Configuration de la trame d'accès défini par logiciel

Guide de déploiement normatif

Juillet 2019

Sommaire

Définition et conception : accès défini par logiciel

L'accès défini par logiciel (SD-Access) de Cisco® est le fruit de l'évolution des conceptions classiques de réseau LAN, que remplacent désormais des réseaux qui mettent en œuvre directement l'intention d'une entreprise. SD-Access est activé par l'entremise d'un ensemble d'applications qui s'exécutent dans le cadre du logiciel Cisco DNA Center pour la conception, la configuration et l'application de politiques en vue de créer avec assurance un réseau filaire et sans fil de réseau sur site intelligent.

Ce guide est utilisé pour le déploiement des éléments des infrastructures de gestion, y compris Cisco DNA Center, le moteur de services de vérification des identités Cisco Identity Services Engine (ISE) et les contrôleurs LAN sans fil de Cisco (WLC) qui sont décrits dans le document connexe suivant : Guide de conception de solution d'accès défini par logiciel. Le déploiement décrit dans ce guide doit être mis en œuvre avant le déploiement d'une trame d'accès défini par logiciel de Cisco, comme le décrit le Guide de déploiement de la trame d'accès défini par logiciel.

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

Vous trouverez le Guide de conception de solution d'accès défini par logiciel, le Guide de déploiement normatif des infrastructures de gestion de l'accès défini par logiciel, le Guide de déploiement normatif de l'accès défini par logiciel pour les réseaux décentralisés, de même que les guides de déploiement, les guides de conception et les documents techniques connexes dans les pages suivantes :

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

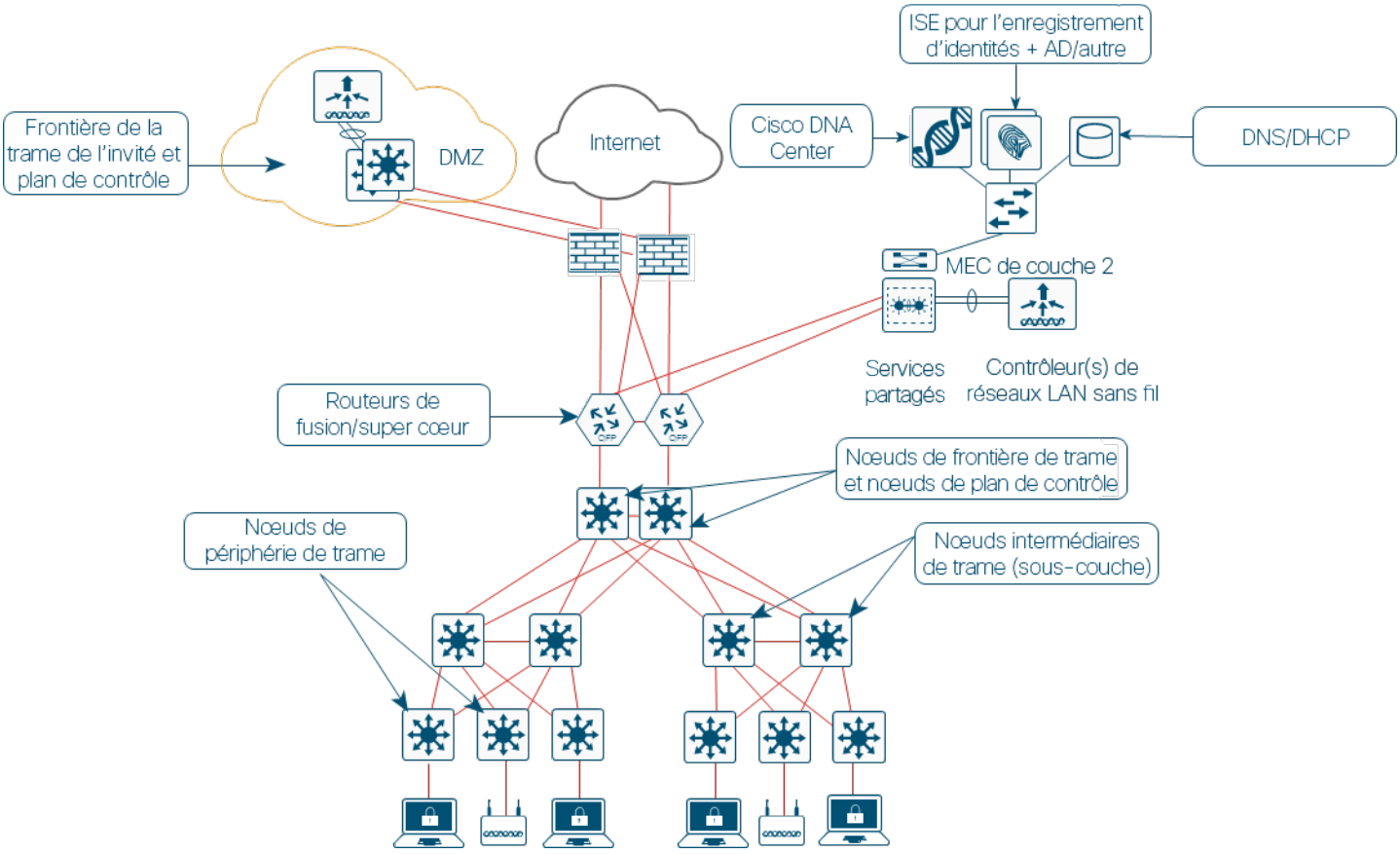
Déploiement : trame d’accès défini par logiciel

Comment lire les commandes de déploiement

Le guide utilise les conventions suivantes pour les commandes que vous saisissez au niveau de l’interface de ligne de commande.
Commandes à saisir à l’invite de l’interface de ligne de commande :
`configure terminal`
Commandes qui précisent 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 l’interface de ligne de commande ou d’un script (les commandes saisies sont en gras) :
`Router# enable`
Longues commandes avec saut de 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 de l’accès défini par logiciel sont déployés dans la topologie décrite dans le Guide de conception de solution d’accès défini par logiciel, comme illustré dans le schéma de topologie. Ce guide se fonde sur l’hypothèse voulant que les infrastructures de gestion de Cisco DNA Center, du moteur de services de vérification des identités Cisco Identity Services Engine (ISE) et des contrôleurs LAN sans fil de Cisco (WLC) soient déjà installées et disponibles, comme le décrit le Guide de déploiement des infrastructures de gestion de l’accès défini par logiciel.

Figure 1. Topologie de validation



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

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

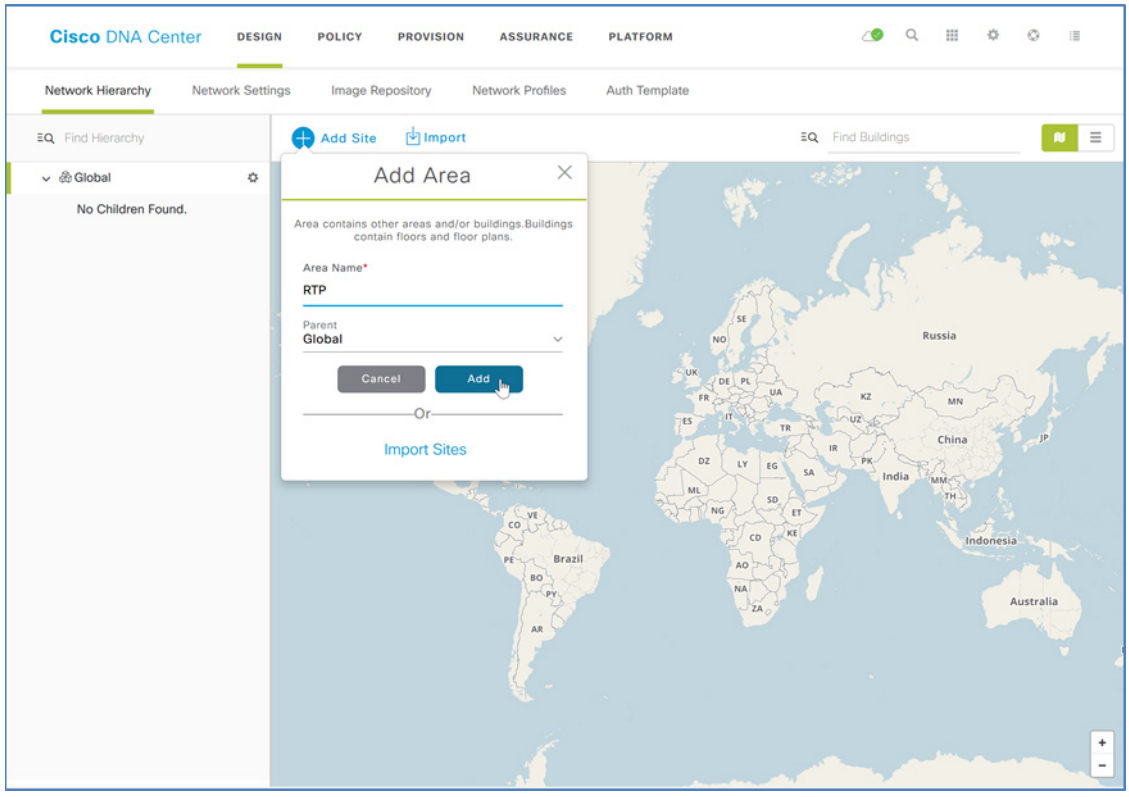
Cisco DNA Center offre une application de conception robuste qui permet aux clients de différentes tailles et échelles de définir facilement leurs sites physiques et leurs ressources communes. À l'aide d'un format hiérarchique intuitif à utiliser, l'application de conception élimine la nécessité de redéfinir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

Grâce à Cisco DNA Center, vous créez une hiérarchie de réseaux dans les zones qui peut prévoir des zones supplémentaires ou d'autres bâtiments et étages dans chaque zone. Les périphériques correspondent aux bâtiments et aux étages pour le provisionnement des services.

Procédure 1. Créez des sites de réseau

Étape 1. Ouvrez une session dans Cisco DNA Center Dans le tableau de bord principal de Cisco DNA Center, accédez à Design (conception) > Network Hierarchy (hiérarchie de réseau).

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



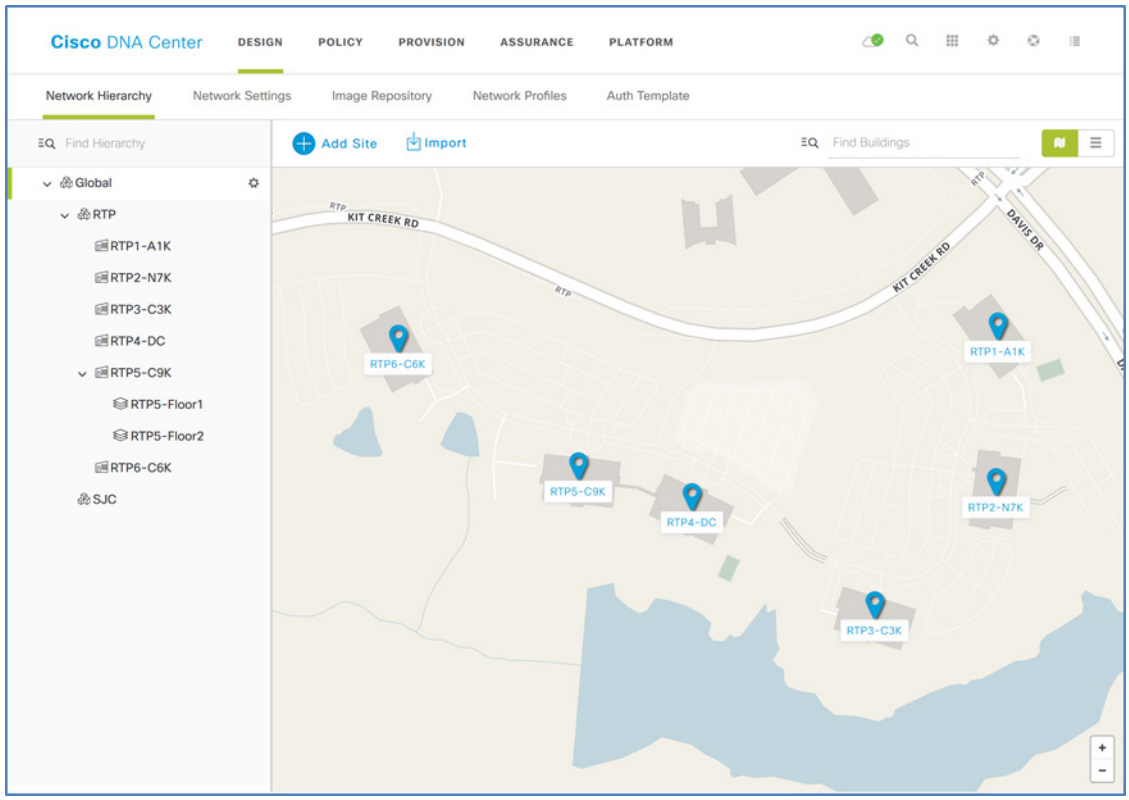
Étape 3. Cliquez sur **Add Site** (ajouter un site), dans le menu déroulant, sélectionnez le bouton **Add Building** (ajouter un bâtiment), indiquez un nom de bâtiment approprié (**Building Name**), sélectionnez le site créé à l'étape précédente comme **Parent**, lancez l'Assistant pour attribuer un 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, préciser la position du bâtiment sur la carte en cliquant sur l'emplacement cible.

Étape 4. Répétez l'étape précédente, au besoin, pour ajouter des sites et des bâtiments, en créant 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 granularité pour les choix de réseau au sein d'un bâtiment, sélectionnez le bâtiment sur la carte (ou sélectionnez l'icône d'engrenage à côté d'un immeuble dans la hiérarchie), choisissez **Add Floor** (ajouter un étage), puis exécutez l'Assistant avec le données.

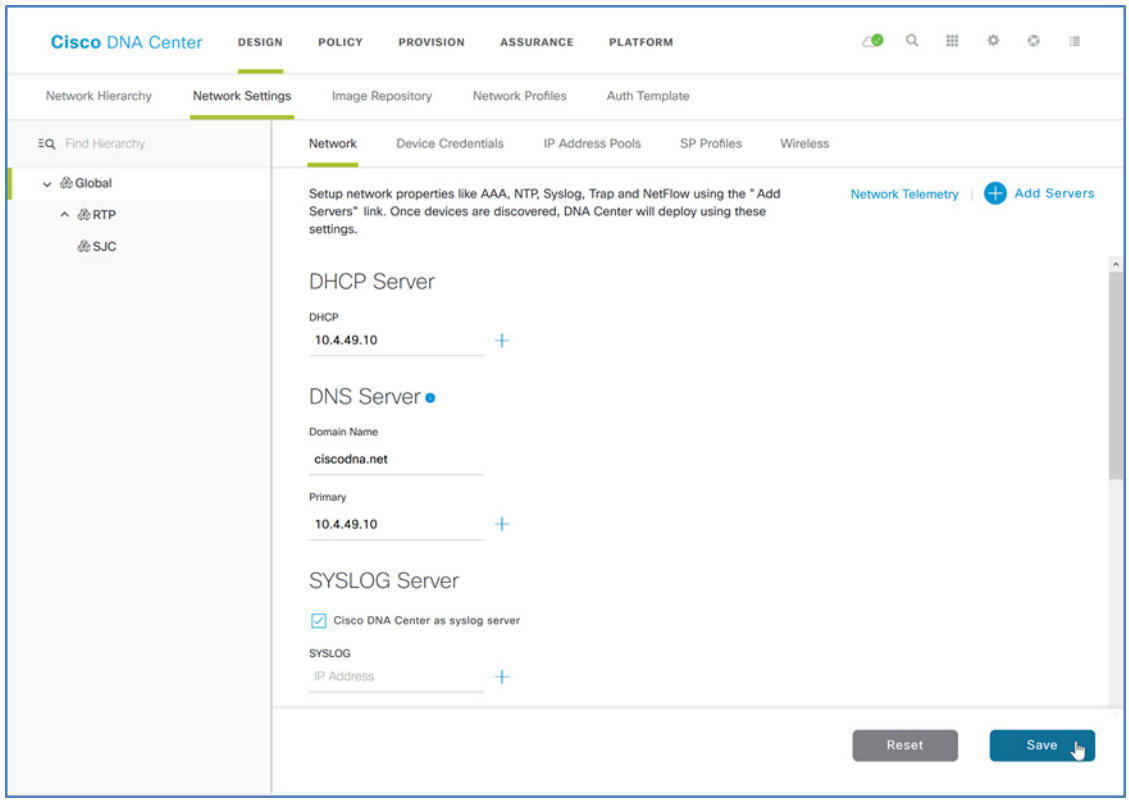
Les étages sont référencés lors de la configuration sans fil. Si vous avez des schémas de cartes de plancher au format DXF, DWG, JPG, GIF ou PNG, ajoutez-les à tout étage défini comme un composant utile pour les déploiements sans fil afin d'afficher les emplacements et la couverture des points d'accès. Vous pouvez ajouter des centaines de sites jusqu'aux limites décrites dans le Guide de conception de solution d'accès défini par logiciel.



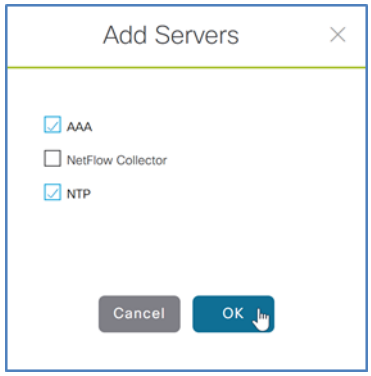
Procédure 2. Configurez des services réseau pour les sites

Configurez les services AAA, DHCP et DNS qui s'alignent sur la hiérarchie dans Cisco DNA Center. Si les services utilisent les mêmes serveurs dans l'ensemble de la hiérarchie, vous pouvez les configurer globalement, et les propriétés héritées de la hiérarchie rendront les paramètres globaux disponibles pour tous les sites. Les différences des différents sites 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 (p. ex., : Global), complétez l'adresse IP du **serveur DHCP** (p. ex., : 10.4.49.10), sous DNS Server (serveur DNS) complétez le nom de domaine (p. ex., : ciscodna.net) et l'adresse IP principale (**Primary**) du serveur (p. ex., : 10.4.49.10), ajoutez les serveurs redondants ou supplémentaires (vous pouvez conserver les sélections par défaut pour utiliser Cisco DNA Center pour le serveur SYSLOG et SNMP), puis cliquez sur **Save** pour enregistrer.



Étape 2. Dans la partie supérieure, à proximité de **Network Telemetry (télémétrie réseau)**, cliquez sur le bouton **+ Add Servers (ajouter des serveurs)**, activez les cases à cocher **AAA** et **NTP**, puis cliquez sur **OK**.



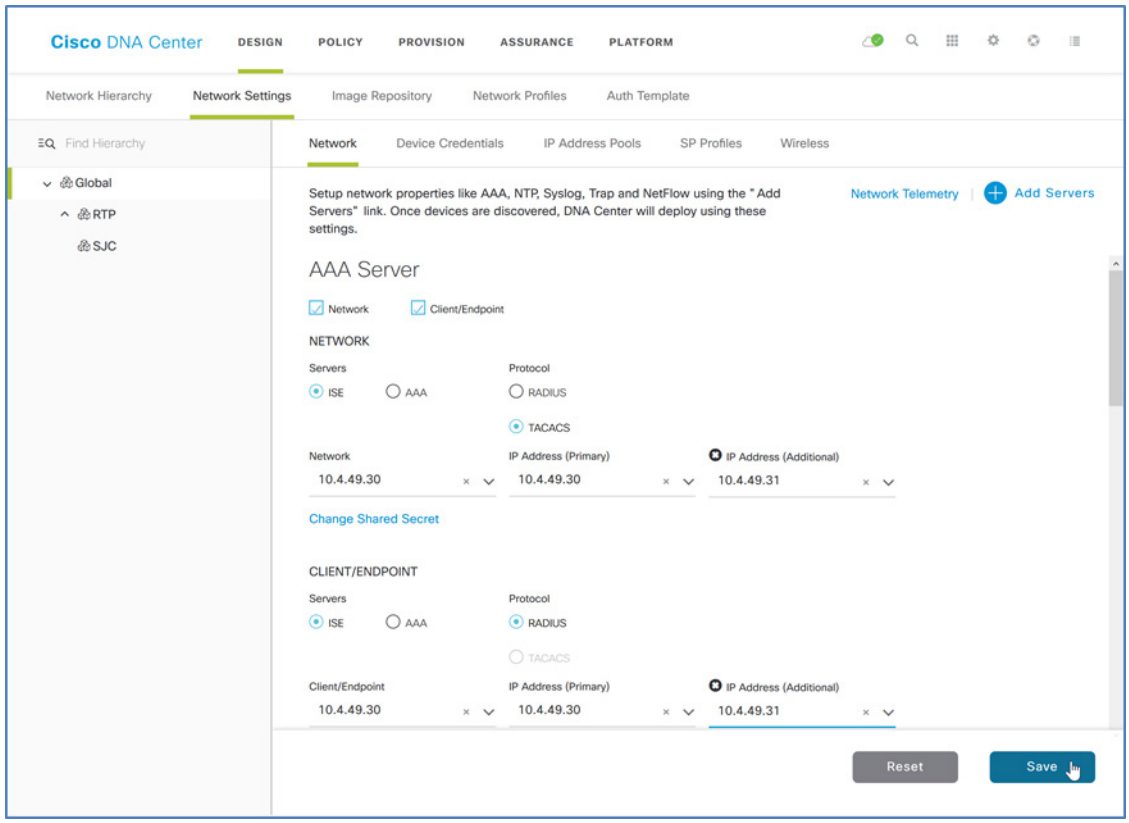
Le volet de configuration est mis à jour avec des sections de configuration disponibles pour le serveur AAA et le serveur NTP (**AAA Server** et **NTP Server**). Vous configurez les services AAA pour l'administration du périphérique de l'infrastructure réseau et pour les terminaux clients qui se connectent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

Conseil technique
De nombreuses entreprises utilisent TACACS pour l'assistance d'administration des périphériques d'infrastructure. Si vous avez l'intention d'activer TACACS sur le serveur ISE utilisé pour l'authentification du 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 pouvez trouver des informations de configuration ISE pour activer l'intégration TACACS en naviguant dans ISE en vue d'accéder à **Work Centers (centre de travail) > Device Administration (administration de périphériques) > Overview (aperçu)**.

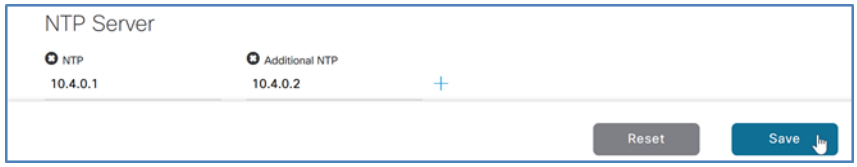
Étape 3. Sous **AAA Server**, cochez les cases **Network (réseau)** et **Client/Endpoint (client/terminal)**, sous **NETWORK**, sélectionnez le bouton radio **ISE**, sous **Network (réseau)** utilisez le menu déroulant pour sélectionner le serveur ISE prédéfini dans la liste (p. ex., 10.4.49.30), sous **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 (p. ex., 10.4.49.30), cliquez sur le bouton plus (**+**), puis sous la liste **IP Address (Additional) (adresse IP (supplémentaire))**, sélectionnez le nœud du serveur ISE redondant (p. ex., 10.4.49.31).

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

Étape 4. Sous **CLIENT/ENDPOINT** et **Servers**, sélectionnez le bouton radio **ISE**, sous **Client/Endpoint (client/terminal)**, utilisez la liste déroulante pour sélectionner le serveur ISE prédéfini dans la liste. Sous **Protocol**, 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 du signe plus (**+**), puis sous **IP Address (Additional) (adresse IP (supplémentaire))**, utilisez le menu déroulant pour sélectionner le nœud de serveur ISE redondant, puis cliquez sur **Save** pour enregistrer.



Étape 5. Dans le même écran, faites défiler l'écran jusqu'à **NTP Server**, ajoutez l'adresse IP (**IP Address**) du serveur NTP (p. ex., 10.4.0.1), si vous avez un ou plusieurs serveurs NTP supplémentaires, cliquez sur le bouton du signe plus (**+**), puis dans le champ **Additional NTP**, ajoutez l'adresse IP des serveurs NTP redondants (p. ex., 10.4.0.2) et cliquez sur **Save** pour 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 trame.

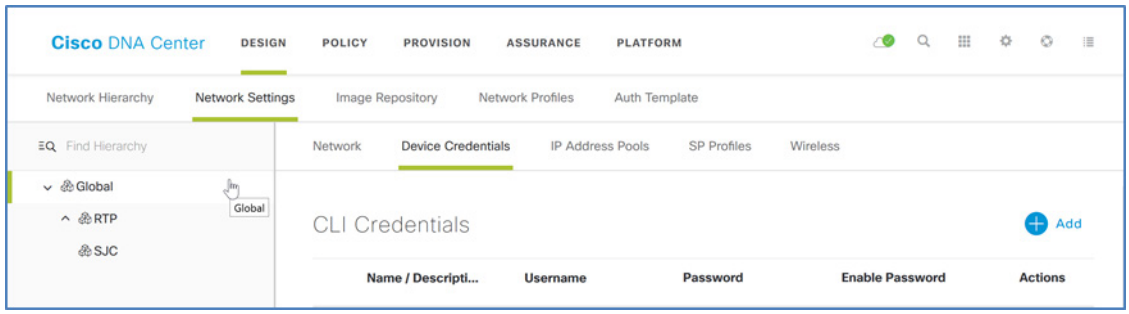
Procédure 3. Ajoutez des coordonnées d'authentification pour les périphériques aux fins de détection et de gestion

Lorsque vous déployez la sous-couche d'accès défini par logiciel à l'aide de périphériques déjà configurés qui sont accessibles via le Cisco DNA Center, vous pouvez détecter et gérer les appareils en fournissant les coordonnées d'authentification de l'interface de ligne de commande et du protocole SNMP (Simple Network Management Protocol).

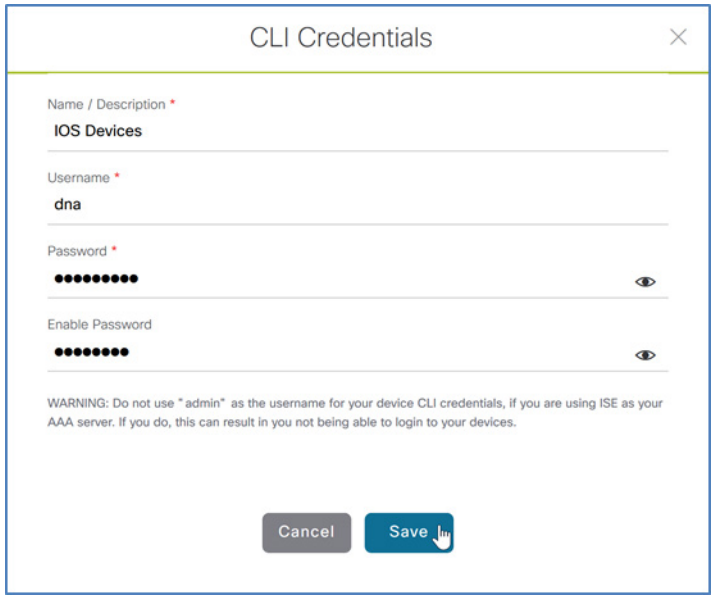
Vous pouvez également déployer des commutateurs LAN sans les configurations existantes dans la sous-couche à l'aide des fonctionnalités d'automatisation de réseau LAN du Cisco DNA Center. La solution Plug and Play de réseau de Cisco (PnP) est le mécanisme permettant d'établir la connectivité et la configuration initiale des commutateurs pris en charge. Pour les déploiements d'automatisation de LAN, vous pouvez également fournir des coordonnées d'authentification CLI et SNMP pour accéder à un ou plusieurs périphériques PnP pris en charge, tels que les commutateurs de la gamme Cisco Catalyst 9500 dans une distribution ou au niveau du cœur. Par l'entremise du protocole de découverte Cisco Discovery Protocol, l'automatisation LAN détecte les commutateurs directement connectés aux interfaces de périphériques d'amorçage sélectionnées et leurs commutateurs voisins immédiats, lesquels doivent tous exécuter l'agent PnP et ne pas avoir de configuration précédente. Les coordonnées d'authentification saisies permettent à Cisco DNA Center et aux appareils d'amorçage de fonctionner ensemble pour configurer les appareils détectés et les ajouter à l'inventaire géré.

