Sicheren LDAP-Zugriff für Fabric Interconnects im verwalteten Intersight-Modus (HTTP-Gerätekonsole und SSH) konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Domänen-LDAP-Authentifizierung mithilfe der LDAP-Richtlinie in einer Intersight-SaaS-Instanz konfigurieren.

Voraussetzungen

Anforderungen

Kenntnisse dieser Themen:

- LDAP-Protokoll (Lightweight Directory Access Protocol)
- DNS-Server (Domain Name Server)
- Cisco Interview

Verwendete Komponenten

- Cisco Intersight SaaS-Instanz
- Microsoft Active Directory
- DNS-Server
- Microsoft Active Directory-Zertifikatdienste (AD CS)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

LDAP ist ein bekanntes Protokoll, das verwendet wird, um über das Netzwerk von einem Verzeichnis auf Ressourcen zuzugreifen. Diese Verzeichnisse speichern Informationen über Benutzer, Organisationen und Ressourcen. LDAP stellt einen Standardprozess für den Zugriff auf und die Verwaltung dieser Informationen bereit, der für Authentifizierungs- und Autorisierungsprozesse verwendet werden kann.

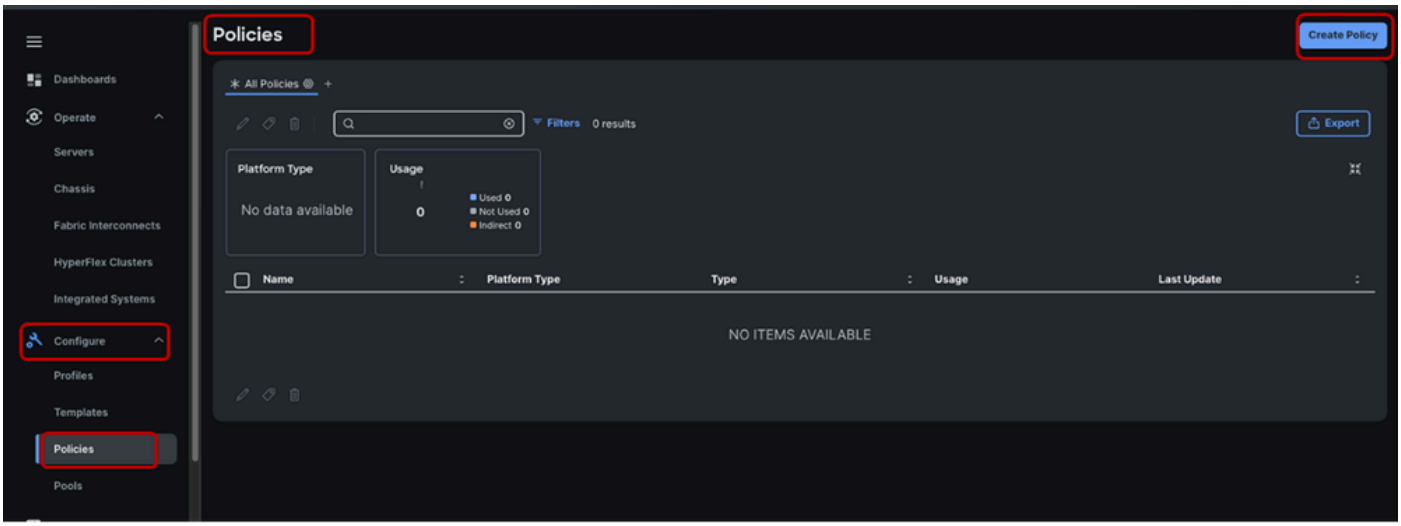
In diesem Dokument wird der Konfigurationsprozess für die Remote-Authentifizierung über sicheres LDAP für die Gerätekonsole oder die CLI (HTTP bzw. SSH) eines Peers von Fabric Interconnects im Managed Intersight-Modus beschrieben.

Konfiguration

Konfigurieren der LDAP-Richtlinie

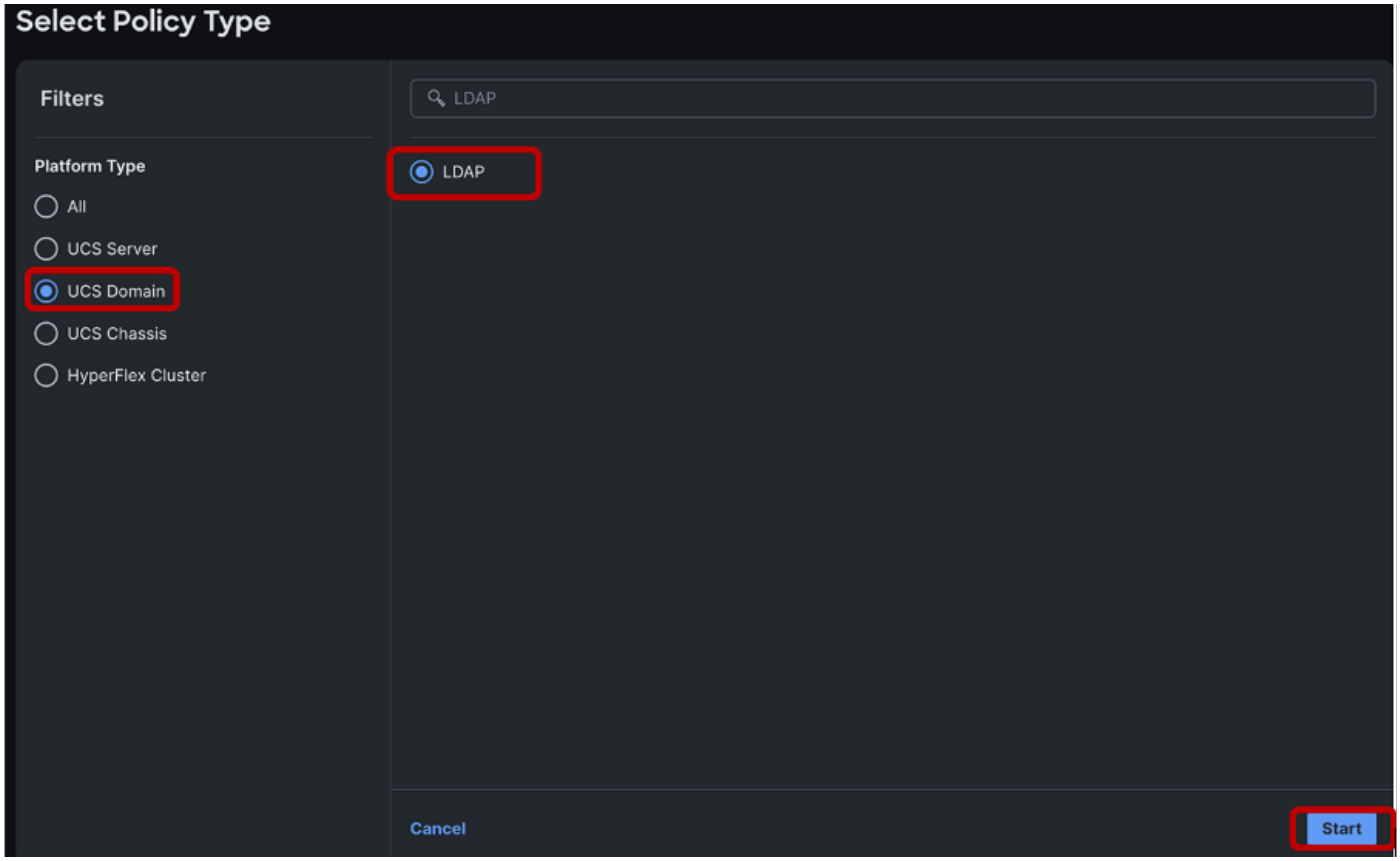
Melden Sie sich zur Konfiguration der LDAP-Richtlinie bei der Intersight-SaaS-Instanz an.

