Configurer l'accès LDAP sécurisé pour les interconnexions de fabric en mode Intersight Manage (HTTP Device Console et SSH)

Table des matières

Introduction

Ce document décrit comment configurer l'authentification LDAP de domaine dans une instance SaaS Intersight à l'aide de la stratégie LDAP.

Conditions préalables

Exigences

Connaissance de ces sujets :

- Protocole LDAP (Lightweight Directory Access Protocol).
- Serveur DNS (Domain Name Server).
- Cisco Intersight

Composants utilisés

- Instance Cisco Intersight SaaS
- Microsoft Active Directory
- Serveur DNS
- Services de certificats Microsoft Active Directory (AD CS)

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

Informations générales

LDAP est un protocole bien connu utilisé pour accéder aux ressources d'un annuaire sur le réseau. Ces répertoires stockent des informations sur les utilisateurs, les organisations et les ressources. LDAP fournit un processus standard d'accès et de gestion de ces informations qui peuvent être utilisées pour les processus d'authentification et d'autorisation.

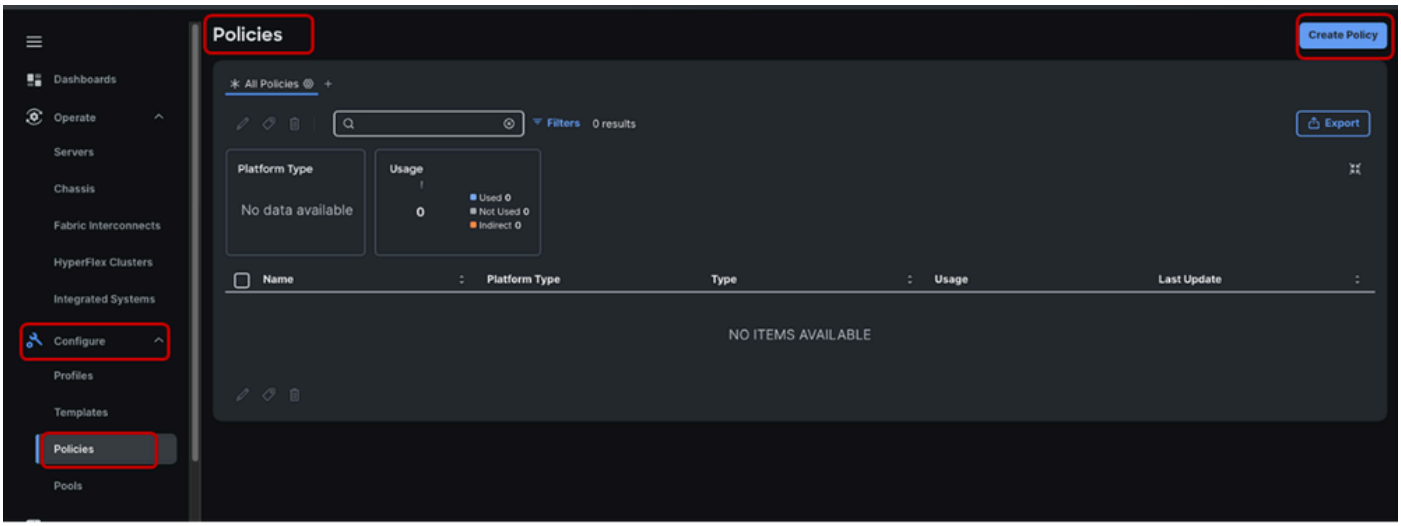
Ce document décrit le processus de configuration pour l'authentification à distance via LDAP sécurisé vers la console de périphérique ou l'interface de ligne de commande (respectivement HTTP ou SSH) d'un homologue d'interconnexions de fabric en mode géré Intersight.

Configuration

Configurer la stratégie LDAP

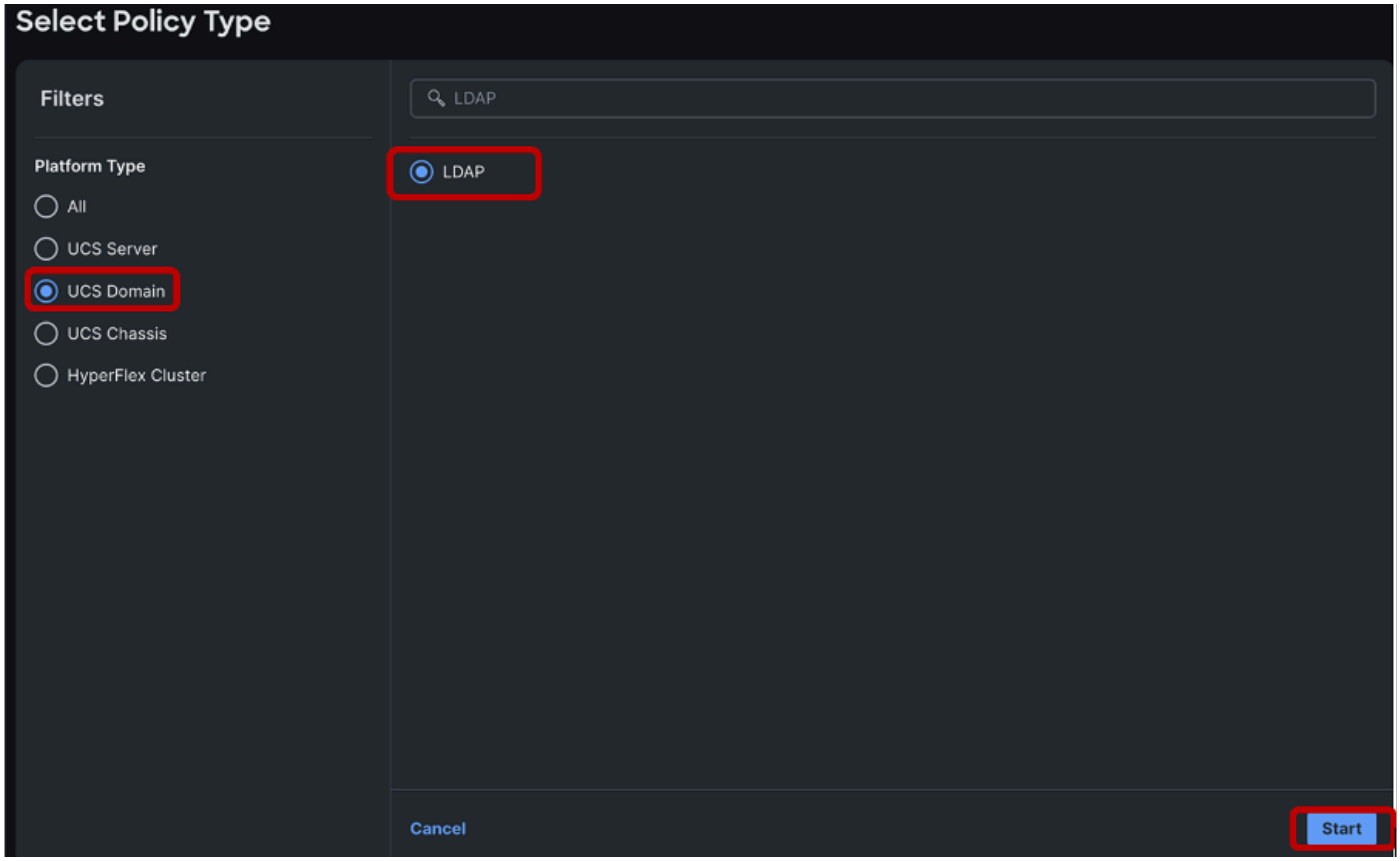
Pour configurer la stratégie LDAP, connectez-vous à l'instance SaaS Intersight.

Accédez à la section Configurer **>** Cliquez sur Stratégies.
Accédez à la fenêtre Stratégies **>** Sélectionnez Créer une stratégie.