Ajoutez les coordonnées d'authentification de l'appareil pour gérer les étendues de la hiérarchie de site créée dans la conception. Ces coordonnées d'authentification permettent de détecter et de gérer le réseau.

Étape 1. Dans Cisco DNA Center, accédez à **Design (conception) > Network Settings (paramètres de réseau) > Device Credentials (coordonnées d'authentification des périphériques)** et sélectionnez un niveau approprié dans la hiérarchie du site dans le volet de gauche (p. ex., Global, pour les coordonnées d'authentification communes dans toute la hiérarchie).



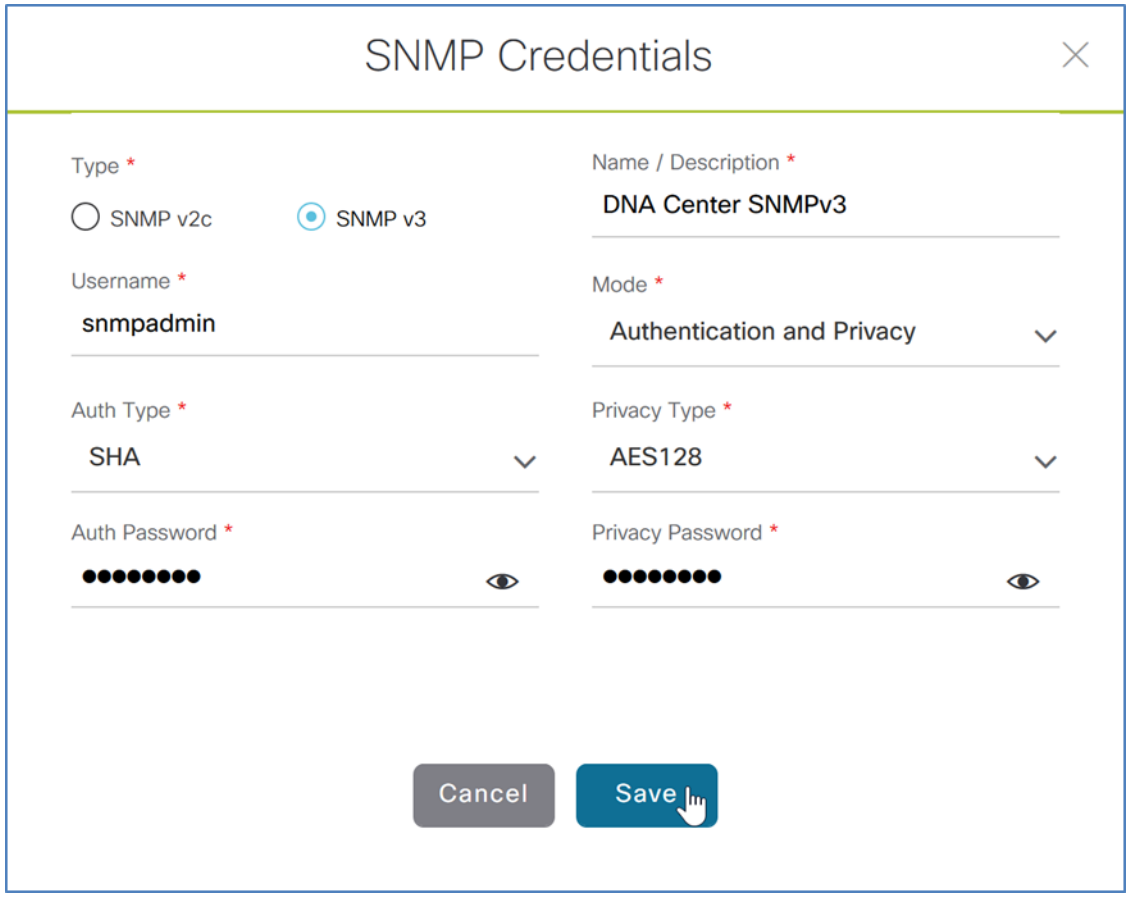
Étape 2. En haut de la section **CLI Credentials (coordonnées d'authentification CLI)**, cliquez sur **Add (ajouter)**, renseignez les champs **Name (nom) / Description** (p. ex. : périphériques iOS), **Username (nom d'utilisateur)**, **Password (mot de passe)**et **Enable Password (activer le mot de passe)**, puis cliquez sur **Save** pour enregistrer.



Attention

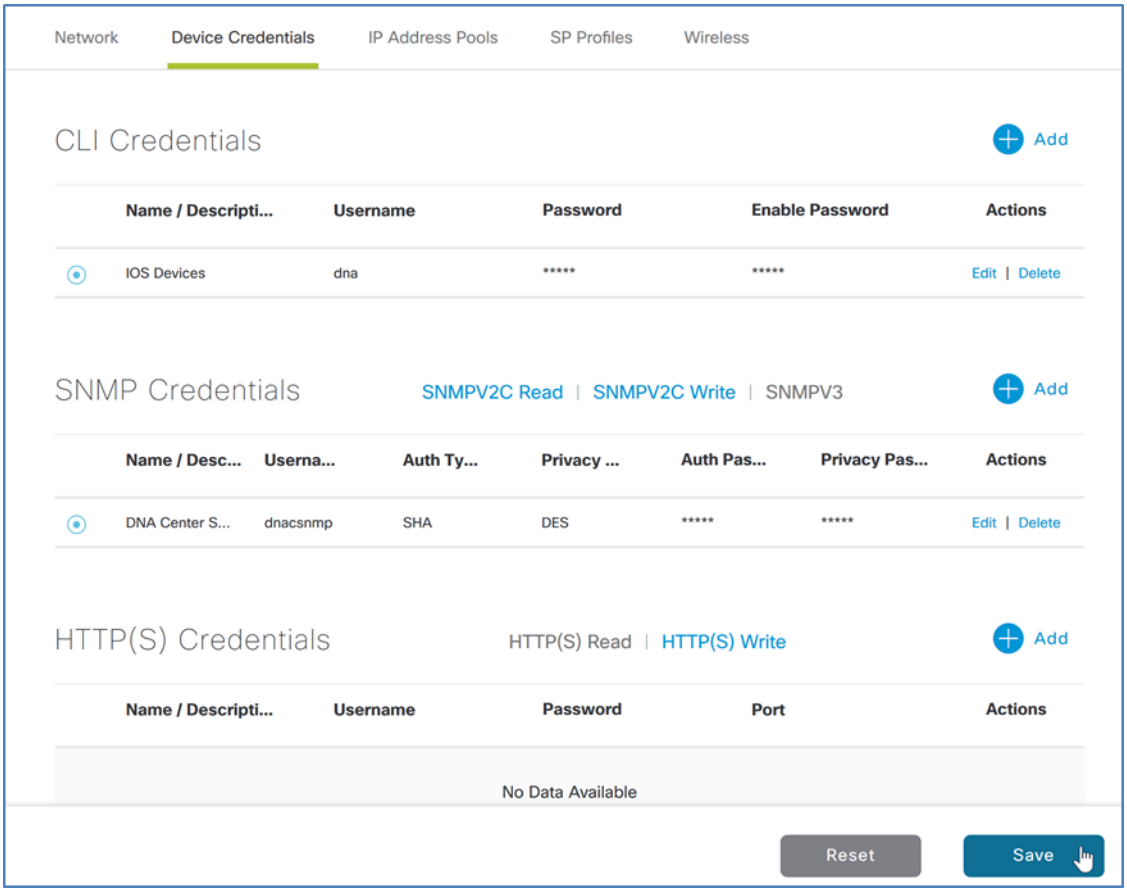
Si vous utilisez ISE en tant que serveur AAA, vous devez éviter d'utiliser **admin** comme nom d'utilisateur pour les coordonnées d'authentification de l'interface de ligne de commande de l'appareil, ce qui peut entraîner un conflit entre le nom d'utilisateur et la connexion de l'administrateur ISE et entraîner une incapacité de se connecter aux appareils.

Étape 3. En haut de la section **SNMP Credentials (coordonnées d'authentification SNMP)**, sélectionnez un type d'informations d'authentification SNMP à mettre à jour (p. ex., SNMPV3). Cliquez sur **Add (ajouter)**, sélectionnez la touche radio dans la ligne à côté des informations d'identification à mettre à jour (une seule information par ligne à la fois), complétez les coordonnées d'authentification (les mots de passe de 12 caractères sont recommandés pour des raisons de compatibilité avec les WLC de Cisco), puis cliquez sur **Save (enregistrer)**.



Étape 4. Répétez les étapes 2 et 3 pour toutes les coordonnées d'authentification supplémentaires requises dans la hiérarchie. Les **CLI Credentials** et **SNMPv3** ou les **SNMPV2C Read** et **SNMPV2C Write** sont les exigences les plus courantes.

Étape 5. Pour chacun des éléments affectés des coordonnées d'authentification de l'interface de ligne de commande et du protocole SNMP, cliquez sur tous les boutons radio pour chaque affectation créée. Après chaque sélection, en bas de l'écran des coordonnées d'authentification de périphérique (Device Credentials), cliquez sur **Save** pour enregistrer. Si vous avez recouru à plusieurs types de coordonnées d'authentification SNMP, répétez cette étape en basculant vers chacune des options d'information d'authentification SNMP, cochez la touche pour l'option, puis cliquez sur **Save** pour enregistrer.



Une confirmation d'achèvement de la création de paramètres communs s'affichera. Les coordonnées d'authentification de périphérique à utiliser pour la détection et la gestion du réseau sont désormais disponibles dans Cisco DNA Center.

Procédure 4. Définissez des ensembles d'adresses IP internationales

Définissez les adresses IP de vos réseaux en les attribuant manuellement dans Cisco DNA Center. Vous pouvez, si vous le souhaitez, envoyer les attributions d'adresses IP à un gestionnaire d'adresses IP (IPAM) (p. ex., Infoblox, BlueCat) en intégrant l'IPAM via les API. Pour procéder à une intégration IPAM, accédez à **System Settings (paramètres de système) > Settings (paramètres) > IP Address Manager** et remplissez le formulaire avec les caractéristiques de votre fournisseur IPAM. Dans cet exemple où vous n'utilisez pas l'intégration IPAM, vous configurez manuellement l'adressage IP et les étendues DHCP sur vos serveurs IPAM pour qu'ils correspondent aux attributions dans Cisco DNA Center.

Les étendues DHCP configurées sur le serveur DHCP doivent prendre en charge les attributions 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 (p. ex. : 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 ensembles d'adresses IP utilisés pendant le processus de réservation d'ensemble. Ces ensembles sont attribués aux sites de votre réseau et les étapes d'attribution sont nécessaires pour les déploiements IPAM manuels et intégrés. Vous avez la possibilité de créer un ensemble global plus grand, puis de réserver un sous-ensemble d'un ensemble à des niveaux inférieurs dans la hiérarchie du site. Les ensembles d'adresses IP sont créés uniquement au niveau global. Vous réservez des adresses dans les ensembles uniquement à des niveaux autres que le niveau global.

Le déploiement décrit dans le présent guide fait appel à des ensembles d'adresses globaux répertoriés dans le tableau. Pour faciliter la compréhension, les espaces d'adressage les plus petits sont utilisés pour la plupart des ensembles d'adresses globaux par rapport à ce qu'une entreprise peut généralement déployer, par exemple un espace d'adressage /16 ou plus. Des ensembles 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 (employé). Bien que l'attribution de l'adresse d'une passerelle IP soit requise dans chaque ensemble, le protocole d'accès défini par logiciel utilise uniquement la passerelle lors de la création d'un réseau de superposition. Le tableau contient également des exemples d'ensembles disponibles pour une sous-couche LAN manuelle et une sous-couche LAN automatisée séparée, ainsi que l'homologation de multidiffusion.

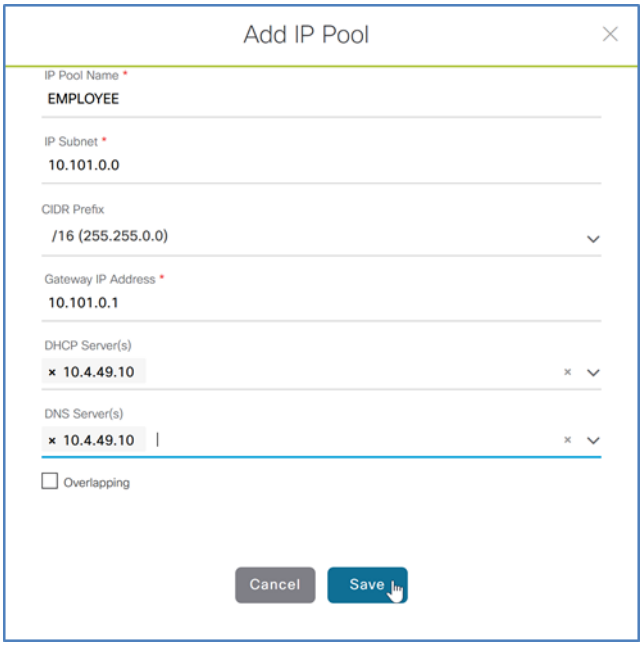
Tableau 1. Exemples d'ensembles d'adresses globaux

Nom de l'ensemble	Réseau/masque	Passerelle IP	Serveur DHCP	Serveur DND
EMPLOYEE (employé)	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 (invité)	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

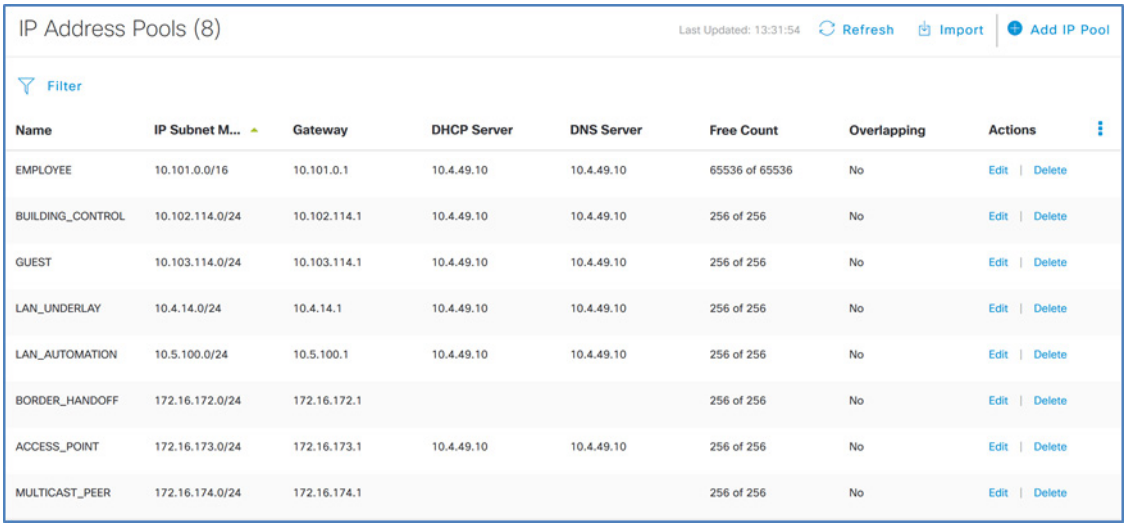
Tableau 2. Exemple de réservations d'ensembles d'adresses de l'ensemble global des employés (EMPLOYEE)

Nom de l'ensemble	Réseau/masque	Passerelle IP	Serveur DHCP	Serveur DND
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 dans Cisco DNA Center un ensemble global qui est consacré au provisionnement de la connectivité du nœud pour le contour de la trame définie par logiciel. Dans Cisco DNA Center, accédez à **DESIGN (conception) > Network Settings (paramètres réseau) > IP Address Pools (ensembles d'adresses IP)**. Dans la hiérarchie du site, à gauche, sélectionnez **Global**, puis cliquez sur **+ Add IP Pool** pour ajouter un ensemble IP. Renseignez les champs **IP Pool Name (nom de l'ensemble IP)**, **IP Subnet (sous-réseau IP)**, **CIDR Prefix (préfixe CIDR)**et **Gateway IP Address (adresse IP de la passerelle)**. Si l'ensemble dispose de clients terminaux, utilisez les menus déroulants pour affecter le ou les serveurs **DHCP** et **DNS**. Ne sélectionnez pas **Overlapping (chevauchement)**. Lorsque vous avez terminé, cliquez sur **Save (enregistrer)**.



Étape 2. Répétez l'étape précédente pour tout ensemble global d'adresses IP supplémentaire comprenant des sous-réseaux au niveau du site et des bâtiments. Les ensembles sont ajoutés à la liste des ensembles globaux.

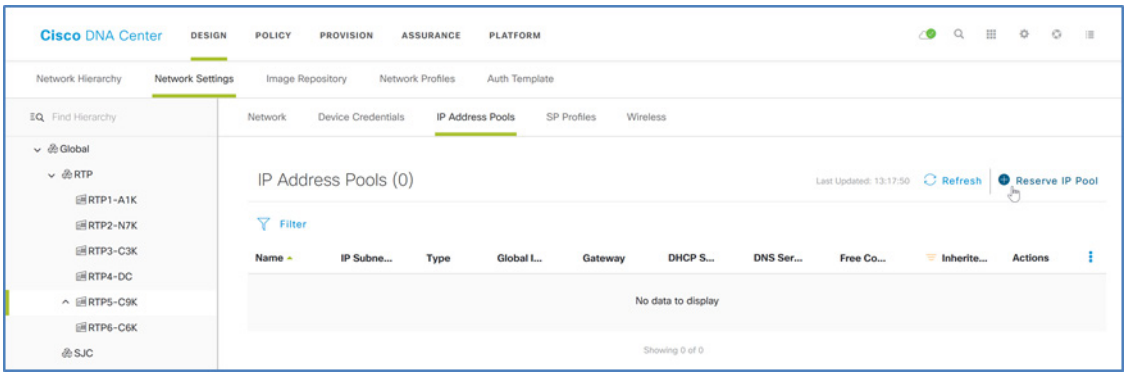


Name	IP Subnet M...	Gateway	DHCP Server	DNS Server	Free Count	Overlapping	Actions
EMPLOYEE	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10	65536 of 65536	No	Edit | Delete
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
GUEST	10.103.114.0/24	10.103.114.1	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

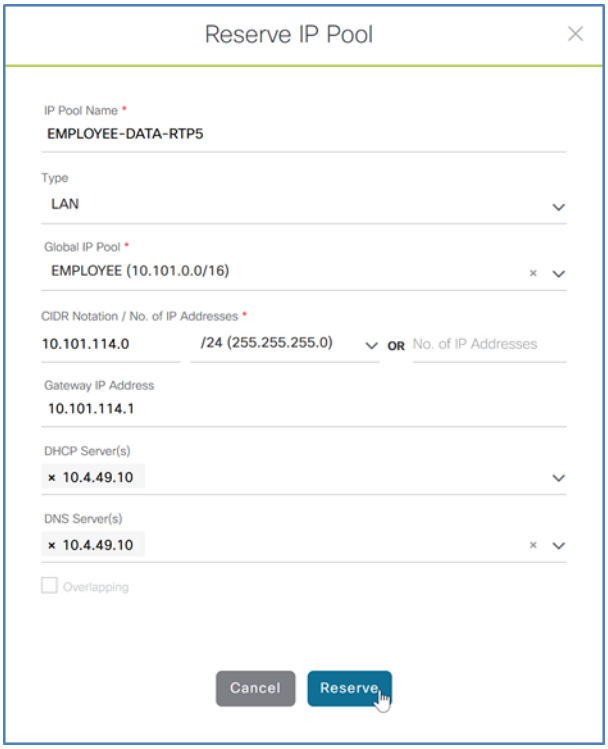
Procédure 5. Réservez des ensembles d'adresses IP

Utilisez les ensembles globaux d'adresses IP définis pour réserver des adresses IP pour les 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 complet des ensembles globaux d'adresses IP pour ce site. Lorsque vous réservez des adresses à partir des ensembles globaux d'adresses IP définis, les serveurs DNS et DHCP peuvent être utilisés dans ces réservations ou encore, ces paramètres peuvent être écrasés.

Étape 1. Dans le Cisco DNA Center, accédez à **DESIGN (conception) > Network Settings (paramètres réseau) > IP Address Pools (ensembles d'adresses IP)**, à gauche dans la hiérarchie du site, sélectionnez un site ou un niveau inférieur pour la réservation d'un ensemble d'adresses IP (p. ex., RTP5-C9K), puis, dans le coin supérieur droit, cliquez sur **Reserve IP Pool**.



Étape 2. Renseignez le champ **IP Pool Name (nom d'un ensemble IP)** (p. ex., EMPLOYEE-DATA-RTP5), sous **Type**, sélectionnez **LAN**, puis sélectionnez la source de réservation de l'ensemble global des adresses IP (**Global IP Pool**) (p. ex. EMPLOYEE), puis sous **CIDR Notation / No. of IP Addresses**, sélectionnez la partie de l'espace d'adressage à utiliser (p. ex., 10.101.114.0/24), attribuez une adresse IP de passerelle (**Gateway IP Address**, par p. ex., : 10.101.114.1), utilisez le menu déroulant pour attribuer le ou les serveurs DHCP (**DHCP Server(s)**) et le ou les serveurs DNS (**DNS Servers(s)**) puis cliquez sur **Reserve (réserver)**.



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

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

Processus : création de la segmentation et des politiques pour le réseau à accès défini par logiciel

Dans le cadre des décisions de conception à prendre dans votre préparation pour votre déploiement de réseau à accès défini par logiciel, vous choisissez des stratégies de segmentation du réseau pour l'entreprise. La macrosegmentation fait appel à des réseaux virtuels secondaires supplémentaires dans la trame et la microsegmentation utilise des balises de groupe dimensionnables pour appliquer des politiques à des groupes d'utilisateurs ou à des profils de périphériques

Utilisez des politiques de groupe pour faciliter le résultat souhaité de l'application des politiques à l'aide de la segmentation. Dans un exemple à l'Université, les ordinateurs des étudiants et des enseignants peuvent être autorisés à accéder aux ressources d'impression, mais les ordinateurs des étudiants ne doivent pas communiquer directement avec les ordinateurs du corps enseignant, et les appareils d'impression ne doivent pas communiquer avec les autres périphériques d'impression.

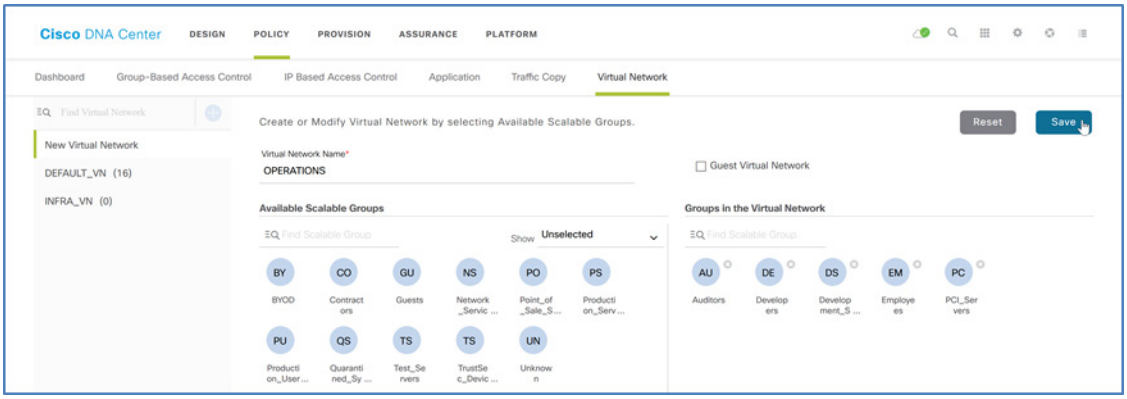
Dans d'autres cas, il faut des mesures supplémentaires d'isolement. Dans un exemple de magasin de vente au détail, les ordinateurs des points de vente ne doivent jamais communiquer avec l'infrastructure de réseau de surveillance vidéo, qui à son tour ne devrait jamais communiquer avec le système de CVC de l'immeuble. Dans les cas où les mesures d'isolement nécessitent une extension de la périphérie du réseau jusqu'au cœur du réseau pour accéder aux services centralisés, la segmentation des macros à l'aide de réseaux virtuels est le meilleur choix. Les exigences gouvernementales et industrielles en matière de conformité, ainsi que les politiques en matière de risque de l'entreprise conduisent souvent à préférer la macrosegmentation.

Afin d'explorer de façon approfondie la conception de la segmentation pour l'accès défini par logiciel et des cas d'utilisation, consultez le Guide de conception de la segmentation de l'accès défini par logiciel sur Cisco.com.

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

Procédure 1. Ajouter un réseau virtuel superposé au réseau d'accès défini par logiciel

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **POLICY (politiques) > Virtual Network (réseau virtuel)**, cliquez sur le signe plus (**+**) pour créer un nouveau réseau virtuel, saisissez un **nom de réseau virtuel** (p. ex., opérations), faites glisser les groupes évolutifs depuis l'espace **Available Scalable Groups (groupes évolutifs disponibles)** vers l'ensemble **Groups in the Virtual Network (groupes dans l'ensemble virtuel)** (p. ex., Auditors, Developers, Development_Servers, Employees et PCI_Servers), puis cliquez sur **Save** pour enregistrer.



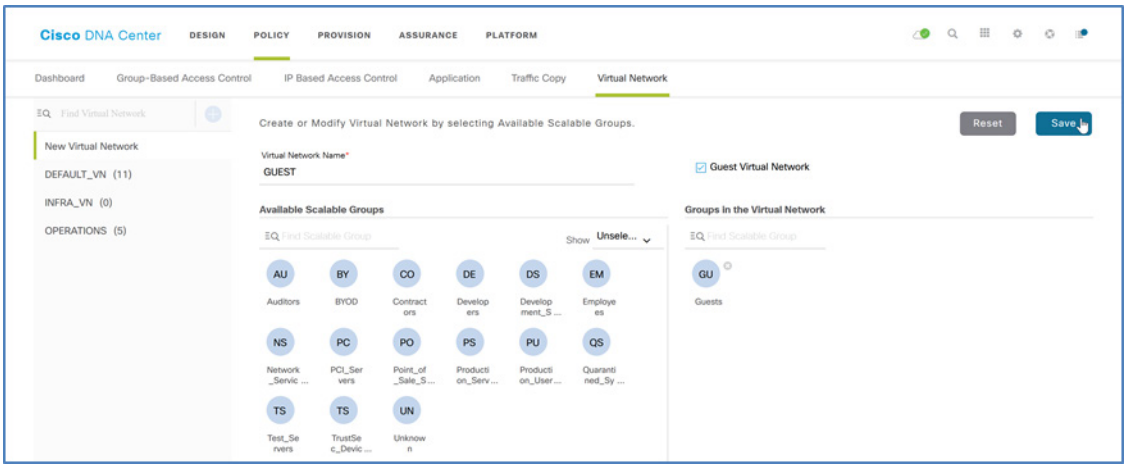
Le réseau virtuel avec les groupes connexes est défini et apparaît dans la liste des réseaux virtuels définis. Ces définitions de réseau virtuel sont disponibles pour le provisionnement des trames.