Navigieren Sie zum Abschnitt Konfigurieren > und klicken Sie auf Richtlinien.
Navigieren Sie zum Fenster "Policys" > Wählen Sie "Policy erstellen".

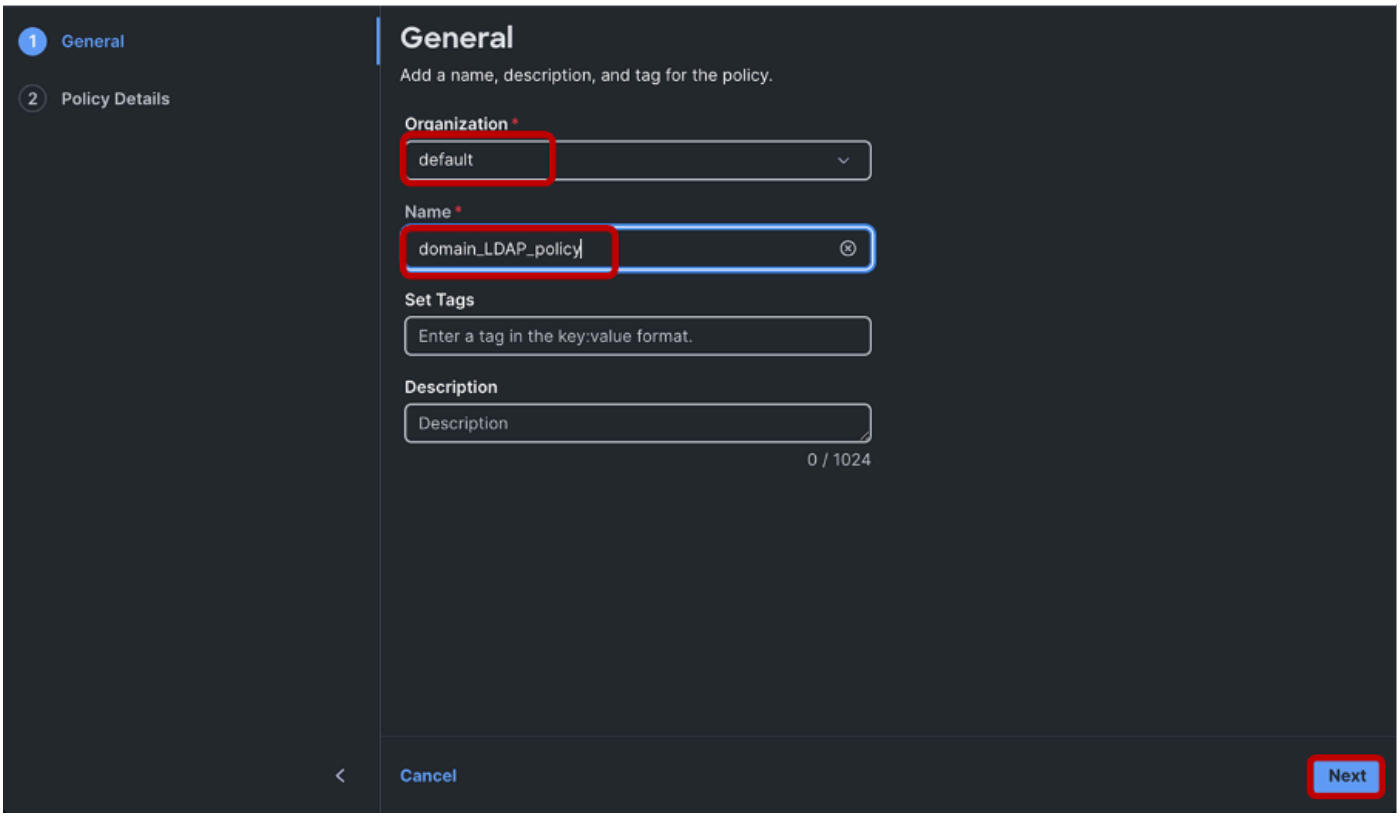


Suchen Sie in der Suchleiste nach "LDAP".

Wählen Sie das Optionsfeld LDAP aus > klicken Sie auf Start.

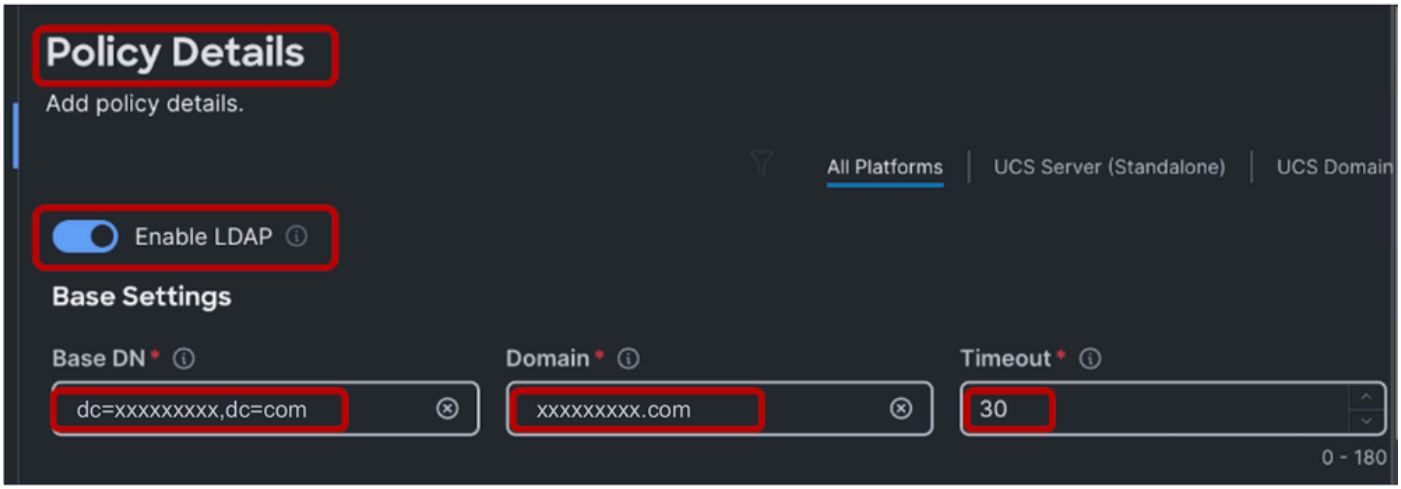


Im Fenster Erstellen > Wählen Sie die gewünschte Organisation aus > Benennen Sie die LDAP-Richtlinie > klicken Sie auf Weiter:



Im Abschnitt "Policy Details" (Richtliniendetails) > Wählen Sie den Schieberegler Enable LDAP (LDAP aktivieren) > Populate the Base DN, Domain and Timeout (Basis-DN, Domäne und Timeout) aus.