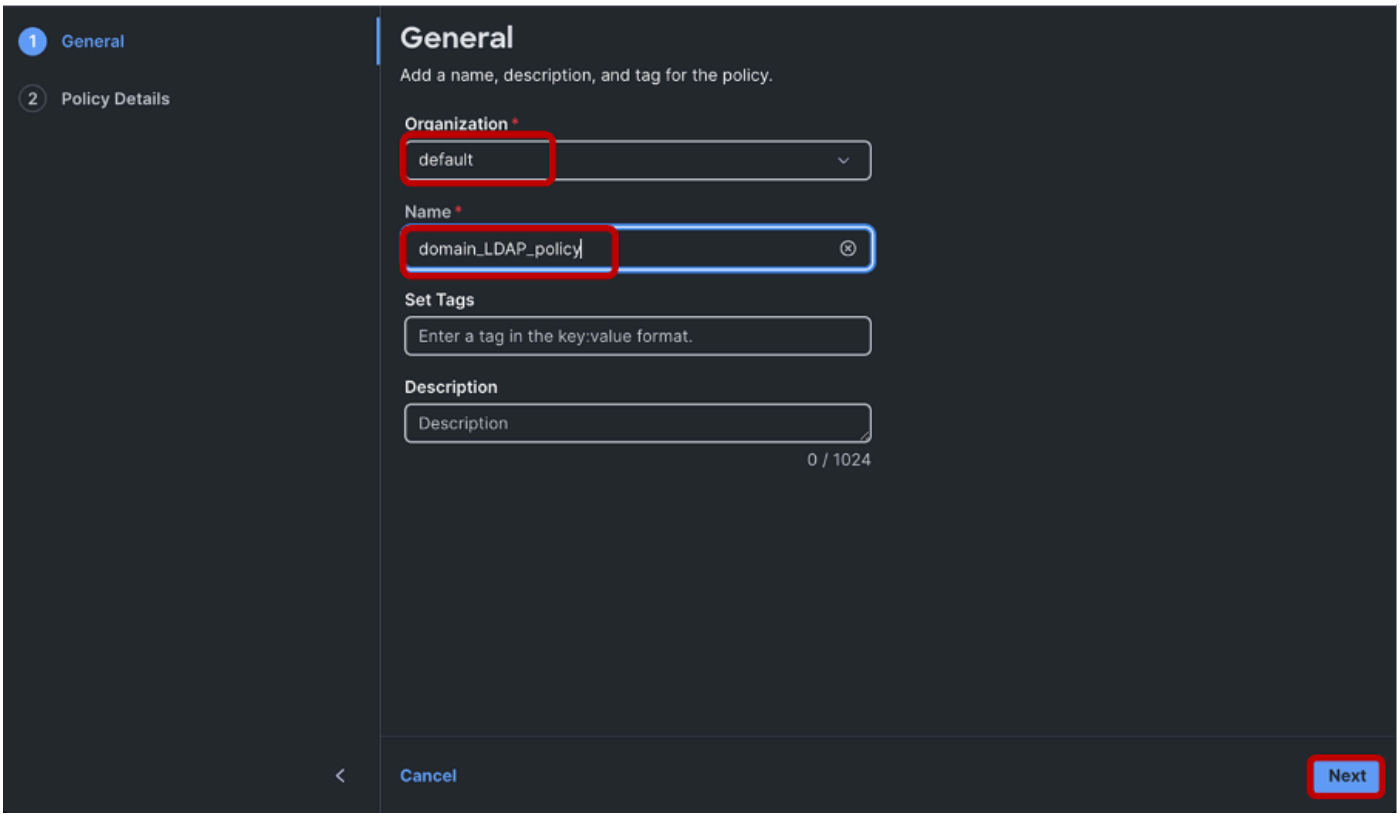


Dans la barre de recherche, recherchez « LDAP ».

Sélectionnez la case d'option LDAP > Cliquez sur Démarrer.

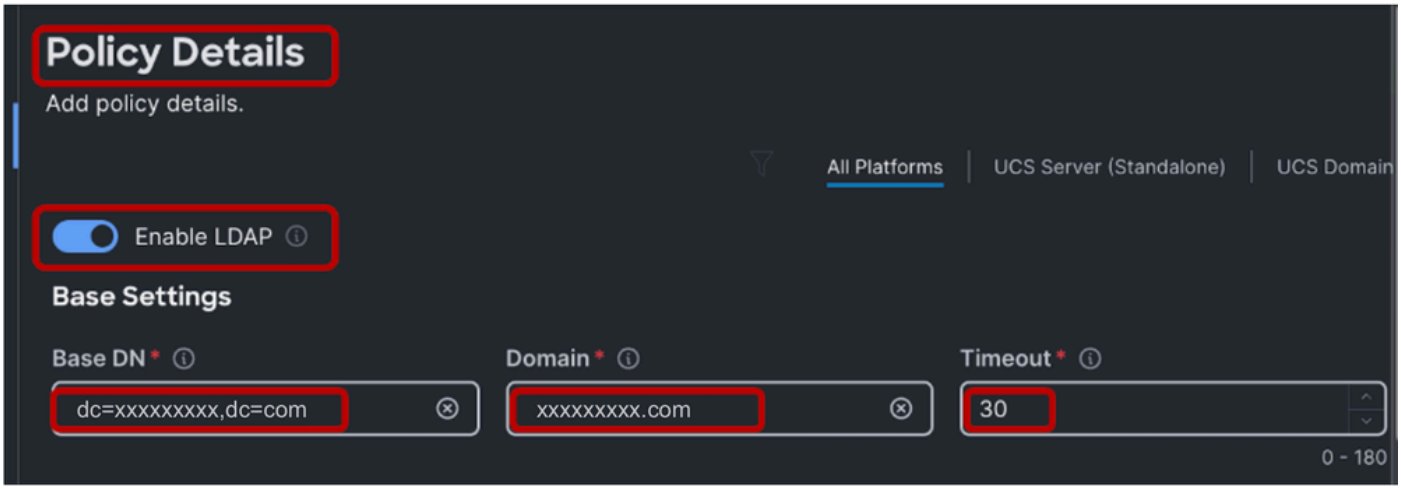


Dans la fenêtre Créer > Choisissez votre organisation > Nommez la stratégie LDAP > Cliquez sur Suivant :



Dans la section Policy Details > Sélectionnez le curseur Enable LDAP > Peuplez les valeurs Base DN, Domain et Timeout.

Les valeurs Timeout, lorsqu'elles sont comprises entre 0 et 29, sont automatiquement définies par défaut sur 30 secondes. Pour cette démonstration, « xxxxxxxxx.com » est le domaine souhaité déjà configuré sur le serveur LDAP et une valeur Timeout de 30 secondes a été spécifiée.

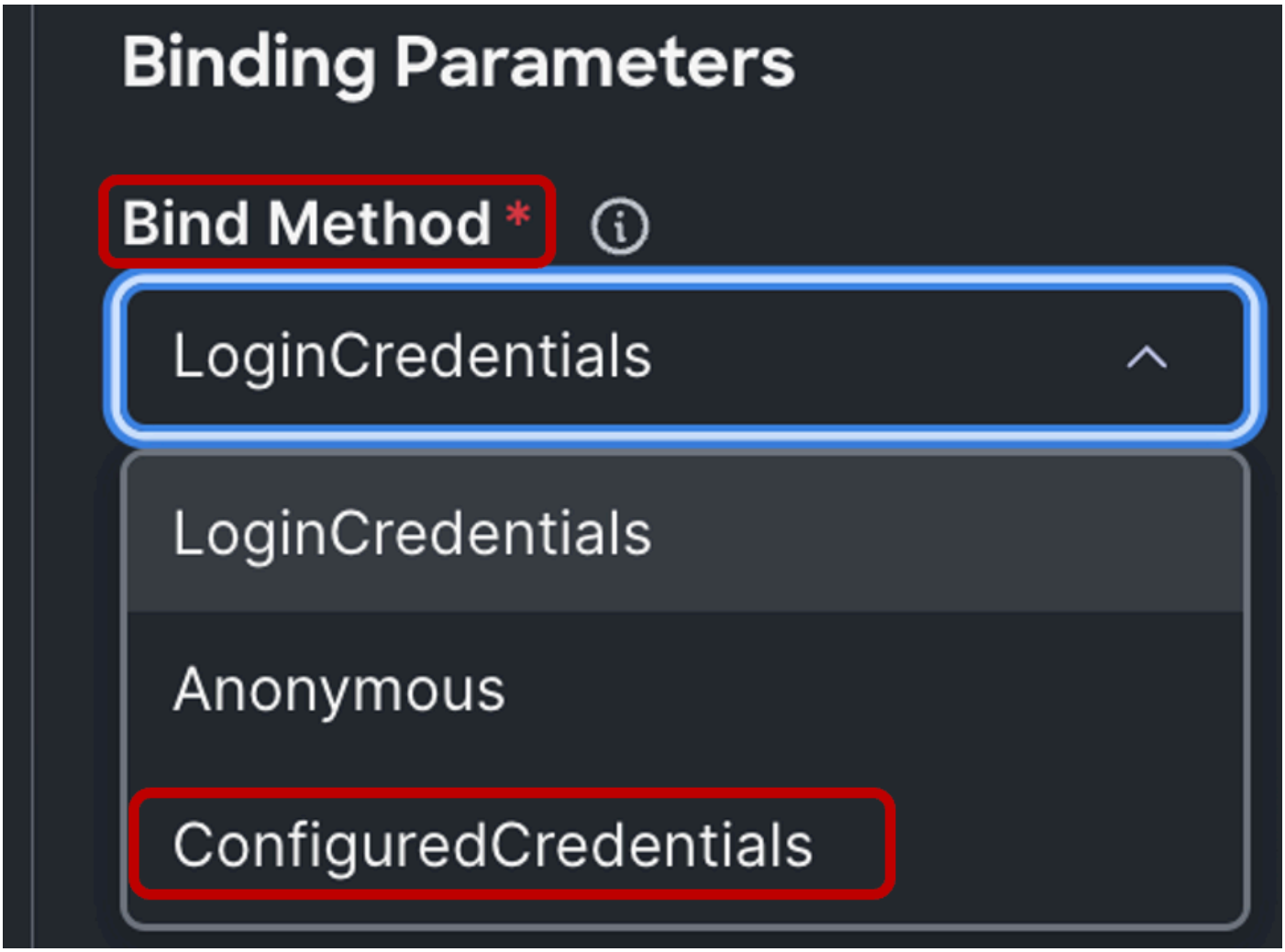


Pour configurer le protocole LDAP sécurisé, activez la case d'option Activer le chiffrement.