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

Étape 2. Si votre entreprise exige des groupes différents des groupes par défaut, créez des groupes personnalisés en accédant à la **POLICY (politiques) > Group-Based Access Control (contrôle d'accès selon le groupe) > Scalable Groups (groupes évolutifs)**, puis cliquez sur **Add Groups (ajouter des groupes)** pour créer un nouveau groupe et SGT.

Étape 3. Répétez les deux premières étapes pour chaque réseau secondaire superposé. Vous pouvez également revenir à ces étapes après la configuration de la trame afin de créer d'autres réseaux de superposition.

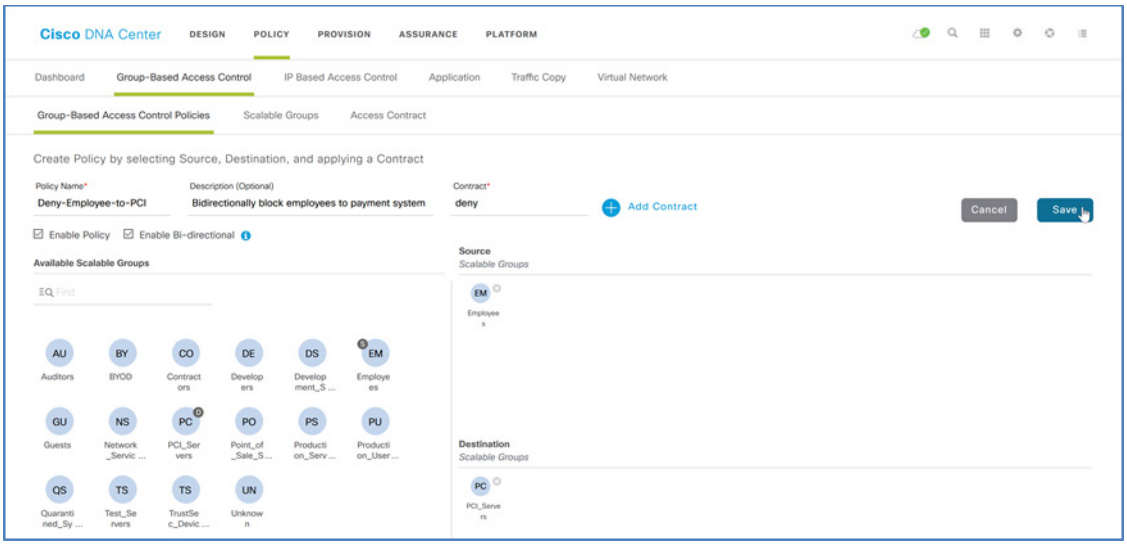
Étape 4. De nombreux réseaux nécessitent un service d'invité pour les utilisateurs sans fil : créez un réseau virtuel d'invité pour prendre en charge cette fonction. Dans le tableau de bord principal de Cisco DNA Center, accédez à **POLICY (politiques) > Virtual Network (réseau virtuel)**, cliquez sur le signe plus (**+**) pour créer un nouveau réseau virtuel, saisissez un nom de réseau virtuel (**Virtual Network Name**, p. ex., GUEST, pour invité), sélectionnez la case à côté de l'option **Guest Virtual Network (réseau virtuel d'invité)**, faites glisser les groupes évolutifs des invités (**Guests**) depuis l'espace **Available Scalable Groups (groupes évolutifs disponibles)** vers l'ensemble **Groups in the Virtual Network (groupes dans l'ensemble virtuel)**, puis cliquez sur **Save** pour enregistrer.



Procédure 2. Créez une politique de microsegmentation à l'aide de SGT

Les politiques de microsegmentation sont définies sur mesure pour le déploiement d'une entreprise. Cet exemple simple montre une règle de base qui peut être utilisée pour empêcher les utilisateurs du groupe des employés de communiquer avec le groupe PCI_Servers. Lorsque les profils d'authentification attribuent de manière appropriée un SGT à un terminal ou à un utilisateur, ISE saisit l'intention de cette politique et la met en application dans le réseau.

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez aux politiques de contrôle de l'accès selon le groupe par le chemin suivant : **POLICY > Group-Based Access Control > Group-Based Access Control Policies**, puis cliquez sur **+ Add Policy (ajouter une politique)**, dans le volet **Available Scalable Groups (groupes évolutifs disponibles)**, faites glisser le groupe **Employees (employés)** et déposez-le dans le volet **Source**, faites glisser le groupe **PCI_Servers** dans le volet de **Destination**, saisissez un nom de politique (**Policy Name**, p. ex., Deny-Employee-to-PCI), saisissez une **Description**, sélectionnez **Enable Policy (activer la politique)**, sélectionnez **Enable Bi-directional (activation bidirectionnelle)**, cliquez sur **+ Add Contract (ajouter un contrat)**, sélectionnez **deny (refuser)**, cliquez sur **OK**, puis cliquez sur **Save** pour enregistrer.



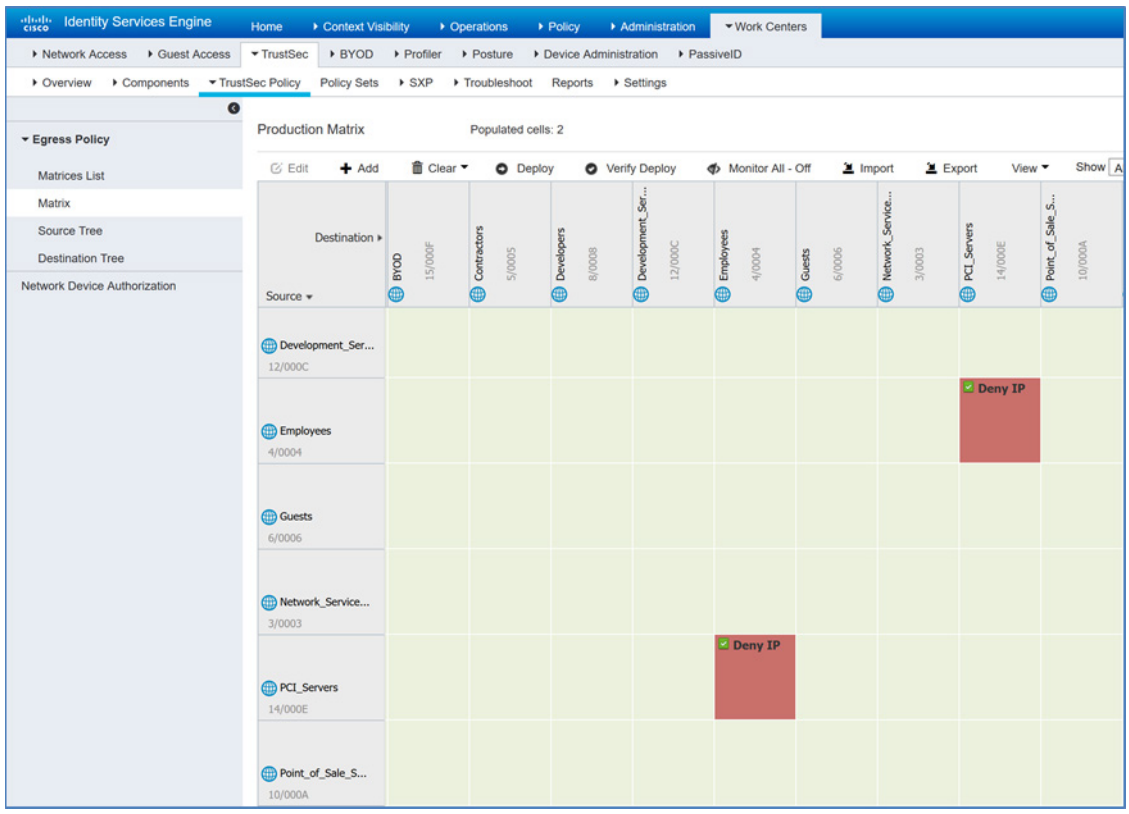
La politique est créée et est répertoriée avec l'état suivant : **CREATED (créée)**. En raison de la sélection de l'option bidirectionnelle, la politique inverse est également créée.

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

L'état passe à **DEPLOYED (déployé)** et les politiques sont disponibles pour application aux trames de l'accès défini par logiciel que Cisco DNA Center crée et sont également disponibles dans ISE, où il est possible de les afficher 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; accédez à **Work Centers > TrustSec > TrustSec Policy**, puis sur le côté gauche, sélectionnez **Matrix**. Vous êtes redirigés pour vous connecter à ISE, qui redirige le navigateur et affiche la matrice de politiques TrustSec.

Vérifiez que les politiques ont été mises à jour vers ISE, pour application 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 de réseau opérationnelle, y compris la connectivité de gestion des appareils. Dans le cadre de l'intégration d'ISE avec Cisco DNA Center qui est illustrée dans le Guide de déploiement normatif de l'accès défini par logiciel pour les réseaux décentralisés, l'ISE est configuré avec l'assistance d'administration des périphériques d'infrastructure TACACS. Pour les configurations TACACS, Cisco DNA Center permet de modifier les appareils détectés afin d'utiliser les services d'authentification et de gestion des comptes de l'ISE, tandis que le basculement local est utilisé par défaut. L'ISE doit être préparé pour prendre en charge les configurations d'administration des appareils envoyées aux périphériques pendant le processus de détection.

Procédure 1. Configuration de la gestion des appareils 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 détection 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 de l'appareil à l'aide des interfaces de bouclage de l'appareil. La configuration SNMP est mise en application dans une procédure ultérieure, dans le cadre de la détection de périphériques.

N'ajoutez pas de configuration à tous les appareils 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 appareils ayant déjà des configurations ne peuvent pas être configurés à l'aide de l'automatisation LAN. Cet exemple présente une configuration faisant appel à Cisco IOS XE sur un commutateur Cisco Catalyst.

Étape 1. Utilisez l'interface de ligne de commande de l'appareil pour configurer le nom d'hôte afin de faciliter l'identification de l'appareil et la désactivation des 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 de l'interface CLI.

```
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 sorte qu'il prenne en charge les trames géantes Ethernet. L'unité de transmission maximale sélectionnée autorise les en-têtes de trame supplémentaires et la compatibilité avec la valeur commune la plus élevée sur la plupart des commutateurs; le nombre arrondi doit être facile à retenir lors de la configuration et du dépannage.

```
system mtu 9100
```

Conseil technique

La connectivité sous-jacente faisant appel à 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 font appel à une commande **system jumbo mtu** au niveau de la configuration globale.

Étape 5. Configurez l'adresse de bouclage du commutateur et attribuez son utilisation par la gestion SSH.

interface Loopback (boucle de l'interface)***0***

adresse IP ***[adresse IP de bouclage de l'appareil]*** 255.255.255.255

ip ssh source-interface Loopback (source ssh ip-boucle de l'interface)***0***

Procédure 2. Configurez les liaisons du réseau sous-jacent 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 par routage, ignorez cette procédure. Les déploiements de couche 2 standard nécessitent cette procédure.

N'ajoutez pas de configuration à tous les appareils que vous avez l'intention de détecter et de configurer à l'aide de la fonction d'automatisation LAN. Les périphériques ayant déjà des configurations ne peuvent pas être configurés à l'aide de l'intégration de l'automatisation LAN sans réinitialiser l'appareil selon les configurations par défaut d'origine.

Étape 1. Configurez les connexions de commutateur dans l'infrastructure du réseau sous-jacent. Répétez cette étape pour chaque liaison avec un commutateur voisin dans la sous-couche de la trame. Si le périphérique sous-jacent est configuré en tant que nœud de frontière de trame et que la connexion doit être utilisée en tant que transfert de la trame 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***, à laquelle s'ajoute ***.00***, et que précède un ID de zone, tel que ***49.0000***, ce qui se traduit par ***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. Activez la connectivité de routage à la frontière vers le voisin de routage externe

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

Pour connecter des appareils 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 courants disponibles en dehors des nœuds de frontière, tels que DNS, DHCP, les WLC et la gestion de Cisco DNA Center, lorsque cette fonction n'est pas directement connectée aux nœuds de réseau d'accès défini par logiciel, en étendant votre réseau d'entreprise existant à la sous-couche à la frontière. La connectivité à Cisco DNA Center est nécessaire pour appliquer d'autres mesures de provisionnement.

L'appareil 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 technologies de VRF connectées avec les interfaces marquées 802.1Q à la frontière, également appelées 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 avec des balises et des sessions BGP supplémentaires, selon les besoins, pour la connectivité du réseau virtuel superposé.

Étape 1. Pour chaque nœud de frontière, si vous configurez un commutateur prenant en charge les interfaces de ligne principale de VLAN, comme les commutateurs de la gamme Cisco Catalyst 9000, 3800 ou 6800, vous devez configurer une ligne principale sur l'interface connectée avec un VLAN attribué pour établir la connectivité sous-jacente de l'homologue de routage pour 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 de ligne principale de commutateur pour établir la connectivité sous-jacente avec le 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 de routage pour la communication sous-jacente et l'homologation BGP ultérieure. La configuration pour l'intégration dans le protocole IS-IS est indiquée. Répétez cette étape pour chaque interface reliant les 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 avec les réseaux en dehors de la trame et activez le protocole BGP sur les interfaces de connexion. Configurez le protocole BGP pour autoriser l'accès de gestion du Cisco DNA Center aux appareils de réseau sous-jacent, 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. Redistribuez 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 WLC. Une route plus spécifique (telle qu'un sous-réseau/24 ou une route d'hôte/32) vers l'adresse IP de WLC doit exister dans le tableau de routage global pour chaque nœud où les points d'accès se connectent pour établir la connectivité. Autorisez les routes plus spécifiques pour les services partagés de WLC et de DHCP qui sont nécessaires au BGP (p. ex., 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. Au moyen de ce processus, les préfixes utilisés correspondent aux préfixes dans le tableau de routage du protocole BGP.

Étape 1. Connectez-vous à chaque nœud de frontière et ajoutez une liste de préfixes (prefix-list) et un tableau de routage (route-map) 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 fait appel à ISIS.

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

Procédure 5. Activez la connectivité du routeur de fusion externe vers le voisin de frontière

Les routeurs de fusion connectés à vos routeurs de périphérie de trame nécessitent une configuration CLI pour la connectivité sous-jacente qui est conforme aux procédures précédentes. Procédez comme suit pour chaque périphérique de routeur fusion externe connecté à une frontière.

Dans cet exemple, le routeur de fusion est configuré au moyen d'une homologation de routage entre un VRF contenant les routes globales à l'échelle de l'organisation et le tableau de routage global à la frontière, pour l'accessibilité de la sous-couche de la trame, sans utiliser le tableau de routage global du routeur de fusion.

Il est également possible d'homologuer le tableau de routage global à l'échelle de l'organisation pour le routeur de fusion et le tableau de routage global à la frontière, sans utiliser de technologies VRF.

Étape 1. Sur chaque routeur de fusion externe, créez le VRF, le différentiateur de route et les routes cibles 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 trame à accès défini par logiciel, 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 de ligne principale, faites-les correspondre à 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 (p. ex., 100) sur la connexion avec balises 802.1Q entre le routeur de fusion et le nœud de frontière.

Étape 3. Créez des cartographies de routage aux routes de balise et évitez les boucles de routage lors de la redistribution entre le protocole IGP utilisé dans le reste du réseau et le protocole BGP, pendant la connexion à l'aide de plusieurs liaisons. Les protocoles IGP peuvent varier : l'exemple donné porte sur EIGRP et présente l'achèvement d'une connectivité de routage d'IS-IS, au protocole BGP, vers le protocole 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'homologation BGP à partir des 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 le protocole BGP dans le protocole IGP pour activer l'accessibilité. Les protocoles IGP peuvent varier : l'exemple illustré porte sur le protocole EIGRP pour 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 l'unité de transmission maximale sur les appareils intermédiaires non gérés

Facultatif

Il est avantageux de faire en sorte que Cisco DNA Center gère tous les périphériques d'un domaine de trame. Cisco DNA Center gère déjà les nœuds de périphérie de la trame et les nœuds de frontière; toutefois, si vous avez des périphériques intermédiaires dans la trame qui ne seront pas gérés par Cisco DNA Center (p. ex., le support matériel ou logiciel n'est pas disponible dans Cisco DNA Center), les appareils doivent toujours satisfaire aux exigences de transport de trafic d'accès défini par logiciel via ces nœuds intermédiaires de trame de transit. Les principales exigences sont les suivantes :

- Il doit s'agir d'appareils de couche 3 qui participent activement à la topologie de routage dans les autres périphériques sous-jacents de la trame.
- Ils doivent être en mesure de transporter les trames étendues offertes par les techniques d'encapsulation de trame.

Pour les appareils des nœuds intermédiaires non gérés de la trame, vous devez définir une unité MTU appropriée (p. ex., 9100) et configurer manuellement le routage avec les autres périphériques de la sous-couche. Dans une pareille situation, les instructions de configuration sont spécifiques au périphérique et ne seront pas traitées plus en détail dans ce guide.

N'ajoutez pas de configuration à tous les appareils 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 déjà des configurations ne peuvent pas être configurés à l'aide de l'automatisation LAN.

Procédure 7. Détecter et gérer les appareils réseau

Vous utilisez Cisco DNA Center pour détecter et gérer les appareils réseau sous-jacents pour l'accès défini par logiciel en autorisant la connectivité IP vers les appareils et en communiquant à Cisco DNA Center des coordonnées d'authentification pour la gestion. Suivez cette procédure pour tous les appareils d'amorçage d'automatisation LAN et tous les autres appareils 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 contraint la détection et peut permettre de gagner du temps. Sinon, pour que les périphériques qui n'utilisent pas l'intégration d'automatisation LAN, vous pouvez fournir un appareil initial pour la détection et commander dans Cisco DNA Center l'utilisation du protocole de découverte Cisco pour chercher des voisins connectés. Lorsque vous utilisez le protocole de découverte Cisco, réduisez le nombre de tronçons par défaut jusqu'à un nombre raisonnable pour accélérer la détection.

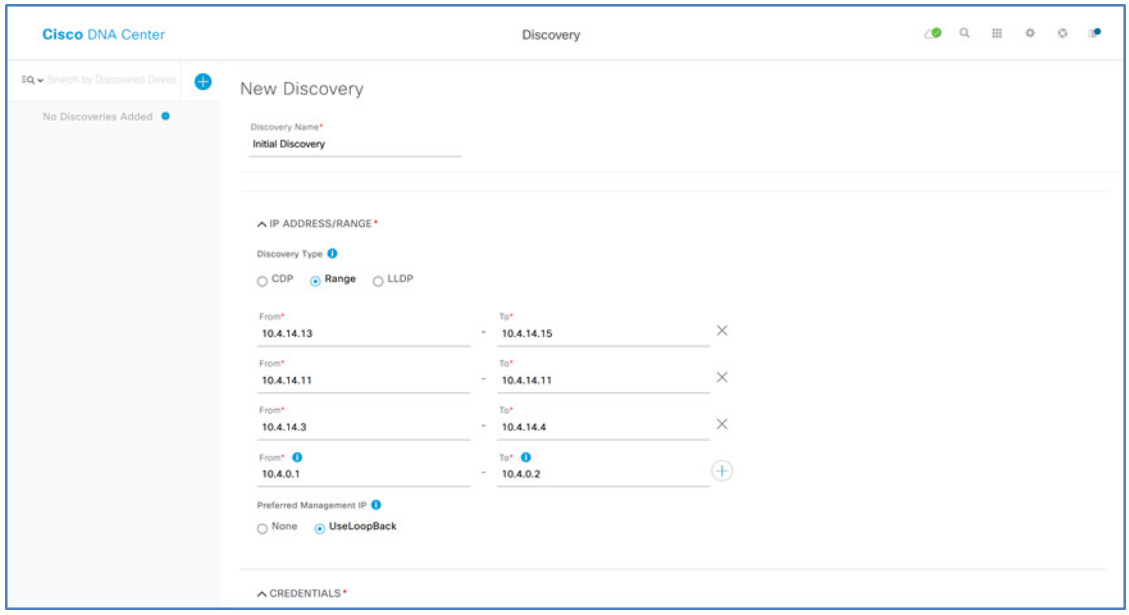
Étape 1. Accédez au tableau de bord principal de Cisco DNA Center, faites défiler l'écran jusqu'à la section **Tools (outils)**, cliquez sur **Discovery (détection)** et indiquez un nom de détection (**Discovery Name**). Sélectionnez la plage (**Range**) et saisissez une adresse IP de bouclage de début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

Conseil technique

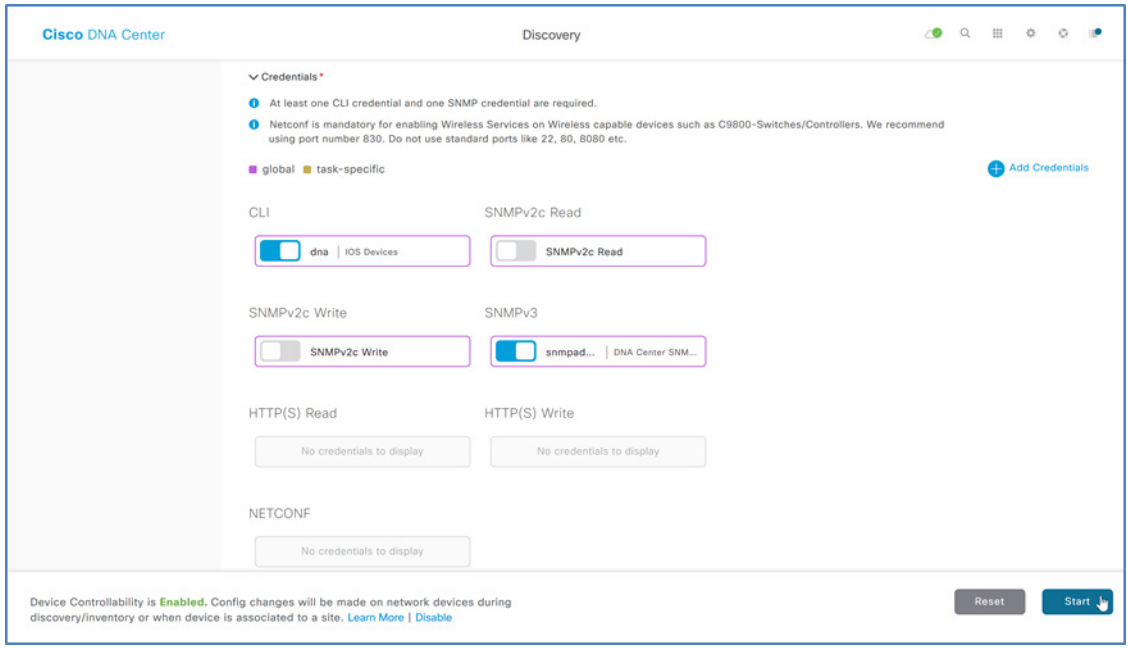
Si vous utilisez un commutateur Cisco Catalyst de la série 6800 avec une très grande configuration, vous pouvez éviter les expirations de détection en ajoutant la commande suivante à ce commutateur dans le mode de configuration :