Der Wert für die Zeitüberschreitung, der zwischen 0 und 29 liegt, wird automatisch auf 30 Sekunden zurückgesetzt. Für diese Demonstration ist "xxxxxxx.com" die gewünschte Domäne, die bereits auf dem LDAP-Server konfiguriert wurde, und es wurde ein Wert für die Zeitüberschreitung von 30 Sekunden angegeben.

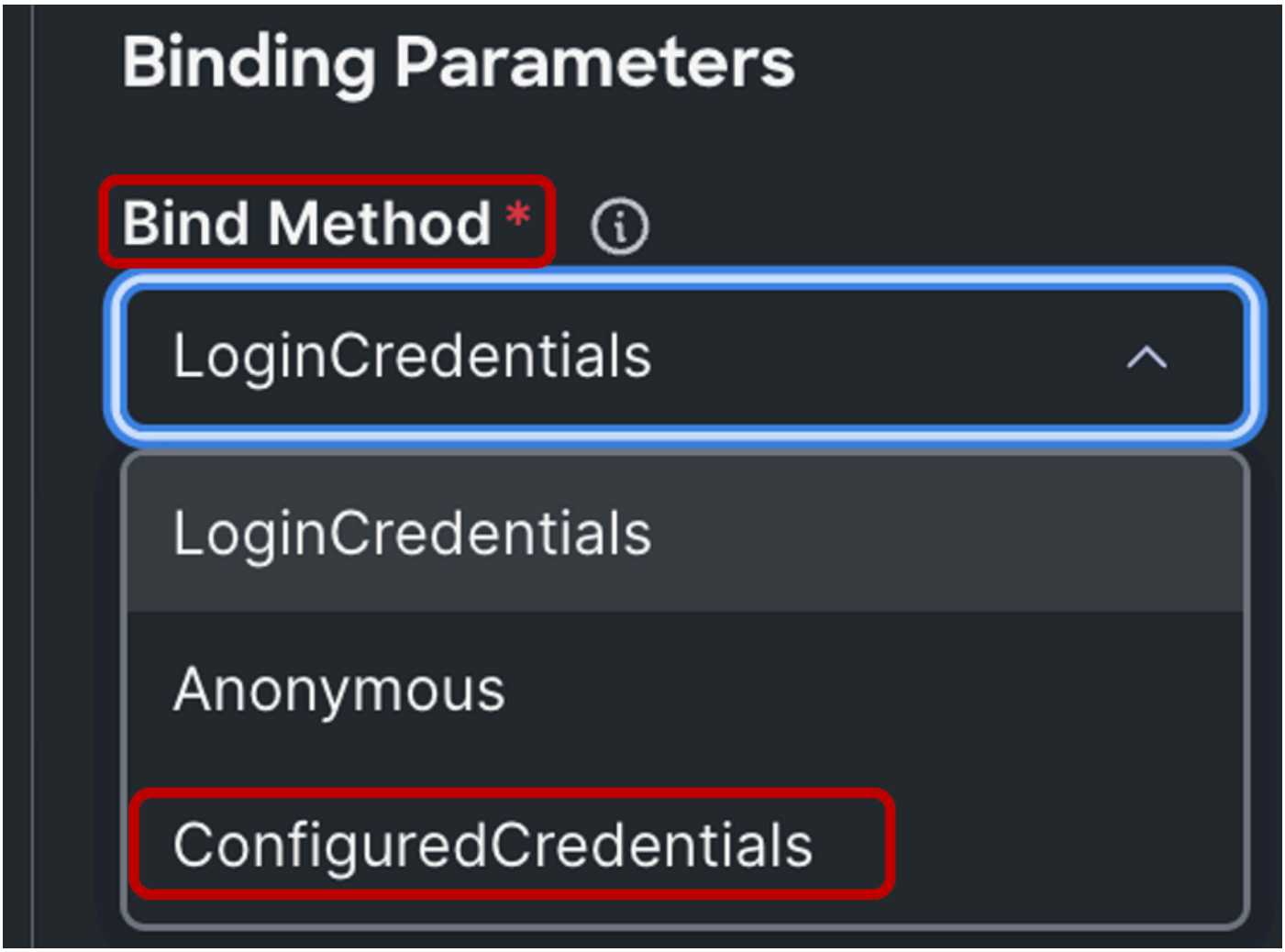


Aktivieren Sie zum Konfigurieren von sicherem LDAP das Optionsfeld Verschlüsselung aktivieren.

Anmerkung: Bei der üblichen LDAP-Konfiguration kann entweder eine IP-Adresse oder ein FQDN verwendet werden, ein signiertes Zertifikat ist jedoch nicht erforderlich. Daher können bei der Konfiguration von "Standard"-LDAP die Option "Verschlüsselung aktivieren", die DNS-Server-Netzwerkverbindungsrichtlinie und ein Zertifikat in den Konfigurationen der Zertifikatverwaltungsrichtlinie ignoriert werden. Für sicheres LDAP ist ein DNS-Server erforderlich, der für die LDAP-Servernamenauflösung konfiguriert ist, sowie ein Root-Zertifikat.

Die Standardeinstellung im Abschnitt "Bindungsparameter" ist "LoginCredentials". Dabei wird die Person verwendet, die die LDAP-Benutzeranmeldeinformationen für den Bindungsvorgang authentifiziert. Dadurch muss kein dedizierter Bind-Benutzer mehr konfiguriert werden.

Für diese Demonstration wird ein Bind-Benutzer konfiguriert. Daher wird die "Bind-Methode" in "ConfiguredCredentials" geändert.