Remarque : La configuration LDAP habituelle peut utiliser une adresse IP ou un nom de domaine complet (FQDN), mais un certificat signé n'est pas obligatoire. Par conséquent, lors de la configuration du protocole LDAP « Standard », l'option Activer le chiffrement, la stratégie de connectivité réseau du serveur DNS et un certificat dans les configurations de stratégie de gestion des certificats peuvent être ignorés. Le protocole LDAP sécurisé nécessite un serveur DNS configuré pour la résolution de noms de serveur LDAP et un certificat racine.

Dans la section Paramètres de liaison, le paramètre par défaut est LoginCredentials, qui utilise l'authentification individuelle des identifiants LDAP de l'utilisateur pour l'opération de liaison. Cela élimine le besoin de configurer un utilisateur Bind dédié.

Pour cette démonstration, un utilisateur Bind est configuré. Par conséquent, la « Méthode de liaison » est remplacée par « ConfiguredCredentials ».

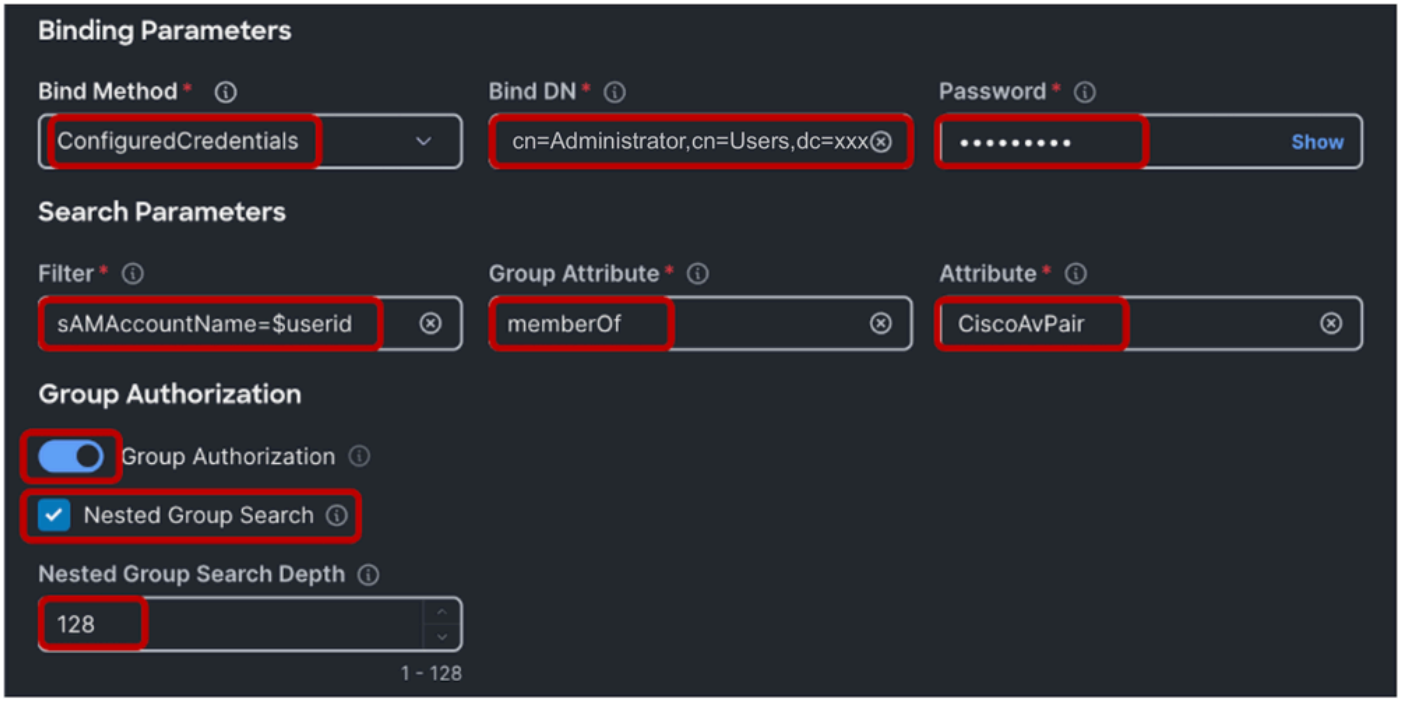


Ajoutez ensuite un DN de liaison (un utilisateur de liaison) et le mot de passe d'utilisateur de liaison. Il peut s'agir de n'importe quel utilisateur configuré dans Windows Active Directory. Dans cette démonstration, l'utilisateur Administrateur est utilisé.

« cn=Administrateur, cn=Utilisateurs, dc=xxxxxxx, dc=com ».

Dans la section Paramètres de recherche, sous Filtre, saisissez « sAMAccountName=$userid ».

Pour Attributs de groupe, ajoutez «memberOf» et dans le champ Attribut, ajoutez «CiscoAvPair». Selon la configuration de votre serveur LDAP, vous pouvez activer l'autorisation de groupe et la recherche de groupe imbriqué. Pour cette démonstration, la profondeur de recherche de groupe imbriqué par défaut est de 128.



Dans la section « Configurer les serveurs LDAP », saisissez l'adresse IP du serveur LDAP ou le nom de domaine complet (FQDN) (requis pour Secure LDAP) et le numéro de port (389).

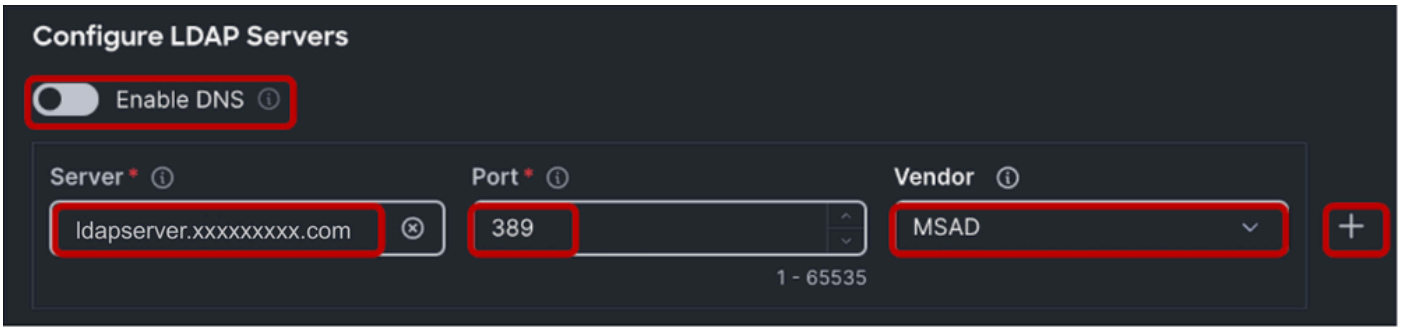
Secure LDAP dans UCS utilise STARTTLS pour activer la communication chiffrée via le port 389.

Notez que la modification du port de 389 à 636 peut entraîner des erreurs d'authentification. Cisco UCS effectue la négociation TLS sur le port 636 pour SSL ; cependant, la connexion initiale est toujours établie sans cryptage sur le port 389.

Sélectionnez le fournisseur du serveur LDAP. Les options de fournisseur disponibles sont OpenLDAP et MSAD (Microsoft Active Directory). Pour cette démonstration, puisque le serveur LDAP utilisé est Windows Server 2019, MSAD est utilisé.

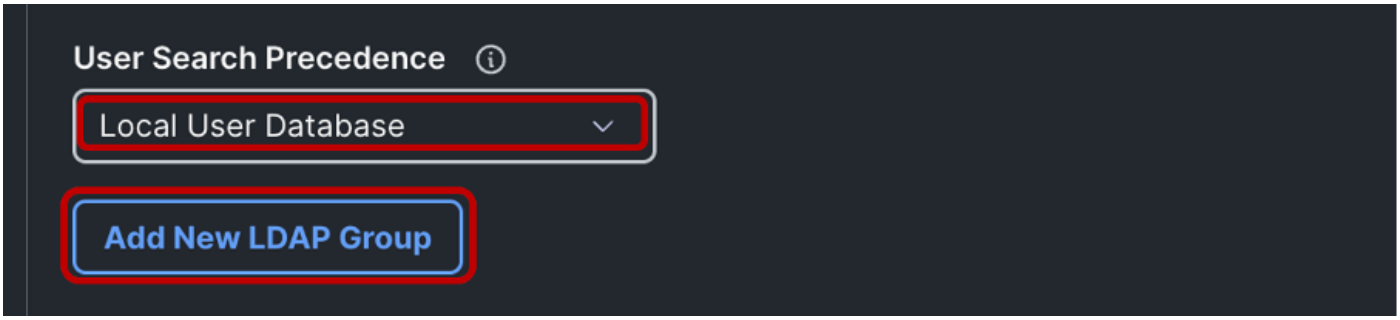
Laissez le bouton Activer DNS désactivé car cette option ne s'applique pas à la configuration LDAP dans le domaine UCS.

