principal (par exemple : SDA-WLC1), en haut et à droite de la fenêtre contextuelle, sélectionnez **High Availability (Haute disponibilité)**, puis vérifiez que **Redundancy State (État de la redondance)** a la valeur **SSO** et que **Sync Status (État de la synchronisation)** a la valeur **Complete (Terminée)**.

Passez à l'étape suivante une fois la configuration de la haute disponibilité terminée.

Étape 8. Accédez au tableau de bord principal de Cisco DNA Center et sélectionnez **DESIGN (CONCEPTION) > Image Repository (Référentiel d'images)**. Recherchez la famille de périphériques et vérifiez la version du logiciel. Si l'image du contrôleur LAN sans fil est la version correcte, continuez. Si l'image doit être mise à jour et qu'elle est répertoriée, cliquez sur l'étoile à côté de l'image pour la marquer comme Golden et mettre à jour le logiciel. Si vous avez besoin d'une image qui ne figure pas dans la liste, en haut de l'écran, cliquez sur Import Image/SMU (Importer une image/SMU), suivez les instructions pour effectuer l'importation, actualisez l'écran et utilisez le menu déroulant pour marquer l'image comme Golden.

Étape 9. Si vous mettez à niveau le périphérique, accédez à **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, sélectionnez le contrôleur LAN sans fil marqué comme **Outdated (Obsolète)**, puis dans le menu **Actions**, sélectionnez **Update OS Image (Mettre à jour l'image du système d'exploitation)**. Confirmez la sélection du périphérique à mettre à jour, utilisez la valeur par défaut **Now (Maintenant)** de la sélection **When (Quand)**, cliquez sur **Apply (Appliquer)**, puis dans la fenêtre contextuelle d'avertissement sur le redémarrage des périphériques, cliquez sur **OK**.

Les images sont distribuées aux périphériques sélectionnés, puis ceux-ci redémarrent pour activer la nouvelle image dès que sa distribution est terminée. Cliquez sur le bouton **Refresh (Actualiser)** pour voir quand l'état **In Progress (En cours)** est retiré.

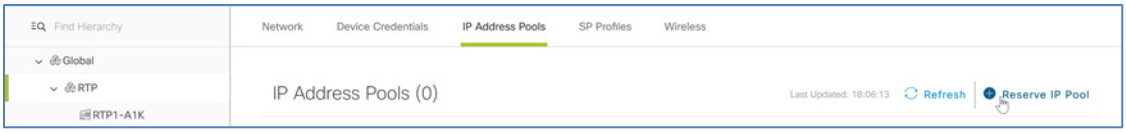
Procédure 2. Créer des pools d'adresses IP pour les points d'accès

Vérifiez qu'un pool global est disponible dans Cisco DNA Center pour l'affectation d'adresses pour les points d'accès devant être gérés par le réseau.

Étape 1. Accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > IP Address Pools (Pools d'adresses IP)**. Dans la hiérarchie du site à gauche, sélectionnez **Global** et examinez la liste des pools d'adresses IP pour rechercher un pool dédié à l'infrastructure de points d'accès (par exemple : ACCESS_POINT).

Étape 2. S'il n'existe pas de pool pour les points d'accès, cliquez sur **+ Add IP Pool (Ajouter un pool d'adresses IP)**, renseignez le **IP Pool Name (Nom du pool d'adresses IP)**, le **IP Subnet (Sous-réseau IP)**, le **CIDR Prefix (Préfixe CIDR)** et la **Gateway IP address (Adresse IP de la passerelle)** (par exemple : ACCESS_POINT, 172.16.173.0, /24, 172.16.173.1), sélectionnez le **DHCP Server (Serveur DHCP)** et le **DNS Server (Serveur DNS)**, puis cliquez sur **Save (Enregistrer)**.

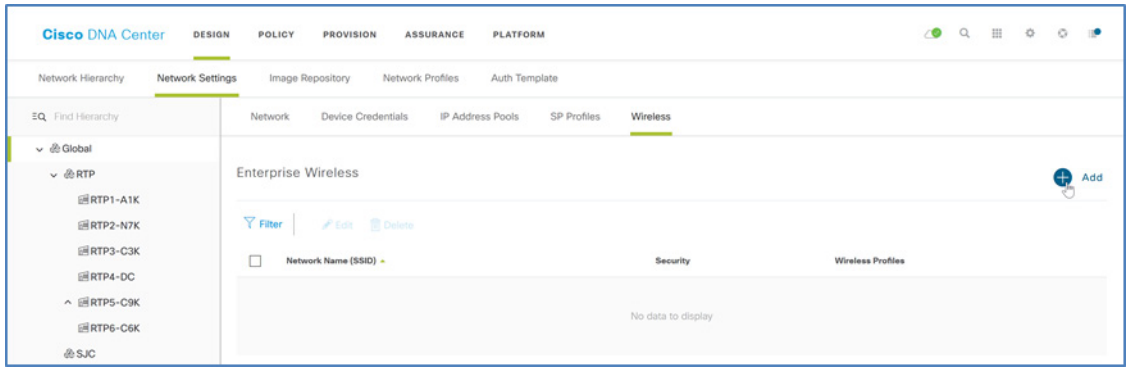
Étape 3. Accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > IP Address Pools (Pools d'adresses IP)**, à gauche dans la hiérarchie du site, sélectionnez un site ou un niveau inférieur pour la réservation d'un pool d'adresses IP (par exemple : RTP5-C9K). Si le pool n'est pas encore réservé, dans le coin supérieur droit, cliquez sur Reserve IP Pool (Réserver le pool d'adresses IP).