```
snmp mib flash cache
```

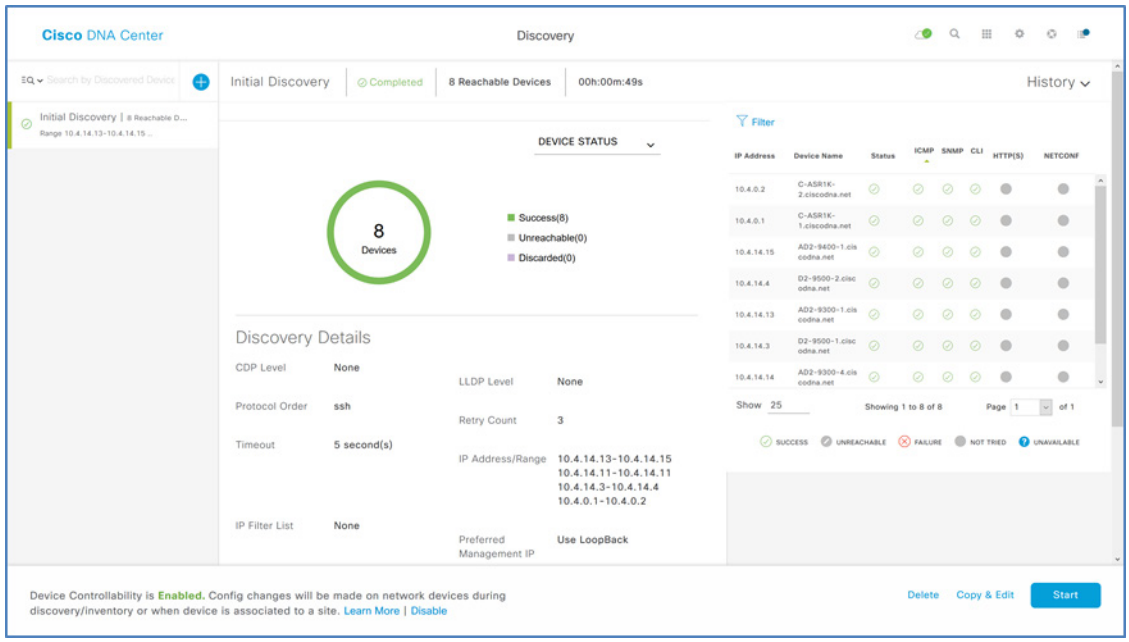
Étape 2. Si vous avez des plages supplémentaires, à côté de la première plage, cliquez sur **+** (signe plus), saisissez la plage supplémentaire et répétez l'opération pour toutes les plages restantes.



Étape 3. Faites défiler l'écran pour vérifier les coordonnées d'authentification de l'interface de ligne de commande utilisées pour la détection et les configurations des coordonnées d'authentification SNMP envoyées au périphérique par la fonction de contrôle de l'appareil (Device Controllability) de Cisco DNA Center, puis cliquez sur **Start (démarrer)** vers le bas.



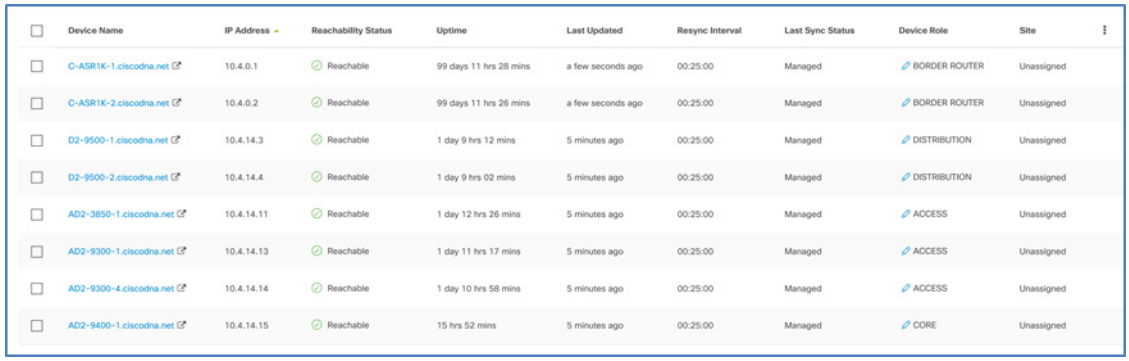
Les informations de détection sont affichées pendant que la détection est exécutée.



À la fin de la détection d'un appareil avec la fonction de contrôle de l'appareil activée, les coordonnées d'authentification attribuées à l'aide de l'interface de ligne de commande et stockées localement sur l'appareil sont utilisées comme sauvegarde. Les coordonnées d'authentification locales sont utilisées uniquement en cas de perte de connectivité vers ISE, qui est utilisé pour accéder aux principaux éléments d'information d'authentification centralisée.

Étape 4. S'il y a des défaillances de détection, examinez la liste des périphériques, réglez le problème et redémarrez la détection pour ces appareils, 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, dans la section **Tools (outils)**, cliquez sur **Inventory (inventaire)**. Les appareils détectés s'affichent. Une fois la collecte d'inventaire terminée, chaque périphérique affiche un état de synchronisation **géré**, ce qui signifie que Cisco DNA Center gère un modèle interne qui reproduit le déploiement physique de l'appareil.



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

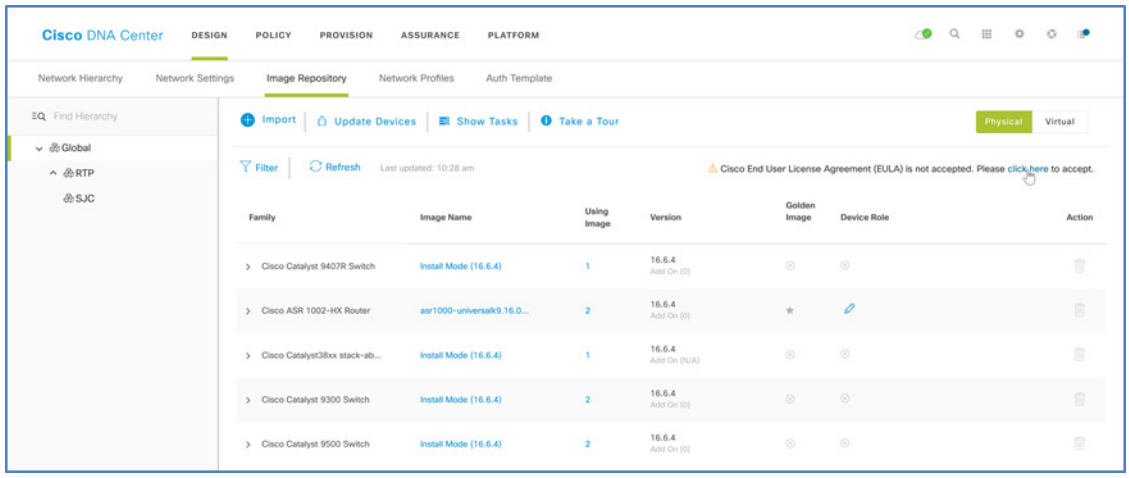
Conseil technique
Sur le côté droit de la ligne de titre du tableau d'inventaire, vous pouvez modifier les colonnes affichées. Utilisez la colonne **Device Role** pour voir le rôle d'appareil attribué par la détection en fonction du type d'appareil et pour ajuster le rôle de manière à refléter le déploiement réel d'un périphérique, tel que l'accès, la distribution, le cœur ou le routeur de frontière, dans le cas où le routeur de frontière dans cet écran a un rôle de périphérique générique ne faisant pas partie de la trame. Le réglage du rôle permet désormais d'améliorer l'apparence des cartes topologiques initiales, plutôt que d'ajuster les rôles dans des procédures ultérieures.

Procédure 8. Gérez les images logicielles pour les périphériques dans l'inventaire

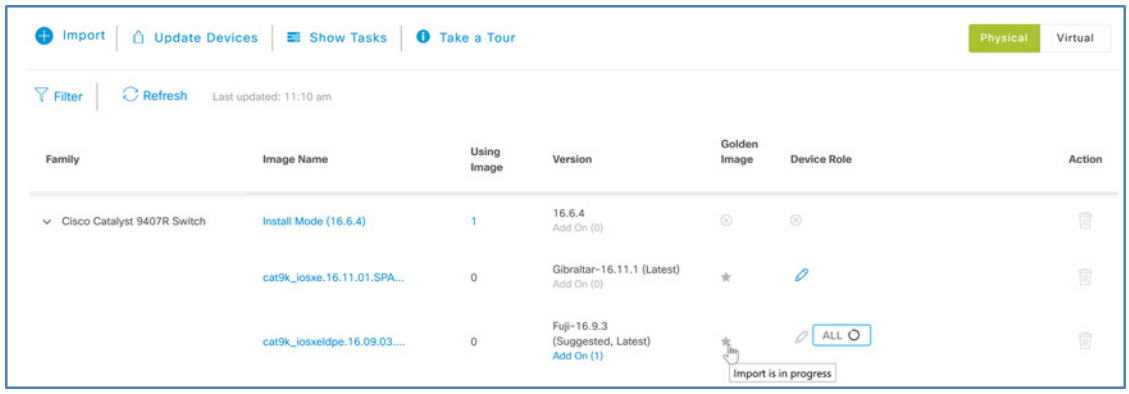
Pour tirer pleinement parti des fonctionnalités de l'accès défini par logiciel, l'ensemble SD-Access dans Cisco DNA Center prévoit des exigences sur le plan de la version logicielle minimale requise pour les périphériques dont il procède à l'installation. La fonction de gestion de l'image logicielle intégrée à Cisco DNA Center permet de mettre à niveau tous les périphériques qui n'exécutent pas une version d'image recommandée. Vous trouverez des images recommandées pour l'accès défini par logiciel (SD-Access) à l'aide de la matrice de compatibilité matérielle et logicielle de l'ensemble SD-Access sur Cisco.com. Les images utilisées pour la validation sont répertoriées dans l'annexe A : liste des produits.

Procédez comme suit pour appliquer les mises à jour logicielles des images et les mises à jour de maintenance logicielle des périphériques, en important les images requises, en marquant les images comme modèles (Golden) et en appliquant des images 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, cliquez sur le **contrat de licence de l'utilisateur final de Cisco** en haut à droite, sélectionnez **Click here (cliquez ici)**, puis cliquez sur **Accept License Agreement (accepter le contrat de licence)**.



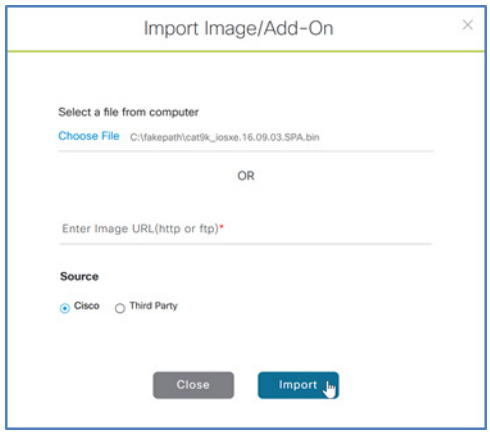
Étape 2. Si vous choisissez de demander à Cisco DNA Center de télécharger une nouvelle image à appliquer à un appareil, dans la colonne **Image Name (nom de l'image)**, cliquez sur la flèche vers le bas en regard de l'image répertoriée pour une famille d'appareils, puis cliquez sur l'étoile de **Golden Image** 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 coordonnées d'authentification sur Cisco.com. Vous pouvez mettre à jour les coordonnées d'authentification de Cisco.com à l'aide de **Settings** (les paramètres, voir l'engrenage) **> System Settings (paramètres de système) > Cisco Credentials (coordonnées d'authentification)**.

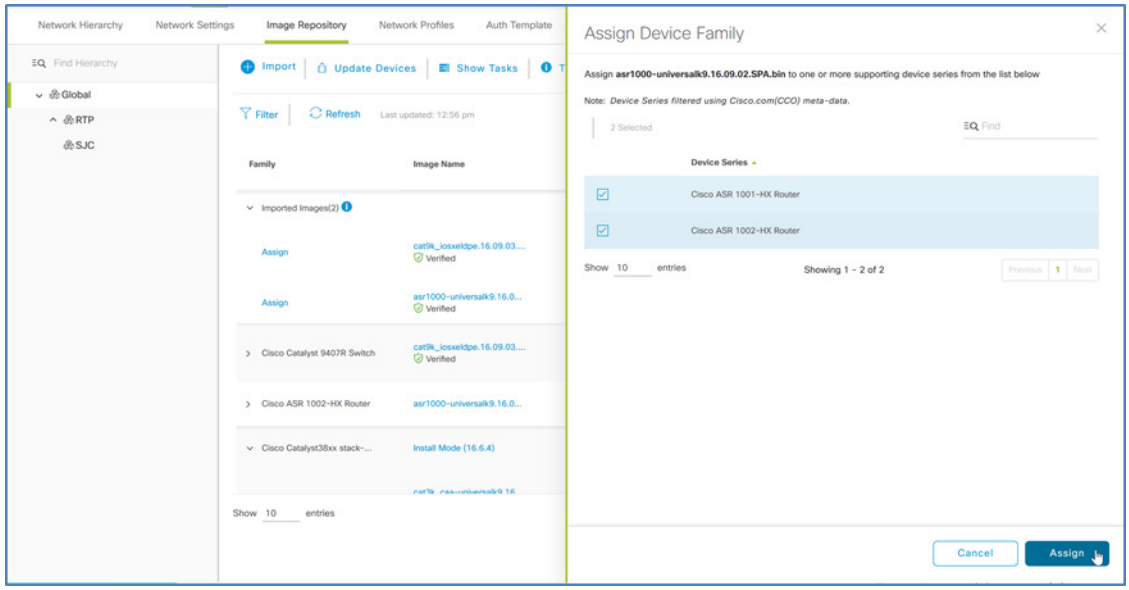
Étape 3. Répétez l'importation et le balisage des images de référence jusqu'à ce que tous les périphériques soient marqués d'une image appropriée.

Étape 4. Si vous choisissez d'importer une image depuis votre ordinateur local, cliquez sur **+ Import**, dans la boîte de dialogue Image/Add-On, 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, attribuez l'image importée aux périphériques. À côté de l'image importée, cliquez sur **Assign (attribuer)**, sélectionnez les appareils qui utilisent l'image, puis dans le menu contextuel, cliquez sur **Assign (attribuer)**.



L'image se trouve dans le référentiel et est disponible pour mise en référence pour ces appareils.

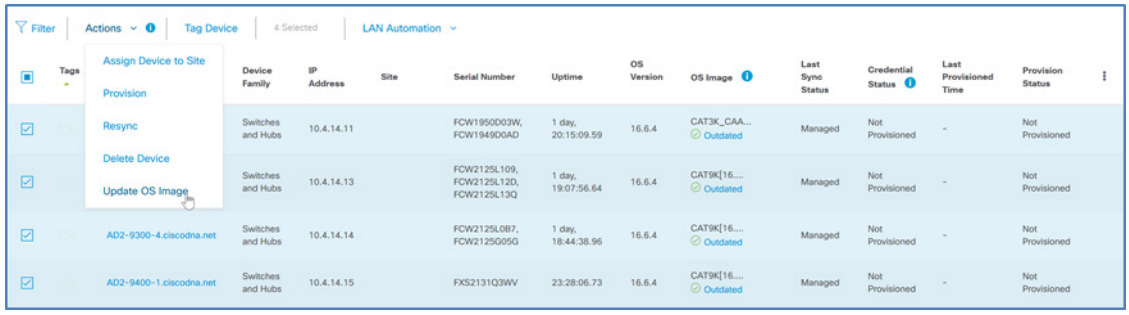
Étape 6. Pour chaque périphérique avec une image qui vient d'être attribuée, cliquez sur l'étoile de **Golden Image** pour marquer l'image appropriée comme préférée pour la plate-forme.

Étape 7. Répétez ces étapes pour toutes les images que vous souhaitez déployer à l'aide de Cisco DNA Center. Tous les types d'appareils avec une image de référence attribuée sont prêts pour la distribution de l'image logicielle.

Procédure 9. Utilisez la gestion des images logicielles pour mettre à jour les logiciels des appareils

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

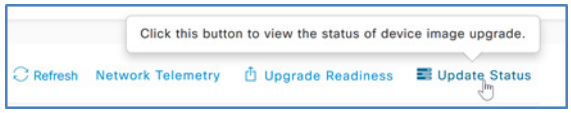
Étape 1. Naviguez jusqu'à **PROVISION (configuration) > Devices (appareils) > Inventory (inventaire)**, sélectionnez tous les périphériques marqués comme obsolètes (**Outdated**), puis dans le menu **Actions**, cliquez sur **Update OS Image (mettre à jour l'image du système d'exploitation)**. Pour plus de contrôle sur les mises à jour, démarrez les mises à jour du système d'exploitation sur les appareils qui peuvent redémarrer sans nuire à la connectivité aux autres périphériques que vous mettez à jour.



Étape 2. Dans l'encadré qui s'affiche, sous **Distribute > When**, sélectionnez **Now (maintenant)**, cliquez sur **Next (suivant)**, sous **Activate (activer)** sélectionnez **Schedule Activation after Distribution is completed (activation de la planification une fois la distribution terminée)**, cliquez sur **Next (suivant)**, puis sous **Confirm (confirmer)**, cliquez sur le bouton **Confirm (confirmer)**.

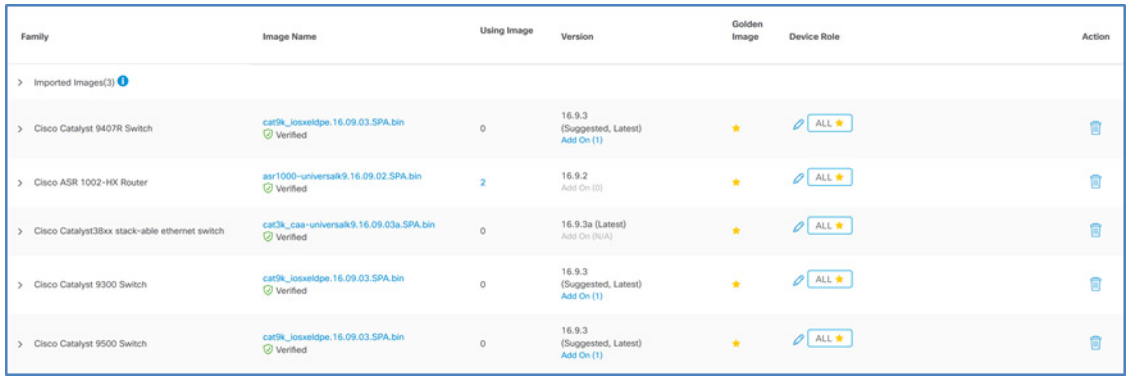
Les images sont distribuées aux appareils sélectionnés.

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



L'écran d'état donne plus de détails que l'écran principal, y compris des explications sur les défaillances. Utilisez le bouton **Refresh (actualiser)** pour observer que l'état en cours (**In Progress**) est remplacé par l'état **Successful (réussite)**.

Étape 4. Répétez cette procédure au besoin pour mettre à jour le logiciel de l'appareil vers les versions requises pour le déploiement du réseau. À l'issue de l'opération, tous les périphériques du déploiement sont associés à une image de référence et l'image est installée.



Processus : configuration du réseau de sous-couche pour l'accès défini par logiciel

Une fois que Cisco DNA Center découvre et dispose d'un contrôle de gestion des périphériques qui exécutent les versions logicielles appropriées pour l'accès défini par logiciel, utilisez Cisco DNA Center pour provisionner les périphériques du réseau sous-jacent.

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

Facultatif

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 d'amorçage (les appareils gérés là où se connecte le nouveau réseau non géré), l'interface de ligne de commande de périphérique et les coordonnées d'authentification SNMP à envoyer par PnP, ainsi que l'ensemble d'adresses IP accessible par réseau pour la connectivité. Bien que ça ne soit pas obligatoire, chaque périphérique d'amorçage est généralement un commutateur attribué dans les procédures ultérieures en tant que frontière et doit disposer d'un mode VTP et d'une configuration MTU appropriés (p. ex., mode VTP transparent, MTU système 9100). Les ports sur le périphérique d'amorçage connecté aux appareils à détecter doivent être en mode de couche 2 (port d'accès c. port routé) et les ports de l'appareil d'amorçage 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 par les appareils d'amorçage pris en charge (les commutateurs utilisés dans cette validation sont répertoriés dans l'annexe). Les commutateurs détectés sont directement connectés aux interfaces du périphérique d'amorçage choisi (les ports de gestion OOB ne peuvent pas être connectés pendant l'intégration des périphériques d'automatisation LAN, car ils bloquent l'automatisation LAN sur les ports non OOB) et jusqu'à un tronçon supplémentaire de commutateurs connectés, à une distance totale de deux tronçons du périphérique d'amorçage. Les coordonnées d'authentification saisies permettent à Cisco DNA Center et aux appareils d'amorçage de fonctionner ensemble pour configurer les appareils détectés et les ajouter à l'inventaire géré. Étant donné que les appareils détectés doivent exécuter l'agent PnP sans configuration précédente, tous les commutateurs précédemment configurés doivent être restaurés dans un état où l'agent PnP est exécuté, à l'aide des commandes suivantes du mode de configuration et du mode d'exécution.

```
(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 de la pile.

Les exigences d'empilage des commutateurs ne changent pas dans le contexte de 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 de regroupement, ou « bundle »). Si vous souhaitez contrôler autant que possible le comportement de la pile et la numérotation des ports, avant de démarrer le processus d'automatisation LAN, vous pouvez ajuster la numérotation de la pile de commutateurs et agir également sur un commutateur pour qu'il adopte un rôle 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
```

Définissez un ou deux périphériques dans l'inventaire qui sont gérés par Cisco DNA Center pour les attribuer au rôle de dispositif d'amorçage sur un site. Les mêmes dispositifs d'amorçage peuvent être utilisés pour plusieurs exécutions de la fonction d'automatisation LAN, ce qui permet d'attribuer les appareils détectés à différents bâtiments ou étages lors de chaque exécution de la fonction.

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, accédez à **PROVISION (configuration) > Devices (périphériques) > Inventory (inventaire)**. Sélectionnez jusqu'à deux périphériques d'amorçage, dans la liste déroulante **Actions**, cliquez sur **Assign Device to Site (attribuer un périphérique au site)**, et dans l'écran **Assign Device to Site**, sélectionnez les attributions de sites des périphériques, puis cliquez sur **Apply (appliquer)**.

Étape 2. Si vous utilisez un appareil d'amorçage de la gamme Catalyst 6800, utilisez la commande de mode de configuration d'interface pour modifier les ports des appareils détectés en ports de couche 2.