Vous pouvez configurer plusieurs serveurs LDAP en cliquant sur l'icône « + » située à l'extrême droite du serveur LDAP configuré.

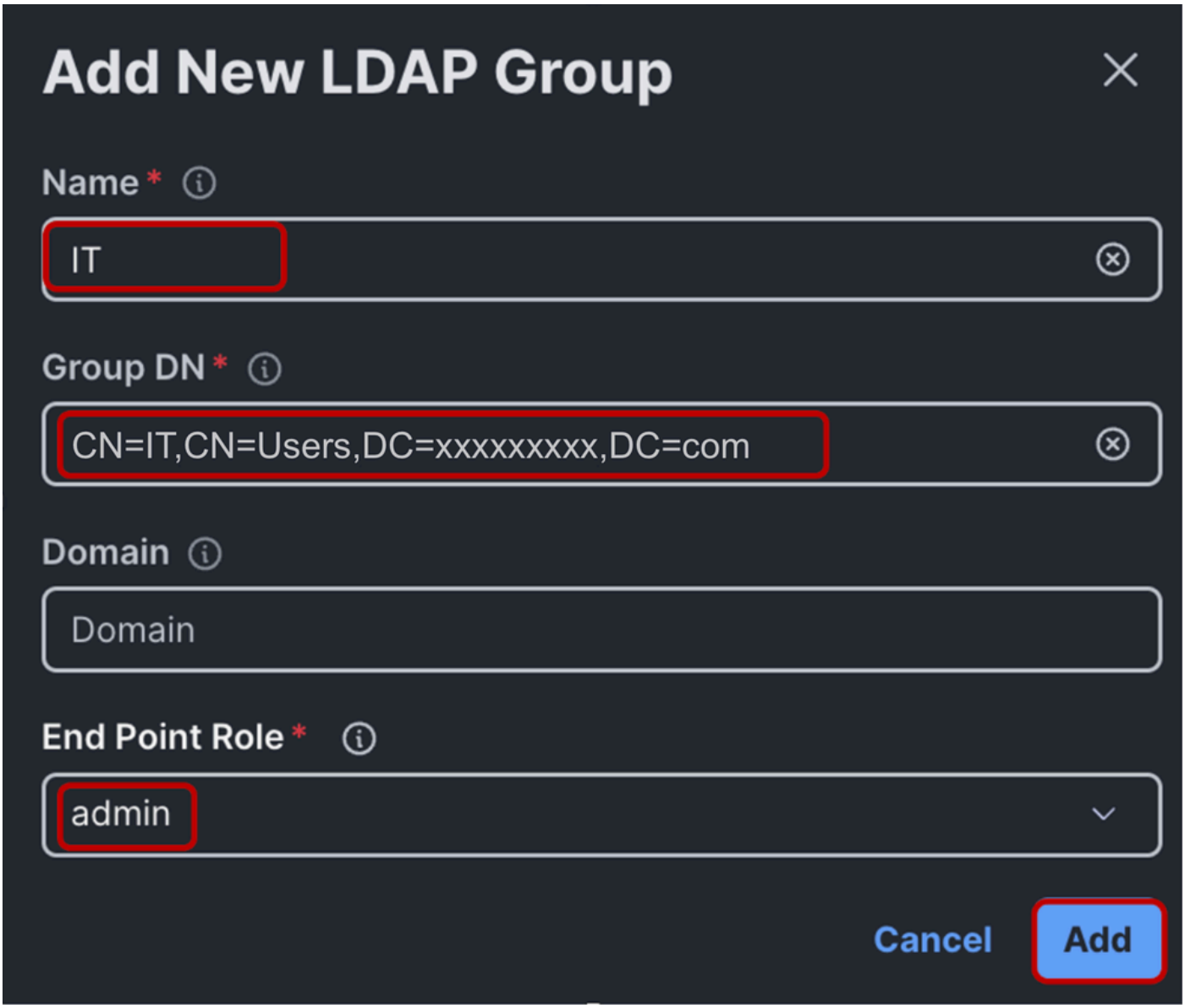


Remarque : Vous pouvez conserver la priorité de recherche d'utilisateur en tant que base de données utilisateur locale ou la remplacer par base de données utilisateur LDAP, selon votre exemple d'utilisation.

Ensuite, continuez à ajouter un DN de groupe correspondant au groupe configuré dans le serveur LDAP, en cliquant sur le bouton Ajouter un nouveau groupe LDAP.



Attribuez un nom au groupe, ajoutez le nom distinctif (DN) du groupe reçu du serveur LDAP et sélectionnez le rôle de point de terminaison souhaité.