Étape 4. Si vous réservez un pool, renseignez **IP Pool Name (Nom du pool d'adresses IP)** (par exemple : ACCESS_POINT-RTP5), sous **Type**, sélectionnez **LAN**, sélectionnez la source du **Global IP Pool (Pool d'adresses IP global)** pour la réservation, sous **CIDR Notation / No. of IP Addresses (Notation CIDR/No. des adresses IP)**, sélectionnez la partie de l'espace d'adressage à utiliser, affectez une **Gateway IP Address (Adresse IP de passerelle)**, le ou les **DHCP Server(s) (Serveur[s] DHCP)** et le ou les **DNS Servers(s) (Serveur[s] DNS)**, puis cliquez sur **Reserve (Réserver)**.

Procédure 3. Concevoir des SSID sans fil de fabric d'entreprise

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > Wireless (Sans fil)**, dans le volet de la hiérarchie de gauche, sélectionnez le niveau **Global** et dans la section **Enterprise Wireless (Sans fil d'entreprise)**, cliquez sur **+ Add (Ajouter)**.



L'Assistant **Create an Enterprise Wireless Network (Créer un réseau sans fil d'entreprise)** apparaît.

Étape 2. À l'aide de l'Assistant **Create an Enterprise Wireless Network (Créer un réseau sans fil d'entreprise)**, fournissez les informations suivantes :

- Saisissez le **Wireless Network Name (SSID) (Nom du réseau sans fil)** (par exemple : Employee)
- Sous le **TYPE OF ENTERPRISE NETWORK (TYPE DE RÉSEAU D'ENTREPRISE)**, sélectionnez Voice (Voix), Data (Données) et Fast Lane (Voie rapide)
- Sélectionnez ou confirmez la **WIRELESS OPTION (OPTION SANS FIL)**.
- Pour **LEVEL OF SECURITY (NIVEAU DE SÉCURITÉ)**, sélectionnez une option (par exemple : WPA2 Enterprise)
- Sous **ADVANCED SECURITY OPTIONS (OPTIONS DE SÉCURITÉ AVANCÉES)**, sélectionnez Adaptive (Adaptative)

Étape 3. Cliquez sur **Next (Suivant)** pour continuer dans l'Assistant et fournissez les informations suivantes :

- Saisissez un **Wireless Profile Name (Nom de profil sans fil)** (par exemple : RTP5-Wireless)
- Sous **Fabric**, sélectionnez **Yes (Oui)**
- Sous **Choose a site (Choisir un site)**, sélectionnez l'emplacement de diffusion du SSID (par exemple : Global/RTP/RTP5-C9K) et incluez les étages à intégrer dans la couverture du SSID (par exemple : Global/RTP/RTP5-C9K/Floor 1)

Étape 4. Cliquez sur **Finish (Terminer)** pour continuer. L'écran **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > Wireless (Sans fil)** s'affiche.

Étape 5. Répétez cette procédure pour les SSID supplémentaires utilisant le même profil de réseau et tous les nouveaux profils d'emplacement à associer à un SSID.

Procédure 4. Concevoir un SSID sans fil de fabric invité

Étape 1. Accédez à **DESIGN (CONCEPTION) > Network Settings (Paramètres réseau) > Wireless (Sans fil)**, dans la section **Guest Wireless (Sans fil pour invités)**, cliquez sur **+ Add (Ajouter)**, et dans l'Assistant **Create a Guest Wireless Network (Créer un réseau sans fil invité)**, fournissez les informations suivantes :

- Saisissez le **Wireless Network Name (SSID) (Nom du réseau sans fil)** (par exemple : Guest)
- Sous **LEVEL OF SECURITY (NIVEAU DE SÉCURITÉ)**, sélectionnez Web Auth (Authentification web)

- Sous **AUTHENTICATION SERVER (SERVEUR D'AUTHENTIFICATION)**, sélectionnez ISE Authentication (Authentification ISE).

Conservez les autres sélections par défaut et cliquez sur **Next (Suivant)** pour continuer dans l'Assistant.

Étape 2. À l'étape **Wireless Profiles (Profils sans fil)**, sélectionnez le **Profile Name (Nom de profil)** correspondant à l'emplacement de déploiement (par exemple : RTP5-Wireless), dans le panneau coulissant, conservez la sélection de **Fabric** par défaut **Yes (Oui)**, conservez les autres informations par défaut, et en bas du panneau, cliquez sur **Save (Enregistrer)**, puis sur **Next (Suivant)**.