```
switchport
```

Après avoir enregistré le changement de configuration, resynchronisez l'appareil 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**.

Conseil technique

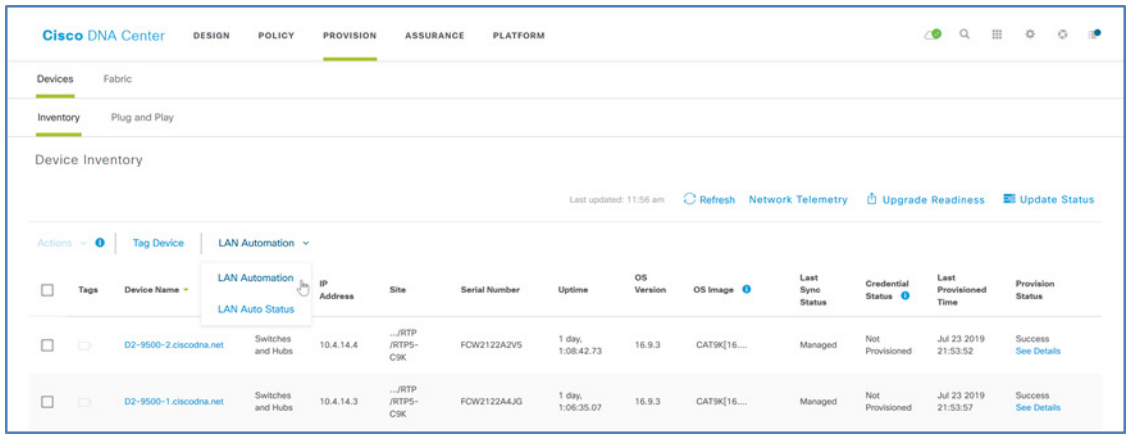
L'ensemble d'adresses IP utilisé pour l'automatisation LAN doit être dimensionné de façon à être beaucoup plus grand que le nombre d'appareils à découvrir. L'ensemble est divisé en deux. Une moitié est utilisée pour les services DHCP du VLAN 1 fournis par les périphériques d'amorçage. La deuxième moitié de l'ensemble est aussi divisée en deux, 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 boucle. Les terminaux ne doivent pas être branchés sur les commutateurs, car ils peuvent épuiser l'ensemble d'adresses IP utilisé par DHCP pour la configuration PnP.

Pour une configuration réussie, les adresses de l'ensemble d'automatisation LAN doivent être accessibles par Cisco DNA Center et ne doivent pas être utilisées ailleurs dans le réseau. Si votre Cisco DNA Center utilise le réseau de gestion dédié facultatif comme port d'accès Web au lieu d'un port unique avec une route par défaut, vous devez vous assurer que la route vers l'ensemble d'adresses IP d'automatisation LAN est disponible via le port d'infrastructure du réseau d'entreprise. Si l'ensemble d'adresses IP n'est pas inclus dans les routes configurées sur Cisco DNA Center, connectez-vous à Cisco DNA Center eau moyen du port SSH 2222, puis connectez-vous en tant que maglev et exécutez la commande suivante :

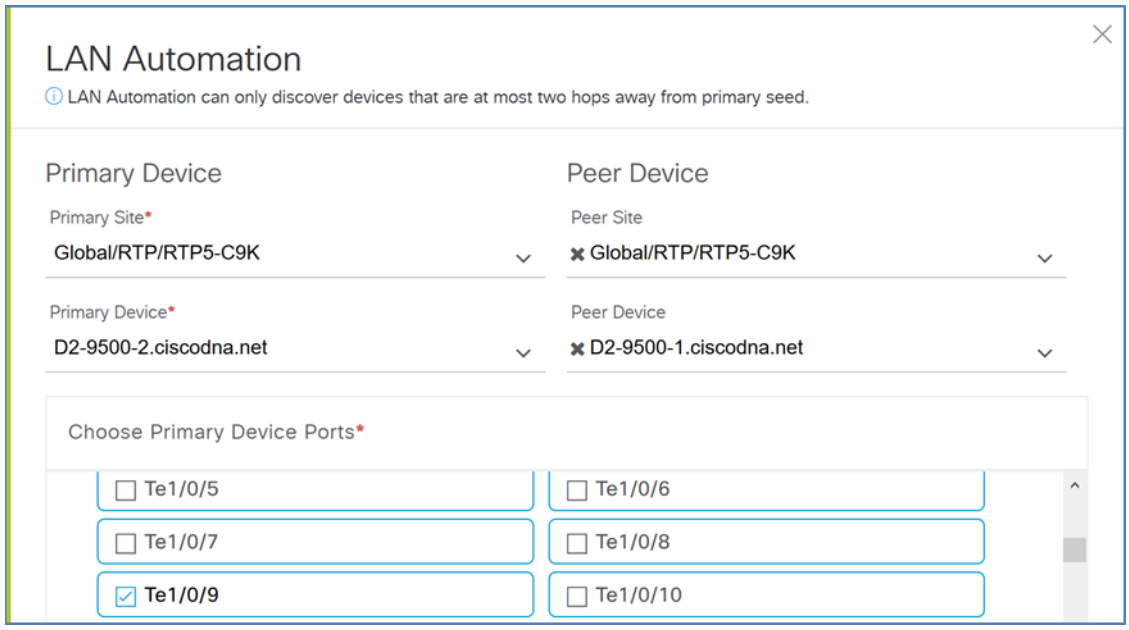
```
sudo maglev-config update
```

Utilisez l'Assistant de configuration pour configurer les routes statiques afin d'ajouter l'ensemble d'adresses IP sur l'adaptateur réseau approprié avant de démarrer l'automatisation du réseau local (LAN).

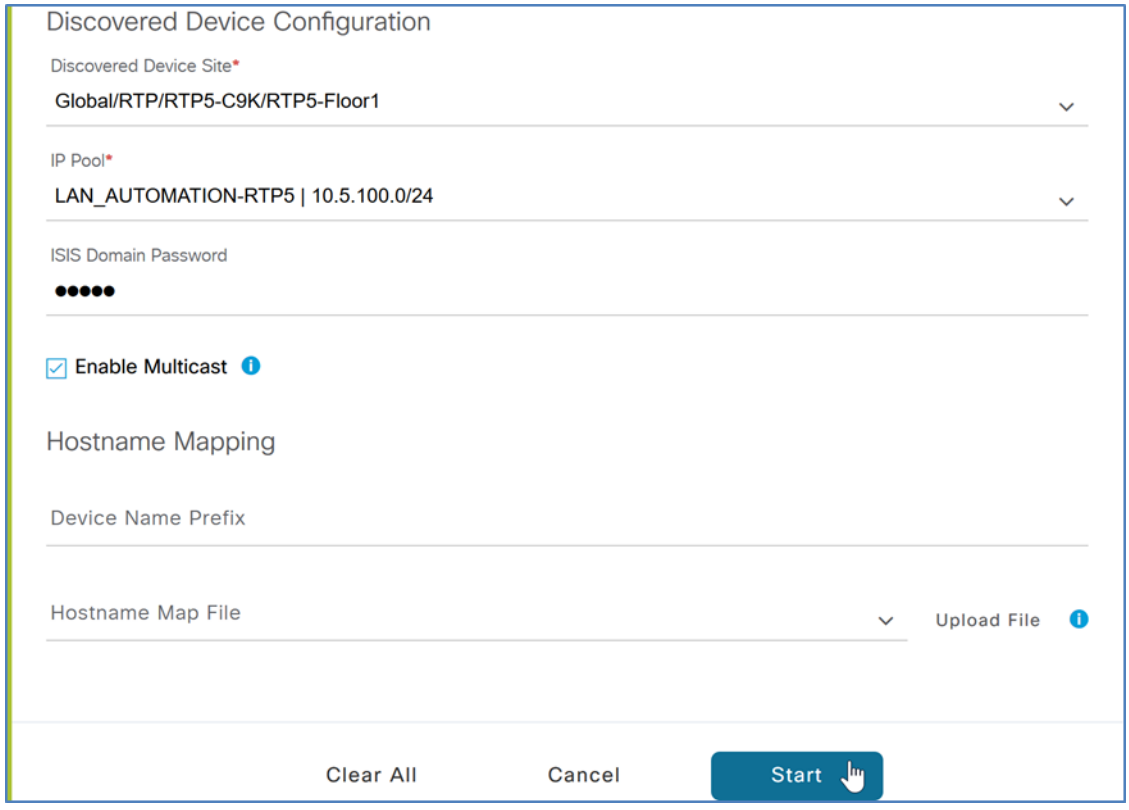
Étape 3. Accédez à **PROVISION (configuration) > Devices (périphériques) > Inventory (inventaire)**. En haut de l'écran, cliquez sur le menu déroulant de l'automatisation du réseau local (**LAN Automation**), puis cliquez sur **LAN Automation**.



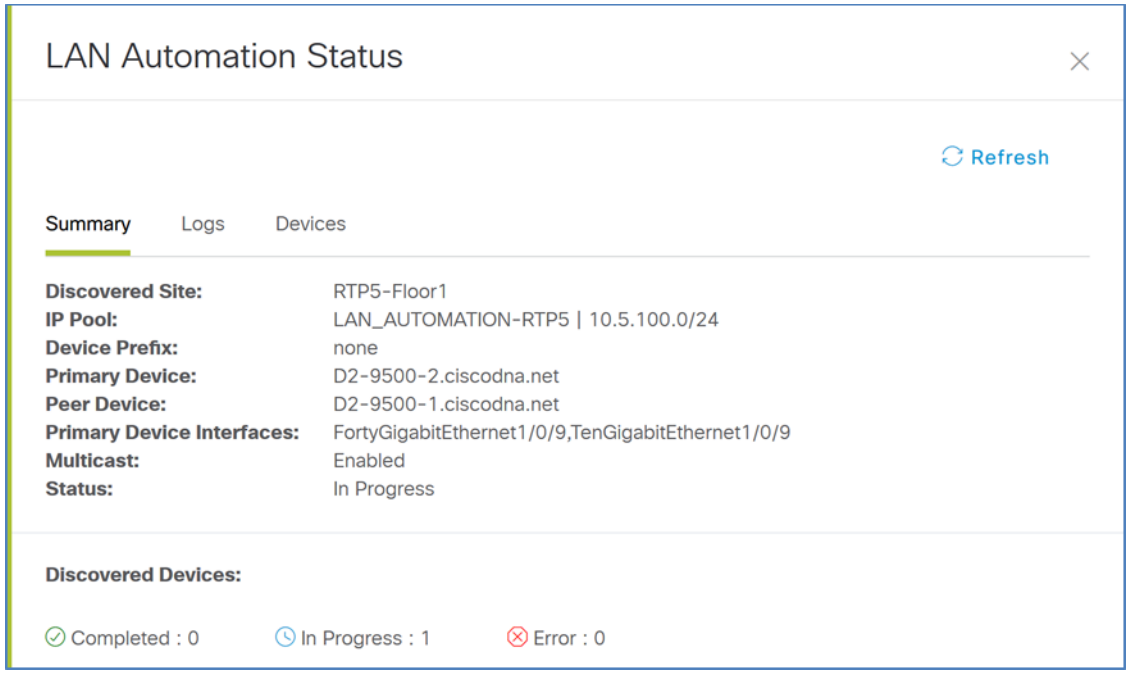
Étape 4. À droite, dans l'encadré de l'automatisation du réseau local, complétez les paramètres de la détection. Sous **Primary Device (appareil principal)**, précisez ce qui suit : **Primary Site* (site principal)**, **Primary Device* (appareil principal)**; indiquez les ports de l'appareil principal (**Choose Primary Device Ports***), et sous **Peer Device (appareil homologue)**, indiquez le **Peer Site (site homologue)** et le **Peer Device (appareil homologue)**.



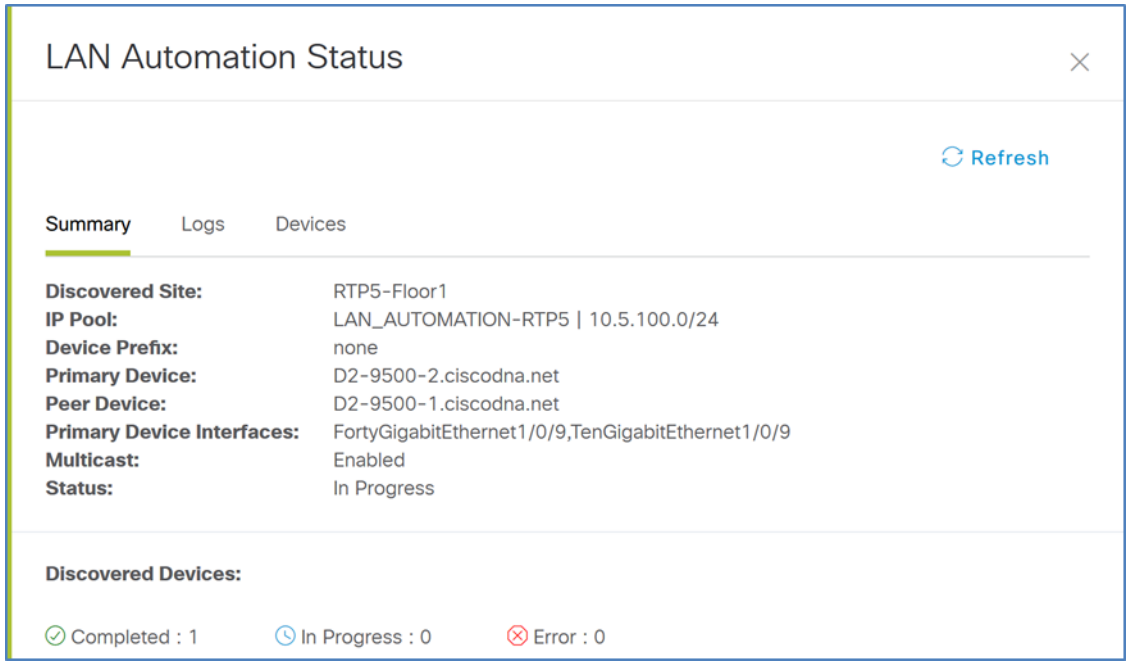
Étape 5. À droite, dans l'encadré de l'automatisation du réseau local, continuez de compléter les paramètres de la détection. Dans la section **Discovered Device Configuration (configuration des appareils détectés)**, indiquez ce qui suit : **Discovered Device Site* (site d'appareil détecté)**, le **IP Pool* (ensemble d'adresses IP)**; le cas échéant, indiquez le mot de passe du domaine ISIS (**ISIS Domain Password**), sélectionnez **Enable Multicast (activer la multidiffusion)**, puis cliquez sur **Start** pour démarrer.



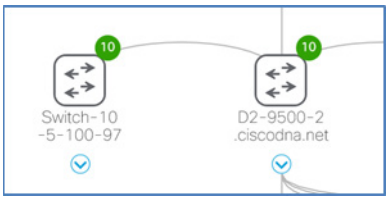
Étape 6. En haut de l'écran, cliquez sur le menu déroulant de l'automatisation du réseau local (**LAN Automation**), puis cliquez sur **LAN Auto Status (état d'automatisation LAN)** pour afficher les progrès.



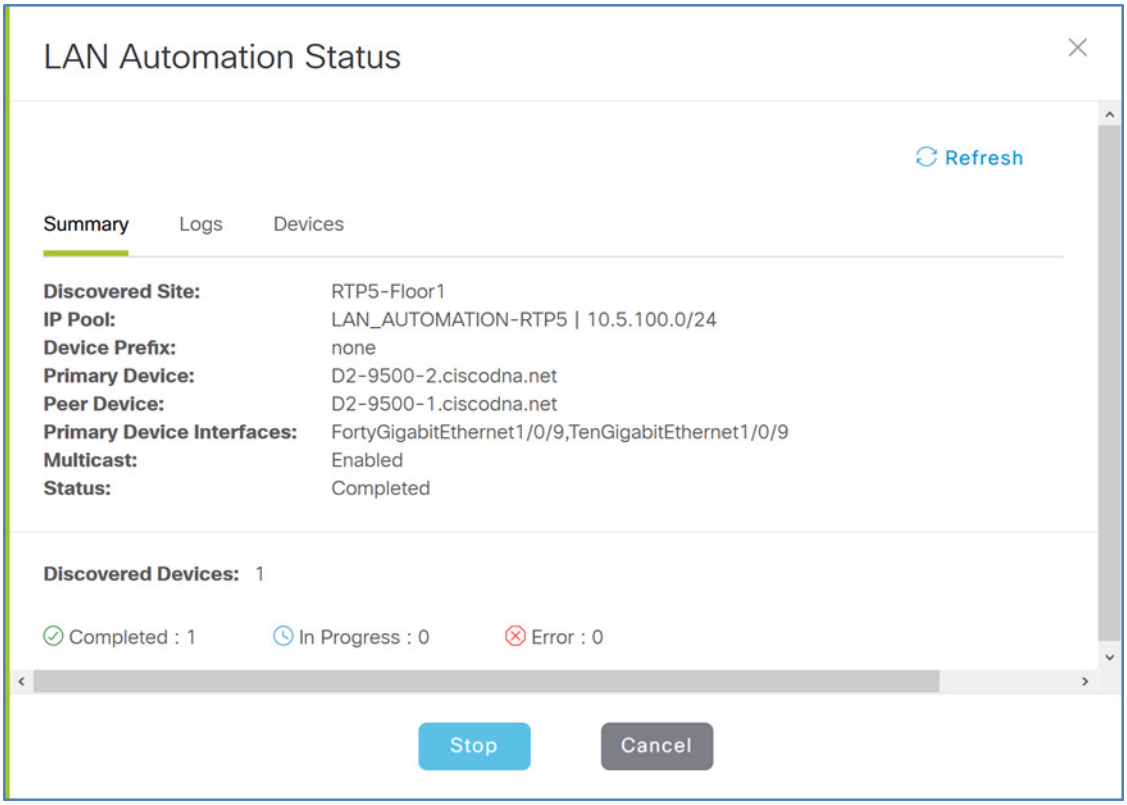
Ne cliquez pas sur **Stop** à cette étape. Attendez que tous les périphériques affichent l'état **Completed (terminé)**, puis passez à l'étape de vérification suivante. L'arrêt prématuré du processus PnP laissera la détection dans un état nécessitant une intervention manuelle pour le rétablissement. La détection des périphériques à un tronçon de plus de l'appareil d'amorçage peut prendre beaucoup plus de temps à atteindre son achèvement.



Étape 7. Accédez au tableau de bord principal du 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.



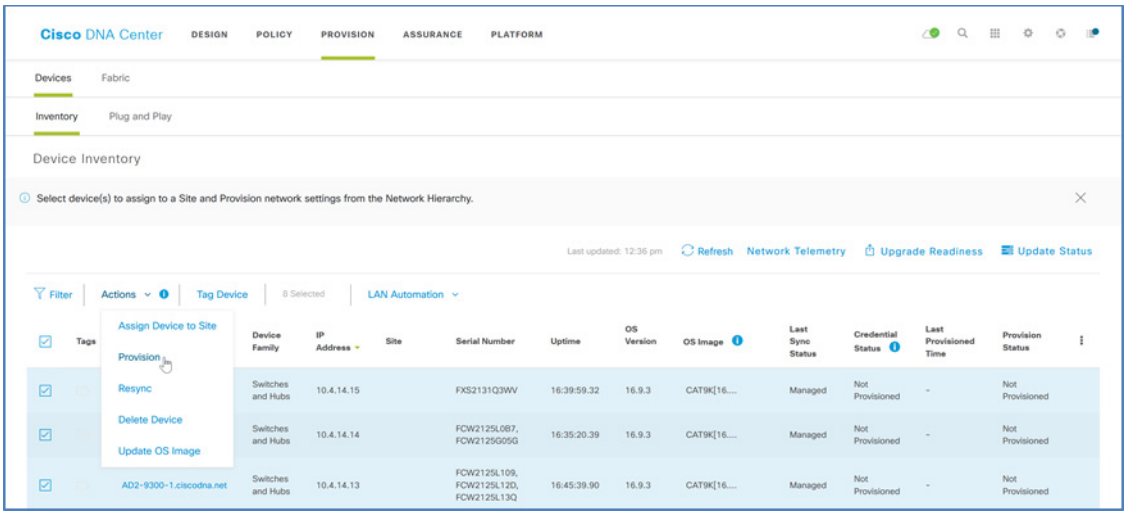
Étape 8. Accédez à **PROVISION (configuration) > Devices (périphériques) > Inventory (inventaire)**. En haut de l'écran, cliquez sur le menu déroulant de l'automatisation du réseau local (**LAN Automation**), puis cliquez sur **LAN Auto Status (état d'automatisation LAN)**. Une fois que les périphériques ont détecté l'état **Completed (terminé)**, cliquez sur **Stop (arrêter)**. L'automatisation LAN se détruit sur toutes les connexions de couche 2 sur le VLAN 1 et le processus de routage sous-jacent IS-IS est utilisé pour l'accessibilité du réseau de routage; les périphériques sont gérés dans l'inventaire.



Procédure 2. Provisionnez des périphériques et les attribuer aux sites pour préparer l'accès défini par logiciel

Provisionnez les périphériques réseau, puis les attribuer à un site en vue de leur intégration dans un réseau à accès défini par logiciel.

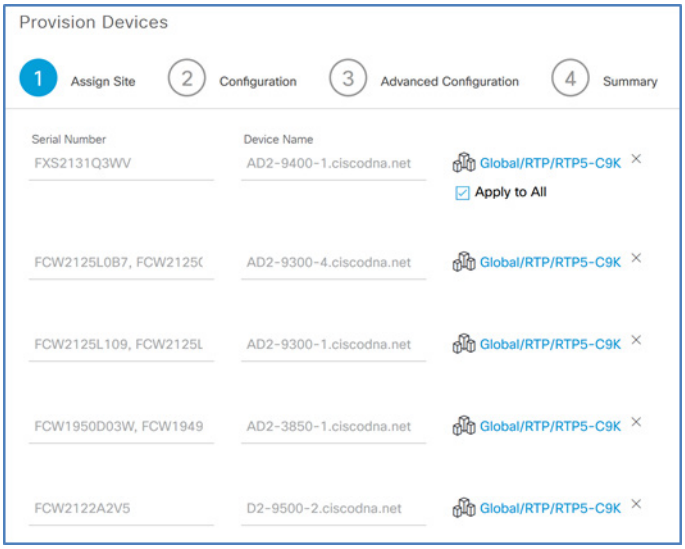
Étape 1. Dans Cisco DNA Center, allez à **PROVISION (configuration) > Devices (périphériques) > Inventory (inventaire)**, sélectionnez les périphériques du même type (p. ex., tous les commutateurs) à provisionner sur le réseau, cliquez sur **Actions**, puis sur **Provision**.



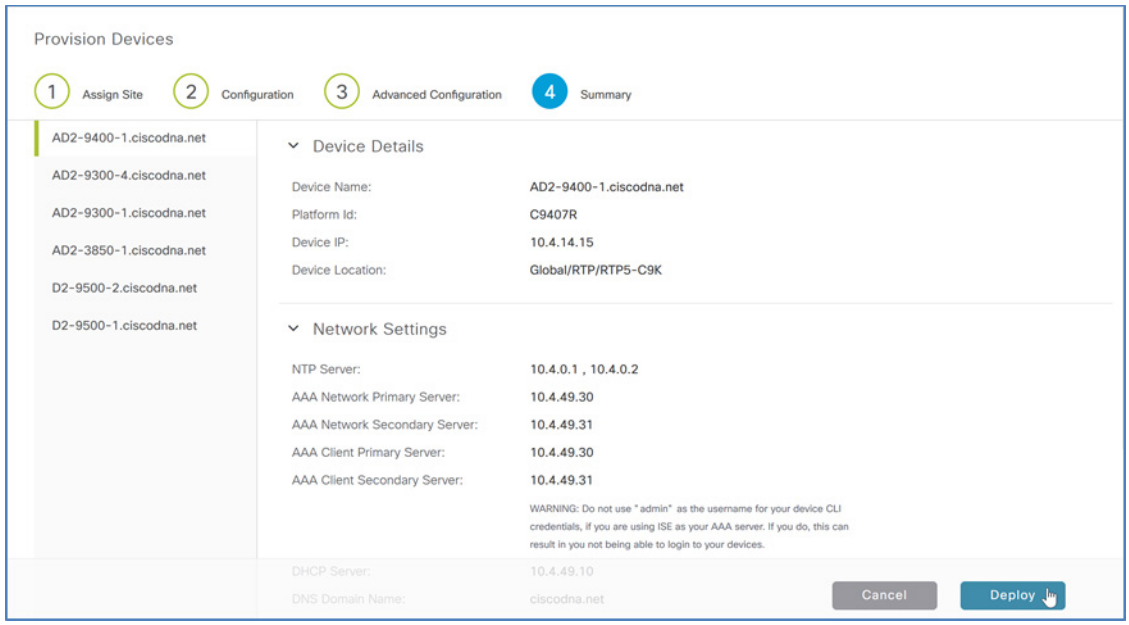
L'écran de l'Assistant de configuration des appareils (**Provision Devices**) apparaît.

Conseil technique
Les périphériques doivent être de même type (par ex., des routeurs) pour être configurés en même temps. Vous pouvez regrouper les opérations de provisionnement en plusieurs petits lots pour les attributions à des sites communs, le cas échéant.

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



Étape 3. Cliquez deux fois sur **Next (suivant)** pour ignorer les écrans **Configuration** et **Advanced Configuration (configuration avancée)**, dans l'écran **Summary (résumé)**, examinez les informations relatives à chaque appareil, puis cliquez sur **Deploy (déployer)**.

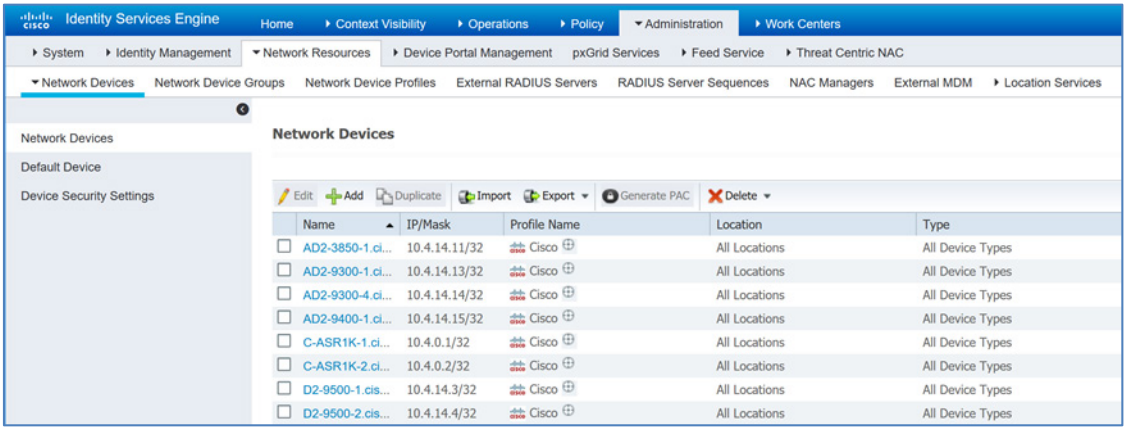


Étape 4. Dans l'écran contextuel, conservez la sélection par défaut **Now (maintenant)**, puis cliquez sur **Apply (appliquer)**.

La configuration de chaque périphérique commence, et des messages d'état apparaissent à mesure que chaque périphérique est provisionné avec succès. L'écran d'inventaire des appareils (Device Inventory) est mis à jour avec l'état de provisionnement (**Provision Status**) et l'état de la synchronisation (**Sync Status**). Utilisez le bouton **Refresh (actualiser)** pour mettre à jour l'état final.

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

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



Processus : configuration du réseau superposé de l'accès défini par logiciel

Un réseau de superposition de trame est créé dans Cisco DNA Center à l'aide des appareils détectés qui ont été ajoutés à l'inventaire et provisionnés sur un site. Cisco DNA Center automatise la configuration des appareils supplémentaires prenant en charge les réseaux de superposition pour l'accès défini par logiciel.

La solution de l'accès défini par logiciel prend en charge le provisionnement des structures de trame suivantes :

- Site de trame : une trame indépendante, y compris les fonctions de nœud de plan de contrôle et de nœud de périphérie, à l'aide d'un nœud de frontière de trame, pour la sortie du site de trame, qui comprend généralement un PSN d'ISE et un WLC en mode de trame
- Site de transit : également connu sous le nom de réseau de transit, connecte un site de trame à un réseau externe (transit fondé sur IP) ou à un ou plusieurs sites de trame en conservant les segments de manière native (transit d'accès défini par logiciel)
- Domaine de trame : englobe un ou plusieurs sites de trames et les sites de transit correspondants.

Les réseaux de transit fondés sur IP connectent la trame à des réseaux externes, généralement à l'aide de VRF-Lite pour la connectivité IP. Les transits d'accès défini par logiciel transportent des informations SGT et VN, qui transportent intrinsèquement la politique et la segmentation entre les sites de trame, créant ainsi un réseau décentralisé. Cette configuration

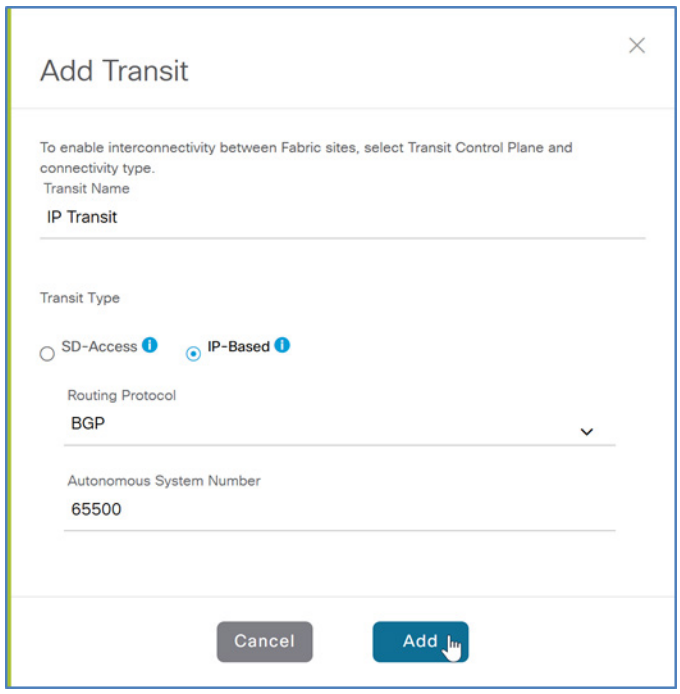
Conseil technique
Le logiciel Cisco DNA Center et le logiciel Cisco IOS répertoriés dans l'annexe ne comportent pas de validation du transit d'accès défini par logiciel, dont il est question dans le Guide de déploiement normatif de l'accès défini par logiciel pour les réseaux décentralisés. Vous trouverez des versions de logiciel alternatives qui peuvent prendre en charge des options supplémentaires en faisant des recherches dans Cisco.com pour trouver la matrice de compatibilité du matériel et des logiciels de l'accès défini par logiciel (SD-Access Hardware and Software Compatibility Matrix).

Le logiciel Cisco DNA Center et le logiciel Cisco IOS répertoriés dans l'annexe ne comportent pas de validation du transit d'accès défini par logiciel, dont il est question dans le Guide de déploiement normatif de l'accès défini par logiciel pour les réseaux décentralisés. Vous trouverez des versions de logiciel alternatives qui peuvent prendre en charge des options supplémentaires en faisant des recherches dans Cisco.com pour trouver la matrice de compatibilité du matériel et des logiciels de l'accès défini par logiciel (SD-Access Hardware and Software Compatibility Matrix).

Procédure 1. Créer un site de transit fondé sur IP, un domaine de trame et des sites de trame

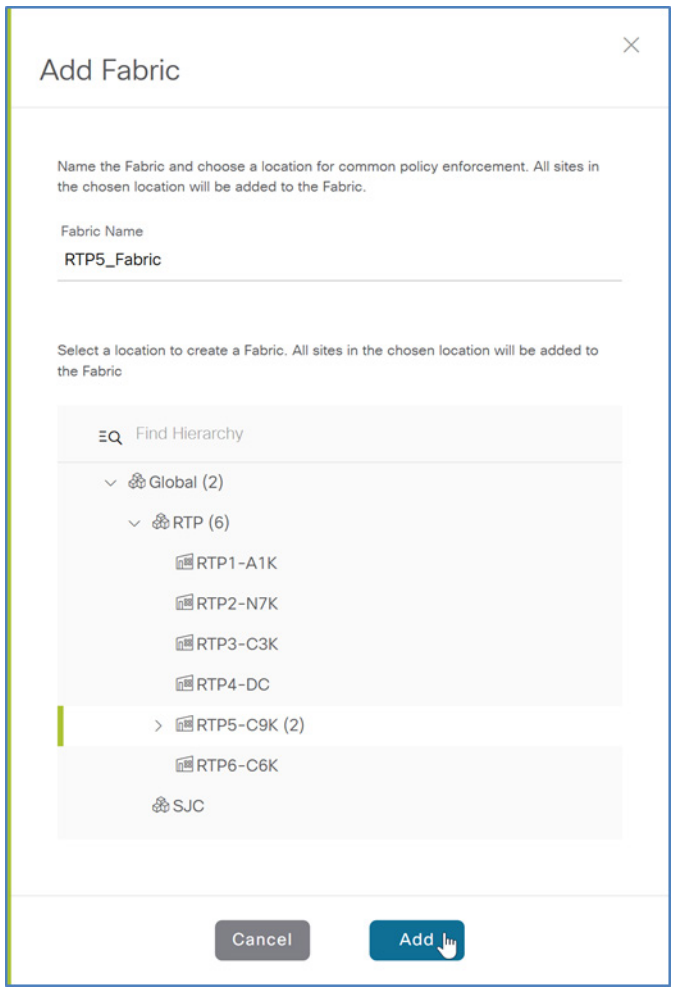
Le site de transit fondé sur l'IP représente le système autonome distant du protocole BGP. Le BGP local est configuré dans le cadre du provisionnement du contour de trame, dans une procédure ultérieure.

Étape 1. Dans Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, en haut à droite, cliquez sur **+ Add Fabric or Transit**, puis cliquez sur **Add Transit (ajouter un transit)**, dans l'encadré déroulant indiquez un nom de transit (sous **Transit Name**, par exemple, IP_Transit), sélectionnez **IP-Based**, puis pour le protocole de routage (**Routing Protocol**), sélectionnez **BGP**, saisissez un **Autonomous System Number (numéro de système autonome)** pour le système autonome du protocole BGP distant (p. ex., 65500), puis cliquez sur **Add (ajouter)**.



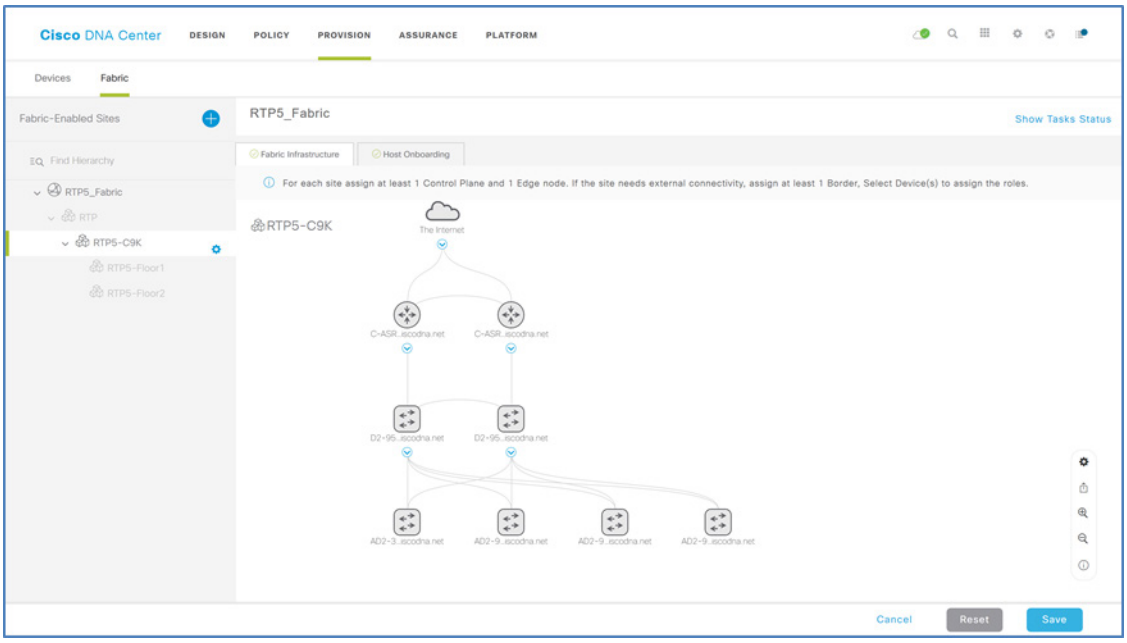
Un message d'état s'affiche et le transit est créé.

Étape 2. Naviguez jusqu'à **PROVISION (configuration) > Fabric (trame)**, en haut à droite cliquez sur **+ Add Fabric or Transit**, cliquez sur **Add Fabric (ajouter une trame)**, dans l'encadré déroulant indiquez un nom de trame (**Fabric Name**, par exemple, RTP5_Fabric), utilisez la hiérarchie du site pour sélectionner un emplacement, y compris les sites pour activer la trame (p. ex., RTP5-C9K), puis cliquez sur **Add (ajouter)**.



La nouvelle trame de réseau sur site a été créée.

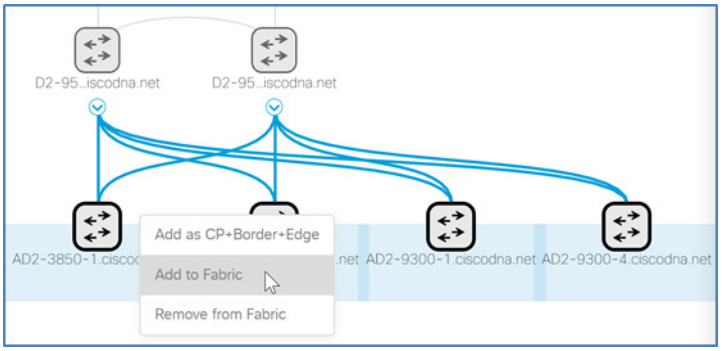
Étape 3. Cliquez sur le nom de domaine de la trame que vous venez de créer (p. ex., RTP5_Fabric), et dans la hiérarchie des sites de trame sur la gauche (**Fabric-Enabled Sites**), sélectionnez le site ajouté à l'étape précédente (p. ex., RTP5-C9K). Une vue de la trame et des sites associés s'affiche.



Si le schéma de topologie de trame illustré n'imite pas la topologie à deux niveaux (distribution/accès) ou à trois niveaux (cœur de réseau/distribution/accès) qui est déployée, corrigez la topologie en accédant à **Tools (outils) > Inventory (inventaire)**, à droite de la ligne de titre pour le tableau d'inventaire, réglez les colonnes affichées pour inclure le rôle de l'appareil (**Device Role**), puis définissez le rôle de manière à refléter le déploiement réel d'un appareil. Revenez à la vue de la topologie du domaine de trame après avoir modifié les rôles de l'appareil pour une vue mise à jour.

Procédure 2. Créez une superposition de trames

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



Les symboles des rôles de périphérie et de trame des icônes bleues apparaissent, représentant le comportement cible prévu pour les appareils.

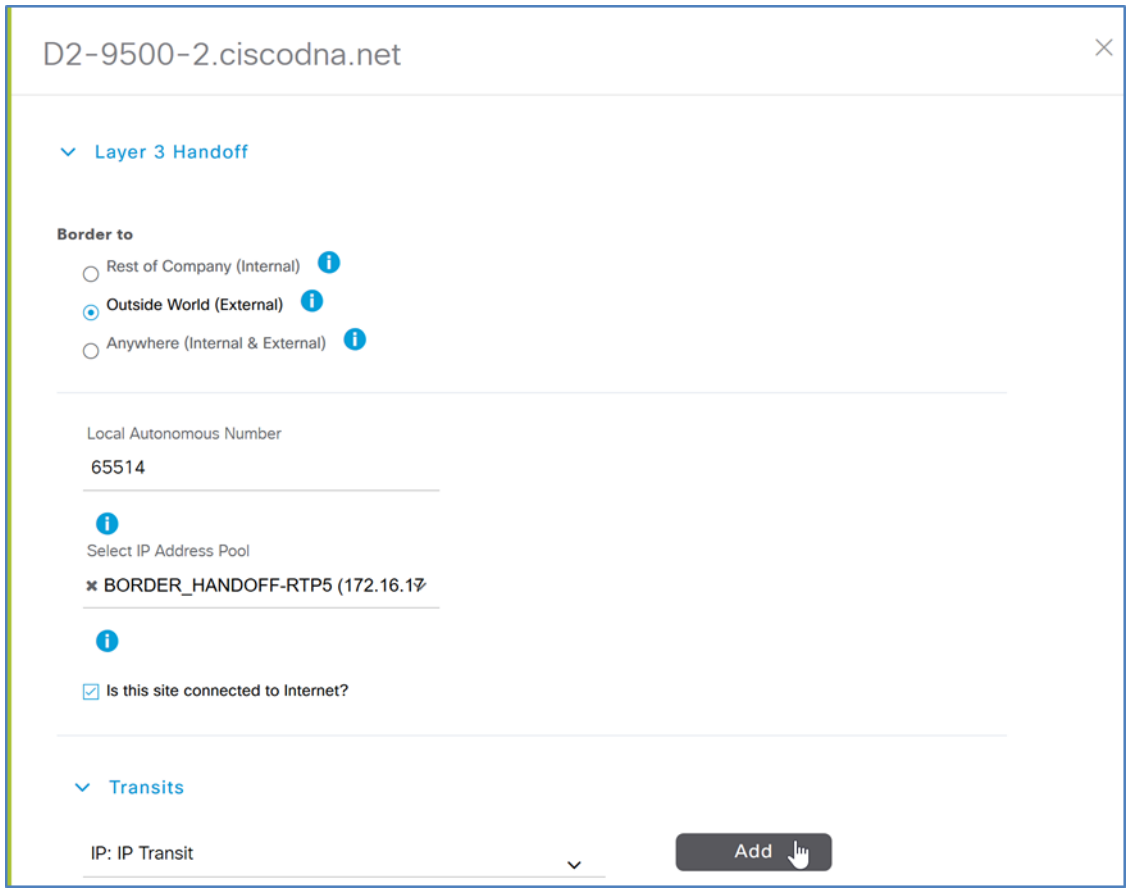
Étape 2. Si vous disposez d'un nœud de trame affecté au rôle de nœud de plan de contrôle sans fonctionnalité de frontière, cliquez dessus, puis dans la zone contextuelle, cliquez sur **Add as CP** (ajouter en tant que plan de contrôle).

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 Cisco Nexus de la gamme 7700 faisant appel au logiciel répertorié dans l'annexe A : liste des produits, vous devez utiliser des nœuds de plan de contrôle dédiés et les connecter directement à la série 7700, suivant une configuration de nœuds de frontière externe. Si votre version du système d'exploitation NX-OS le nécessite, activez la licence MPLS. Configurez le LDP MPLS sur les liaisons physiques vers les nœuds du plan de contrôle pour prendre en charge la connectivité du plan de contrôle.

Étape 3. Cliquez sur un appareil pour effectuer le rôle de frontière de trame, dans la zone contextuelle, cliquez soit sur **Add as Border** ou **Add as CP+Border** (si vous ignorez l'étape précédente) et complétez la boîte de dialogue supplémentaire. Sous **Layer 3 Handoff (transmission de couche 3)**, sélectionnez **Border** (p. ex., Outside World (External)), fournissez le numéro autonome local (**BGP Local Autonomous Number**) (p. ex., 65514), sous **Select IP Address Pool (sélectionner l'ensemble d'adresses IP**), sélectionnez l'ensemble global configuré précédemment pour la fonctionnalité de connectivité de frontière (p. ex., 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 (p. ex., pour IP : IP Transit), puis cliquez sur le bouton **Add** grisé pour ajouter.

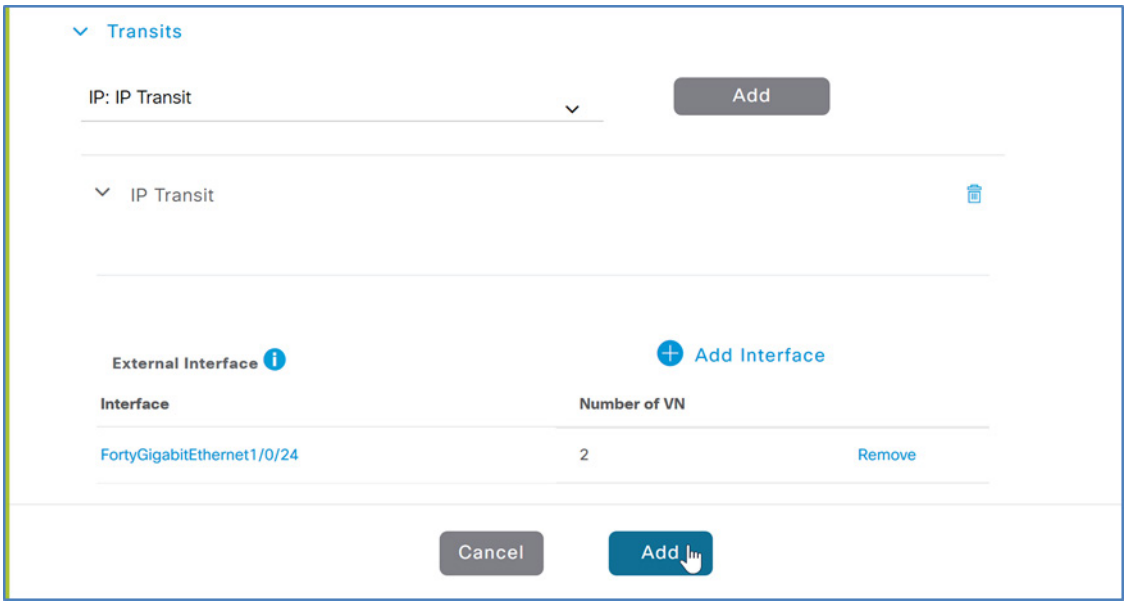


Une section supplémentaire relative au transit IP (**IP Transit**) apparaît.

Conseil technique

Si la frontière est le seul chemin pour quitter la trame jusqu'au 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 au niveau du 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** Text, cliquez sur **+ Add Interface** qui apparaît, dans la zone déroulante, sélectionnez l'interface de la connexion au routeur de fusion en dehors de la trame, sous le numéro de du système autonome distant du protocole BGP (**Remote AS Number**) pour l'appareil en dehors de la trame qui s'affiche, développez le panneau de sélection **Virtual Network (réseau virtuel)**, sélectionnez chaque réseau virtuel utilisé dans la trame pour l'ajouter au transfert de couche 3 en dehors de la trame (p. ex., INVRA_VN, OPERATIONS), cliquez sur **Save (enregistrer)**, puis sur **Add (Ajouter)**.

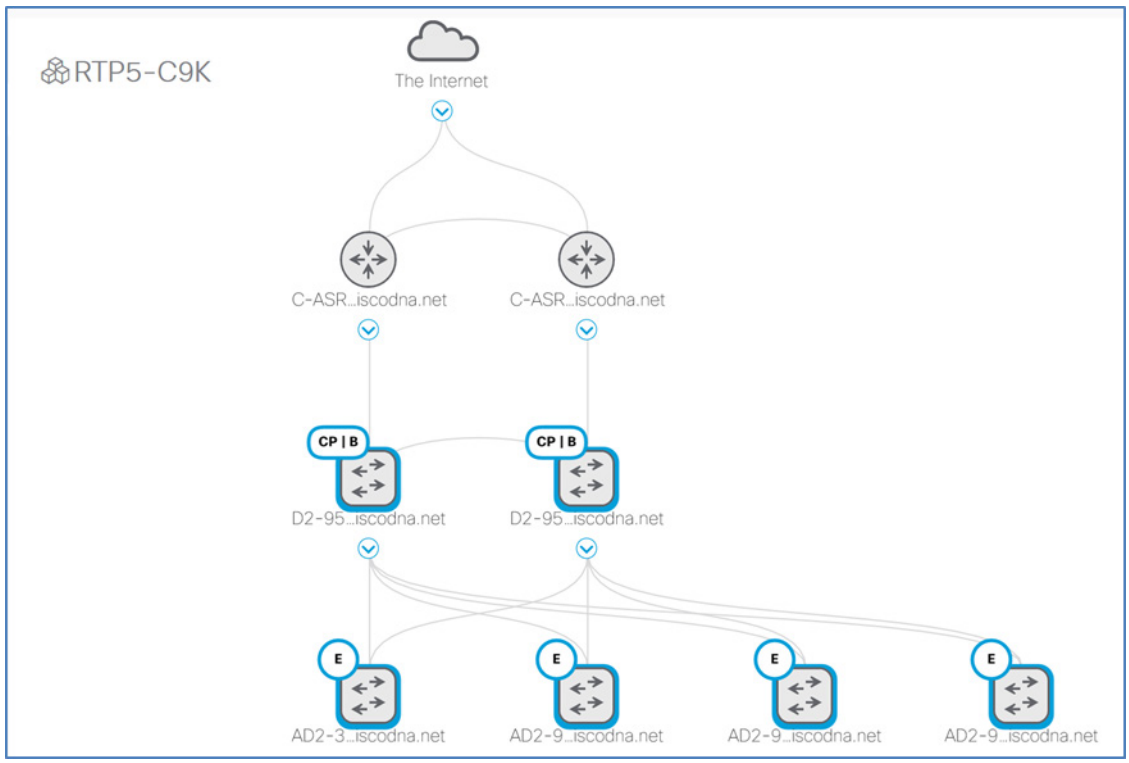


Prenez connaissance de toute information contextuelle supplémentaire.

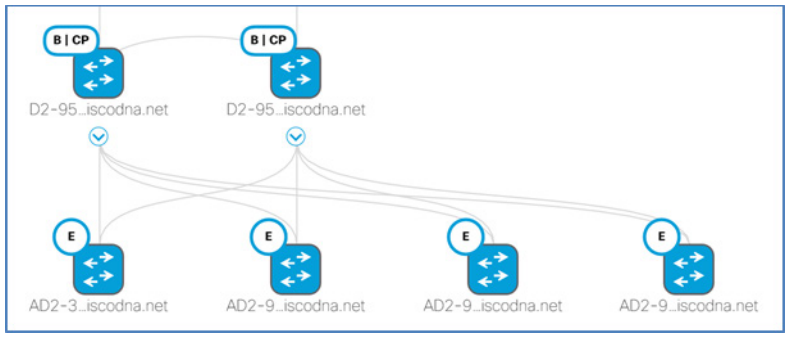
Étape 5. Si vous disposez d'un nœud de frontière de trame supplémentaire, répétez les deux étapes précédentes pour ce dernier.

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 avec balises, comme le décrivent les processus de configuration de la gestion sur un périphérique de frontière pour la détection de réseau. Lors de l'utilisation de la version d'accès défini par logiciel 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 attribués aux nœuds dans la trame, en bas, cliquez sur **Save (enregistrer)**, utilisez le choix par défaut **Maintenant (now)**, puis cliquez sur **Apply (appliquer)**. Votre domaine de trame de réseau sur site a été créé.



Les icônes de trame deviennent bleues, indiquant votre intention de créer la trame. Le provisionnement réel des périphériques peut prendre plus de temps.



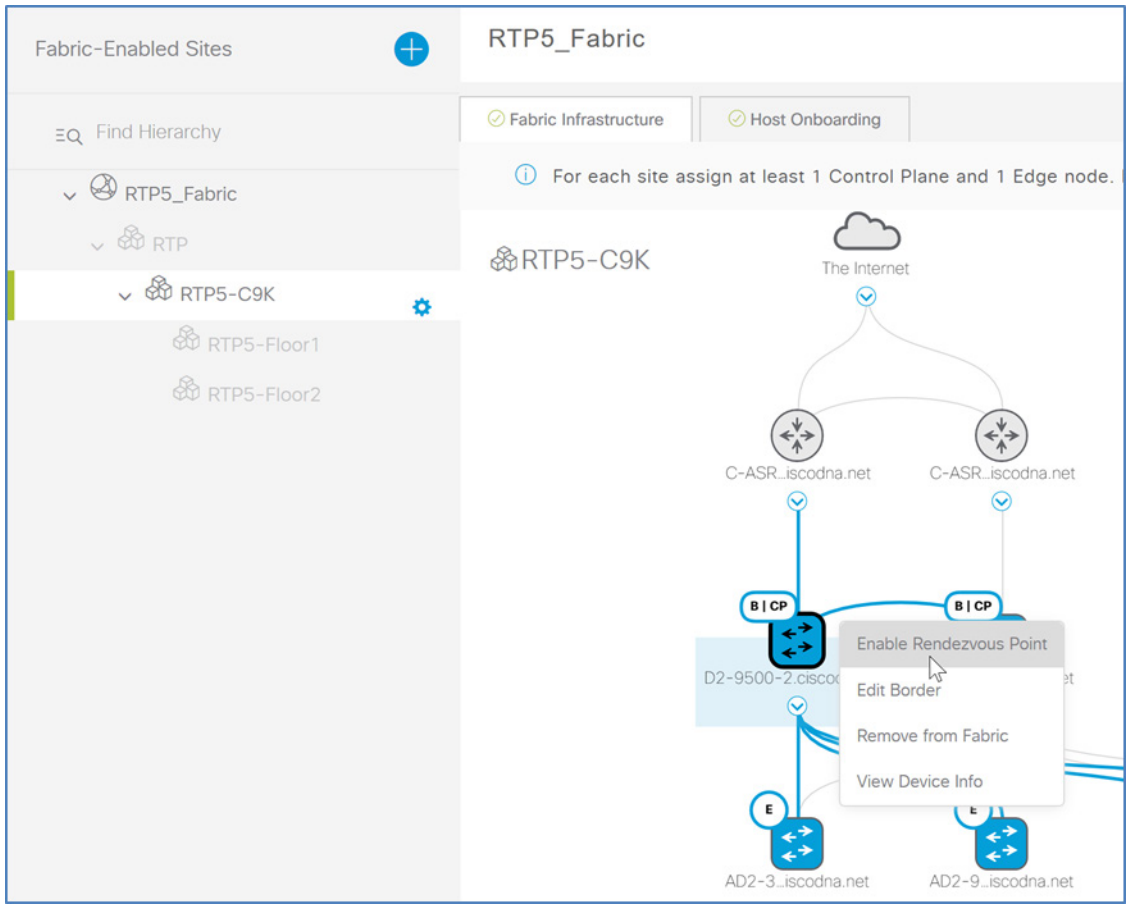
Procédure 3. Activez la multidiffusion pour la trame

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

Les trames à accès défini par logiciel peuvent prendre en charge une multidiffusion de toute source (ASM) et une multidiffusion de sources précise (SSM). Les sources peuvent se trouver dans trame ou en dehors de la trame, et la configuration du point de rendez-vous (RP) n'est disponible que sur les nœuds de frontière de trame. Les messages PIM sont en monodiffusion entre les nœuds frontières et la périphérie de trame, et les paquets de multidiffusion sont répliqués à l'extrémité des périphériques de frontière de trame vers les nœuds de périphérie de trame.

Étape 1. Un ensemble global consacré dans Cisco DNA Center aux interfaces IP de monodiffusion est utilisé pour configurer la multidiffusion pour chaque réseau virtuel où la multidiffusion est activée. S'il n'y en a pas, reportez-vous à la procédure pour définir des ensembles globaux d'adresses IP pour en créer un.

Étape 2. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabrics (trames)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de trame (p. ex., RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Fabric Infrastructure**, cliquez sur un nœud de frontière de trame, puis sélectionnez **Enable Rendezvous Point** pour activer le point de rendez-vous.



Étape 3. Dans la fenêtre contextuelle des groupes de multidiffusion associés aux réseaux virtuels (**Associate Multicast Pools to VNs**) à droite, sous Associate Virtual Networks, sélectionnez le réseau virtuel (p. ex., OPERATIONS), sous **Select IP Pools**, choisissez l'ensemble créé pour la multidiffusion (p. ex., MULTICAST_PEER-RTP5), cliquez sur **Next**, sélectionnez un réseau virtuel (p. ex., OPERATIONS), puis cliquez sur **Enable** pour l'activer.

Étape 4. Pour des nœuds de frontière de trame supplémentaires, répétez les étapes précédentes. En bas de l'écran, cliquez sur **Save (enregistrer)**, puis sur **Apply (appliquer)**.

Cisco DNA Center met en application les configurations de multidiffusion vers les nœuds de trame et crée les homologations de bouclage et de MSDP (Multicast Source Discovery Protocol) pour la communication de l'état du point RP (rendezvous point) 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 trame, à côté du nom du site, cliquez sur l'icône de l'engrenage, cliquez sur **Enable Native Multicast for IPv4 (activer la multidiffusion native pour IPv4)**, en bas cliquez sur **Save (enregistrer)**, dans la fenêtre déroulante, conservez la sélection par défaut **(Now)**, puis cliquez sur **Apply (appliquer)**.

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

Procédure 4. Activez la connectivité eBGP pour la connexion du réseau virtuel au voisin (fusion) avec le routeur de frontière

L'application d'accès défini par logiciel dans Cisco DNA Center configure le transfert BGP du nœud de frontière de trame sur les réseaux externes. Dans la version d'accès défini par logiciel décrite, vous configurez manuellement les homologues de réseau externe des appareils de frontière au moyen des informations de l'homologation VRF-Lite et du protocole BGP compatibles.

Étape 1. Utilisez l'interface de ligne de commande pour vous connecter aux appareils de frontière afin d'observer les configurations automatisées pour la connectivité IP en dehors de la frontière créée par l'application d'accès défini par logiciel du 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

Vous pouvez éviter les échecs de connectivité entre les nœuds de frontière et les routeurs de fusion en déployant une paire résiliente de nœuds de frontière reliés par une connexion directe. Pour activer la redirection du trafic automatique, créez une relation de voisinage iBGP entre les nœuds de frontière pour chaque réseau virtuel configuré. Prenez en charge plusieurs connexions logiques à l'aide du balisage 802.1Q en utilisant les configurations des ports de ligne principale sur les commutateurs et les sous-interfaces sur les routeurs.

Étape 2. Connectez-vous à chaque appareil de fusion en dehors de la trame qui est connecté à la frontière, en vous servant de la configuration des frontières comme guide, et configurez 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 trame.