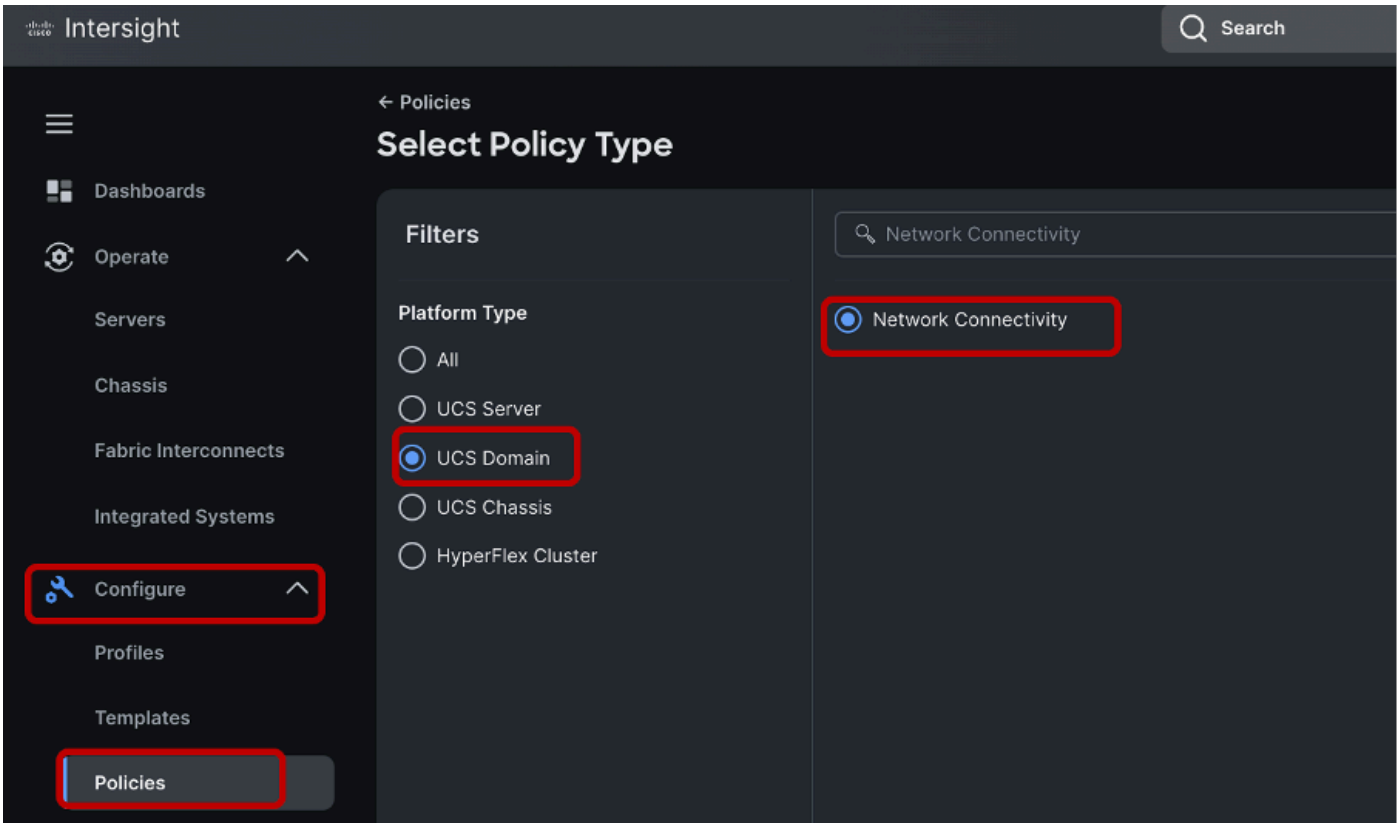


Cliquez sur Ajouter > Sélectionner Créer pour créer la stratégie LDAP

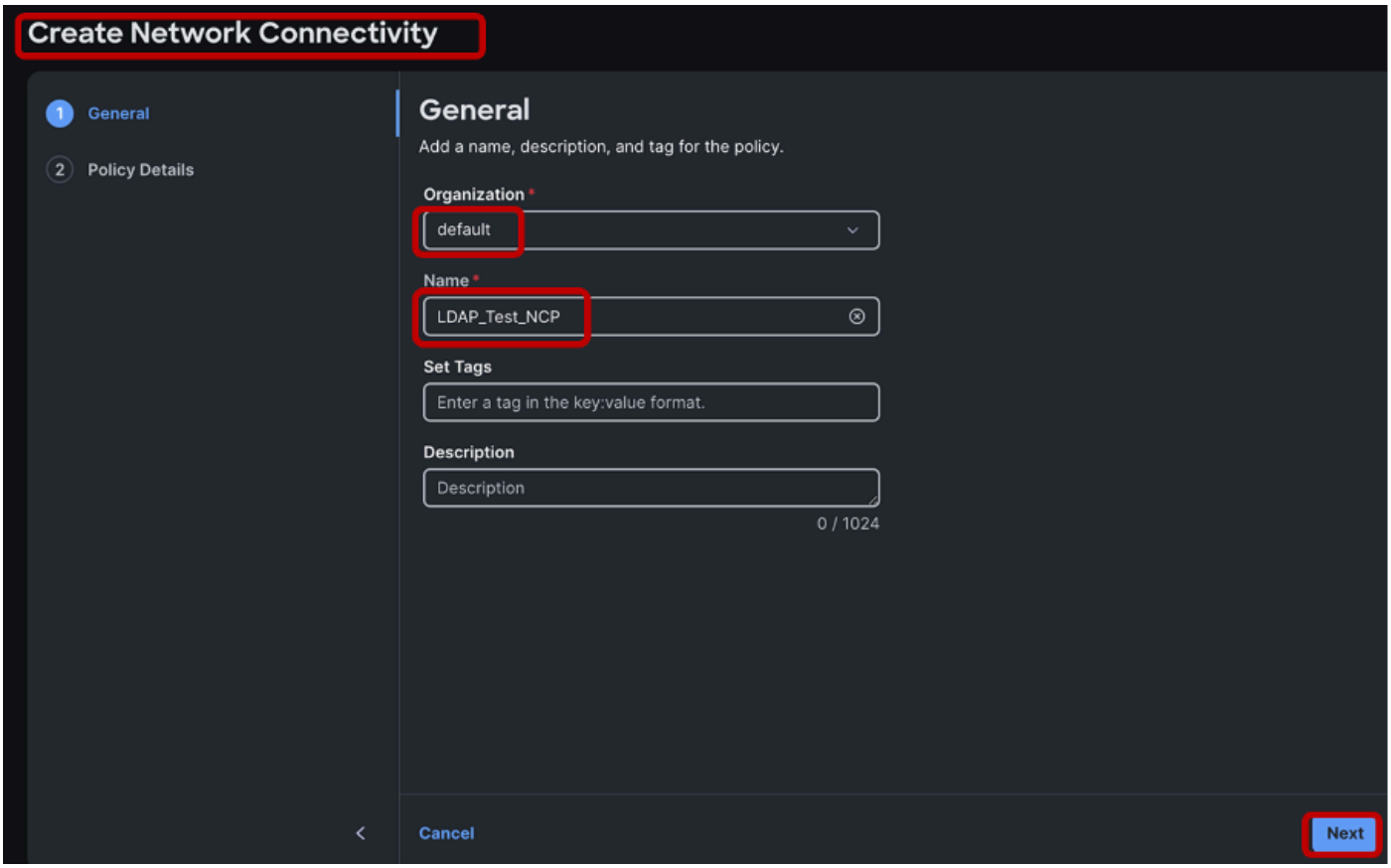
Remarque : Pour la configuration de stratégie LDAP de domaine, le seul rôle de point final pris en charge est « admin » au moment de la création de ce document.

Configurer la stratégie de connectivité réseau

Configurez un serveur DNS pour le domaine UCS en créant une stratégie de connectivité réseau.

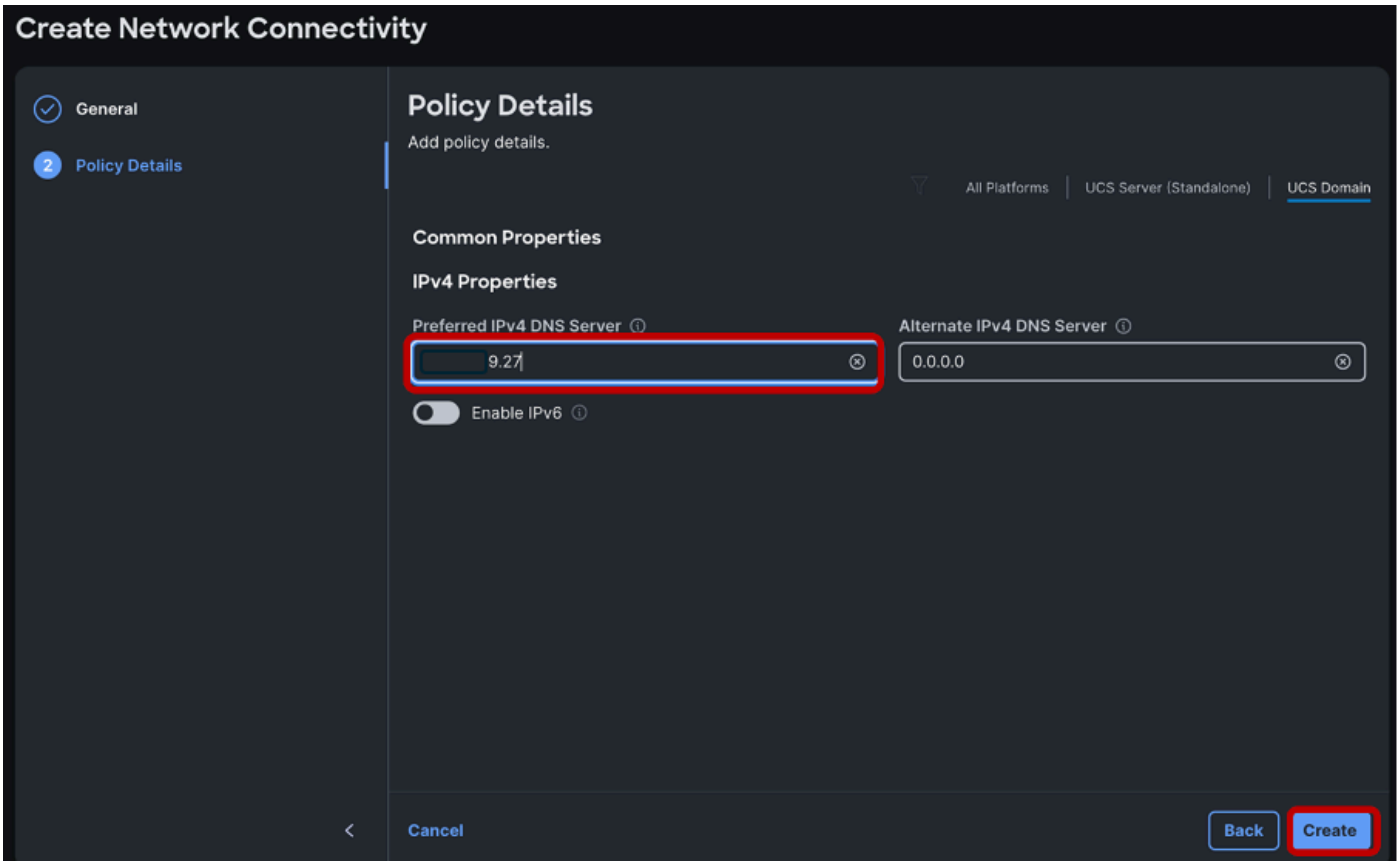


Sélectionnez l'organisation appropriée > Saisissez le nom de la stratégie > Cliquez sur Suivant.



