Intersight Manageモードでのファブリックインターコネクトのセキュアldapアクセスの設定（HTTPデバイスコンソールおよびSSH）

内容

はじめに

このドキュメントでは、LDAPポリシーを使用してIntersight SaaSインスタンスでドメインLDAP認証を設定する方法について説明します。

前提条件

要 件

次の項目に関する知識：

- Lightweight Directory Access Protocol(LDAP)プロトコル。
- ドメインネームサーバ(DNS)サーバ。
- Cisco Intersight

使用するコンポーネント

- Cisco Intersight SaaSインスタンス
- Microsoft Active Directory
- DNS サーバ
- Microsoft Active Directory証明書サービス(AD CS)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

LDAPは、ネットワークを介してディレクトリからリソースにアクセスするために使用される既知のプロトコルです。これらのディレクトリには、ユーザ、組織、およびリソースに関する情報が格納されます。LDAPは、その情報にアクセスして管理するための標準プロセスを提供します。このプロセスは、認証および認可プロセスに使用できます。

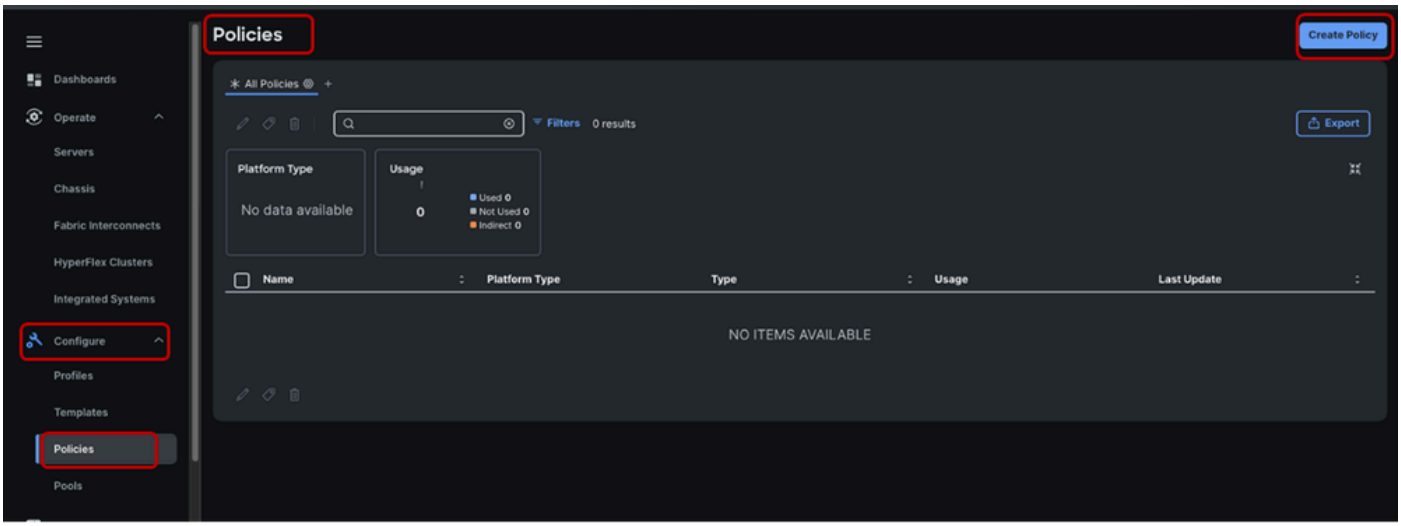
このドキュメントでは、セキュアLDAPを使用して、Intersight Managed ModeのFabric Interconnectのピアのデバイスコンソール(WLC)またはCLI（それぞれHTTPまたはSSH）に対するリモート認証の設定プロセスについて説明します。

コンフィギュレーション

LDAPポリシーの設定

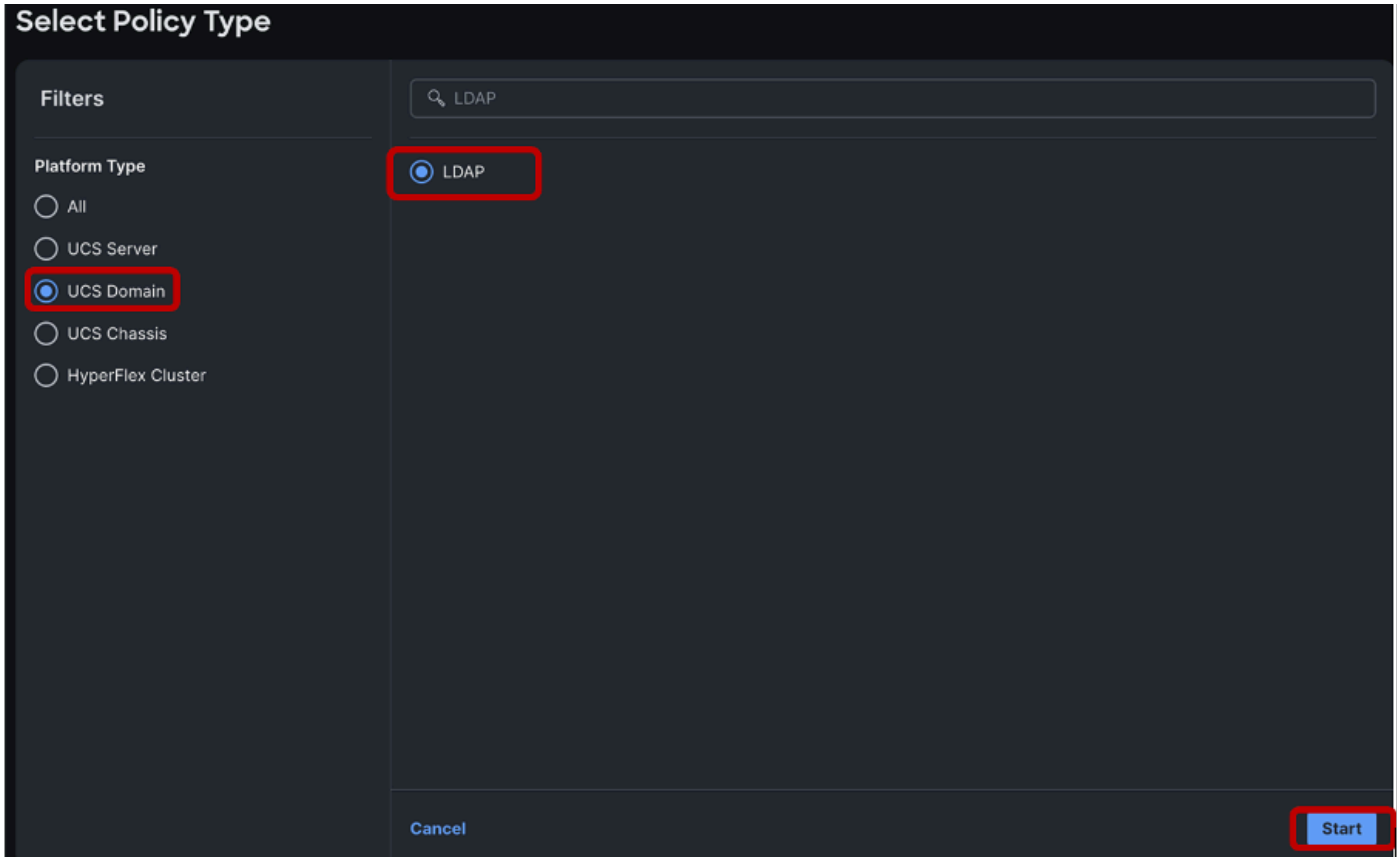
LDAPポリシーを設定するには、Intersight SaaSインスタンスにログインします。