```
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 configurée 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
```

Configurez-le de la même façon pour le routeur de fusion.

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

Conseil technique

Le nom de 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 sur le voisin. Certains appareils prennent en charge la configuration de la sous-interface VLAN directement sur les lignes principales, et d'autres périphériques nécessitent que des interfaces VLAN soient créées et associées à une ligne principale. 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 configurée 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 au tableau de routage global.

```
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 de BGP vers la frontière pour prendre en charge la connectivité de chaque VRF associé à chaque réseau virtuel dans la trame.

```
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 configurée 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
```

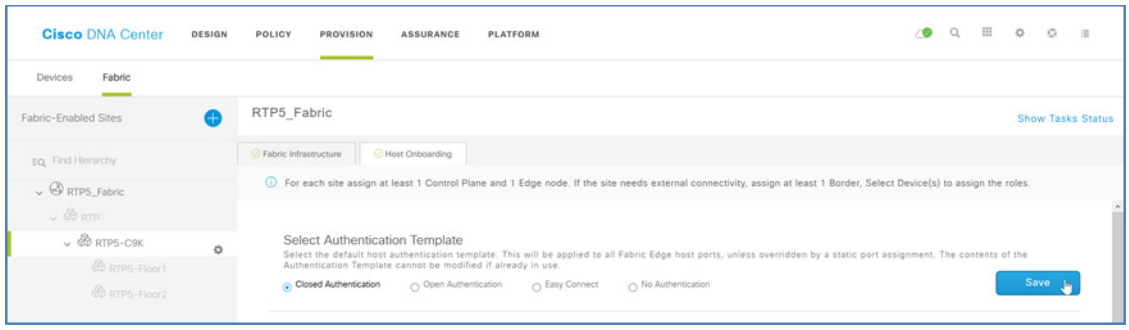
Configurez les éléments suivants sur le routeur de fusion :

```
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
```

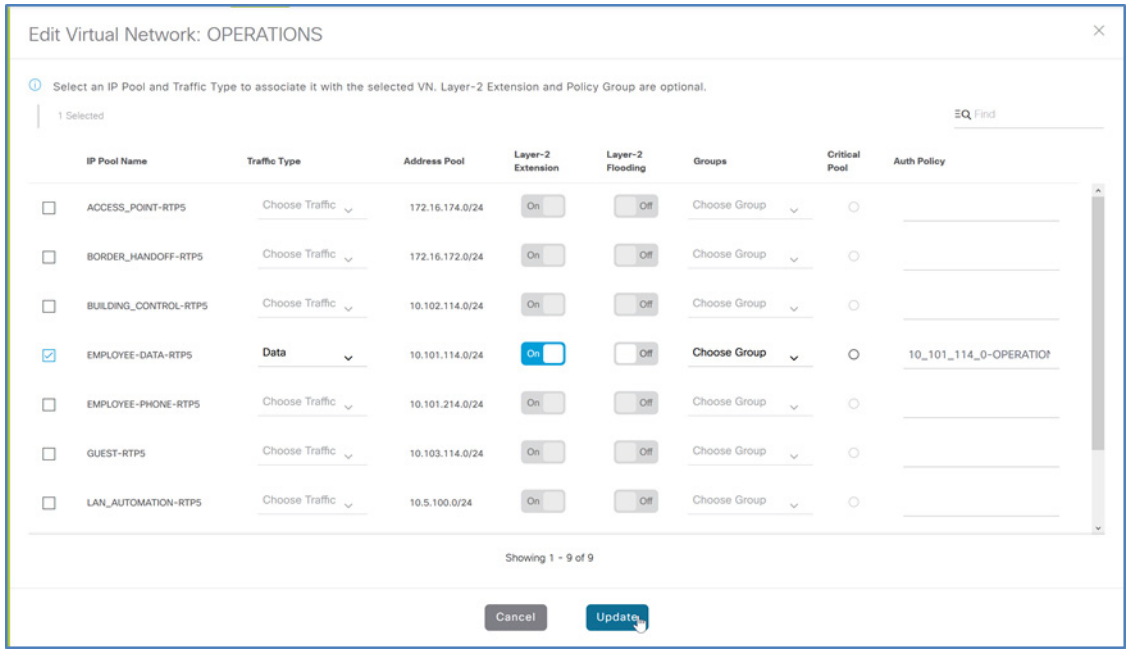
Procédure 5. Affectez des clients filaires au réseau virtuel et activez la connectivité

Étape 1. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabrics (trames)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de trame (p. ex., RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Host Onboarding**, sous **Select Authentication template**, choisissez **Closed Authentication**, puis en haut cliquez sur **Save** et ensuite **Apply** pour enregistrer et appliquer.