Étape 3. À l'étape **Portal Customization (Personnalisation du portail)**, cliquez sur **+ Add (Ajouter)**. L'écran **Portal Builder (Concepteur de portail)** s'affiche.

Étape 4. Indiquez un nom de **Guest Portal (Portail invité)** (par exemple : Guest-RTP5), procédez aux personnalisations souhaitées, puis, en bas de l'écran, cliquez sur **Save (Enregistrer)**. Un portail d'authentification web d'invité est généré pour le site et vous revenez à l'écran précédent.

Étape 5. Cliquez sur **Finish (Terminer)**.

La conception du réseau local sans fil est créée et est prête à être déployée.

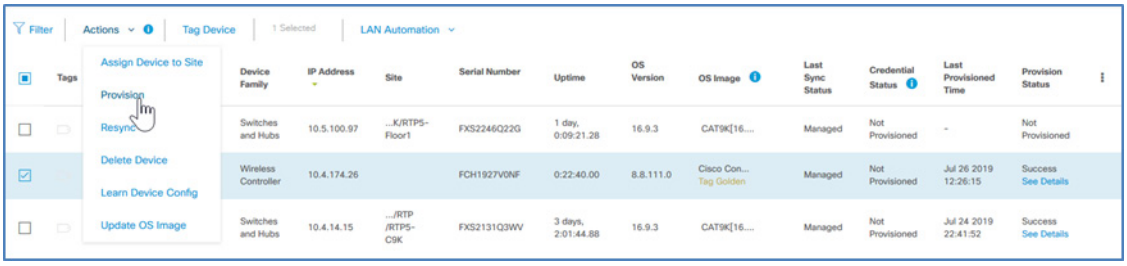
Procédure 5. Provisionner le contrôleur LAN sans fil pour l'intégration de fabric SD-Access sans fil

Une fois la conception SD-Access sans fil terminée, envoyez la configuration de l'application de conception vers le contrôleur LAN sans fil.

Étape 1. Accédez à PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire), recherchez le contrôleur LAN sans fil et cochez la case en regard de celui-ci, puis, en haut de l'écran, dans la liste déroulante Actions, sélectionnez Provision (Provisionner). L'Assistant Provision Devices (Provisionner des périphériques) s'ouvre.

Conseil technique

Lorsqu'une paire de contrôleurs LAN sans fil est configurée en mode SSO haute disponibilité, un seul contrôleur LAN sans fil apparaît dans l'inventaire de Cisco DNA Center. Vous pouvez vérifier qu'une paire SSO haute disponibilité est configurée en cliquant sur le nom du périphérique, puis sur l'onglet **High Availability (Haute disponibilité)**.



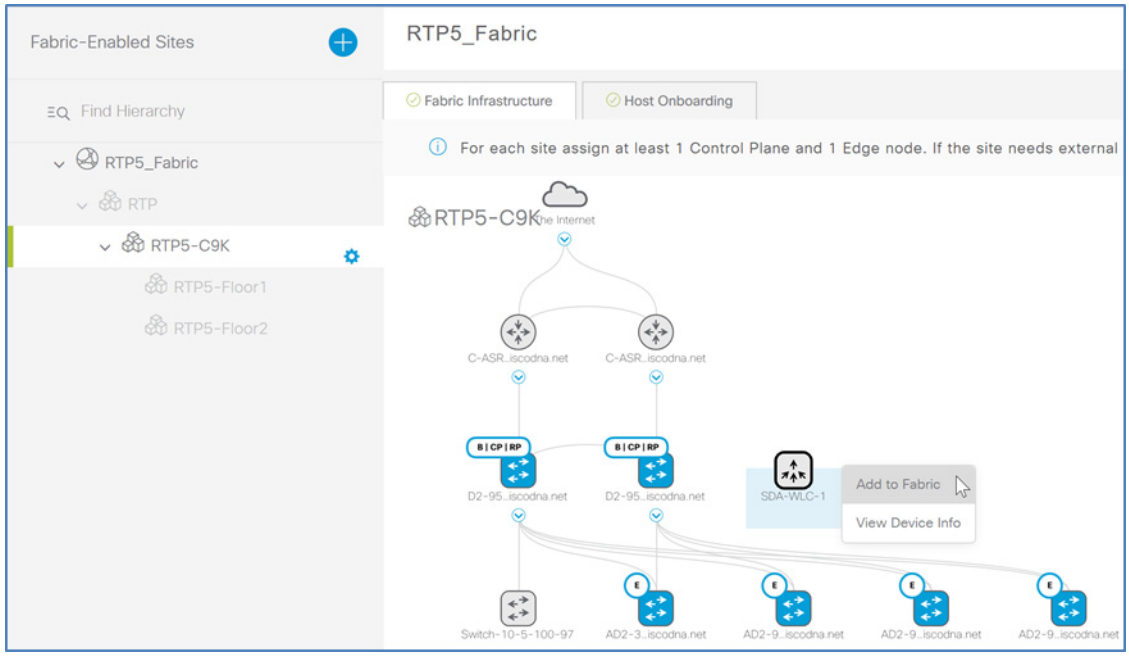
Étape 2. Affectez le site (par exemple : Global/RTP/RTP5-C9K), cliquez sur **Next (Suivant)**, à l'étape **Configuration** sous **Managed AP Location (Emplacement de point d'accès géré)**, sélectionnez les affectations d'étage supplémentaires pour les points d'accès gérés par le contrôleur LAN sans fil (par exemple : Global/RTP/RTP5-C9K/Floor 1), cliquez sur **Next (Suivant)**, puis à l'étape **Advanced Configuration (Configuration avancée)**, cliquez sur **Next (Suivant)**.