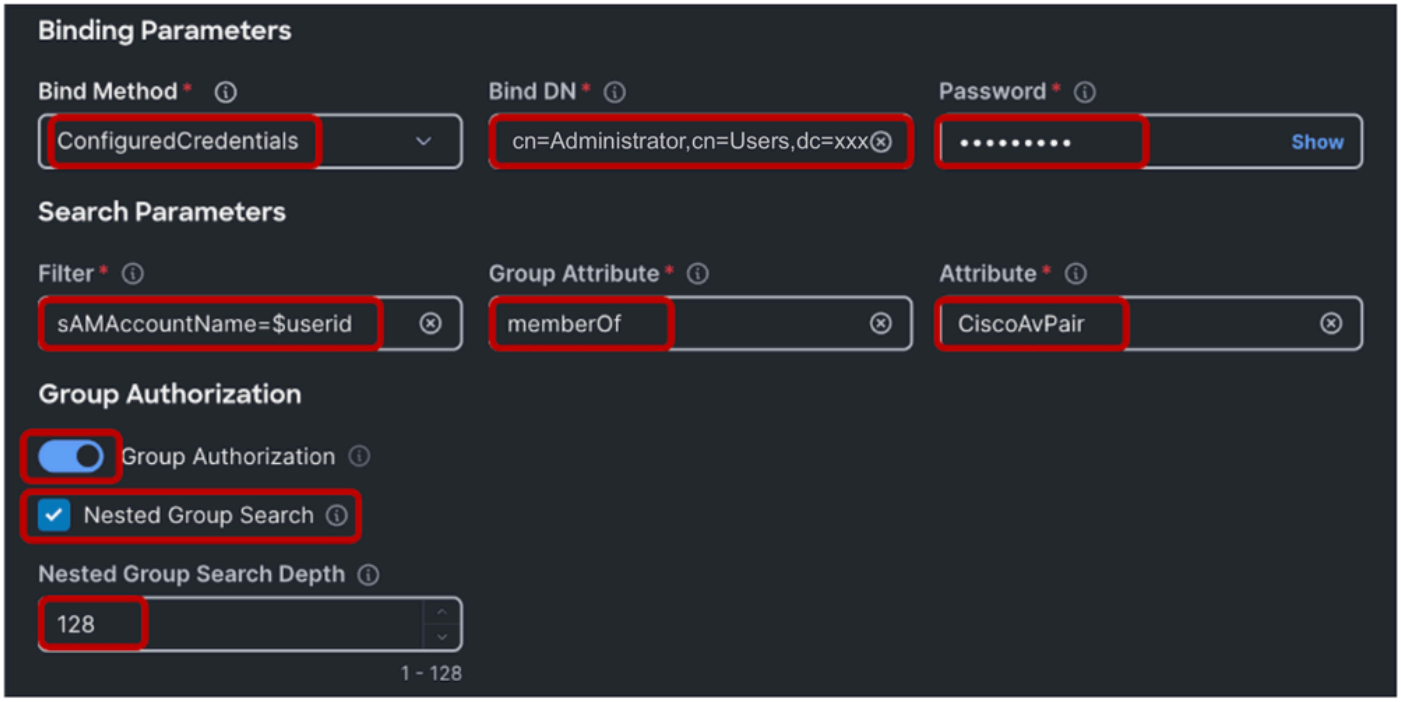


Fügen Sie dann eine Bind-DN (ein Bind-Benutzer) und das Bind-Benutzerkennwort hinzu. Dies kann eine beliebige Benutzerkonfiguration in Windows Active Directory sein. In dieser Demonstration wird der Administrator-Benutzer verwendet.

"cn=Administrator,cn=Users,dc=xxxxxxxxx,dc=com".

Geben Sie im Abschnitt "Suchparameter" unter "Filter" "sAMAccountName=$userid" ein.

Fügen Sie für Gruppenattribute "memberOf" und im Feld "Attribute" "CiscoAvPair" hinzu. Je nach LDAP-Serverkonfiguration können Sie die Gruppenautorisierung und die Suche nach verschachtelten Gruppen aktivieren. Für diese Demonstration wird die Standardsuchtiefe für verschachtelte Gruppen bei 128 verwendet.



Geben Sie im Abschnitt "LDAP-Server konfigurieren" > die IP-Adresse oder den FQDN (erforderlich für sicheres LDAP) und die Portnummer (389) des LDAP-Servers ein.

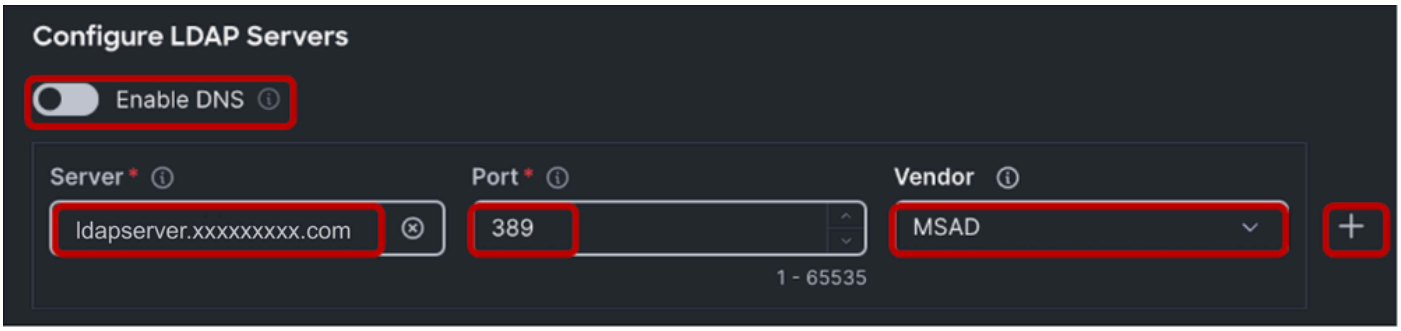
Secure LDAP im UCS verwendet STARTTLS, um die verschlüsselte Kommunikation über Port 389 zu aktivieren.

Beachten Sie, dass eine Änderung des Ports von 389 in 636 zu Authentifizierungsfehlern führen kann. Cisco UCS führt TLS-Aushandlung an Port 636 für SSL durch. Die erste Verbindung wird jedoch immer unverschlüsselt auf Port 389 hergestellt.

Wählen Sie den LDAP-Serveranbieter aus. Die verfügbaren Anbieteroptionen sind OpenLDAP und MSAD (Microsoft Active Directory). Da es sich bei dem verwendeten LDAP-Server um Windows Server 2019 handelt, wird für diese Demonstration MSAD verwendet.