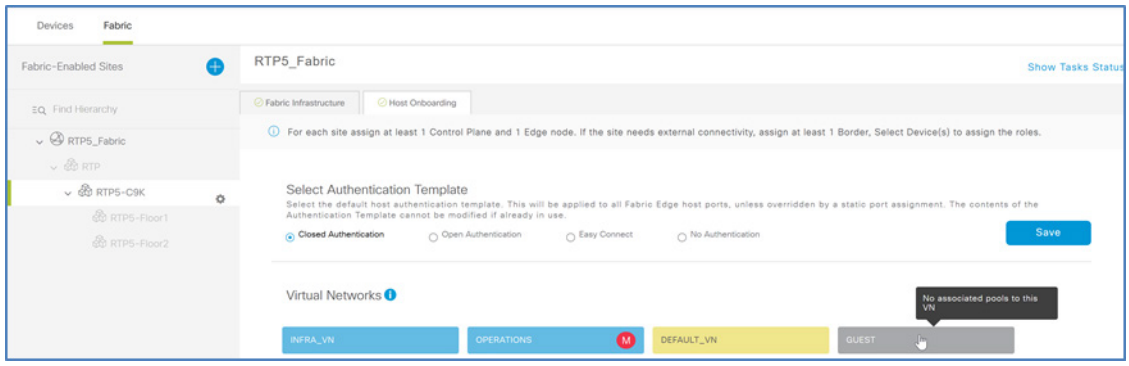
L'authentification fermée (Closed Authentication) est définie par défaut pour les ports hôtes, ce qui nécessite une authentification 802.1x pour qu'un terminal se connecte à la trame; ce paramètre peut être remplacé par un port destiné à d'autres fins, par exemple, les ports de points d'accès.

Étape 2. Sous **Virtual Networks (réseaux virtuels)**, sélectionnez un réseau à utiliser pour les clients filaires (p. ex., : OPERATIONS), dans le panneau déroulant pour modifier le réseau virtuel des opérations (**Edit Virtual Network: *OPERATIONS***), sélectionnez les noms des ensembles d'adresses IP (**IP Pools**) à ajouter au réseau virtuel (p. ex., EMPLOYEE-DATA-RTP5), sélectionnez un type de trafic (**Traffic Type**) de données (**Data**), assurez-vous que l'extension de couche 2 (**Layer 2 Extension**) est activée (**On**). Vous pouvez aussi choisir de modifier le nom de la politique d'authentification (**Auth Policy**) pour qu'il soit significatif pour le site, cliquez sur **Update (mettre à jour)**, puis cliquez sur **Apply (appliquer)**.

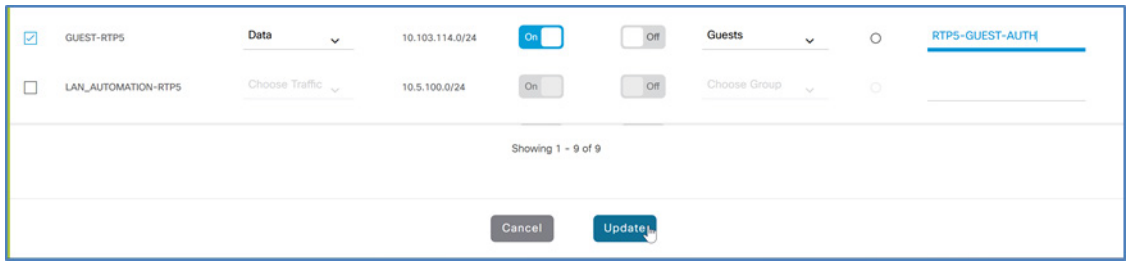


Un message d'état s'affiche, puis l'écran **Host Onboarding** s'affiche.

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



Étape 4. Dans le panneau déroulant pour modifier le réseau virtuel des opérations (**Edit Virtual Network: *GUEST***), sélectionnez les noms des ensembles d'adresses IP (**IP Pools**) à ajouter au réseau virtuel (p. ex., EMPLOYEE-DATA-RTP5), sélectionnez un type de trafic (**Traffic Type**) de données (**Data**), assurez-vous que **l'extension de couche 2** (Layer 2 Extension) est activée (**On**). Vous pouvez aussi choisir de modifier le nom de la politique d'authentification (**Auth Policy**) 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** s'affiche.

Procédure 6. Activez les ports de périphérie de trame pour l'intégration des clients

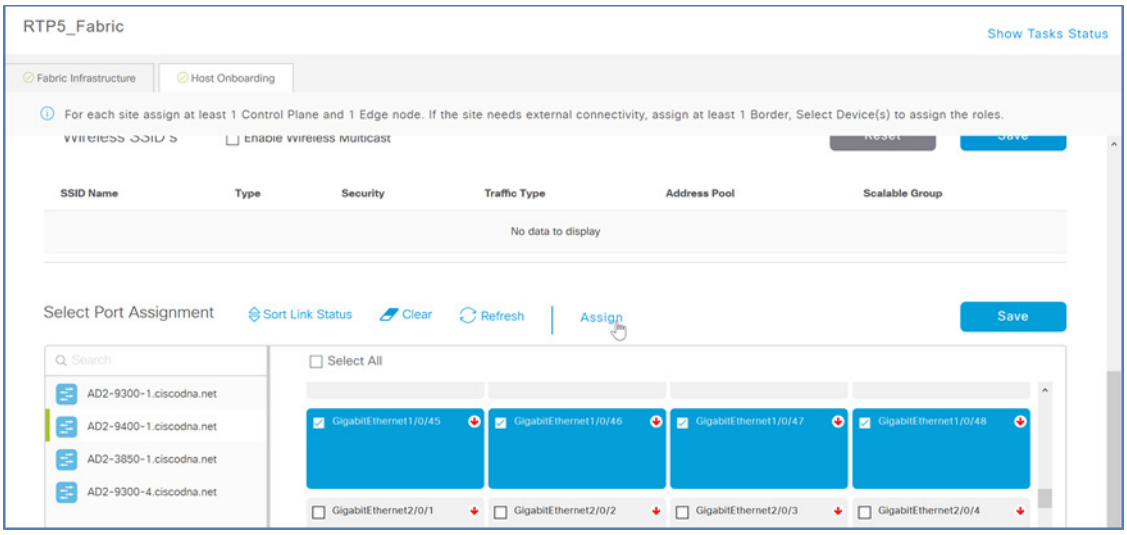
Facultatif

Remplacer le modèle d'authentification par défaut (authentification fermée, ou Closed Authentication) attribué 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 appareils connectés à l'IOT ou lors de l'attribution manuelle d'un ensemble d'adresses à un port.

Répétez cette procédure pour chaque commutateur de périphérie de trame avec les clients qui se connectent aux ports de périphérie de trame, ce qui nécessite un remplacement du modèle d'authentification par défaut.

Étape 1. Accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabrics (trames)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche, cliquez sur le site de trame (p. ex., RTP5-C9K), en haut de l'écran, cliquez sur l'onglet **Host Onboarding**, et sous **Select Port Assignment**, dans la colonne de auche, choisissez un commutateur.

Étape 2. Dans la liste des ports de commutateur, sélectionnez un ensemble de ports de périphérie de trame filaire pour participer à un réseau virtuel de trame, puis cliquez sur **Assign (attribuer)**.



Étape 3. Dans l'encadré déroulant, sélectionnez le **type d'appareil connecté** approprié (par exemple : appareils utilisateur (IP-téléphone, ordinateur, ordinateur portable)), sélectionnez le **pool d'adresses** (par exemple : 10_101_114_0 (employee-Data-RTP5)), sélectionnez le **groupe** (exemple : Employees), sélectionnez un **pool de voix** si nécessaire, sélectionnez un **modèle d'authentification** (exemple : aucune authentification), puis cliquez sur **mettre à jour**.

Étape 4. À droite de la section **Select Port Assignment**, sélectionnez **Save (enregistrer)**, conservez la sélection par défaut **Now (maintenant)**, puis cliquez sur **Apply (appliquer)**.

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

Les périphériques peuvent désormais se connecter aux ports de périphérie de trame au moyen de la superposition de réseau filaire et de la méthode d'authentification créée.

Conseil technique
L'attribution de groupe est utilisée pour attribuer un groupe de manière statique si le port de périphérie de la trame ne reçoit pas son attribution dynamiquement à l'aide d'un serveur d'authentification, ce qui est utile pour certains types de périphériques utilisés dans une entreprise. Si l'option « aucune authentification » (No Authentication) est sélectionnée comme méthode d'authentification, Cisco DNA Center met en application le modèle d'authentification global par défaut sélectionné dans la section « Select Authentication template » en haut de l'écran. Cisco DNA Center applique la configuration des ports lorsque vous sélectionnez l'authentification fermée (Closed Authentication), mais aussi lorsque vous sélectionnez « Open Authentication » (authentification ouverte).

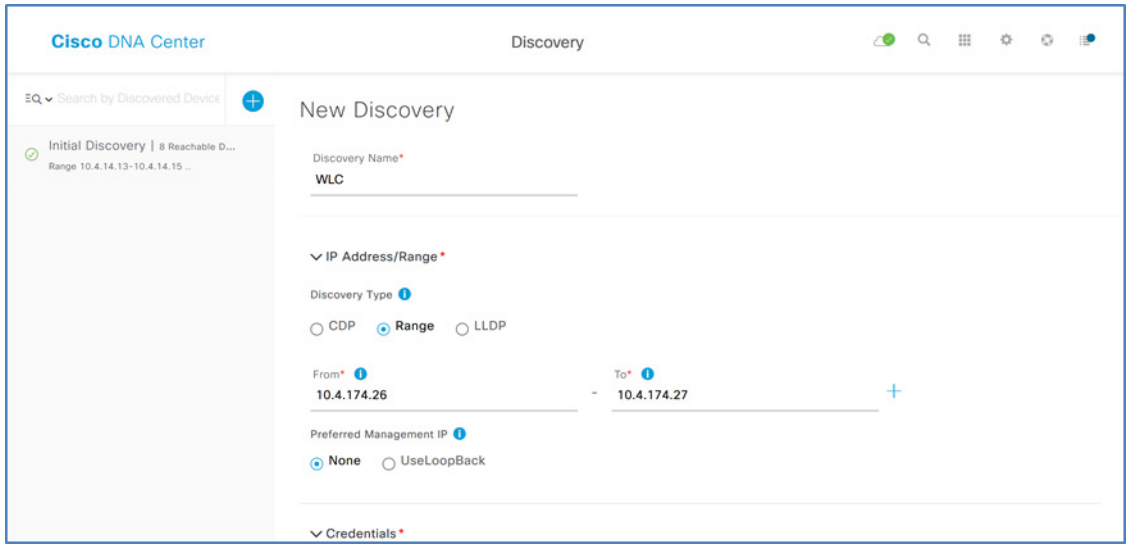
Processus : intégration de la technologie d'accès sans fil défini par logiciel dans la trame

Le processus d'installation des contrôleurs LAN sans fil pour l'accès défini par logiciel est décrit dans le Guide de déploiement normatif de l'accès défini par logiciel pour les réseaux décentralisés. Ce processus d'intégration sans fil suppose que les contrôleurs sont disponibles pour s'intégrer dans la trame à l'aide de Cisco DNA Center.

Procédure 1. Ajoutez les contrôleurs sans fil dans l'inventaire et créez une paire SSO HA.

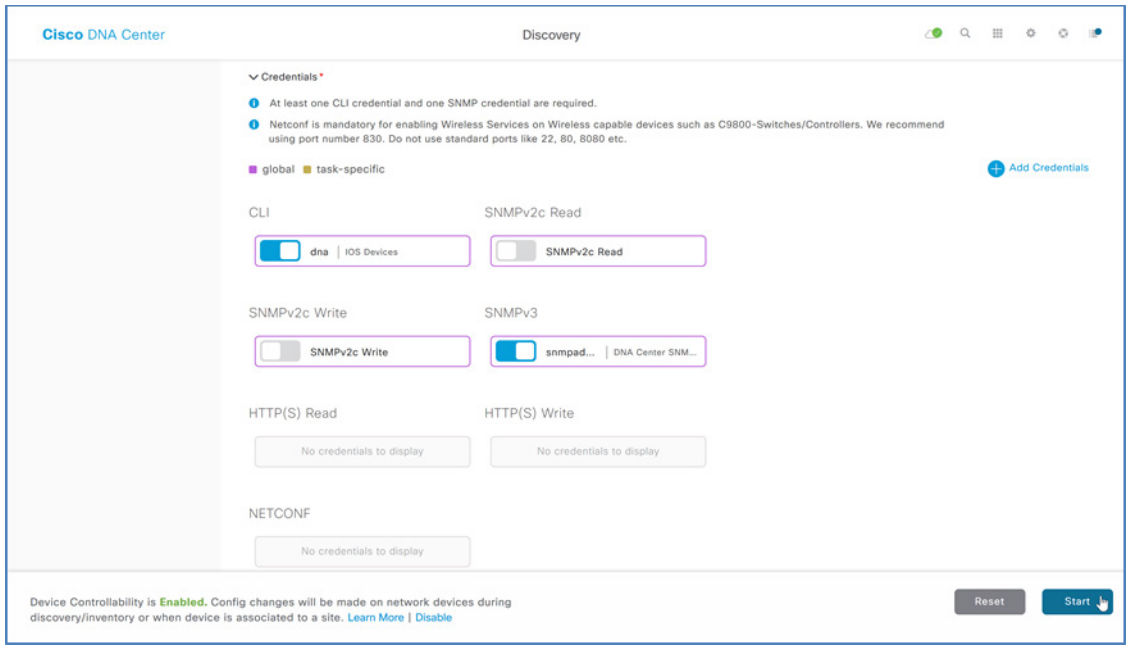
Si les contrôleurs LAN sans fil ne se trouvent pas dans l'inventaire Cisco DNA Center, vous devez les ajouter avant l'intégration sans fil. Pour la résilience, vous devez également utiliser deux WLC de même type pour créer une paire SSO HA.

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 nom de détection (**Discovery Name**). Sélectionnez la plage (**Range**) et saisissez une adresse IP de bouclage de début et de fin pour les plages d'adresses IP (**IP Ranges**) (pour couvrir une seule adresse, saisissez cette adresse pour le début et la fin de la plage). Pour ce qui concerne l'adresse IP de gestion préférée (**Preferred Management IP**), utilisez **None (aucune)**.

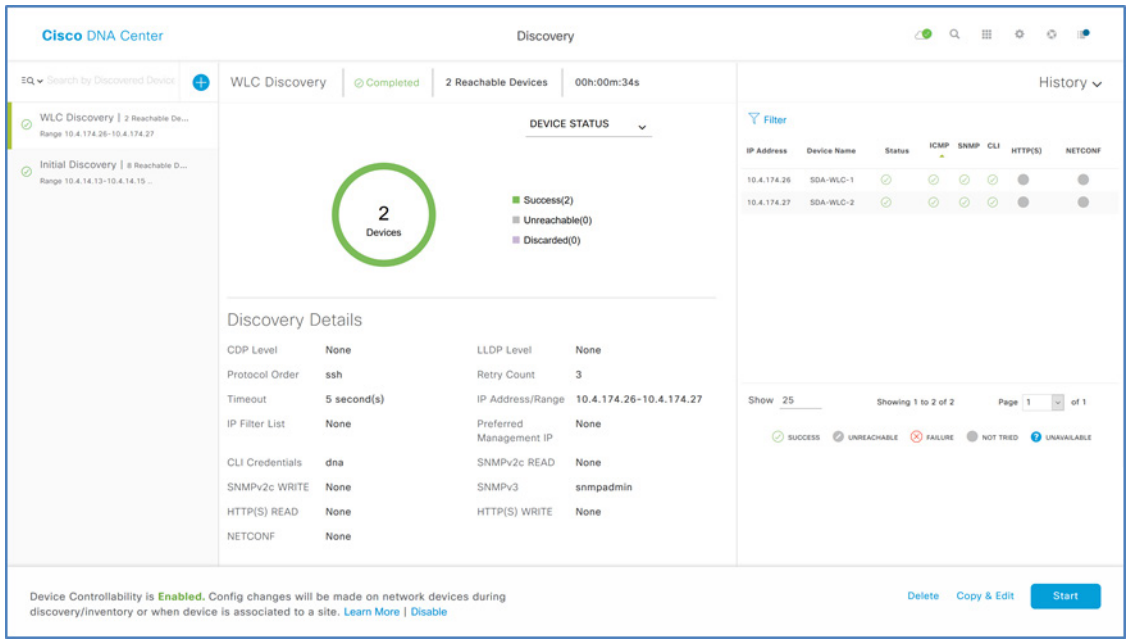


Étape 2. Si vous avez des plages supplémentaires, à côté de la première plage, cliquez sur **+** (signe plus), saisissez la plage supplémentaire et répétez l'opération pour toutes les plages restantes.

Étape 3. Faites défiler l'écran pour vérifier les coordonnées d'authentification de l'interface de ligne de commande utilisées pour la détection et les configurations des coordonnées d'authentification SNMP envoyées au périphérique par la fonction de contrôle de l'appareil (Device Controllability). Si vous avez des coordonnées d'authentification propres à la détection des appareils, cliquez sur **+ Add Credentials**, ajoutez chaque nouvelle information, enregistrez les changements, 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, réglez le problème et redémarrez la détection pour ces appareils, 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, dans la section **Tools (outils)**, cliquez sur **Inventory (inventaire)**. Les appareils détectés s'affichent. Une fois la collecte d'inventaire terminée, chaque périphérique affiche un état de synchronisation **géré**, ce qui signifie que Cisco DNA Center gère un modèle interne qui reproduit le déploiement physique de l'appareil.

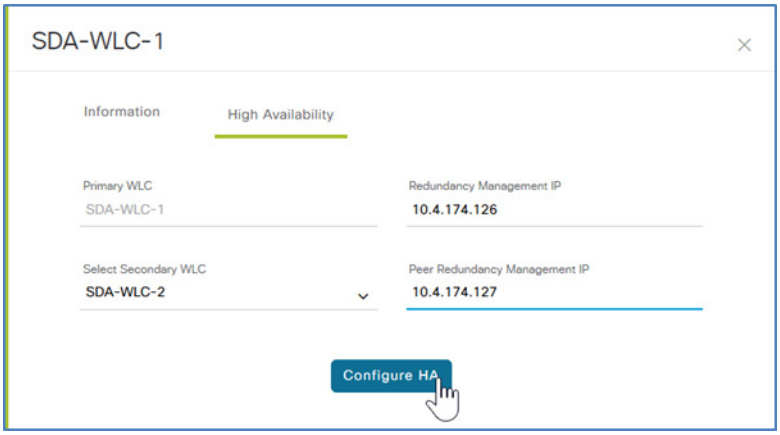
Cisco DNA Center peut désormais accéder aux périphériques, synchroniser l'inventaire de configuration et apporter des modifications de configuration aux périphériques.

Conseil technique

Sur le côté droit de la ligne de titre du tableau d'inventaire, vous pouvez modifier les colonnes affichées. Utilisez la colonne **Device Role** pour voir le rôle d'appareil attribué par la détection en fonction du type d'appareil et pour ajuster le rôle de manière à refléter le déploiement réel d'un périphérique, tel que l'accès, la distribution, le cœur ou le routeur de frontière, dans le cas où le routeur de frontière dans cet écran a un rôle de périphérique générique ne faisant pas partie de la trame. Le réglage du rôle permet désormais d'améliorer l'apparence des cartes topologiques initiales, plutôt que d'ajuster les rôles dans des procédures ultérieures. Pour les WLC, l'attribution au rôle de base permet de rapprocher l'appareil de l'emplacement par défaut de ces appareils.

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

Étape 6. Si vous créez une paire de contrôle d'accès à haute disponibilité (SSO HA) avec un ensemble de contrôleurs qui ne sont pas associés actuellement, accédez au tableau de bord principal Cisco DNA Center, allez à **PROVISION > Devices > Inventory**, cliquez sur le texte du nom de l'appareil du WLC principal (**Device Name**, par exemple, SDA-WLC1), à droite dans le menu contextuel en haut de l'écran, sélectionnez **High Availability (haute disponibilité)**, sous **Select Secondary WLC**, sélectionnez le deuxième WLC dans la paire SSO HA (p. ex., SDA-WLC-2), fournissez l'adresse IP de gestion de la redondance (**Redundancy Management IP**) et le protocole IP de gestion de la redondance des homologues (**Peer Redundancy Management IP**) (p. ex., 10.4.174.126, 10.4.174.127), cliquez sur **Configure HA**, puis cliquez sur **OK**dans la fenêtre contextuelle d'avertissement de redémarrage.



Dans le navigateur, les 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 Actualiser en haut de l'écran pour actualiser l'affichage jusqu'à ce que les WLC en mode HA s'affichent en tant qu'appareil unique. Vérifiez l'état de la haute disponibilité en cliquant sur le texte du nom de l'appareil (**Device Name**) du WLC principal (p. ex., SDA-WLC1), sur le côté droit de la fenêtre contextuelle en haut, sélectionnez **High Availability (haute disponibilité)**, puis vérifiez que l'état de la redondance (**Redundancy State**) est défini pour **SSO**et que l'état de la synchronisation (**Sync Status**) est **Complete (terminé)**.

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 pour consulter **DESIGN (conception) > Image Repository (référentiel d'images)**. Recherchez la famille de périphériques et vérifiez la version du logiciel. Si l'image du WLC est la version correcte, continuez. Si l'image doit être mise à jour et que l'image est répertoriée, cliquez sur l'étoile à côté de l'image pour marquer l'image 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, suivez les instructions pour importer, actualiser l'écran, et utilisez le menu déroulant de l'appareil pour marquer l'image.

Étape 9. Si vous mettez à jour l'appareil, accédez à **PROVISION (configuration) > Devices (appareils) > Inventory (inventaire)**, sélectionnez le WLC marqué comme obsolète (**Outdated**), puis dans le menu **Actions**, cliquez sur **Update OS Image (mettre à jour l'image du système d'exploitation)**. Confirmer la sélection de l'appareil à mettre à jour, utiliser la valeur par défaut **du moment d'exécution**, qui est réglée sur **Now (maintenant)**, cliquez sur **Appliquer (apply)**, puis, dans la fenêtre contextuelle de l'avertissement sur les appareils en cours de redémarrage, cliquez sur **OK**.

Les images sont distribuées au périphérique sélectionné, puis le périphérique redémarre pour activer la nouvelle image dès que la distribution de l'image est terminée. Utilisez le bouton **Refresh (actualiser)** pour observer la suppression de l'état en cours (**In Progress**).

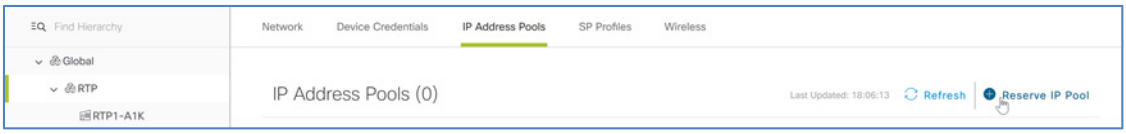
Procédure 2. Créer des ensembles d'adresses IP pour les points d'accès

Vérifiez qu'un ensemble global est disponible dans Cisco DNA Center pour l'attribution d'adresses pour les points d'accès à gérer par le réseau.

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

Étape 2. S'il n'existe pas d'ensemble pour les points d'accès, cliquez sur **+ Add IP Pool**, renseignez le champ **IP Pool Name (nom de l'ensemble d'adresses IP)**, **IP Subnet (sous-réseau IP)**, **CIDR Prefix**et **Gateway IP address (adresse IP de passerelle)** (p. ex., ACCESS_POINT, 172.16.173.0, /24, 172.16.173.1), sélectionnez le serveur DHCP (**DHCP Server**) et le serveur DNS (**DNS Server**), puis cliquez sur **Save (enregistrer)**.

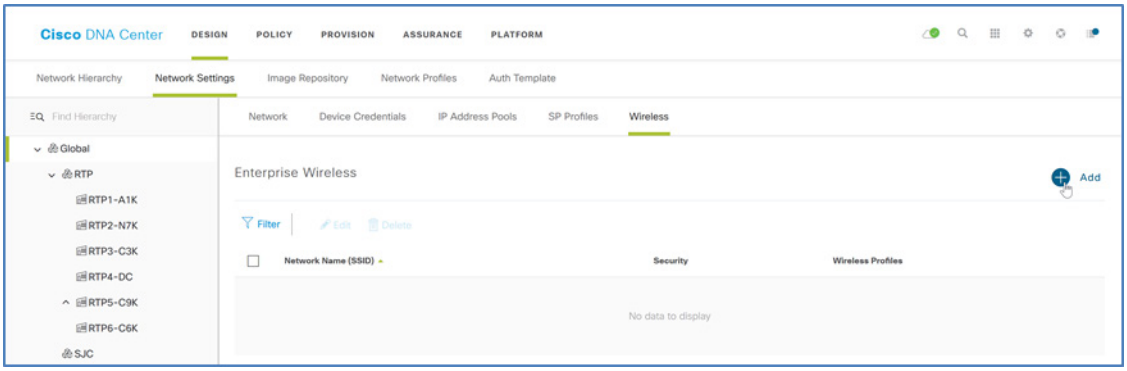
Étape 3. Accédez à **DESIGN (conception) > Network Settings (paramètres réseau) > IP Address Pools (ensembles d'adresses IP)**, à gauche dans la hiérarchie du site, sélectionnez un site ou un niveau inférieur pour la réservation d'un ensemble d'adresses IP (p. ex., RTP5-C9K). Si l'ensemble n'est pas encore réservé, dans le coin supérieur droit, cliquez sur Reserve IP Pool.



Étape 4. Si vous réservez un ensemble renseignez le champ **IP Pool Name (nom d'un ensemble IP)** (p. ex., ACCESS_POINT-RTP5), sous **Type**, sélectionnez **LAN**, puis sélectionnez la source de réservation de l'ensemble global des adresses IP (**Global IP Pool**), puis sous **CIDR Notation / No. of IP Addresses**, sélectionnez la partie de l'espace d'adressage à utiliser, attribuez une adresse IP de passerelle (**Gateway IP Address**), le ou les serveurs DHCP (**DHCP Server(s)**) et le ou les serveurs DNS (**DNS Servers(s)**) puis cliquez sur **Reserve (réserver)**.

Procédure 3. Concevoir les SSID sans fil d'entreprise pour la trame

Étape 1. Dans le tableau de bord principal de Cisco DNA Center, naviguez jusqu'à **DESIGN (conception) > Network Settings (paramètres réseau) > Wireless (sans fil)**, à gauche dans la hiérarchie du site, puis sélectionnez le niveau **Global (général)**, dans la section **Enterprise Wireless (sans fil d'entreprise)** et cliquez sur **+ Add (ajouter)**.



L'assistant de **création d'un réseau sans fil d'entreprise** s'affiche.

Étape 2. À l'aide de l'assistant de **création d'un réseau sans fil d'entreprise**, entrez les informations suivantes :

- **Wireless Network Name (nom du réseau sans fil) (SSID)** (p. ex. : Employee)
- Sous **TYPE OF ENTERPRISE NETWORK (type de réseau d'entreprise)**, sélectionnez Voice and Data (voix et données) et Fast Lane (voie rapide).
- Sélectionnez ou confirmez **WIRELESS OPTION (option sans fil)**
- Pour le **niveau de sécurité** sélectionnez une option (p. ex. : WPA2 Enterprise)
- Sous **ADVANCED SECURITY OPTIONS (options de sécurité avancées)**, sélectionnez Adaptive (capacité d'adaptation)

Étape 3. Cliquez sur **Next (suivant)** pour continuer dans l'assistant et entrez les informations suivantes :

- **Wireless Profile Name (nom de profil sans fil)** (p. ex. : RTP5-Wireless)
- Sous **Fabric (trame)**, sélectionnez **Yes (oui)**
- Sous **Choose a site (choisir un site)**, sélectionnez l'emplacement de diffusion du SSID (p. ex. : Global/RTP/RTP5-C9K) et inscrivez les étages à ajouter à la couverture du SSID (p. ex. : Global/RTP/RTP5-C9K/Floor 1)

Étape 4. Cliquer 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 autres SSID en 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 invité pour la trame

Étape 1. Naviguez jusqu'à **DESIGN (conception) > Network Settings (paramètres réseau) > Wireless (sans fil)**, puis cliquez sur **+ Add (ajouter)** dans la section **Guest Wireless (sans fil invité)** qui se trouve dans l'assistant de **création d'un réseau sans fil invité**, et entrez les informations suivantes :

- **Wireless Network Name (nom du réseau sans fil) (SSID)** (p. ex. : 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 **nom du profil** correspondant à l'emplacement du déploiement (p. ex. : RTP5-Wireless), puis conservez la sélection de **Yes (oui)** dans le panneau déroulant **Fabric (trame)** ainsi que les autres informations par défaut, et cliquez sur **Save (enregistrer)** en bas du panneau, puis sur **Next (suivant)**.