Configureセクションに移動し> Policiesをクリックします。
「ポリシー」ウィンドウ>「ポリシーの作成」を選択します。

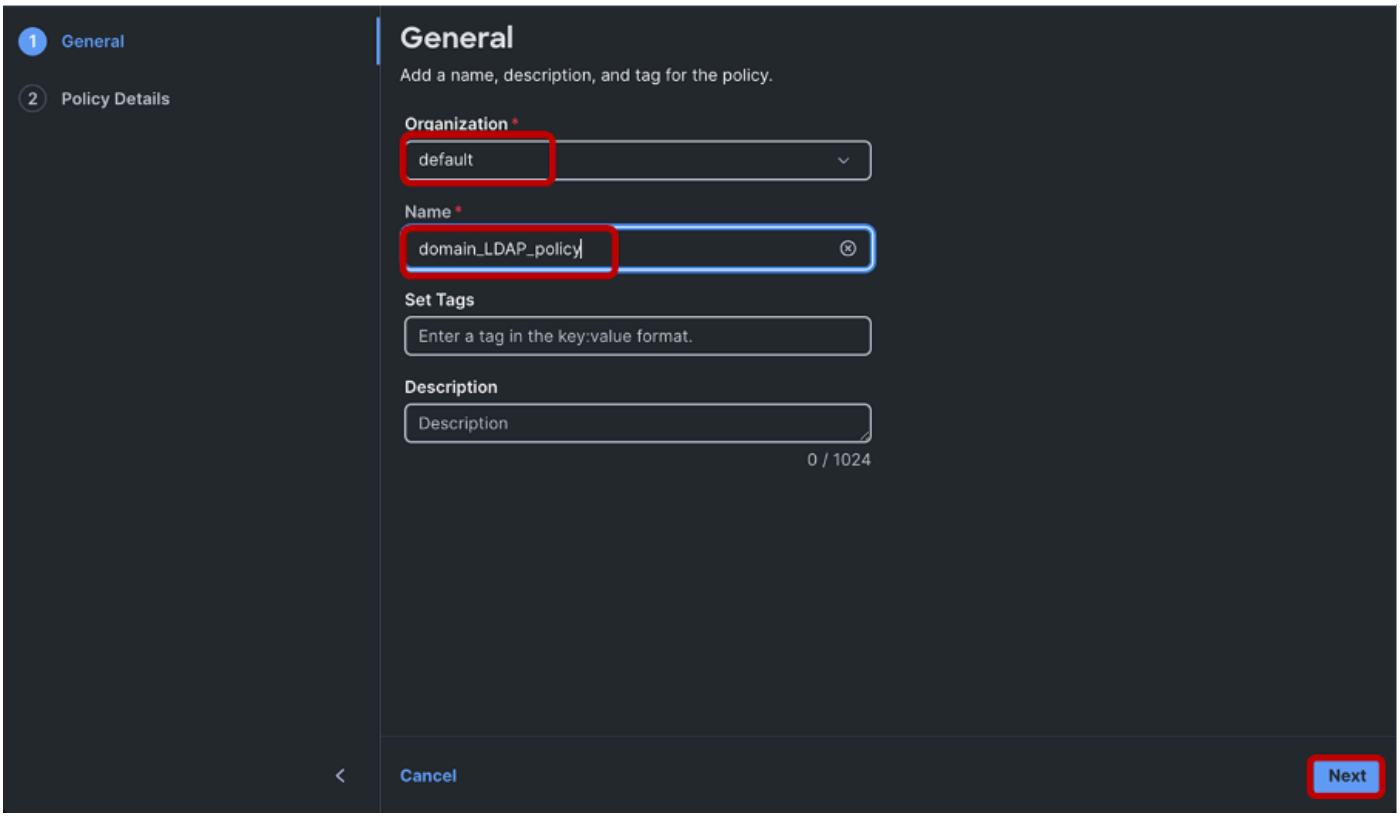


検索バーで「LDAP」を検索します。

LDAPオプションボタンを選択> Startをクリックします。

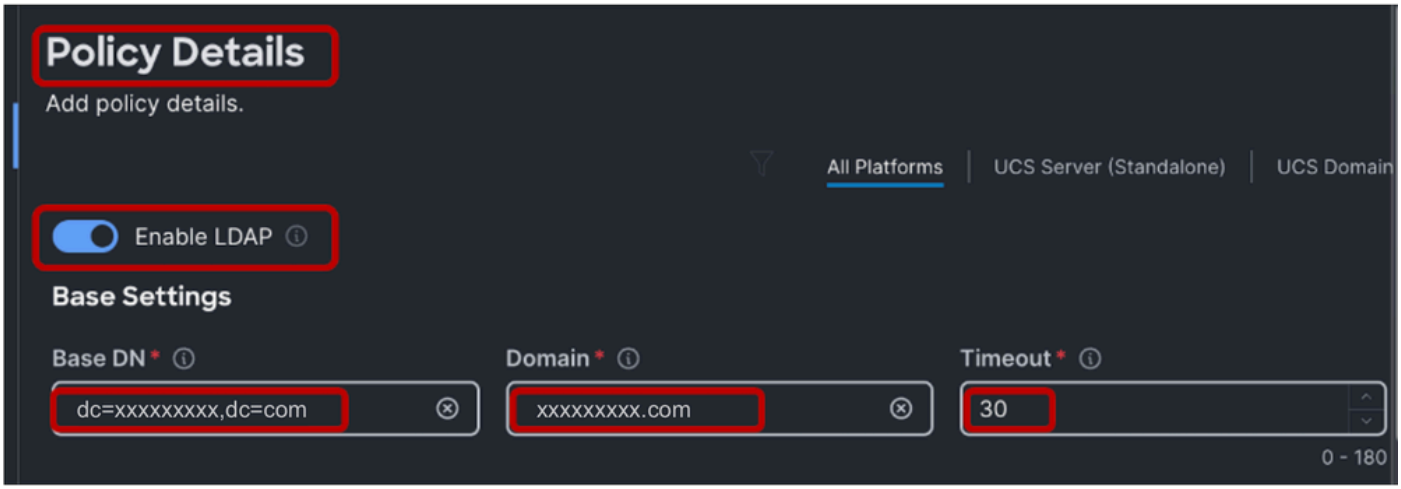


Createウィンドウで、目的の組織を選択> LDAPポリシーに名前を付けます> Nextをクリックします。



Policy Detailsセクションで、Enable LDAPスライダを選択し、Base DN、Domain、およびTimeoutの値を入力します。

Timeoutの値を0 ~ 29の間で設定すると、自動的にデフォルトの30秒に設定されます。このデモンストレーションでは、「xxxxxxxxx.com」はLDAPサーバですでに設定されている目的のドメインであり、30秒のタイムアウト値が指定されています。

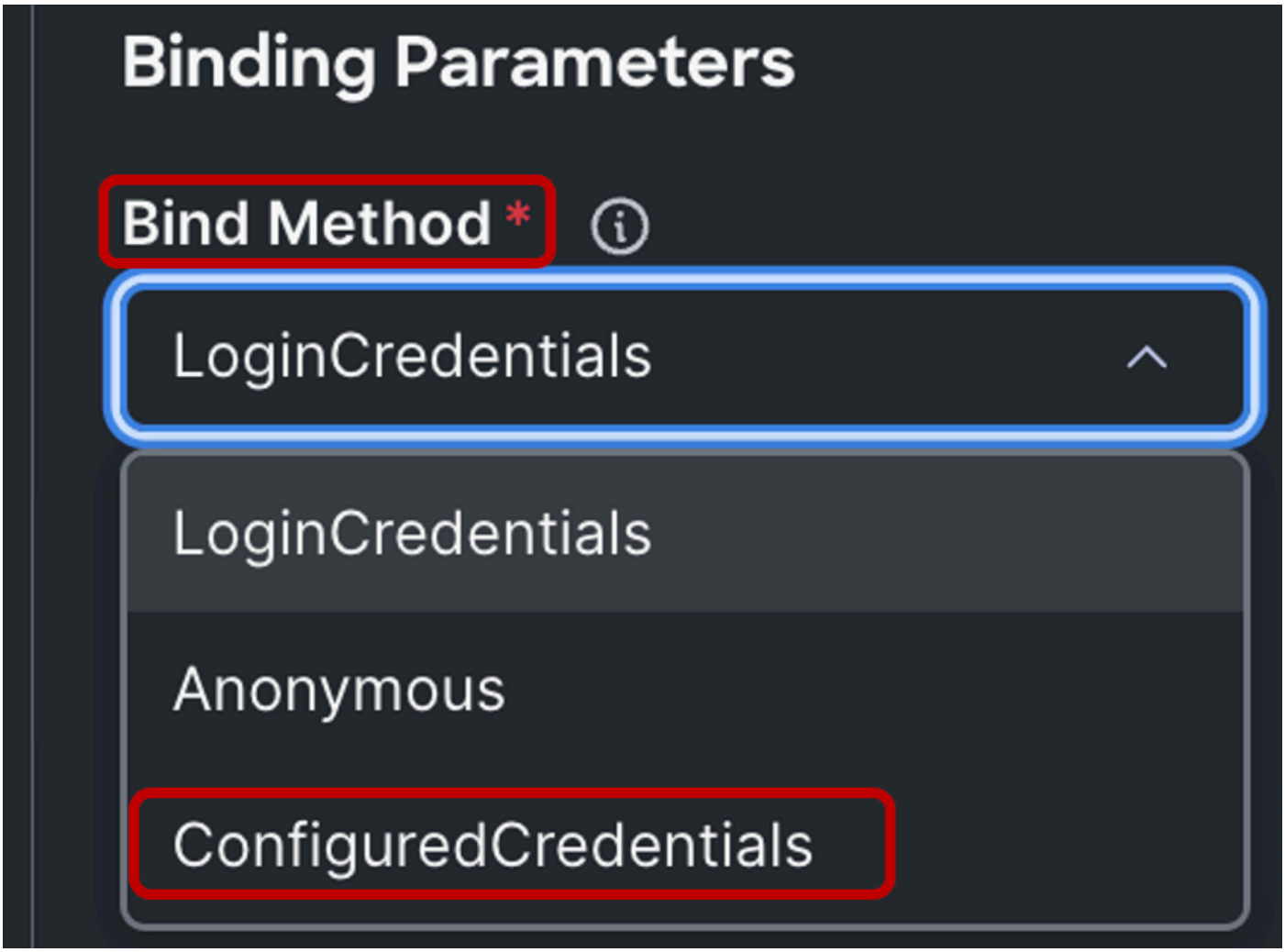


Secure LDAPを設定するには、Enable Encryptionオプションボタンを有効にします。

注：通常のLDAP設定ではIPアドレスまたはFQDNを使用できますが、署名付き証明書は必須ではありません。そのため、「標準」LDAPを設定する場合、Enable Encryptionオプション、DNS Server Network Connectivity Policy、およびCertificate Management Policy設定のCertificateは無視できます。Secure LDAPでは、LDAPサーバの名前解決とルート証明書が設定されたDNSサーバが必要です。