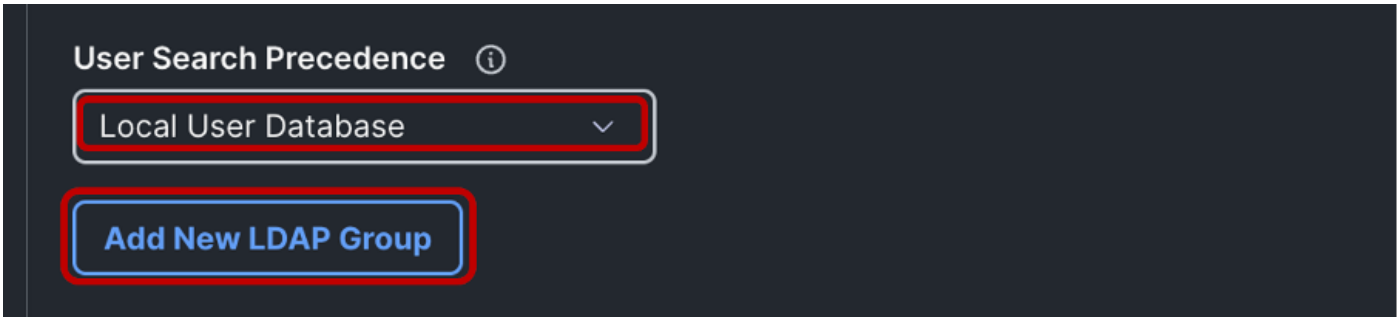
Lassen Sie die Schaltfläche Enable DNS (DNS aktivieren) AUS, da diese Option nicht für die LDAP-Konfiguration in der UCS-Domäne gilt.

Sie können mehrere LDAP-Server konfigurieren, indem Sie auf das "+"-Symbol ganz rechts neben dem konfigurierten LDAP-Server klicken.

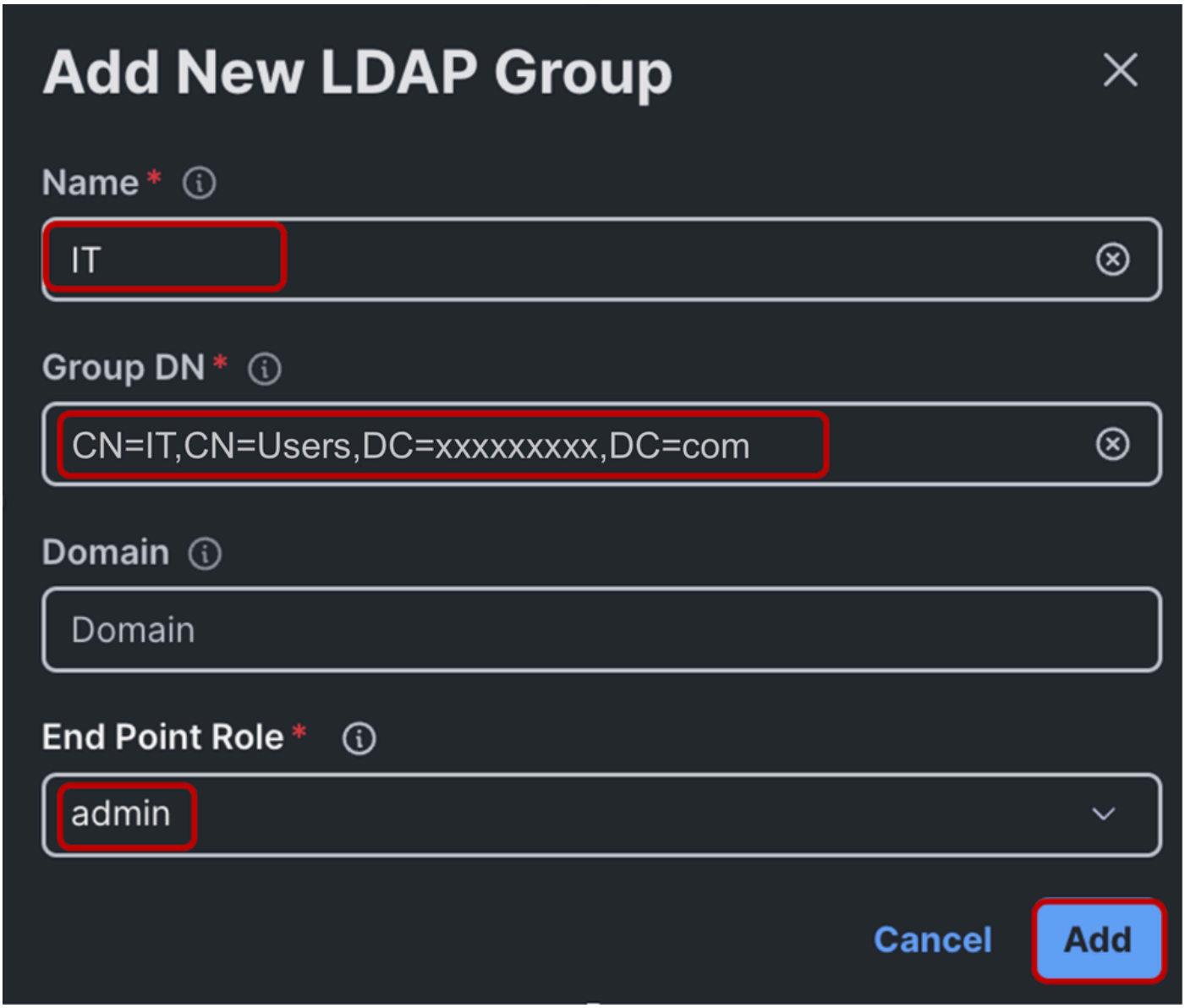


Anmerkung: Sie können die Rangfolge der Benutzersuche als lokale Benutzerdatenbank beibehalten oder je nach Anwendungsfall in die LDAP-Benutzerdatenbank ändern.

Als Nächstes fügen Sie eine Gruppen-DN hinzu, die der im LDAP-Server konfigurierten Gruppe entspricht, indem Sie auf die Schaltfläche Neue LDAP-Gruppe hinzufügen klicken.



Geben Sie der Gruppe einen Namen, fügen Sie die vom LDAP-Server empfangene Gruppen-DN hinzu, und wählen Sie die gewünschte Endpunktrolle aus.