Définissez une adresse IPv4 de serveur DNS préféré et cliquez sur Create pour enregistrer la

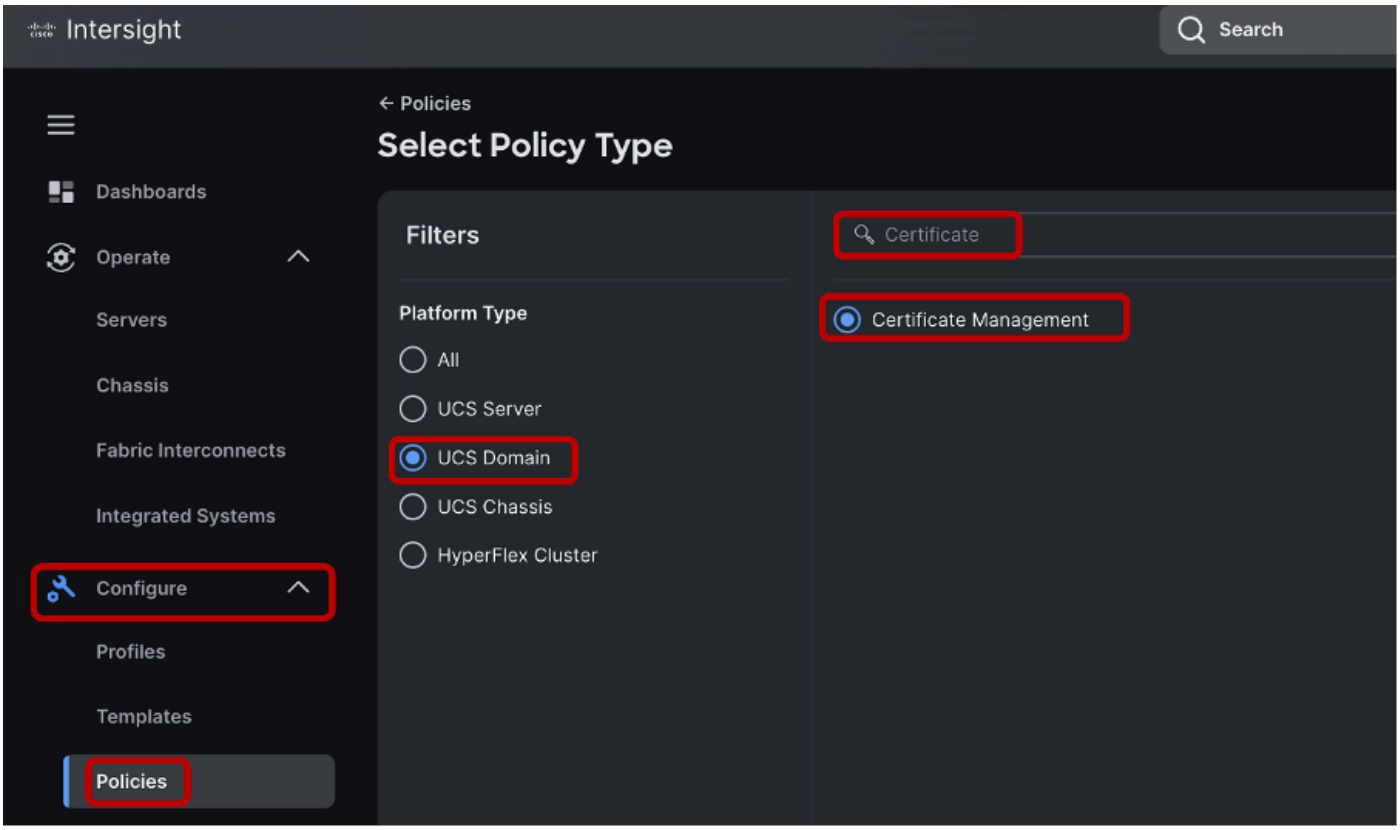
stratégie.



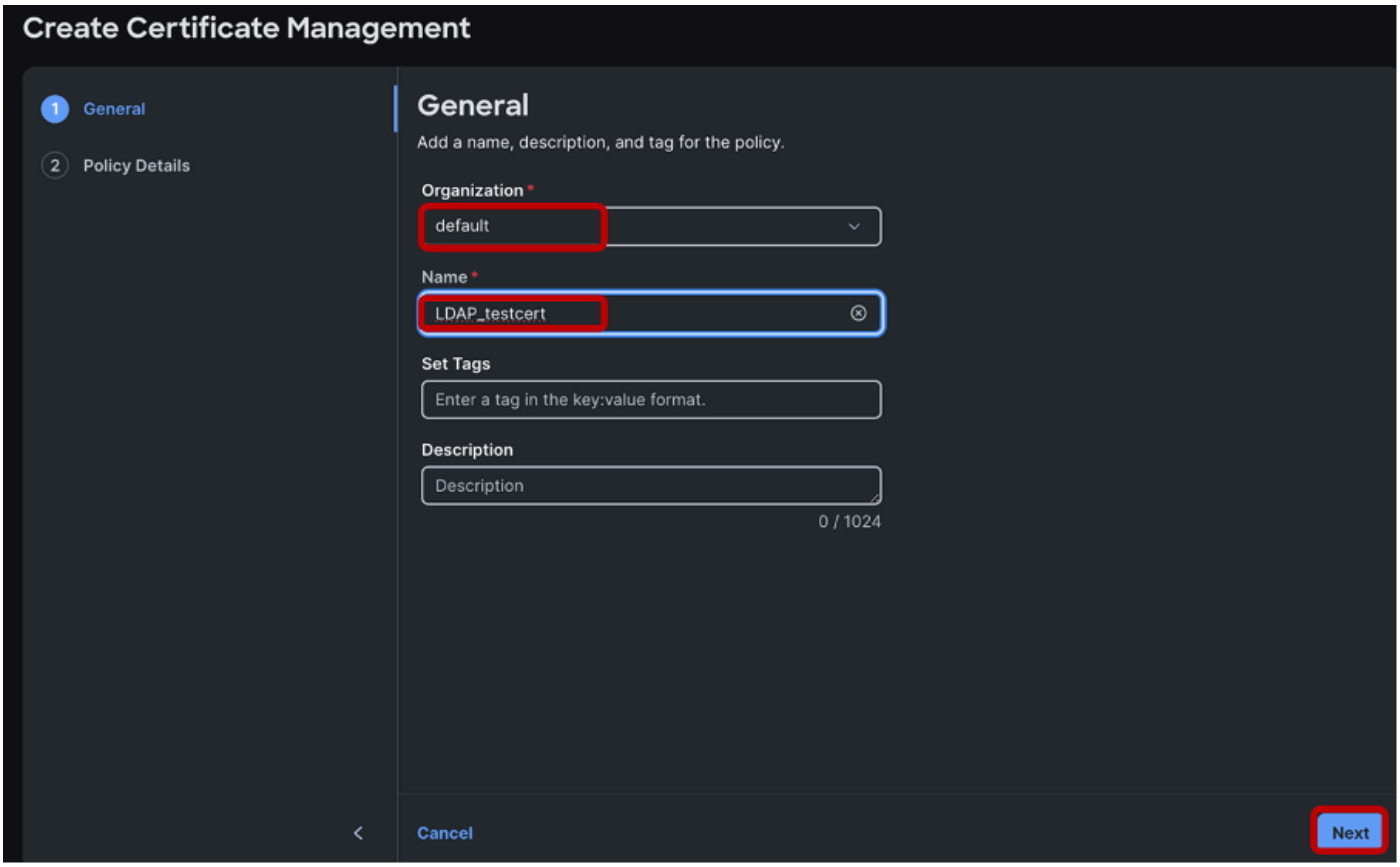
Assurez-vous qu'une adresse IP de serveur DNS est configurée et accessible pour la résolution de noms. Assurez-vous que la résolution de noms est fonctionnelle pour le serveur LDAP et les interconnexions de fabric au sein du domaine. Pour cette démonstration, le serveur DNS se trouve sur la même instance de machine Windows que le serveur LDAP.

Configurer la stratégie de gestion des certificats

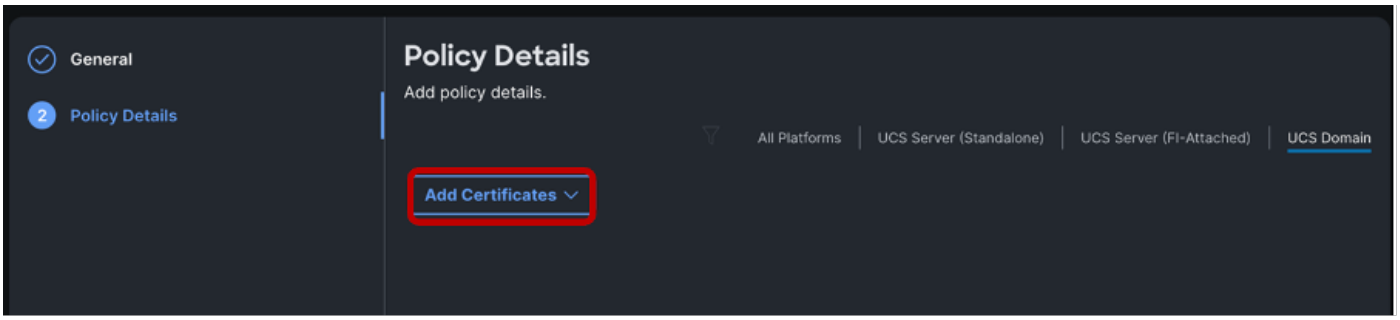
Configurez ensuite une stratégie de gestion des certificats. Cette opération est nécessaire au fonctionnement du cryptage LDAP.