Binding Parametersセクションのデフォルト設定はLoginCredentialsです。この設定では、バインド操作のためにユーザのLDAPクレデンシャルを認証する個人が使用されます。これにより、専用のバインドユーザを設定する必要がなくなります。

このデモンストレーションでは、バインドユーザを設定します。したがって、「バインドメソッド」は「ConfiguredCredentials」に変更されます。

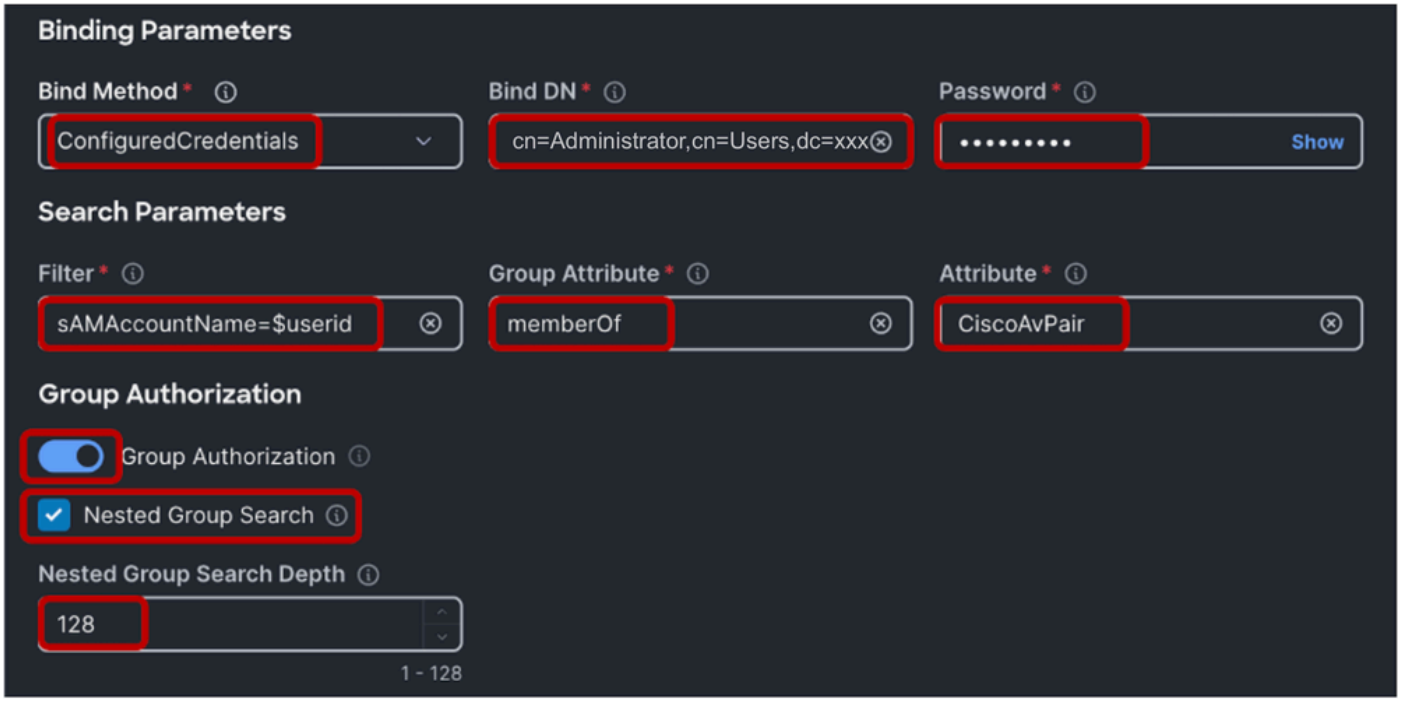


次に、バインドDN（バインドユーザ）とバインドユーザパスワードを追加します。これは、Windows Active Directory上で設定された任意のユーザにできます。このデモンストレーションでは、Administratorユーザを使用します。

「cn=Administrator,cn=Users,dc=xxxxxxxxx,dc=com'」と入力します。

検索パラメータセクションのフィルタに、「sAMAccountName=$userid」と入力します。

Group Attributesでは、「memberOf」を追加し、Attributeフィールドでは「CiscoAvPair」を追加します。LDAPサーバの設定に応じて、グループ許可とネストグループ検索を有効にできます。このデモンストレーションでは、デフォルトのNested Group Search Depth(128)を使用します。



「LDAPサーバの設定」セクションで、LDAPサーバのIPアドレスまたはFQDN（セキュアLDAPに必要）とポート番号(389)を入力します。

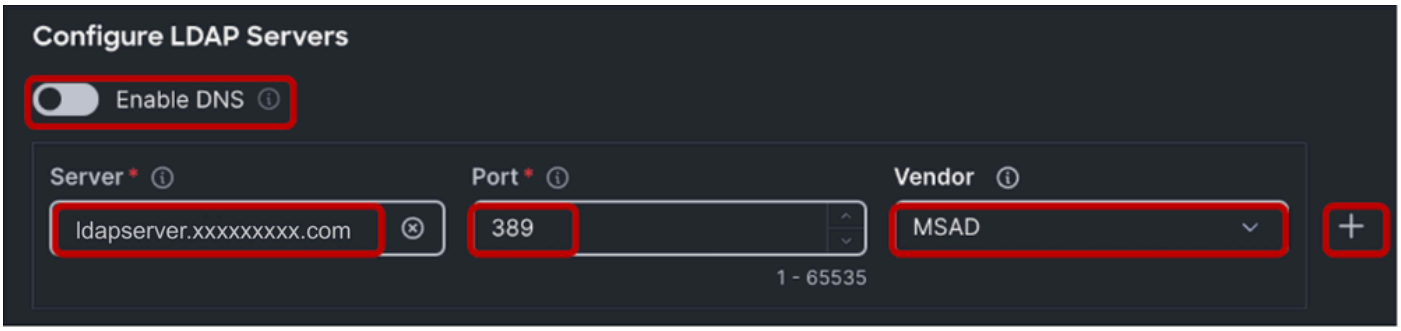
UCSのSecure LDAPはSTARTTLSを使用して、ポート389を使用した暗号化通信を有効にします。

ポートを389から636に変更すると、認証エラーが発生する可能性があることに注意してください。Cisco UCSはSSLのポート636でTLSネゴシエーションを実行しますが、最初の接続は常にポート389で暗号化されずに確立されます。

LDAPサーバベンダーを選択します。使用可能なベンダーオプションは、OpenLDAP(Microsoft Active Directory)およびMSAD(Microsoft Active Directory)です。 このデモンストレーションでは、使用中のLDAPサーバはWindows Server 2019であるため、MSADが使用されます。

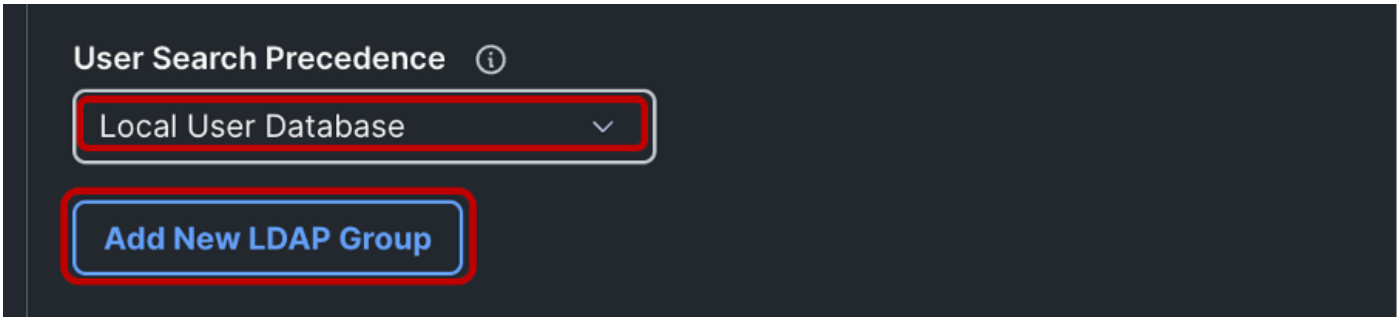
このオプションはUCSドメインのLDAP設定には適用されないため、Enable DNSボタンはオフのままにします。