Étape 3. À l'étape **Summary (Résumé)**, passez en revue les configurations, cliquez sur **Deploy (Déployer)**, dans le volet coulissant, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

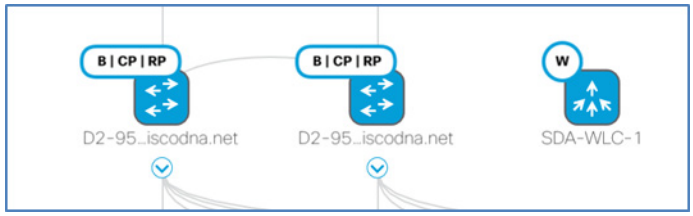
Le contrôleur LAN sans fil est affecté au site et le provisionnement commence. Utilisez le bouton **Refresh (Actualiser)** jusqu'à ce que **Provision Status (État du provisionnement)** affiche **Success (Réussi)** avant de continuer.

Procédure 6. Provisionner SD-Access sans fil dans la fabric

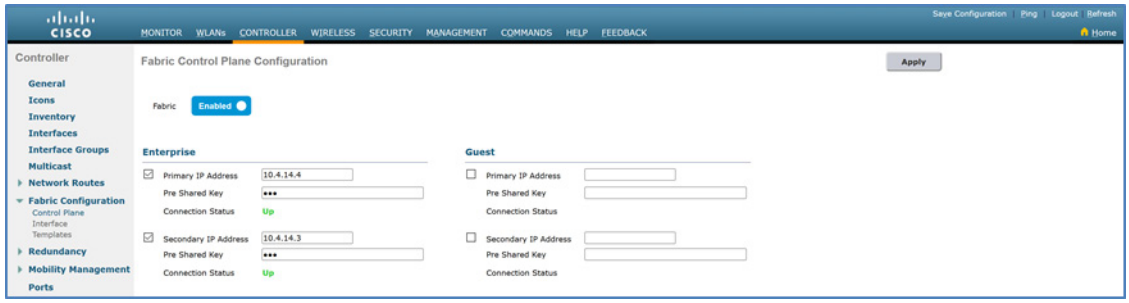
Étape 1. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabric**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), à gauche dans la section de navigation **Fabric-Enabled Sites (Sites prenant en charge la fabric)**, cliquez sur le site associé (par exemple : Global/RTP/RTP5-C9K), cliquez sur le contrôleur LAN sans fil, puis dans la zone contextuelle, cliquez sur **Add to Fabric (Ajouter à la fabric)**.



Étape 2. En bas de l'écran, cliquez sur **Save (Enregistrer)**, dans le menu coulissant, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**. Les configurations de contrôleur LAN sans fil sont créées pour établir une connexion sécurisée au plan de contrôle de fabric.



Vous pouvez vérifier que la paire de contrôleurs LAN sans fil est intégrée dans la fabric à partir de la console de gestion de contrôleur LAN sans fil en accédant à **CONTROLLER (CONTRÔLEUR) > Fabric Configuration (Configuration de fabric) > Control Plane (Plan de contrôle)**, qui indique que l'intégration de fabric est activée avec l'état de connexion up (activée).



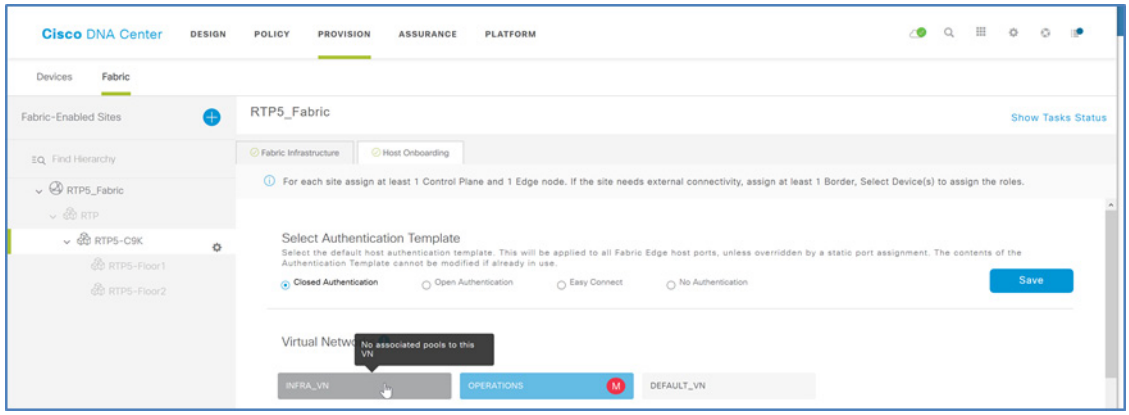
Procédure 7. Activer l'intégration des points d'accès dans la fabric sans fil