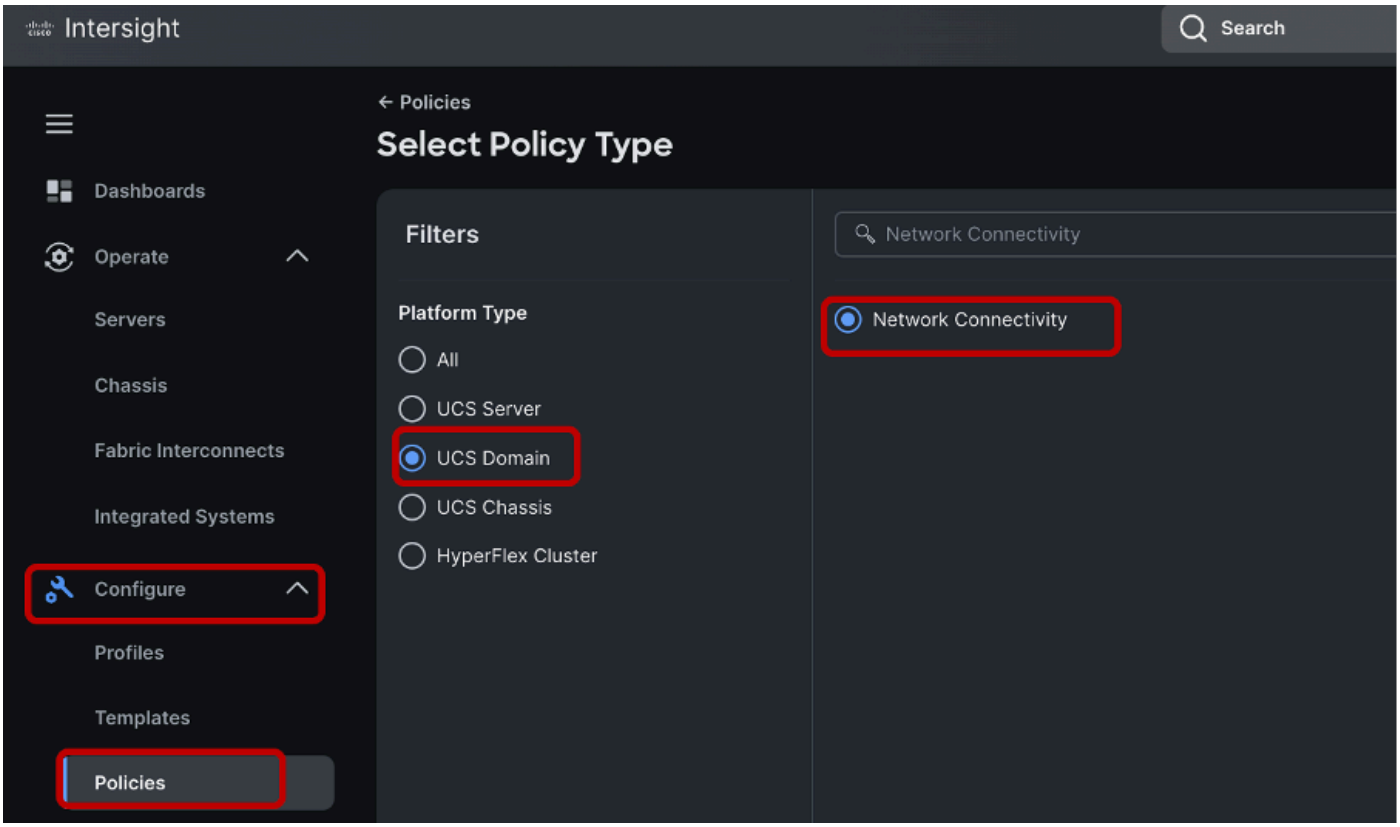


Klicken Sie auf Hinzufügen > Wählen Sie Erstellen aus, um die LDAP-Richtlinie zu erstellen.

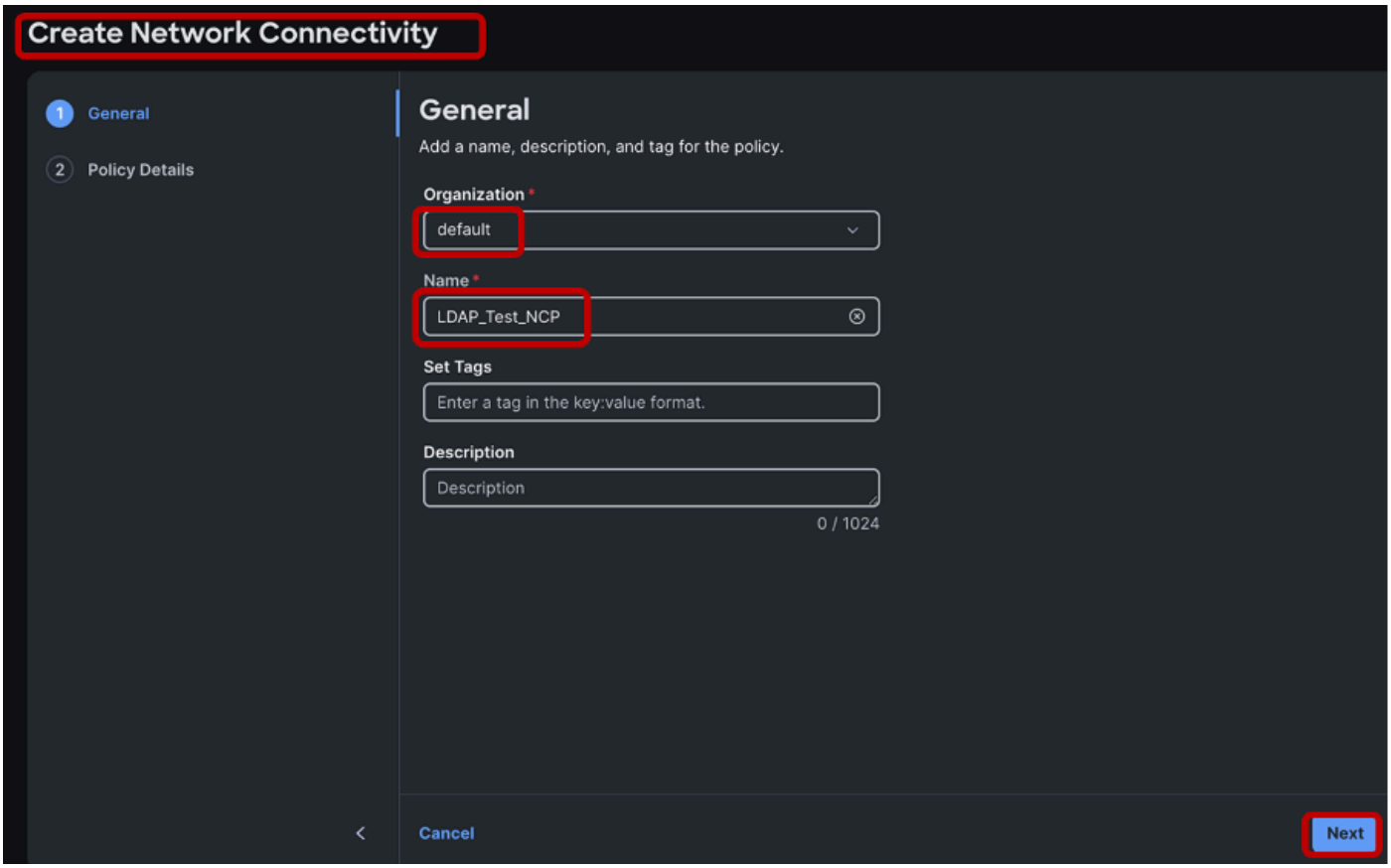
Anmerkung: Bei der Konfiguration der LDAP-Domänenrichtlinien ist die einzige unterstützte Endpunktrolle zum Zeitpunkt der Dokumenterstellung "admin".