複数のLDAPサーバを設定するには、Configured LDAPサーバの右端にある「+」アイコンをクリックします。

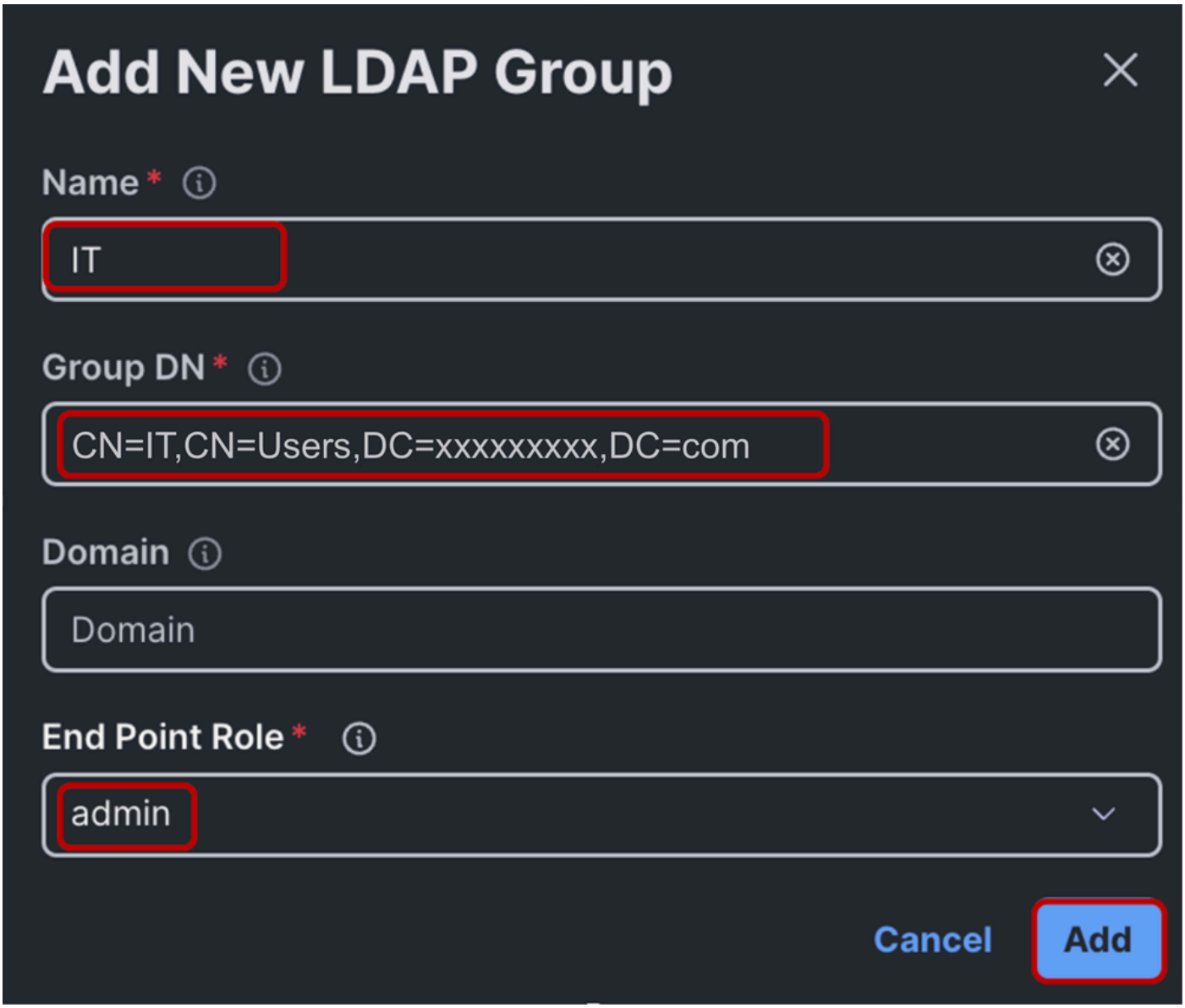


注：ユーザ検索の優先順位はローカルユーザデータベースのままにするか、ユースケースに応じてLDAPユーザデータベースに変更できます。

次に、Add New LDAP Groupボタンをクリックして、LDAPサーバで設定されたグループに対応するグループDNの追加に進みます。



グループに名前を付け、LDAPサーバから受信したグループDNを追加し、目的のエンドポイントロールを選択します。

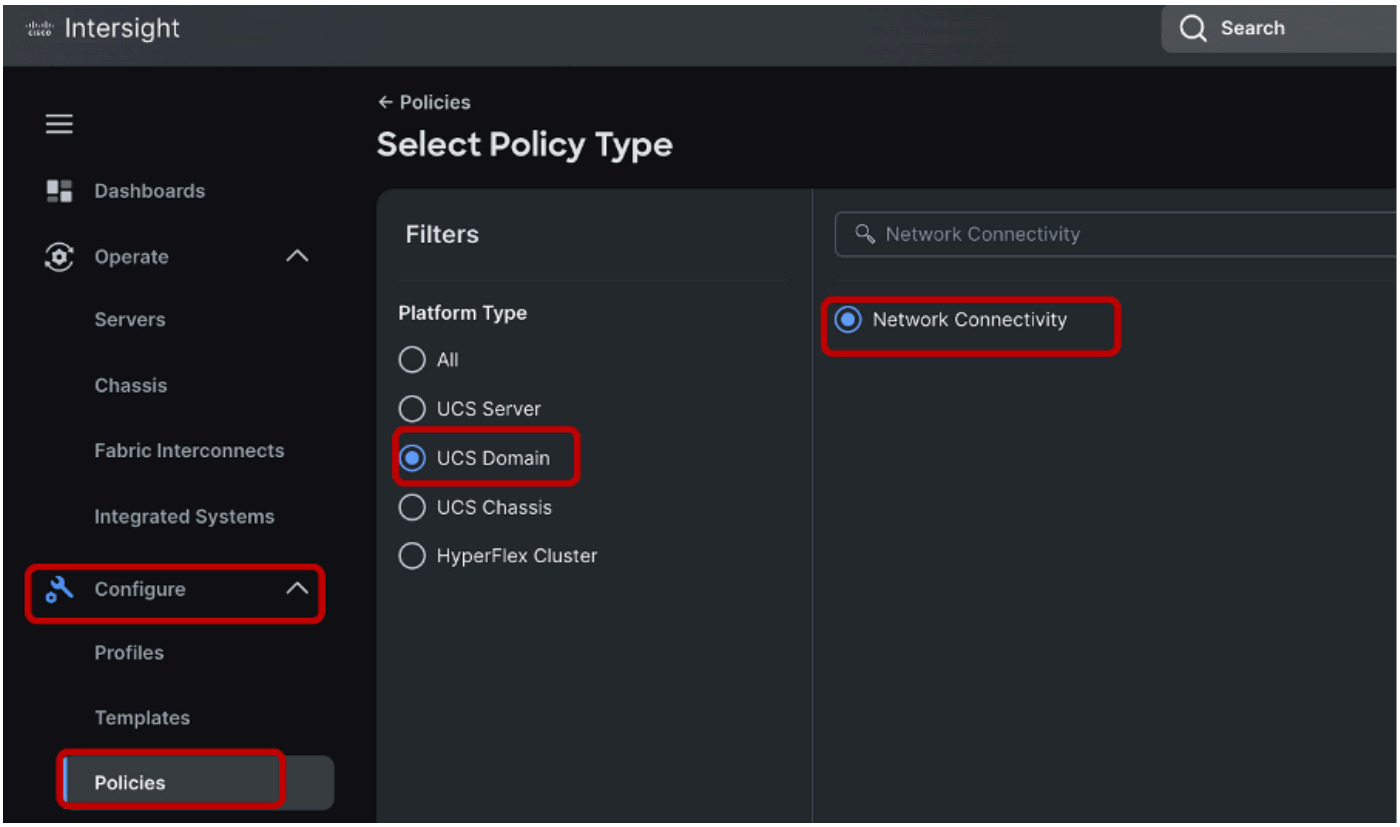


Add > Select Createの順にクリックして、LDAPポリシーを作成します

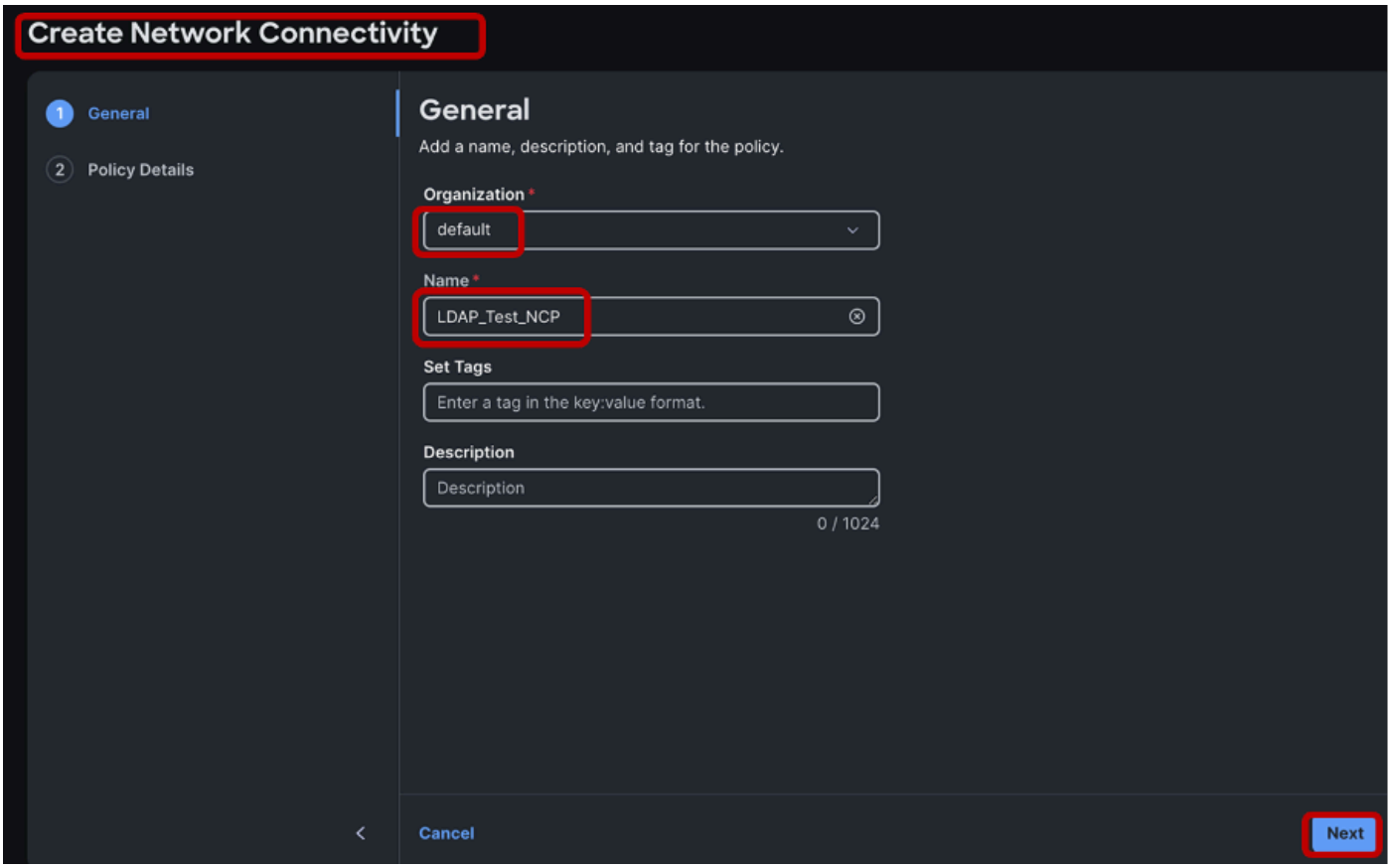
注：ドメインLDAPポリシー設定では、このドキュメントの作成時点でサポートされているエンドポイントロールは「admin」だけです。