Les points d'accès sont des hôtes qui rejoignent la fabric et sont affectés à un VN nommé INFRA_VN. Ce VN spécial pour les périphériques d'infrastructure, tels que les points d'accès, permet la communication de gestion entre les points d'accès au niveau des nœuds de périphérie de la fabric à l'aide du plan de contrôle de la fabric et du contrôleur LAN sans fil placé hors de la fabric, dans le cadre de la connectivité de routage global.

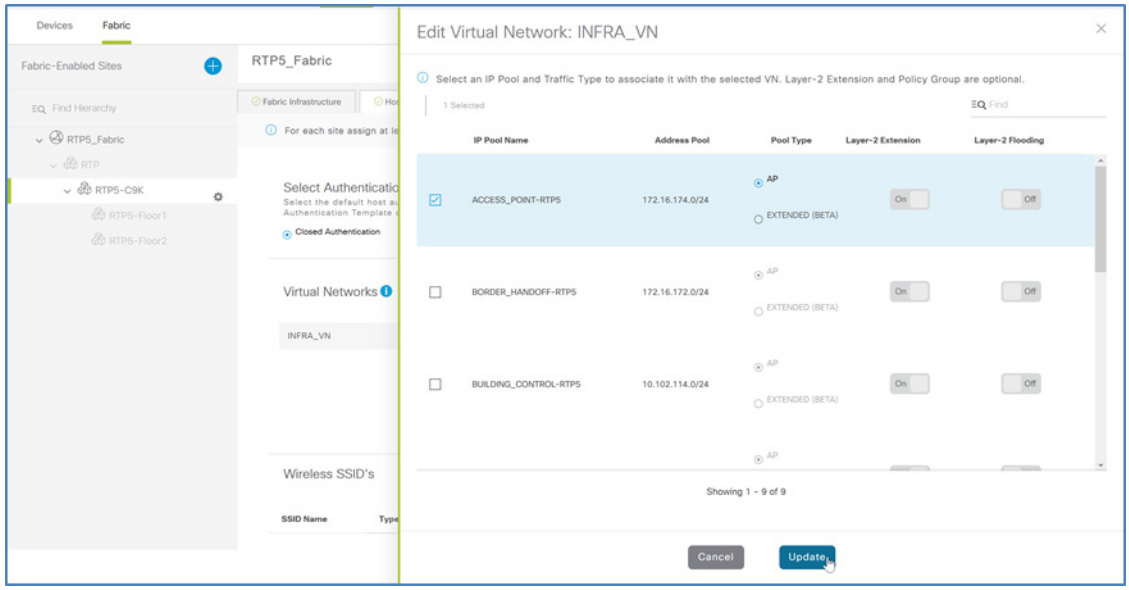
Étape 1. Connectez les points d'accès à utiliser pour la fabric directement à un nœud de périphérie dans la fabric.

Étape 2. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabric Domains (Domaines de fabric)**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), à gauche dans la section de navigation **Fabric-Enabled Sites (Sites prenant en charge la fabric)**, cliquez sur le site associé (par exemple : Global/RTP/RTP5-C9K), puis cliquez sur **Host Onboarding (Intégration d'hôte)**.

Étape 3. Sous **Virtual Networks (Réseaux virtuels)**, sélectionnez **INFRA_VN**.