Étape 3. À l'étape **Portal Customization (personnalisation du portail)**, cliquez sur **+ Add (ajouter)**. L'écran de **création de portails** s'affiche.

Étape 4. Indiquez un nom pour **Guest Portal (portail invité)** (p. ex. : Guest-RTP5), puis personnalisez l'écran au besoin et, en bas de l'écran, cliquez sur **Save (enregistrer**). Un portail d'authentification Web invité est généré pour le site et vous êtres redirigé à l'écran précédent.

Étape 5. Cliquez sur **Terminer**.

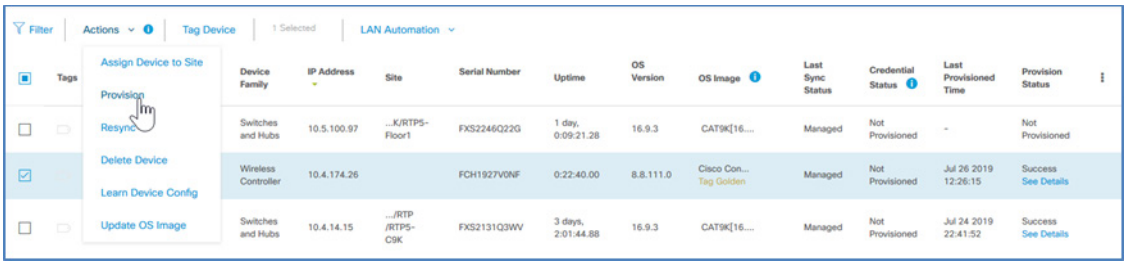
La conception du réseau LAN sans fil est créée et est prête à être déployée.

Procédure 5. Mettre le contrôleur WLC à disposition pour l'intégration de la trame sans fil SD-Access

Une fois la conception du réseau sans fil SD-Access terminée, poussez la configuration de l'application de conception vers le contrôleur WLC.

Étape 1. Naviguez jusqu'à PROVISION (mise à disposition) > Devices (appareils) > Inventory (inventaire), puis repérez le contrôleur WLC et cochez la case correspondante, puis, dans le menu déroulant Actions en haut de l'écran, sélectionnez Provision (mise à disposition). L'assistant de mise à disposition des appareils s'affiche.

Conseil technique
Lorsqu'un jumelage de contrôleurs WLC est configuré en mode HA SSO, un seul contrôleur WLC apparaît dans l'inventaire de Cisco DNA Center. Vous pouvez vérifier la configuration du jumelage HA SSO en cliquant sur le nom de l'appareil, puis sur l'onglet **High Availability (haute disponibilité)**.



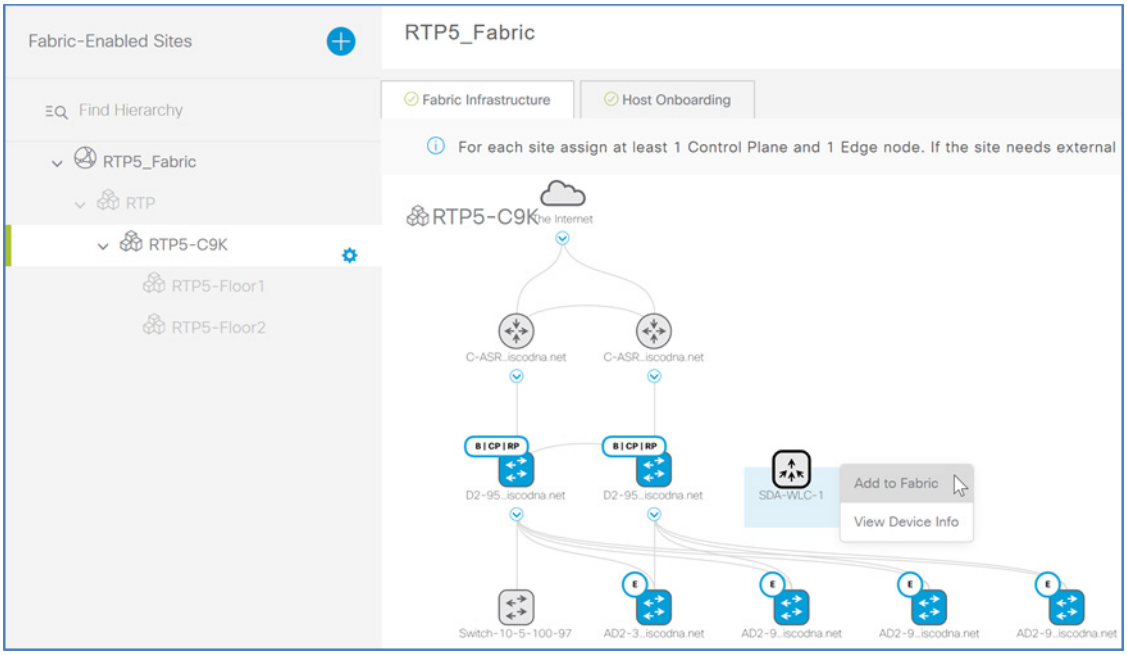
Étape 2. Affectez le site (p. ex : Global/RTP/RTP5-C9K), puis cliquez sur **Next (suivant)**. À l'étape **Configuration**, sélectionnez les étages supplémentaires à affecter pour les points d'accès gérés par le contrôleur WLC (p. ex. : Global/RTP/RTP5-C9K/Floor 1) sous **Managed AP Location (emplacement de points d'accès gérés)**, puis cliquez sur **Next (suivant)**, et à nouveau sur **Next (suivant)** à l'étape **Advanced Configuration (configuration avancée)**.

Étape 3. À l'étape **Summary (récapitulation)**, passez en revue les configurations, puis cliquez sur **Deploy (déployer)** et, dans le panneau déroulant, conserver la sélection par défaut de **Now (maintenant)** et cliquez sur **Apply (appliquer)**.

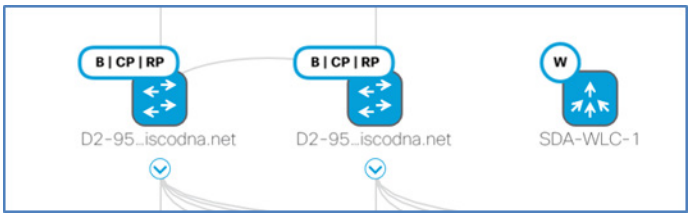
Le contrôleur WLC est affecté au site et la mise à disposition commence. Utilisez le bouton **Refresh (actualiser)** jusqu'à ce que l'état **Provision Status** n'affiche **Success (réussite)** avant de continuer.

Procédure 6. Mettre à disposition le réseau sans fil SD-Access dans la trame

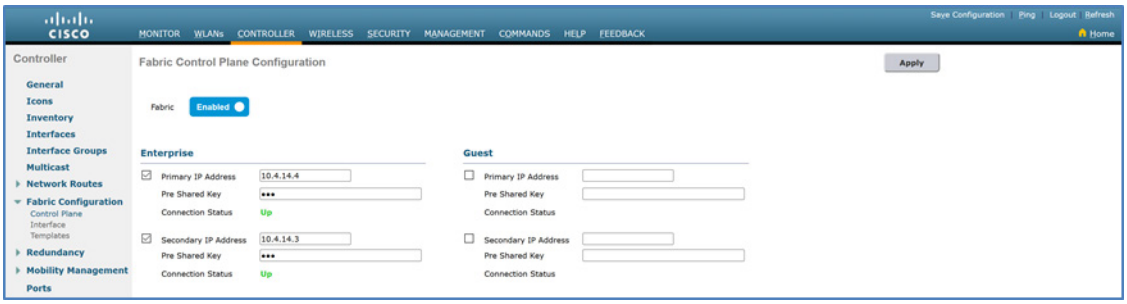
Étape 1. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabric (trame)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche **Fabric-Enabled Sites**, cliquez sur le site connexe (p. ex., Global/RTP/RTP5-C9K), cliquez sur le contrôleur WLC, puis cochez la case **Add to Fabric (ajouter à la trame)**.



Étape 2. En bas de l'écran, cliquez sur **Save (enregistrer)**, conservez la sélection par défaut **Now (maintenant)** dans le menu déroulant, puis cliquez sur **Apply (appliquer)**. Les configurations du contrôleur WLC sont créées pour établir une connexion sécurisée au panneau de contrôle de la trame.



Vous pouvez vérifier que le jumelage du contrôleur WLC est intégré dans la trame à partir de la console de gestion du contrôleur WLC en naviguant jusqu'à **CONTROLLER (contrôleur) > Fabric configuration (configuration de la trame) > Control Plane (panneau de contrôle)**, qui indique que l'intégration de la trame est activée (voir l'état de la connexion).



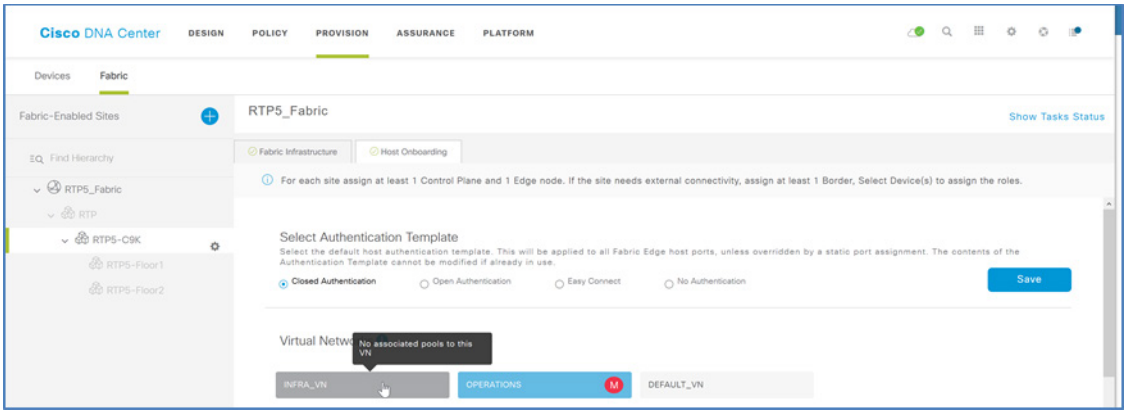
Procédure 7. Activer l'intégration des points d'accès dans la trame sans fil

Les points d'accès sont des hôtes qui rejoignent la trame et sont affectés à un réseau virtuel nommé INFRA_VN. Ce réseau virtuel spécial pour les dispositifs d'infrastructures, tels que les points d'accès, permet la communication de gestion entre les points d'accès au niveau des nœuds de périphérie de la trame à l'aide du panneau de contrôle de la trame et du contrôleur WLC situé à l'extérieur de la trame dans le cadre de la connectivité de routage global.

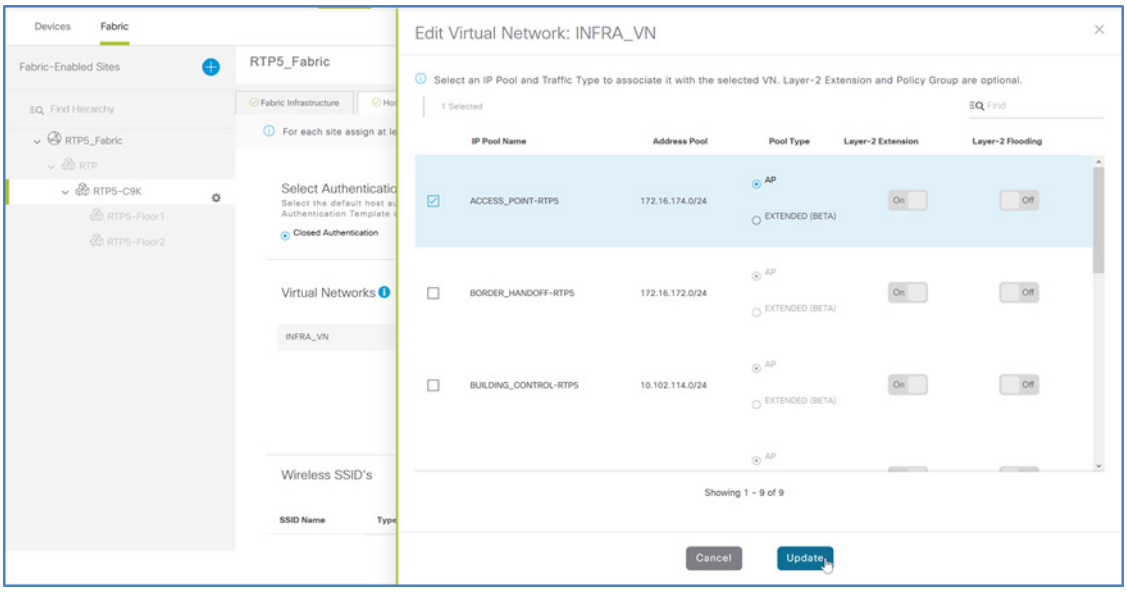
Étape 1. Connectez les points d'accès à utiliser pour la trame directement à un nœud de périphérie dans la trame.

Étape 2. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabric Domains (domaines de trame)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche **Fabric-Enabled Sites**, cliquez sur le site connexe (p. ex., Global/RTP/RTP5-C9K), puis cliquez sur **Host Onboarding (intégration de l'hôte)**.

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

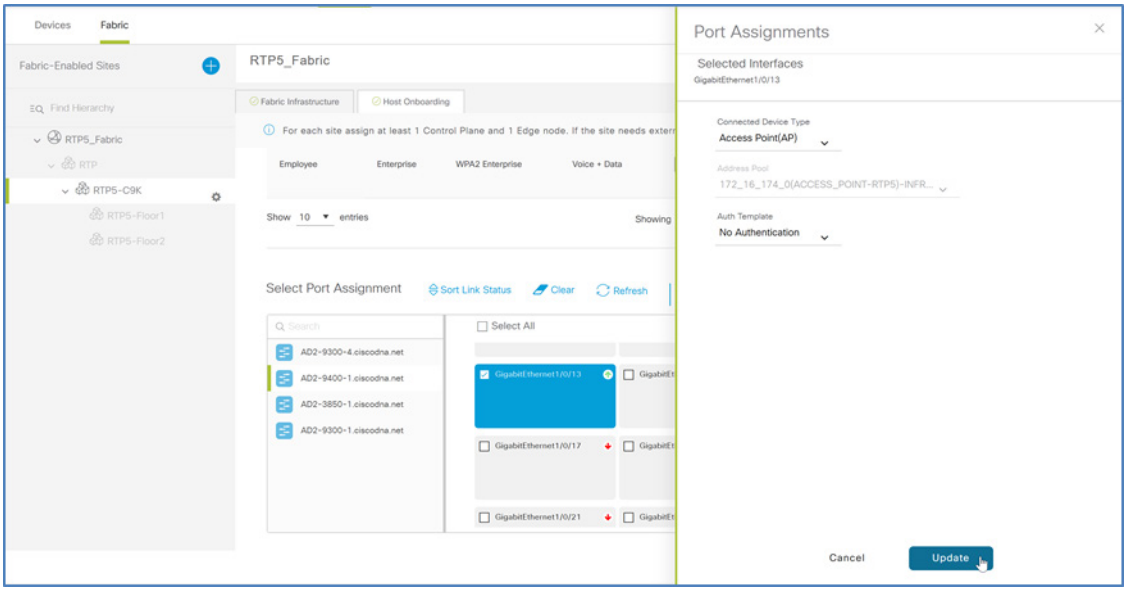


Étape 4. Cochez la case adjacente au nom de l'ensemble d'adresses IP pour les points d'accès (par exemple : ACCESS_POINT-RTP5), sous **Pool Type (type d'ensemble)**, sélectionnez **AP (point d'accès)**, puis cliquez sur **Update (mettre à jour)**.



Étape 5. Dans le panneau déroulant Modify Virtual Network (modifier le réseau virtuel), maintenez la sélection par défaut **Now (maintenant)**, puis cliquez sur **Apply (appliquer)**.

Étape 6. Sous **Select Port Assignment (sélectionner l'attribution des ports)**, sélectionnez un commutateur, sélectionnez les ports du commutateur à utiliser pour les points d'accès, sélectionnez **Assign (affecter)**, dans le panneau déroulant **Port Assignments (affectation des ports)**, sous **Connected Device Type (type de périphérique connecté)**, sélectionnez **Access Point (AP) (point d'accès)**, conservez le sélection **Address Pool (ensemble d'adresses)** par défaut, sous **Auth Template (modèle d'authentification)**, sélectionnez **No Authentication (aucune authentification)**, puis cliquez sur **Update (mettre à jour)**.



Conseil technique

Cisco DNA Center permet l'intégration automatique des points d'accès par la configuration d'une macro CDP sur les commutateurs de périphérie de trame lorsque le modèle d'authentification doit être défini sur **No Authentication (aucune authentification)**. Vous pouvez également utiliser les configurations des ports de commutateur dans Cisco DNA Center pour attribuer un port à l'ensemble des adresses IP pour les points d'accès.

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

Étape 8. Une fois que tous les ports à l'appui de points d'accès ont été sélectionnés, en haut de la section **Select Port Assignment**, 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 autorisant les points d'accès à 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 WLC. Une route plus spécifique (telle qu'un sous-réseau/24 ou une route d'hôte/32) vers les adresses IP de WLC doit exister dans le tableau de routage global pour chaque nœud où les points d'accès se connectent pour établir la connectivité. Redistribuez le routage de WLC à la frontière dans le processus de routage IGP de sous-couche à des fins 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 du Cisco DNA Center, sous **PROVISION (configuration) > Devices (appareils) > Inventory (inventaire)**, puis, en haut, dans le menu déroulant **Actions**, sélectionnez **Resync**. Les points d'accès associés aux WLC sont ajoutés à l'inventaire sans attendre l'actualisation de l'inventaire.

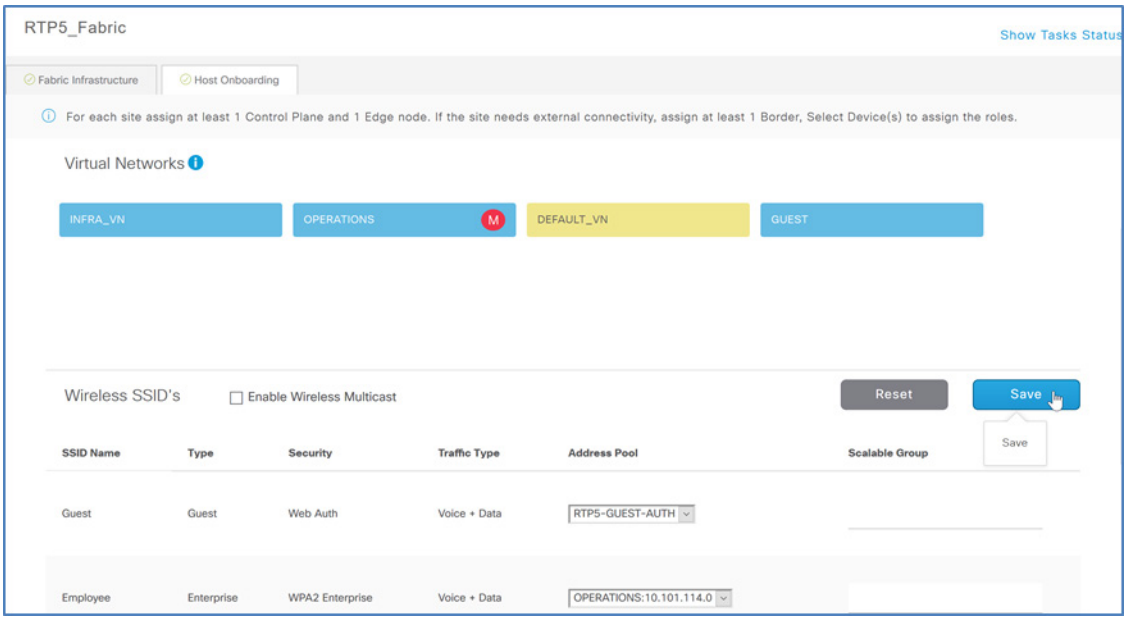
Étape 10. Accédez au tableau de bord principal du Cisco DNA Center, sous **PROVISION (configuration) > Devices (appareils) > Inventory (inventaire)**, sélectionnez les points d'accès à ajouter et en haut, dans le menu déroulant **Actions**, sélectionnez **Provision (configuration)**.

Étape 11. Dans l'écran **Provision Devices (configurer les appareils)**, attribuez les points d'accès à un étage (p. ex., Global/RTP/RTP5-C9K/ Floor 1), cliquez sur **Next (suivant)**pour le profil RF (**RF Profile**), si vous n'avez pas créé le vôtre, sélectionnez **TYPICAL**, puis cliquez sur **Next**. Dans la page du résumé (**Summary**), cliquez sur **Deploy (déploiement)**, puis, dans le panneau déroulant, laissez la sélection par défaut **Now (maintenant)**, puis cliquez sur **Apply (appliquer)**. Prenez connaissance des avertissements concernant les redémarrages.

Procédure 8. Affectez des clients sans fil au réseau virtuel et activez la connectivité

Étape 1. Dans le tableau de bord de Cisco DNA Center, accédez à **PROVISION (configuration) > Fabric (trame)**, sous **Fabric Domains (domaines de trame)**, cliquez sur le site de trame créé (p. ex., RTP5_Fabric), dans le volet de navigation de gauche **Fabric-Enabled Sites**, cliquez sur le site connexe (p. ex., Global/RTP/RTP5-C9K), puis cliquez sur l'onglet **Host Onboarding**.

Étape 2. Dans la section **Wireless SSID's**, pour chaque **nom SSID**, sélectionnez un ensemble d'adresses connexe (**Address Pool**), sélectionnez un groupe évolutif correspondant (**Scalable Group**), cliquez sur **Save (enregistrer)**, conservez la sélection par défaut **Now (maintenant)**, puis cliquez sur **Apply** pour appliquer.



Les appareils 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. Cet ensemble validé ne contient toutefois pas toutes les possibilités. D'autres options matérielles sont répertoriées dans le Guide de conception de solutions d'accès défini par logiciel, la matrice de compatibilité des produits d'accès défini par logiciel et les fiches techniques de Cisco DNA Center peuvent présenter des directives au-delà de ce qui a été mis à l'essai dans le cadre de ce guide. Les fichiers mis à jour des ensembles Cisco DNA Center sont régulièrement publiés et disponibles dans les listes de mises à jour et d'ensembles.

Tableau 3. Cisco DNA Center

Produit	Numéro de pièce	Version du logiciel
Dispositif Cisco DNA Center	DN2-HW-APL-L (châssis à base de M5)	1.2.10.4 (système 1.1.0.754)

Tableau 4. Ensembles Cisco DNA Center

Tous les ensembles exécutés sur le Cisco DNA Center lors de la validation sont répertoriés : tous les ensembles ne sont pas inclus dans le cadre du test de validation de l'accès défini par logiciel.

Ensemble	Version
Politique d'application	2.1.28.170011
Assurance – Base	1.2.11.304
Assurance – 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
IU de Cisco DNA Center	1.2.11.19
Canal de commande	2.1 28.60244
Intégration des périphériques	2.1.18.60024
Plate-forme DNAC	1.0.8.8
Gestion d'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
Trace du chemin	2.1.28.60244
SD-Access	2.1.28.60244.9

Tableau 5. Gestion des identités

Domaine fonctionnel	Produit	Version du logiciel
Serveur Cisco ISE	Plateforme de services d'identité Cisco Identity Services Engine	2.4 correctif 6

Tableau 6. Frontière de la trame d'accès défini par logiciel (SD-Access) et plan de contrôle

Domaine fonctionnel	Produit	Version du logiciel
Frontière et plan de contrôle	Commutateurs Cisco Catalyst, gamme 9500	16.9.3
Frontière et plan de contrôle	Commutateurs de la gamme Cisco Catalyst 9400	16.9.3
Frontière et plan de contrôle – petit site	Commutateurs Cisco Catalyst 3850 XS (fibre optique de 10 Gbits/s)	16.9.3
Frontière et plan de contrôle	routeurs à services intégrés, gamme Cisco 4000	16.9.2
Frontière et plan de contrôle – grand site	routeurs d'agrégation de services des gammes Cisco ASR 1000-X et 1000-HX	16.9.2
Frontière	Châssis Cisco Catalyst 6807 à 7 logements avec moteur de supervision 6T ou moteur de supervision 2T et gamme 6800 à 32 ports, 10 GE avec DFC4 intégré double	15.5(1)SY2
Frontière	Commutateurs Cisco Catalyst 6880-X et 6840-X	15.5(1)SY2
Frontière externe	Châssis de commutateur Cisco Nexus 7700 à 2 logements avec module de supervision amélioré 2 et Cisco Nexus 7700 série M3 48 ports 1/10 module Gigabit Ethernet	8.3(2)
Plan de contrôle	Routeur de services nuagiques de Cisco, série 1000V	16.9.2

Tableau 7. Périphérie de trame d'accès défini par logiciel

Domaine fonctionnel	Produit	Version du logiciel
Périphérie de trame	Cisco Catalyst, série 9300 – empilable	16.9.3
Périphérie de trame	Cisco Catalyst, série 9400 avec moteur de supervision-1 – châssis modulaire	16.9.3
Périphérie de trame	Cisco Catalyst, série 3850 – empilable	16.9.3

Domaine fonctionnel	Produit	Version du logiciel
Périphérie de trame	Cisco Catalyst, série 3650 – autonome avec empilage en option	16.9.3
Périphérie de trame	Cisco Catalyst, série 4500E avec Supervisor 8-E – châssis modulaire	3.10.2E

Tableau 8. Accès sans fil défini par logiciel

Domaine fonctionnel	Produit	Version du logiciel
Contrôleur réseau sans fil	Contrôleurs sans fil, série 8540, 5520 et 3504 de Cisco	8.8.111.0 (8.8 MR1)
Points d'accès en mode de trame	Cisco Aironet®, série 1800, 2800 et 3800 (vague 2)	8.8.111.0 (8.8 MR1)

Tableau 9. Commutateurs d'automatisation LAN testés pour ce guide (non inclus dans toutes les possibilités)

Domaine fonctionnel	Produit
Cisco Catalyst, série 9500 (versions de performances standard)	Périphérique d'amorçage
Commutateurs Cisco Catalyst 3850 XS (fibre optique de 10 Gbits/s)	Périphérique d'amorçage
Cisco Catalyst, série 9300 – empilable	Périphérique détecté depuis le périphérique d'amorçage
Cisco Catalyst, série 9400 avec moteur de supervision-1 – châssis modulaire	Périphérique détecté depuis le périphérique d'amorçage (interface 10 Gbits/s)
Cisco Catalyst, série 3850 – empilable	Appareil découvert
Cisco Catalyst, série 3650 – autonome avec empilage en option	Appareil détecté
Cisco Catalyst, série 4500E avec Supervisor 8-E – châssis modulaire	Appareil détecté

Commentaires

Pour obtenir des commentaires et des suggestions sur ce guide et sur les guides connexes, participez à la discussion sur la communauté Cisco à 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**.