ネットワーク接続ポリシーの設定

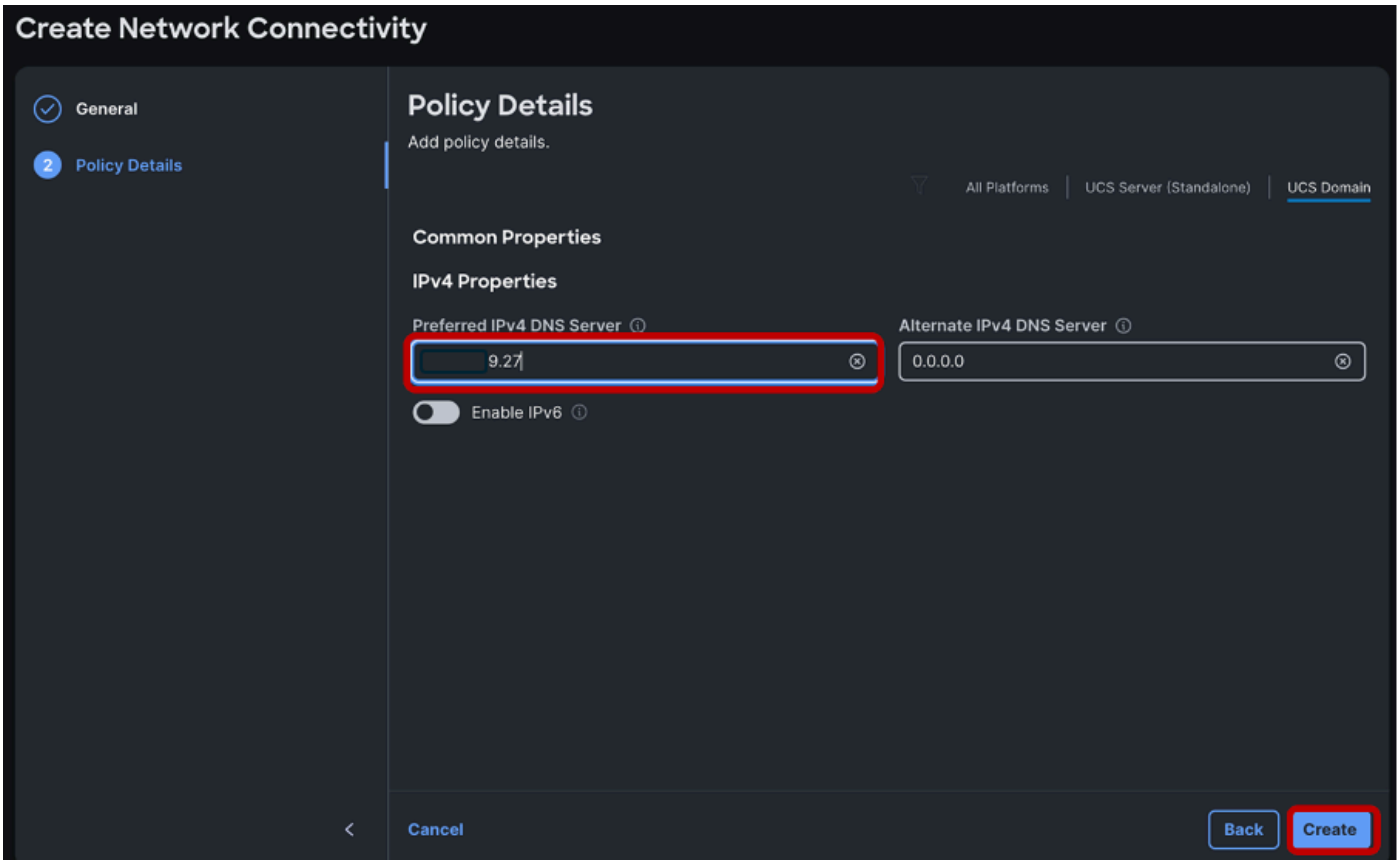
ネットワーク接続ポリシーを作成して、UCSドメインのDNSサーバを設定します。



該当する組織を選択>ポリシーの名前を入力>次へをクリックします。



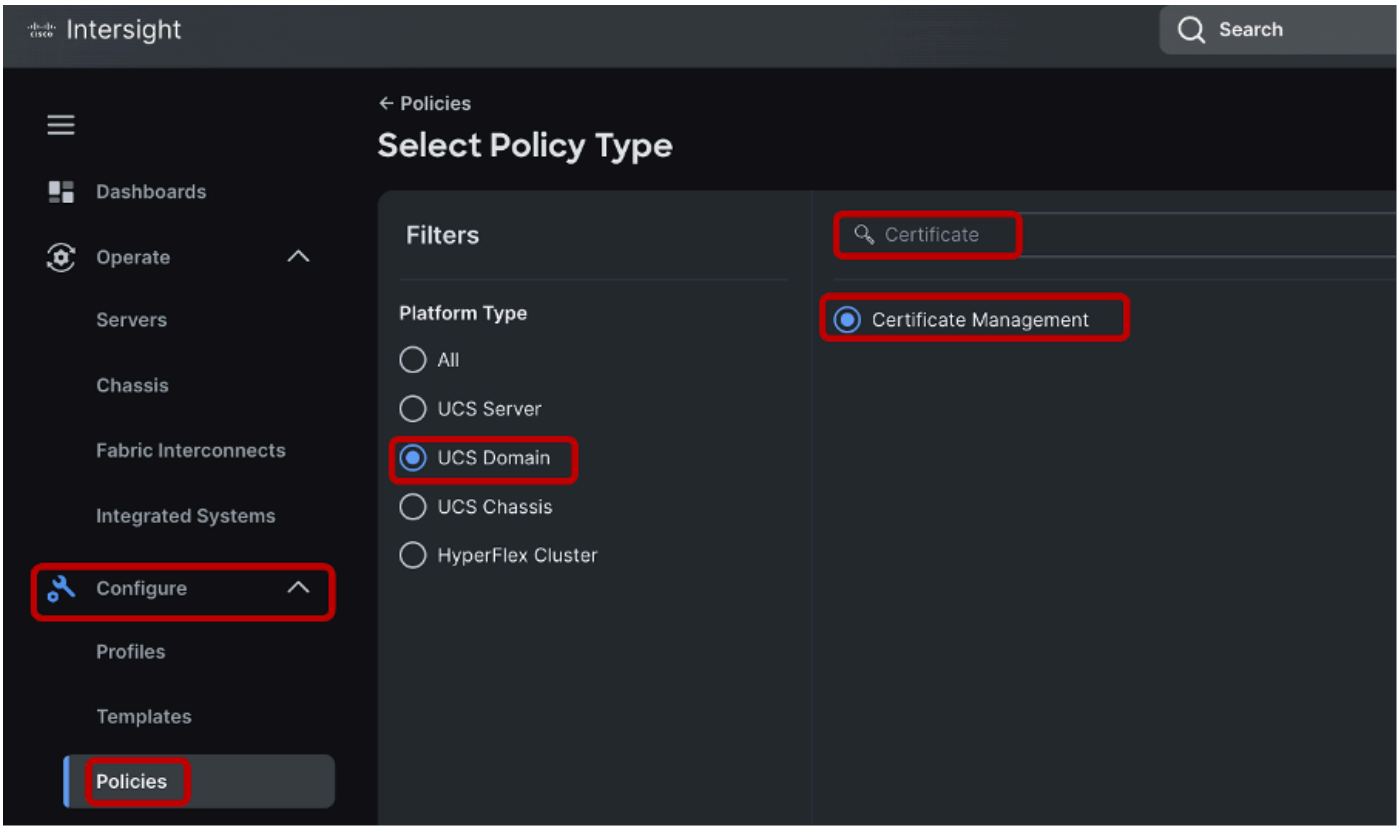
Preferred DNSサーバのIPv4アドレスを定義し、Createをクリックしてポリシーを保存します。



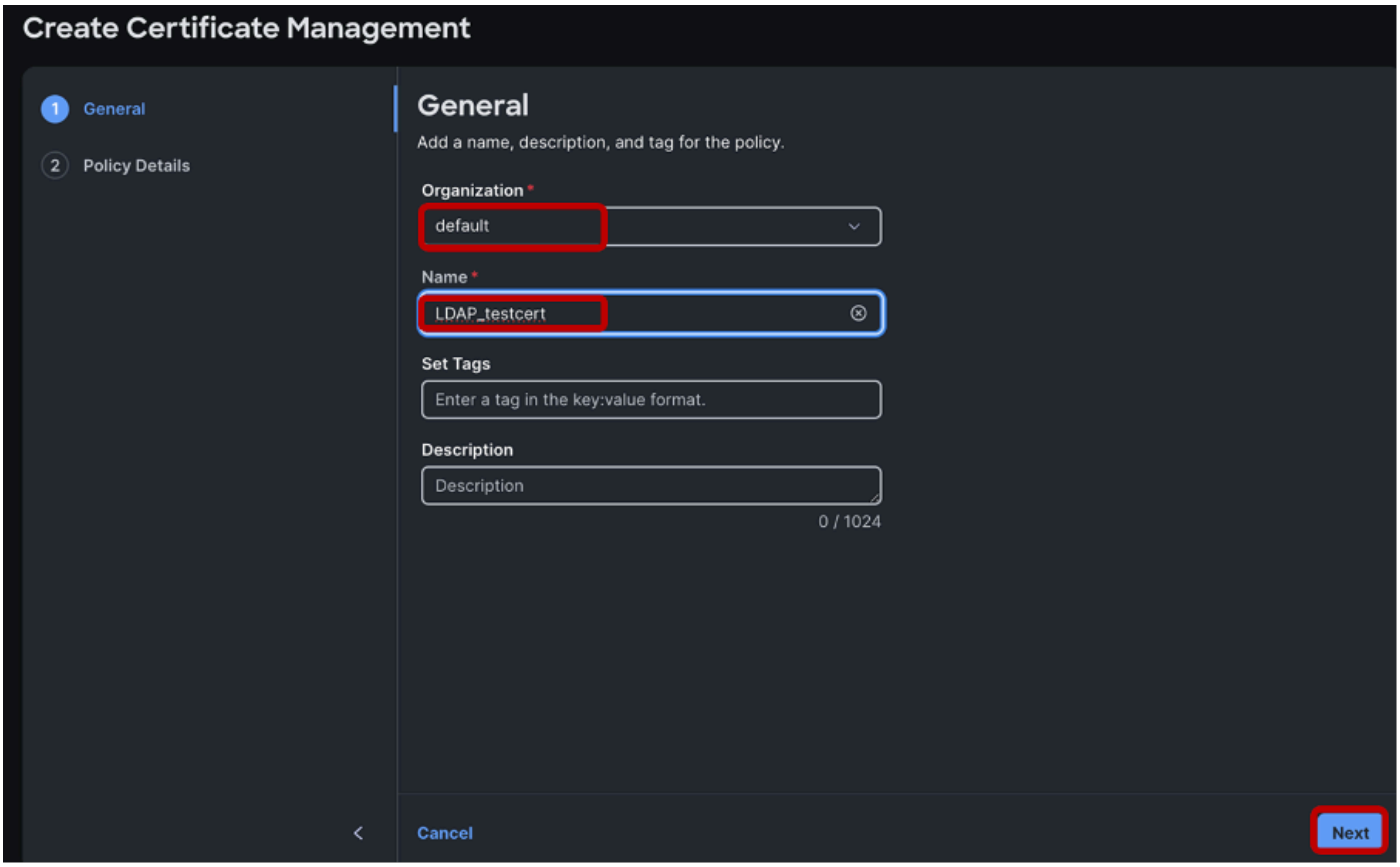