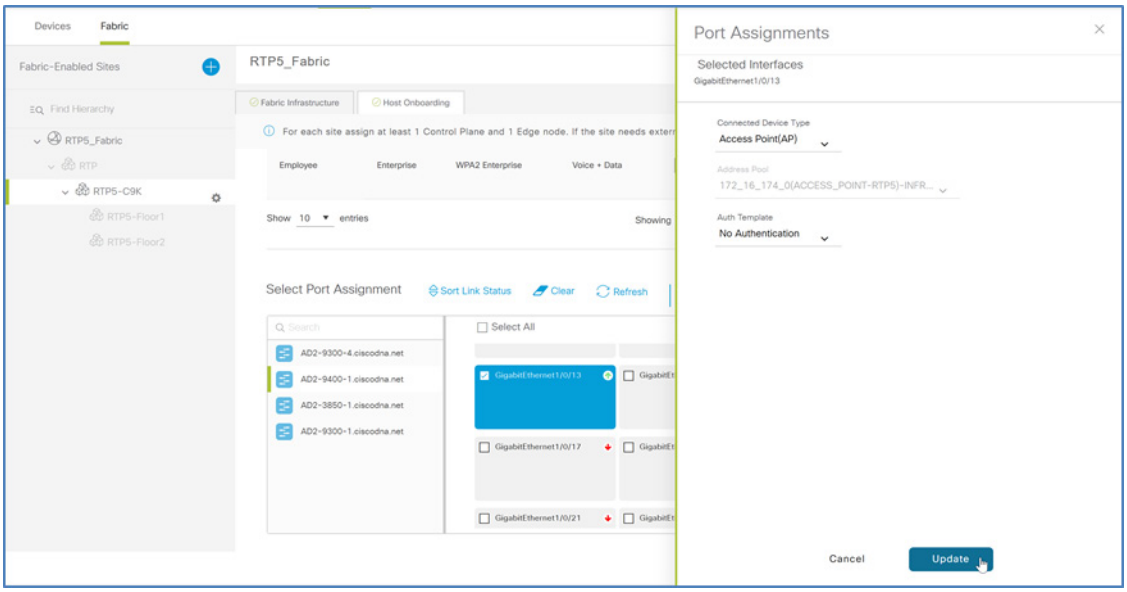


Étape 4. Cochez la case en regard du nom du pool d'adresses IP pour les points d'accès (par exemple : ACCESS_POINT-RTP5), sous **Pool Type (Type de pool)** sélectionnez **AP (Point d'accès)**, puis cliquez sur **Update (Mettre à jour)**.



Étape 5. Dans le panneau coulissant Modify Virtual Network (Modifier le réseau virtuel), conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

Étape 6. Sous **Select Port Assignment (Sélectionner l'affectation des ports)**, sélectionnez un commutateur, sélectionnez les ports du commutateur à utiliser pour les points d'accès, sélectionnez **Assign (Affecter)**, dans la fenêtre coulissante **Port Assignments (Affectation des ports)**, sous **Connected Device Type (Type de périphérique connecté)**, sélectionnez **Access Point (AP) (Point d'accès)**, laissez la sélection **Address Pool (Pool d'adresses)** par défaut, sous **Auth Template (Modèle d'authentification)** sélectionnez **No Authentication (Pas d'authentification)**, puis cliquez sur **Update (Mettre à jour)**.



Conseil technique

Cisco DNA Center permet l'intégration automatique des points d'accès en provisionnant une macro CDP sur les commutateurs de périphérie de la fabric lorsque le modèle d'authentification est défini sur **No Authentication (Pas d'authentification)**. Vous pouvez également utiliser les configurations des ports de commutateur dans Cisco DNA Center pour affecter un port au pool d'adresses IP pour les points d'accès.

Étape 7. Répétez l'étape précédente pour tous les commutateurs supplémentaires dont des ports sont utilisés pour les points d'accès.

Étape 8. Une fois que vous avez sélectionné tous les ports prenant en charge les points d'accès, en haut de la section **Select Port Assignment (Sélectionner l'affectation de port)**, cliquez sur **Save (Enregistrer)**, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.

Une fois la mise à jour terminée, les ports de commutateur de nœuds de périphérie connectés aux points d'accès sont activés avec une configuration de surveillance de périphérique reconnaissant les points d'accès et permettant à ceux-ci d'obtenir une connectivité réseau.

Conseil technique

Une route par défaut dans la sous-couche ne peut pas être utilisée par les points d'accès pour atteindre le contrôleur LAN sans fil. Une route plus spécifique (telle qu'un sous-réseau /24 ou une route d'hôte /32) vers les adresses IP de contrôleur LAN sans fil doit exister dans la table de routage globale sur chaque nœud où les points d'accès se connectent pour établir la connectivité. Redistribuez la route de contrôleur LAN sans fil à la frontière dans le processus de routage IGP sous-jacent pour plus d'efficacité. Vous pouvez également créer des entrées statiques sur chaque nœud de périphérie prenant en charge les points d'accès.

Étape 9. Accédez au tableau de bord principal de Cisco DNA Center, sous **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, puis en haut, dans le menu déroulant **Actions**, sélectionnez **Resync (Resynchroniser)**. Les points d'accès associés aux contrôleurs LAN sans fil sont ajoutés à l'inventaire sans attendre l'actualisation de celui-ci.