Netzwerkverbindungsrichtlinie konfigurieren

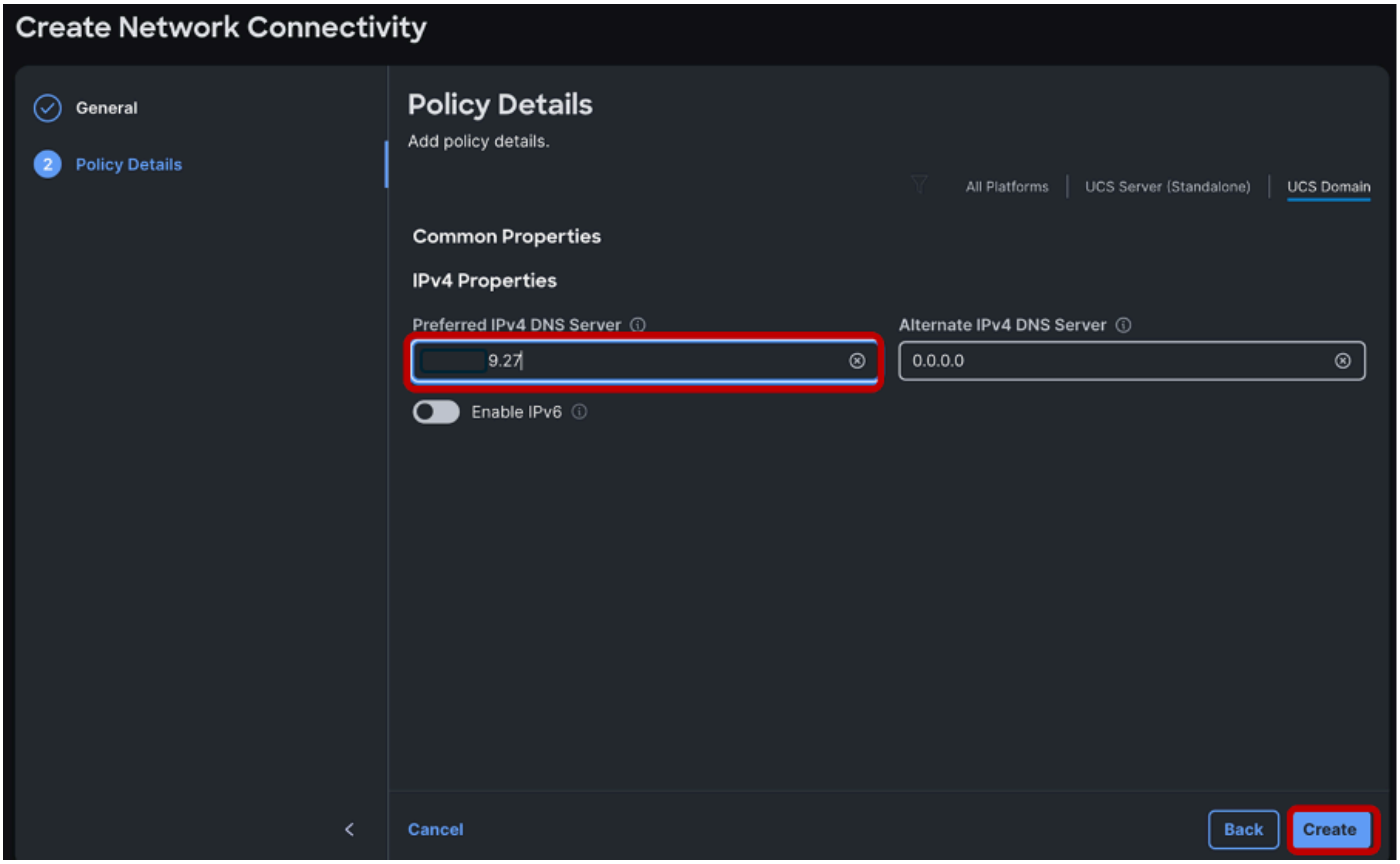
Konfigurieren Sie einen DNS-Server für die UCS-Domäne, indem Sie eine Netzwerkverbindungsrichtlinie erstellen.



Wählen Sie die entsprechende Organisation aus > geben Sie den Namen der Richtlinie ein > klicken Sie auf Weiter.



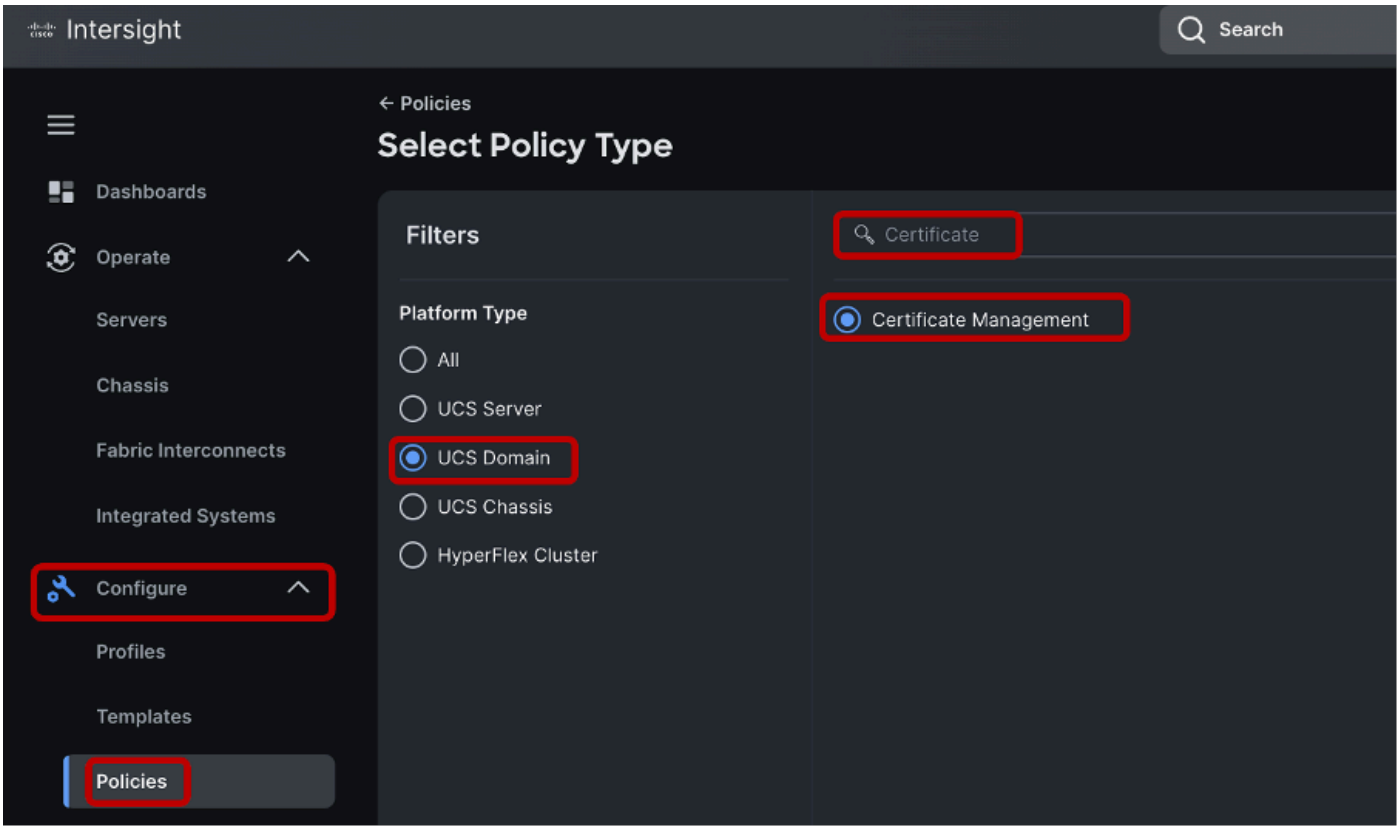
Definieren Sie eine IPv4-Adresse des bevorzugten DNS-Servers, und klicken Sie auf Erstellen, um die Richtlinie zu speichern.