DNSサーバのIPアドレスが設定され、名前解決で到達可能であることを確認します。名前解決がドメイン内のLDAPサーバとファブリックインターコネクトで機能していることを確認します。このデモンストレーションでは、DNSサーバはLDAPサーバと同じWindowsマシンインスタンス上にあります。

証明書管理ポリシーの設定

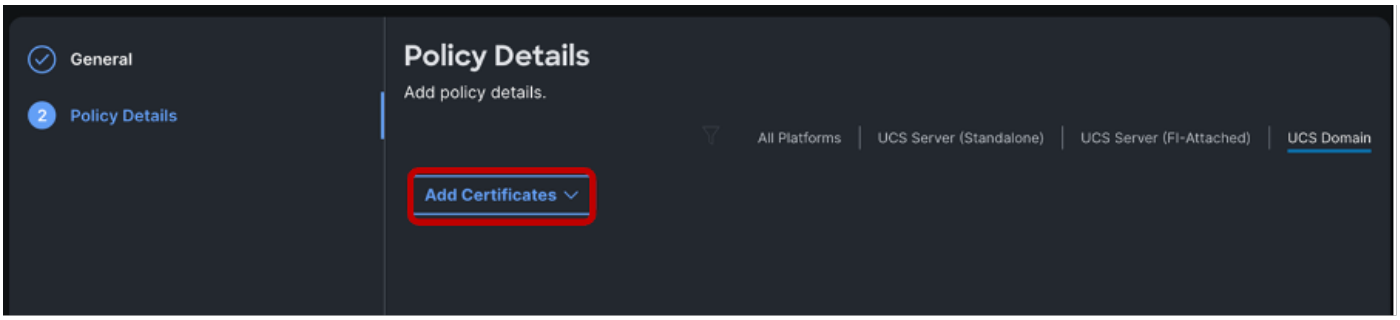
次に、証明書管理ポリシーを設定します。これは、LDAP暗号化を機能させるために必要です。