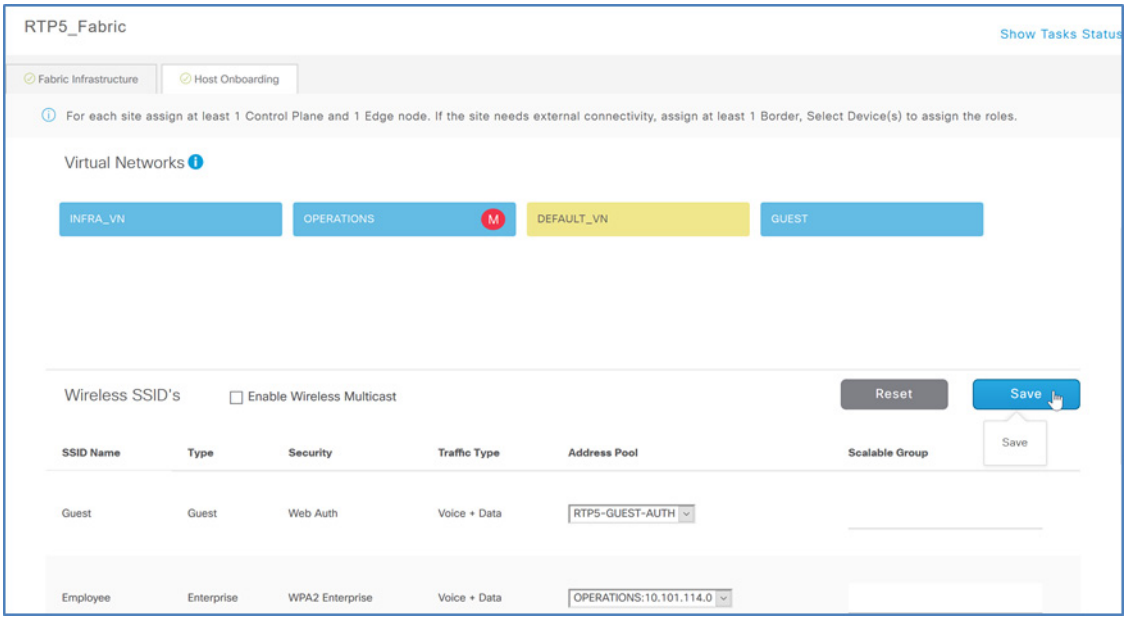
Étape 10. Accédez au tableau de bord principal de Cisco DNA Center, sous **PROVISION (PROVISIONNER) > Devices (Périphériques) > Inventory (Inventaire)**, et en haut, dans le menu déroulant **Actions**, sélectionnez **Provision (Provisionner)**.

Étape 11. Dans l'écran **Provision Devices (Provisionner les périphériques)**, affectez les points d'accès à un étage (par exemple : Global/RTP/RTP5-C9K/Floor 1), cliquez sur **Next (Suivant)**, pour **RF Profile (Profil RF)**, si vous n'avez pas créé le vôtre, sélectionnez **TYPICAL (Standard)**, puis cliquez sur **Next (Suivant)**, dans la page **Summary (Résumé)**, cliquez sur **Deploy (Déployer)**, puis, dans le panneau coulissant, laissez la sélection par défaut **Now (Maintenant)** et cliquez sur **Apply (Appliquer)**. Accusez réception des éventuels avertissements concernant les redémarrages.

Procédure 8. Affecter des clients sans fil à un VN et activer la connectivité

Étape 1. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (PROVISIONNER) > Fabric**, sous **Fabric Domains (Domaines de fabric)**, cliquez sur le site de fabric créé (par exemple : RTP5_Fabric), à gauche dans la section de navigation **Fabric-Enabled Sites (Sites prenant en charge la fabric)**, cliquez sur le site associé (par exemple : Global/RTP/RTP5-C9K), puis cliquez sur l'onglet **Host Onboarding (Intégration d'hôte)**.

Étape 2. Dans la section **Wireless SSID's (SSID sans fil)**, pour chaque **SSID Name (Nom de SSID)**, sélectionnez un **Address Pool (Pool d'adresses)** associé, sélectionnez un **Scalable Group (Groupe évolutif)** associé, cliquez sur **Save (Enregistrer)**, conservez la sélection par défaut **Now (Maintenant)**, puis cliquez sur **Apply (Appliquer)**.



Les périphériques peuvent désormais se connecter via les réseaux sans fil.

Annexe A : liste des produits

Les produits et versions logicielles suivants ont été inclus dans le cadre de la validation dans ce guide de déploiement, et ce jeu validé ne contient pas toutes les possibilités. D'autres options matérielles sont répertoriées dans le document associé Guide de conception de solutions SD-Access, la Matrice de compatibilité des produits SD-Access et les Fiches techniques de Cisco DNA Center, qui peuvent contenir des informations allant au-delà de ce qui a été testé dans le cadre de ce guide. Des fichiers de package Cisco DNA Center mis à jour sont régulièrement publiés et disponibles dans les listes de packages et de mises à jour.

Tableau 3. Cisco DNA Center

Produit	Référence	Version logicielle
Appliance Cisco DNA Center	DN2-HW-APL-L (Châssis basé sur M5)	1.2.10.4 (Système 1.1.0.754)

Tableau 4. Packages Cisco DNA Center

Tous les packages fonctionnant sur Cisco DNA Center lors de la validation sont répertoriés ; tous les packages ne sont pas inclus dans le cadre du test de validation SD-Access.