Sélectionnez l'organisation appropriée, nommez la politique > Cliquez sur Suivant

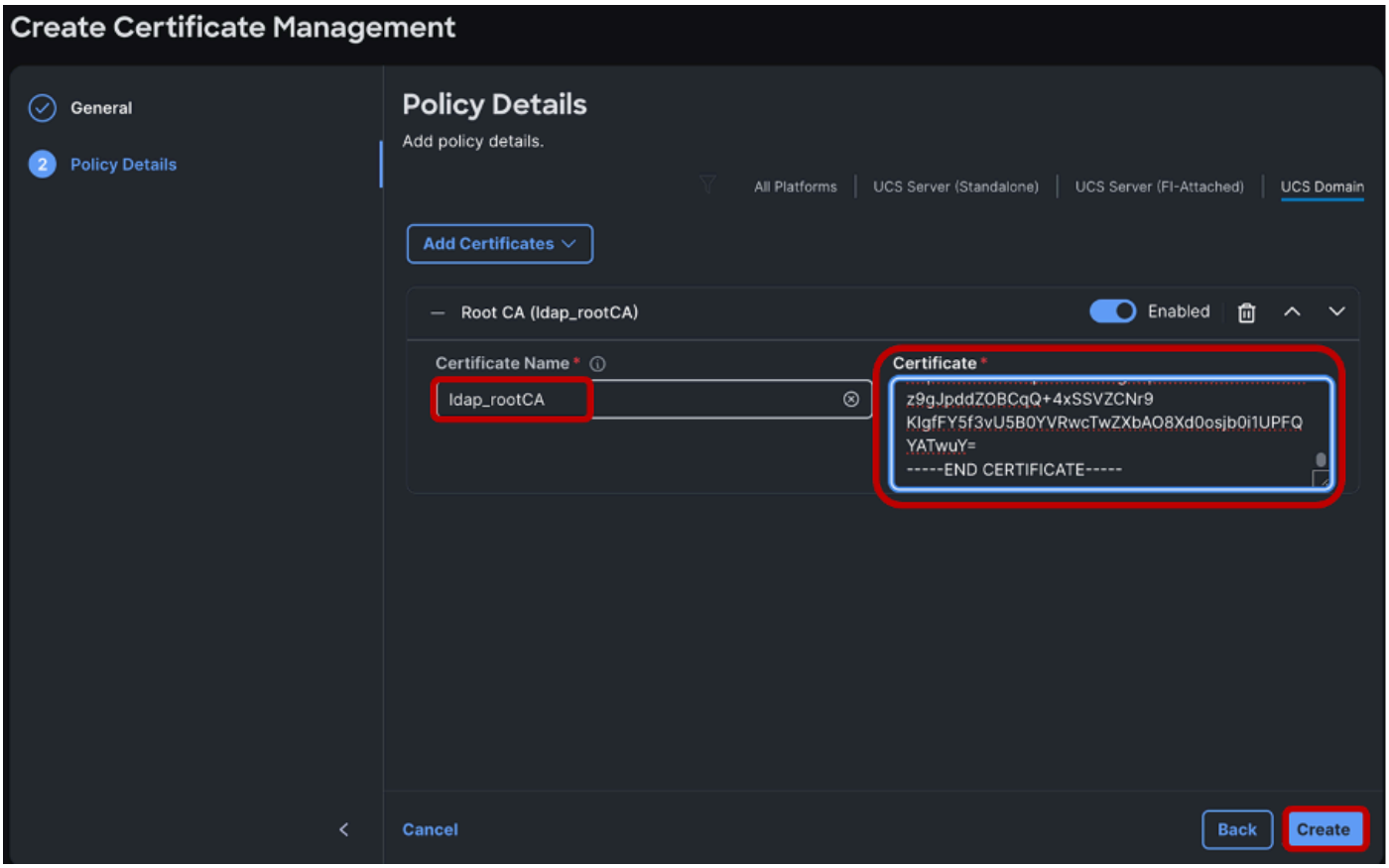


Cliquez sur Ajouter des certificats.

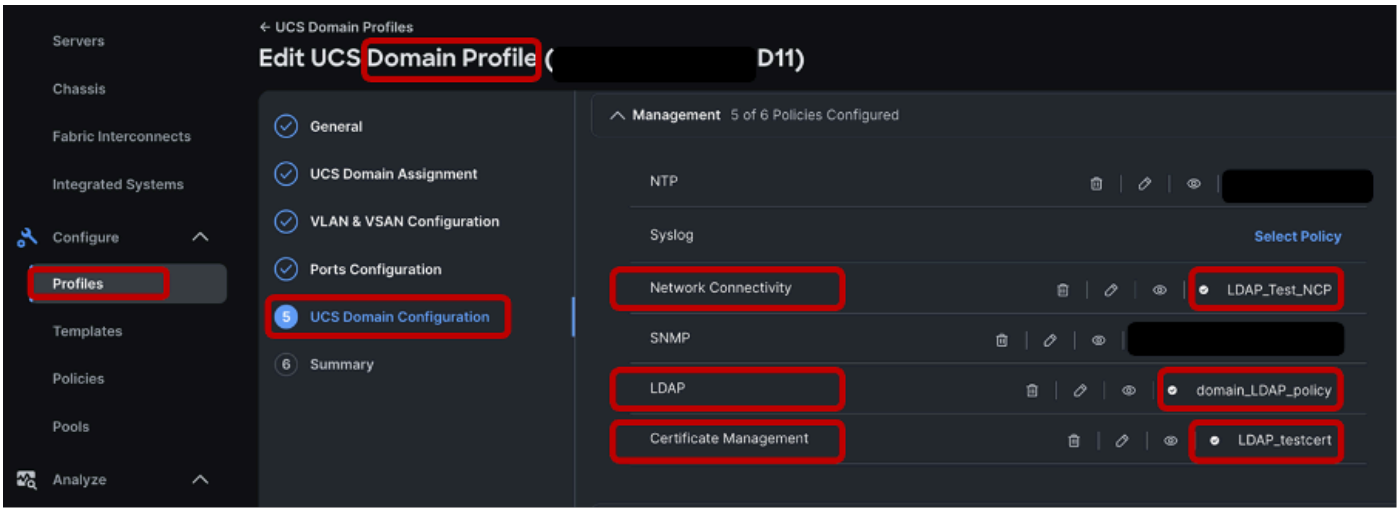


Nommez le certificat et collez-le dans le certificat racine à partir des services de certificats Microsoft Active Directory.

Cliquez sur Créer.



Une fois que les stratégies LDAP, de connectivité réseau et de gestion des certificats ont été créées, référencez les stratégies nouvellement créées dans le profil de domaine souhaité, sous la section « Configuration du domaine UCS », comme indiqué.



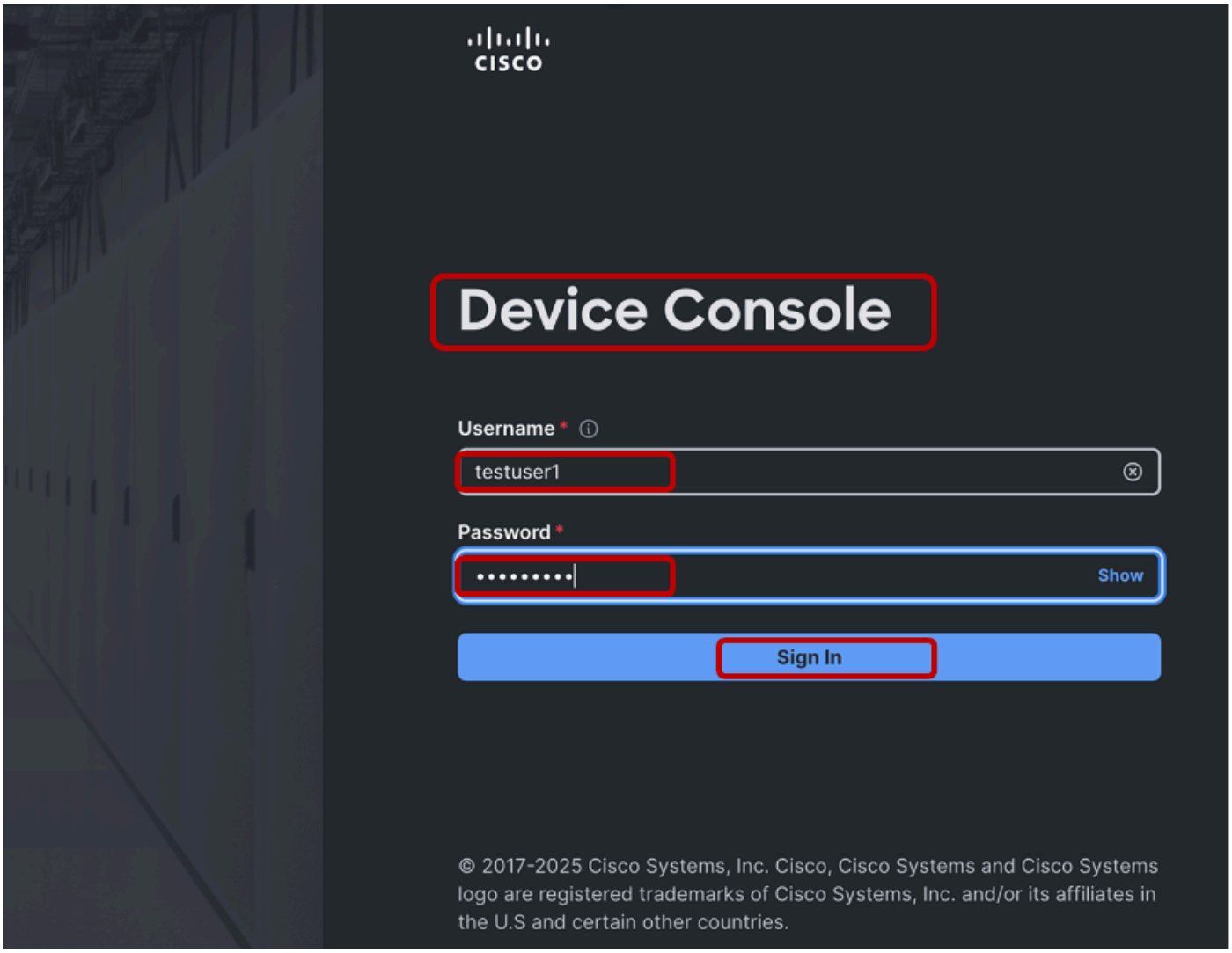
Cliquez sur Next (Suivant), Save and Deploy (Enregistrer et déployer le profil de domaine).