該当する組織を選択し、ポリシーに名前を付けて> Nextをクリックします

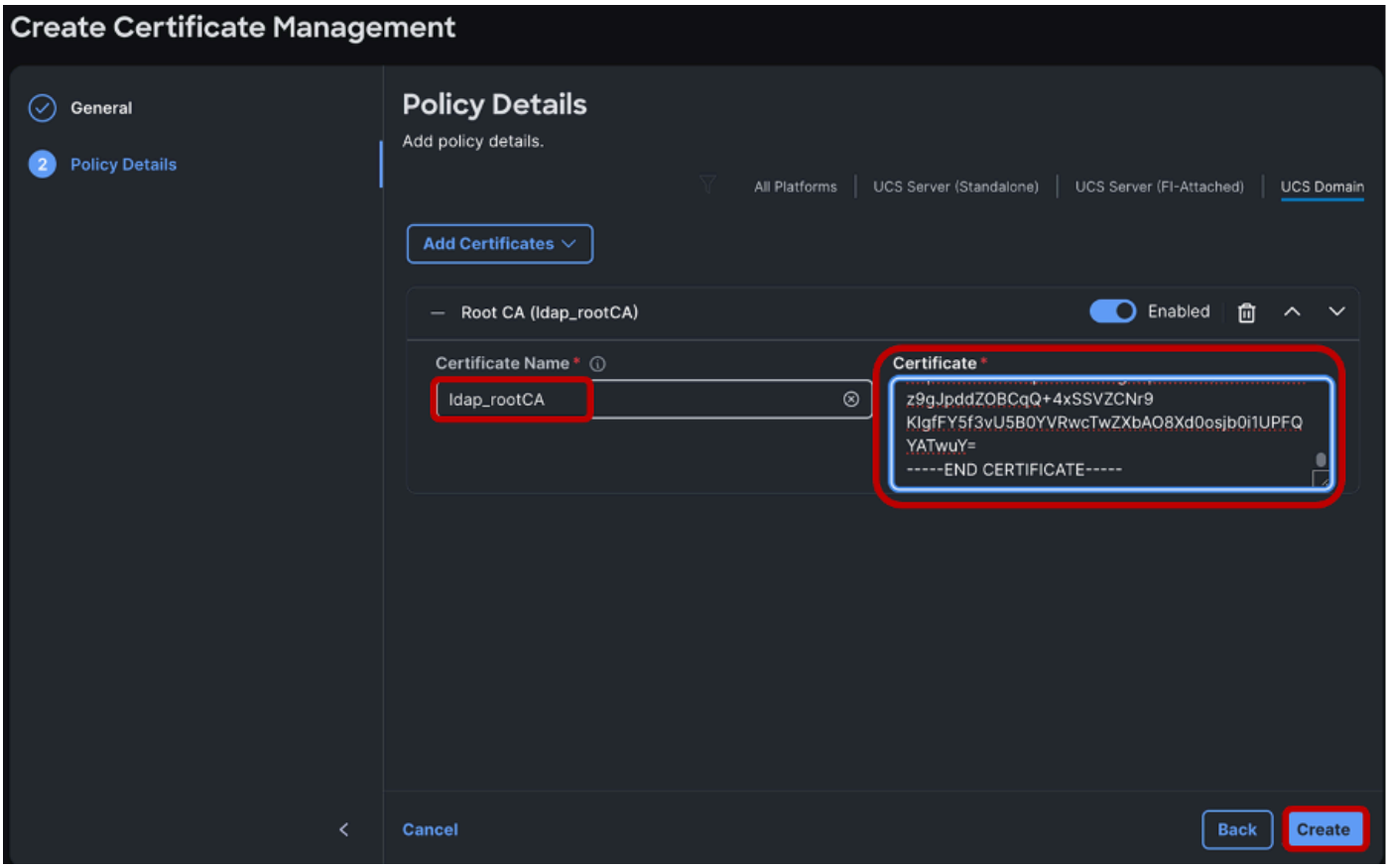


Add Certificatesをクリックします。

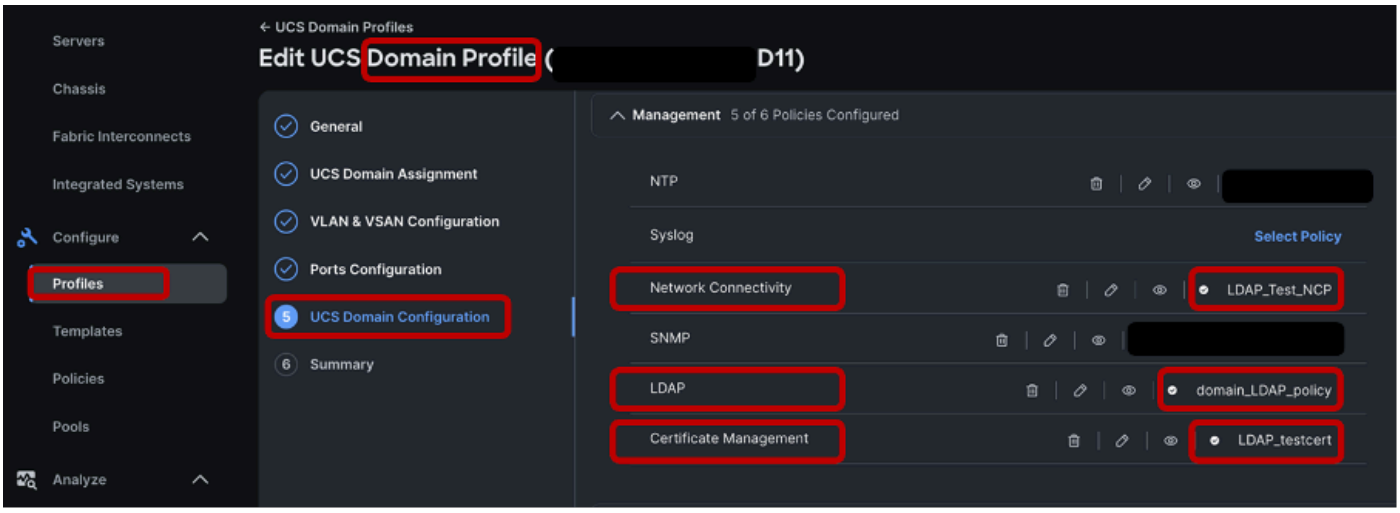


証明書に名前を付け、Microsoft Active Directory Certificate Servicesからのルート証明書に貼り付けます。

[Create] をクリックします。



LDAP、ネットワーク接続、および証明書管理ポリシーを作成した後、次に示すように、「UCSドメイン設定」セクションで、目的のドメインプロファイルに新しく作成したポリシーを参照します。



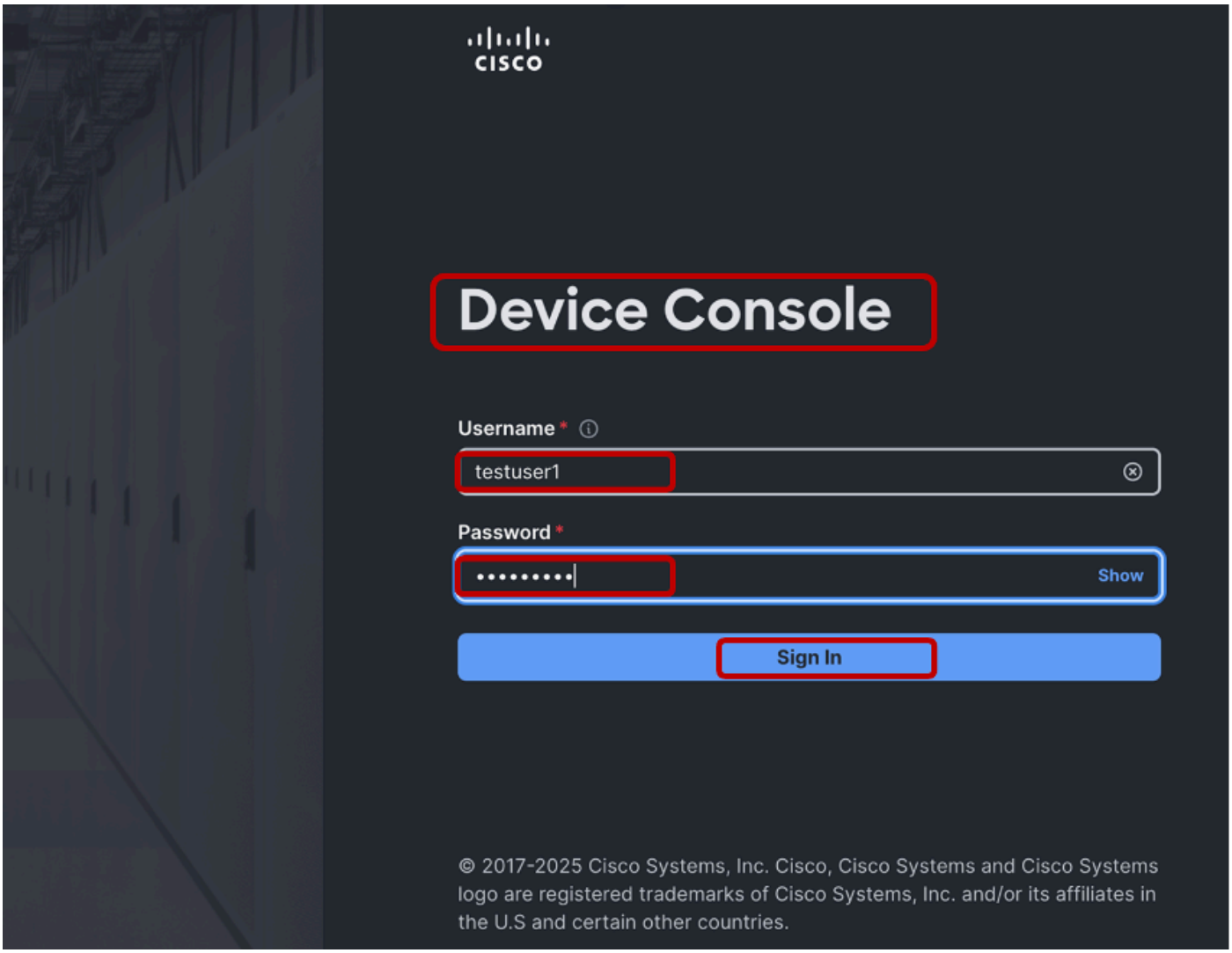
Next, Save and Deploy the domain profileをクリックします。