Pack	Version
Politique relative aux applications	2.1.28.170011
Contrôle du fonctionnement – Base	1.2.11.304
Contrôle du fonctionnement – Capteur	1. 2.10.254
Automatisation – Base	2.1.28.600244.9
Automatisation – Capture intelligente	2.1.28.60244
Automatisation – Capteur	2.1.28.60244
Interface utilisateur de Cisco DNA Center	1.2.11.19
Exécuteur de commandes	2.1. 28.60244
Intégration des périphériques	2.1.18.60024
Plate-forme Cisco DNA	1.0.8.8
Gestion des images	2.1.28.60244
NCP – Base	2.1.28.60244
NCP – Services	2.1.28.60244.9
Plate-forme de contrôleur de réseau	2.1.28.60244.9
Network Data Platform – Analyse de base	1.1.11.8
Network Data Platform – Cœur	1.1.11.77
Network Data Platform – Gestionnaire	1.1.11.8
Path Trace	2.1.28.60244
SD-Access	2.1.28.60244.9

Tableau 5. La gestion des identifications

Domaine fonctionnel	Produit	Version logicielle
Serveur Cisco ISE	Cisco ISE (Identity Services Engine)	2.4 Patch 6

Tableau 6. Frontière de fabric et plan de contrôle SD-Access

Domaine fonctionnel	Produit	Version logicielle
Frontière et plan de contrôle	Commutateurs Cisco Catalyst 9500	16.9.3
Frontière et plan de contrôle	Commutateurs Cisco Catalyst 9400	16.9.3
Frontière et plan de contrôle – petit site	Commutateurs Cisco Catalyst 3850 XS (fibre optique de 10 Gbit/s)	16.9.3
Frontière et plan de contrôle	Routeurs à services intégrés Cisco 4000	16.9.2
Frontière et plan de contrôle – grande échelle	Routeurs à services d'agrégation des séries Cisco ASR 1000-X et 1000-HX	16.9.2
Frontière du réseau	Châssis Cisco Catalyst 6807 à 7 logements avec moteur de supervision 6T ou moteur de supervision 2T et 6800 32 ports 10 GE avec double DFC4 intégré	15.5(1)SY2
Frontière du réseau	Commutateurs Cisco Catalyst 6880-X et 6840-X	15.5(1)SY2
Frontière externe	Commutateurs Cisco Nexus 7700 avec châssis à 2 logements avec module de supervision 2 amélioré et Cisco Nexus 7700 M3-Series 48 ports avec module 1/10 Gigabit Ethernet	8.3(2)
Plan de contrôle	Routeurs de services cloud Cisco 1000V	16.9.2

Tableau 7. Périphérie de la fabric SD-Access

Domaine fonctionnel	Produit	Version logicielle
Périphérie de la fabric	Série Cisco Catalyst 9300 – empilable	16.9.3
Périphérie de la fabric	Série Cisco Catalyst 9400 avec moteur de supervision-1 – châssis modulable	16.9.3
Périphérie de la fabric	Série Cisco Catalyst 3850 – empilable	16.9.3
Périphérie de la fabric	Série Cisco Catalyst 3650 – autonome avec empilage en option	16.9.3
Périphérie de la fabric	Série Cisco Catalyst 4500E avec superviseur 8-E – châssis modulable	3.10.2E

Tableau 8. SD-Access sans fil

Domaine fonctionnel	Produit	Version logicielle
Contrôleur LAN sans fil	Contrôleurs sans fil des séries Cisco 8540, 5520 et 3504	8.8.111.0 (8.8 MR1)
Points d'accès en mode fabric	Séries Cisco Aironet® 1800, 2800 et 3800 (phase 2)	8.8.111.0 (8.8 MR1)

Tableau 9. Commutateurs d'automatisation LAN testés pour ce guide (n'incluent pas toutes les possibilités)

Domaine fonctionnel	Produit
Série Cisco Catalyst 9500 (versions à performances standard)	Périphérique de départ
Commutateurs Cisco Catalyst 3850 XS (fibre optique 10 Gbit/s)	Périphérique de départ
Série Cisco Catalyst 9300 – empilable	Périphérique détecté par le périphérique de départ
Série Cisco Catalyst 9400 avec moteur de supervision-1 – châssis modulable	Périphérique détecté par le périphérique de départ (interface 10 Gbit/s)
Série Cisco Catalyst 3850 – empilable	Périphérique détecté
Série Cisco Catalyst 3650 – autonome avec empilage en option	Périphérique détecté
Série Cisco Catalyst 4500E avec superviseur 8-E – châssis modulable	Périphérique détecté

Commentaires

Pour faire des commentaires et des suggestions sur ce guide et sur les guides associés, rejoignez la discussion dans la Communauté Cisco sur https://cs.co/en-cvds.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco, à l'adresse : **www.cisco.com/go/offices**.