Une fois le déploiement du profil de domaine réussi, la configuration LDAP sécurisée pour le domaine IMM est terminée.

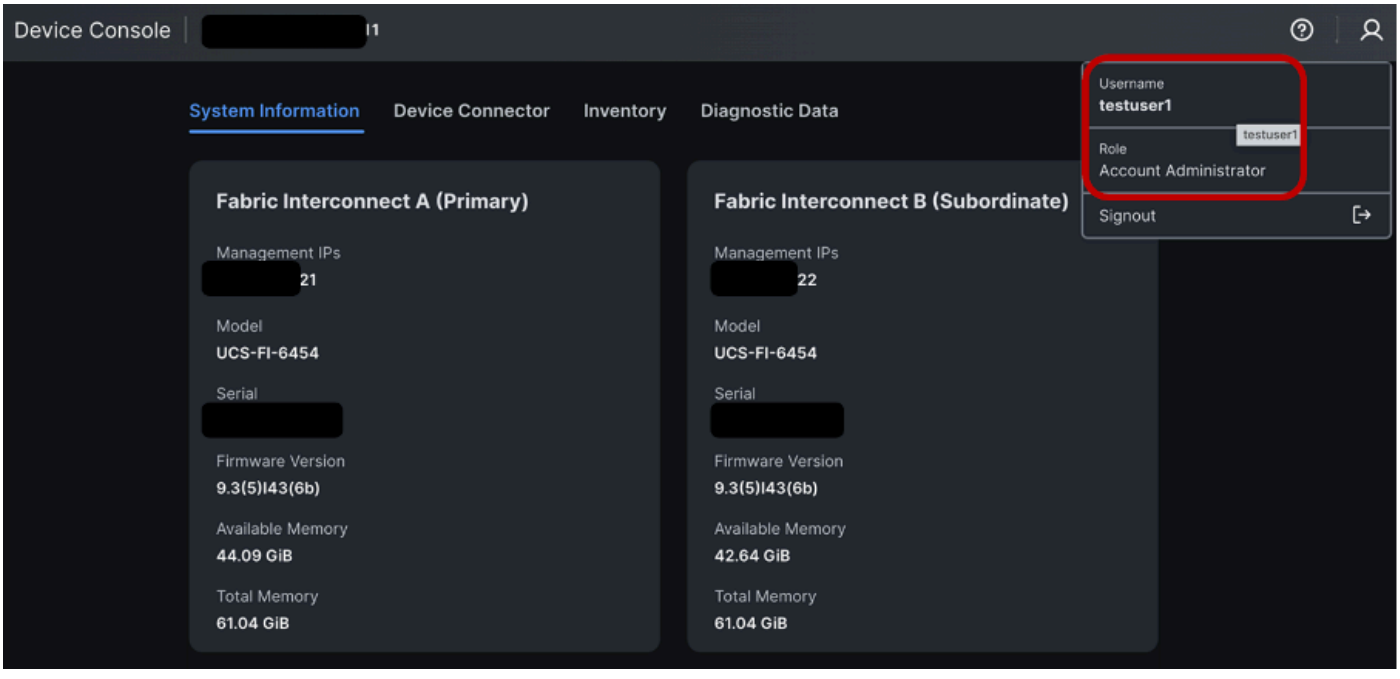
Vérification

Pour vérifier, essayez de vous connecter à l'interface utilisateur graphique de la console du périphérique et à l'interface de ligne de commande Fabric Interconnects en utilisant l'un des utilisateurs LDAP/Active Directory configurés.

Connexion à la console du périphérique test

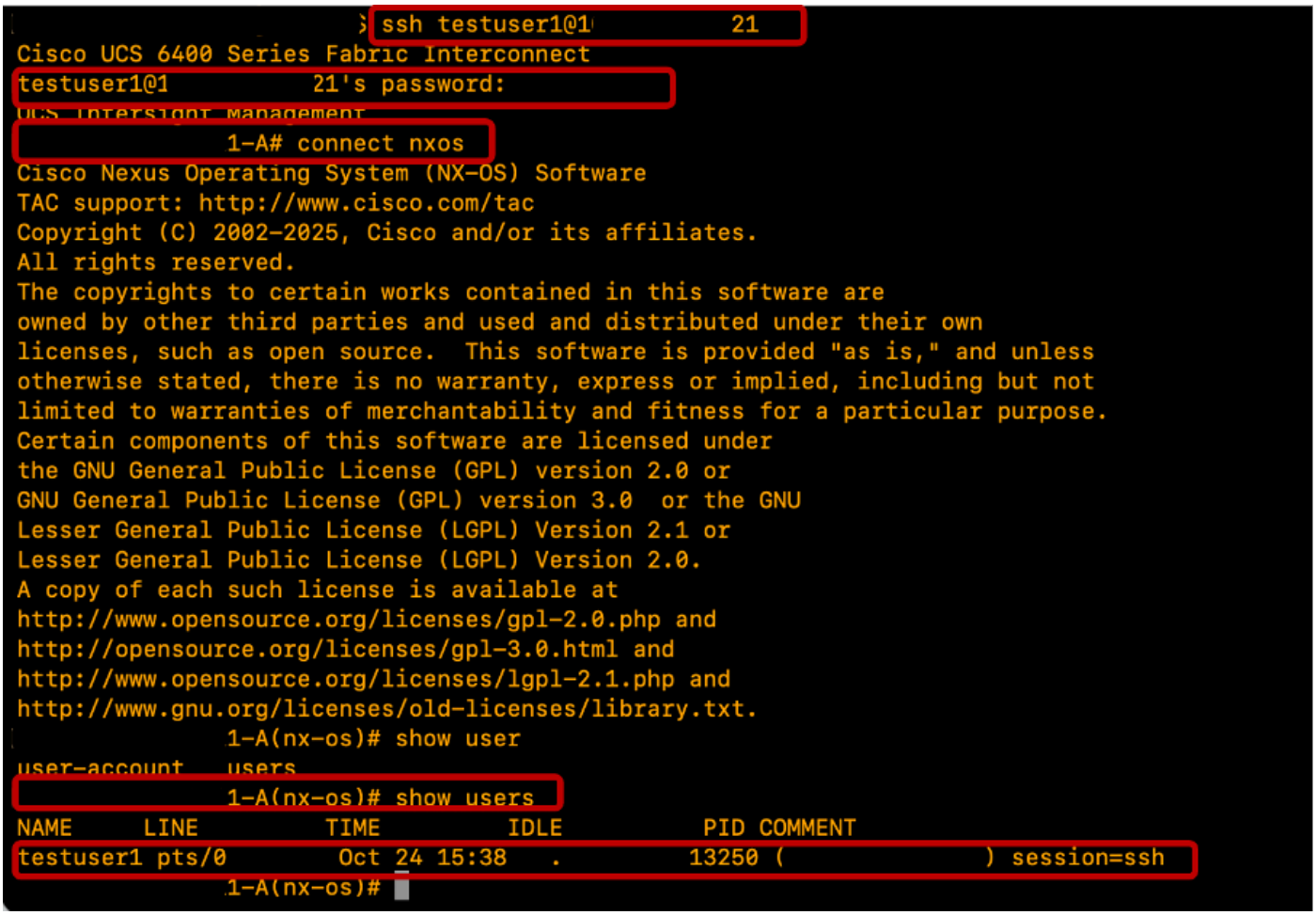


La connexion à la console du périphérique Testuser1 a réussi.



Test FIs SSH Login

La connexion SSH de Testuser1 a réussi.



Informations connexes

- Centre d'aide Intersight
- Guide d'administration de Cisco Intersight Managed Mode Fabric Interconnect

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

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