ドメインプロファイルの導入が成功すると、IMMドメインのセキュアLDAP設定が完了します。

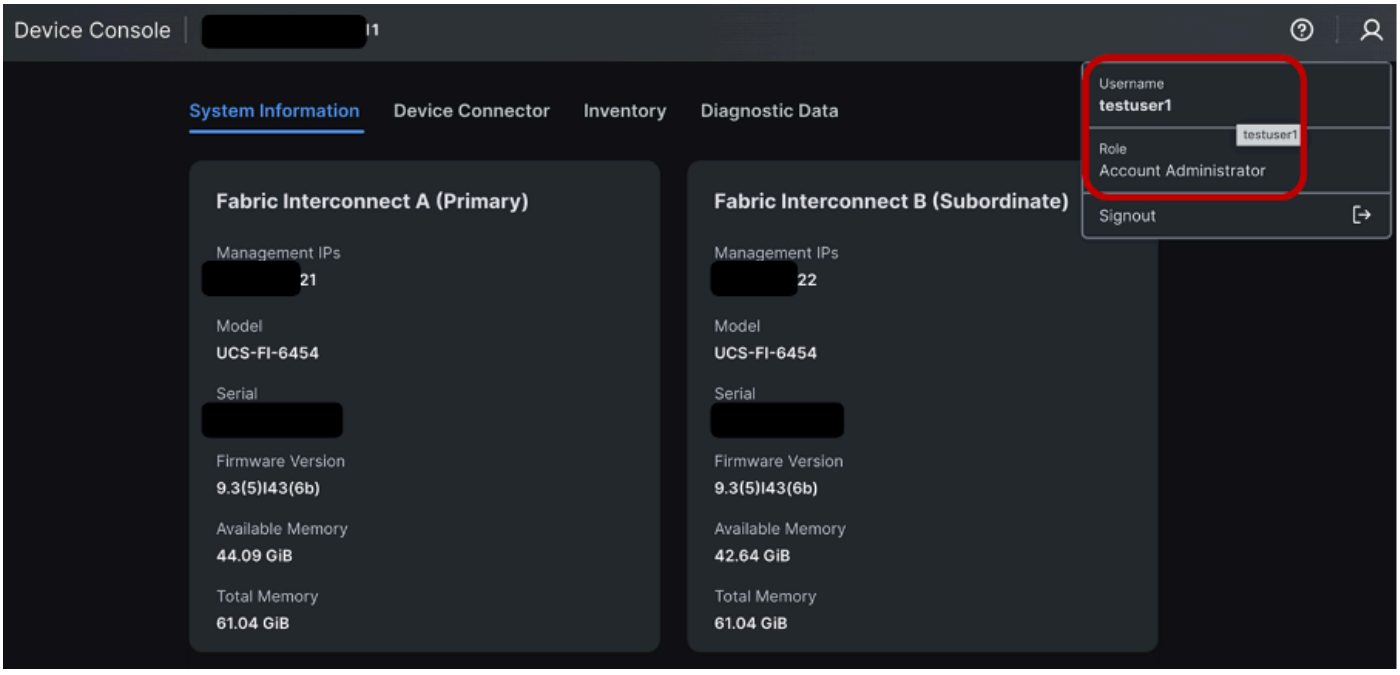
検証

これを確認するには、設定済みのLDAP/Active Directoryユーザのいずれかを使用して、デバイスコンソールGUIおよびFabric Interconnects CLI(FI)にログインします。

デバイスコンソールのログインのテスト

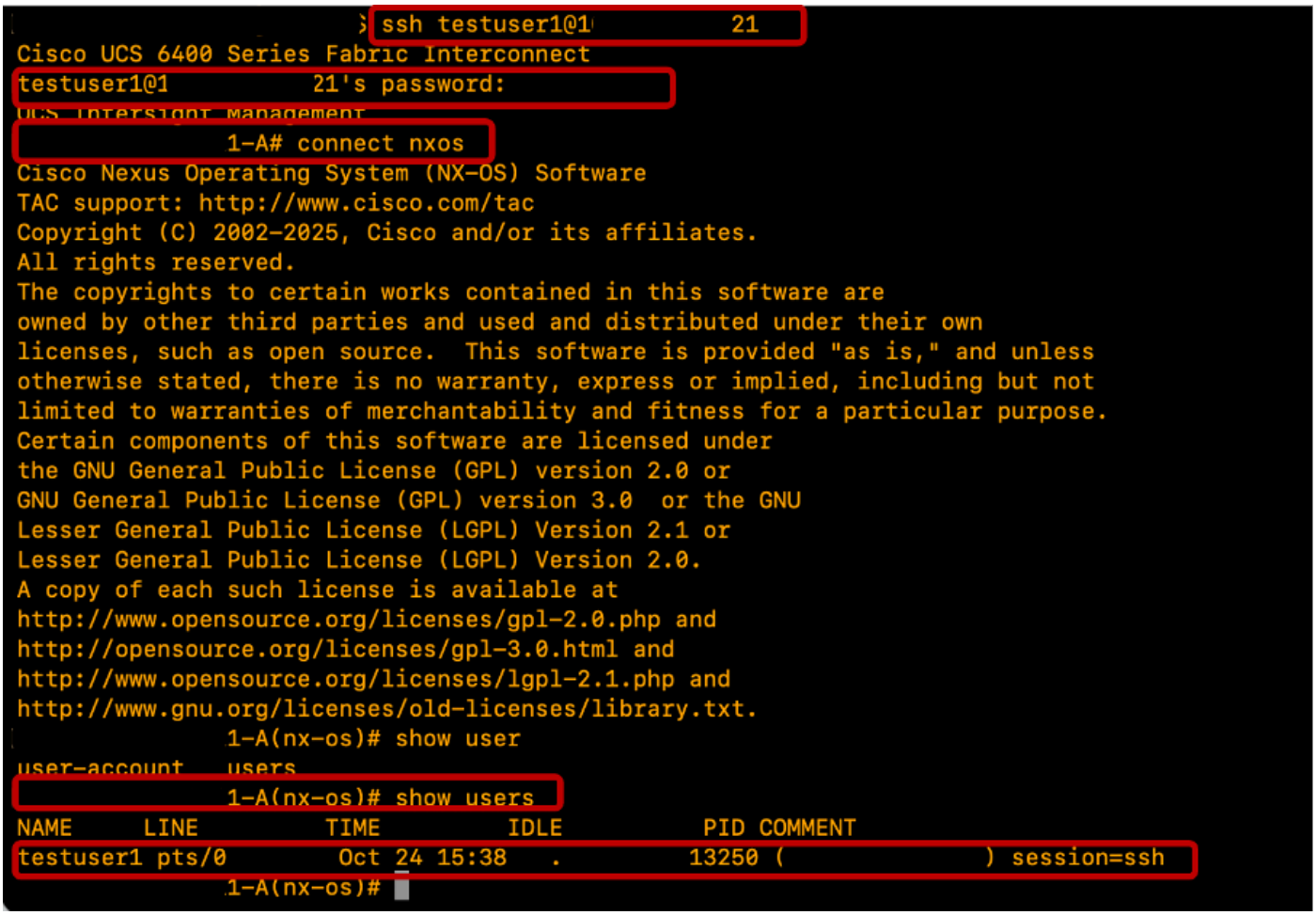


Testuser1デバイスコンソールログインが成功しました。



FIのSSHログインのテスト

Testuser1 SSHログインが成功しました。



関連情報

- Intersightヘルプセンター
- Cisco Intersightマネージドモードファブリックインターコネクト管理ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。