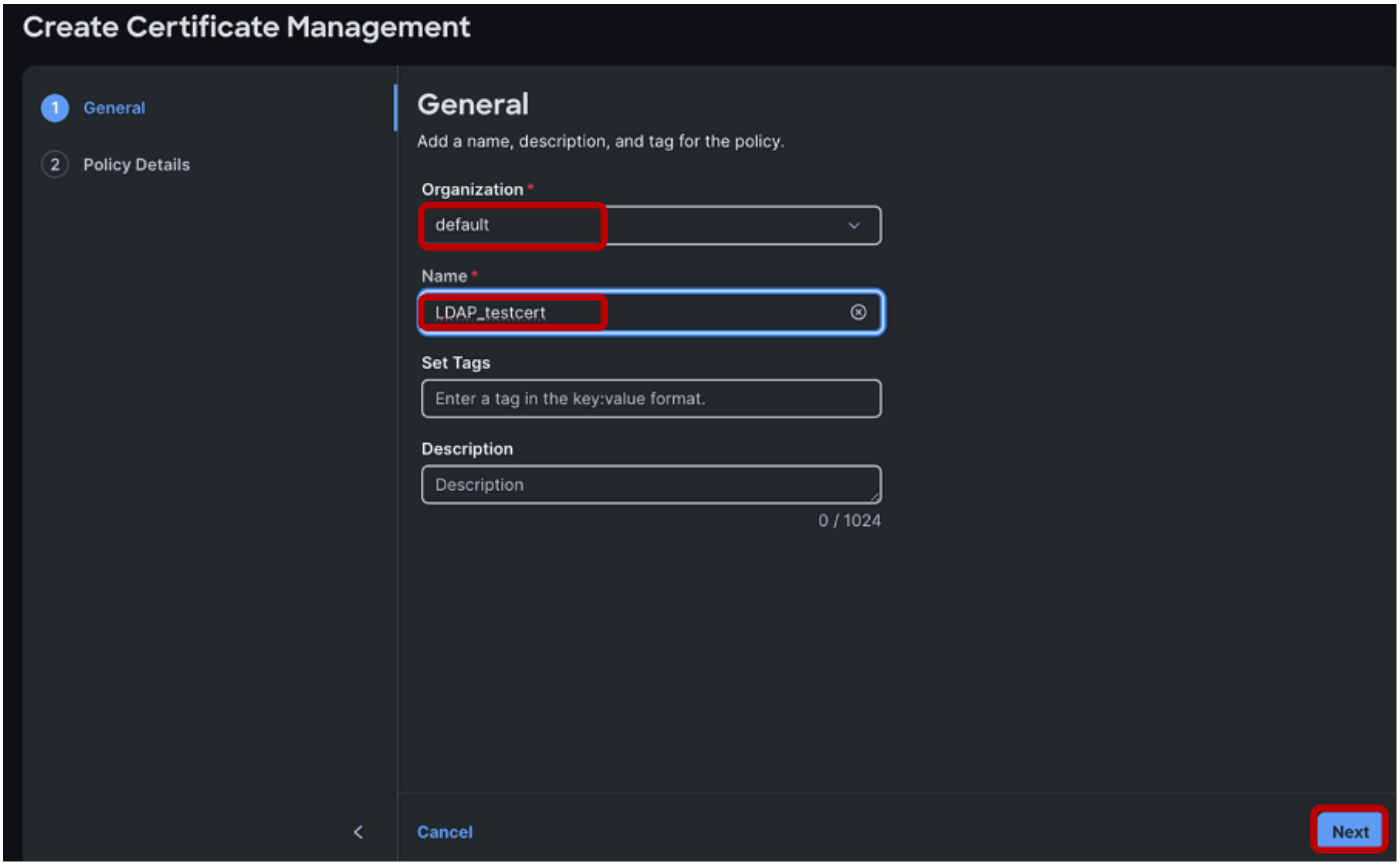
Stellen Sie sicher, dass eine IP-Adresse des DNS-Servers konfiguriert ist und für die Namensauflösung erreichbar ist. Stellen Sie sicher, dass die Namensauflösung für den LDAP-Server und die Fabric Interconnects in der Domäne funktioniert. Bei dieser Demonstration befindet sich der DNS-Server auf derselben Windows-Systeminstanz wie der LDAP-Server.

Zertifikatverwaltungsrichtlinie konfigurieren

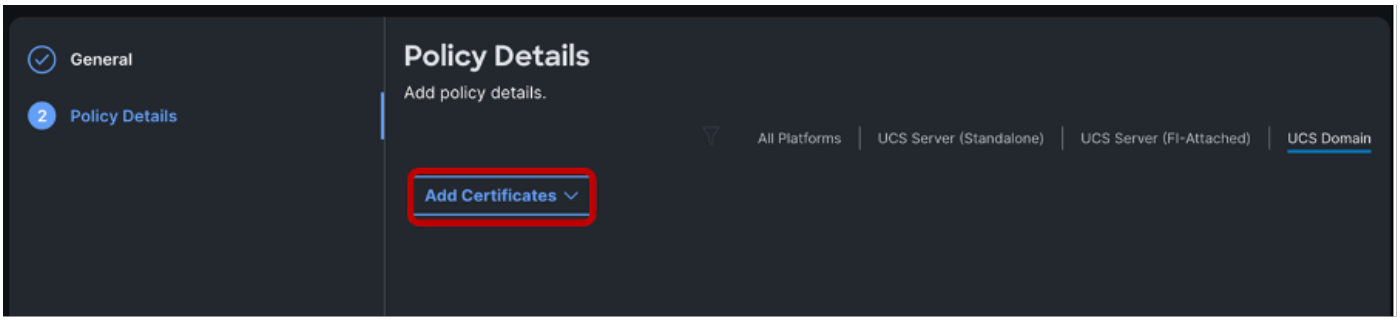
Konfigurieren Sie als Nächstes eine Richtlinie für die Zertifikatsverwaltung. Dies ist erforderlich, damit die LDAP-Verschlüsselung funktioniert.



Wählen Sie die entsprechende Organisation aus, nennen Sie die Richtlinie, und klicken Sie auf "Weiter".

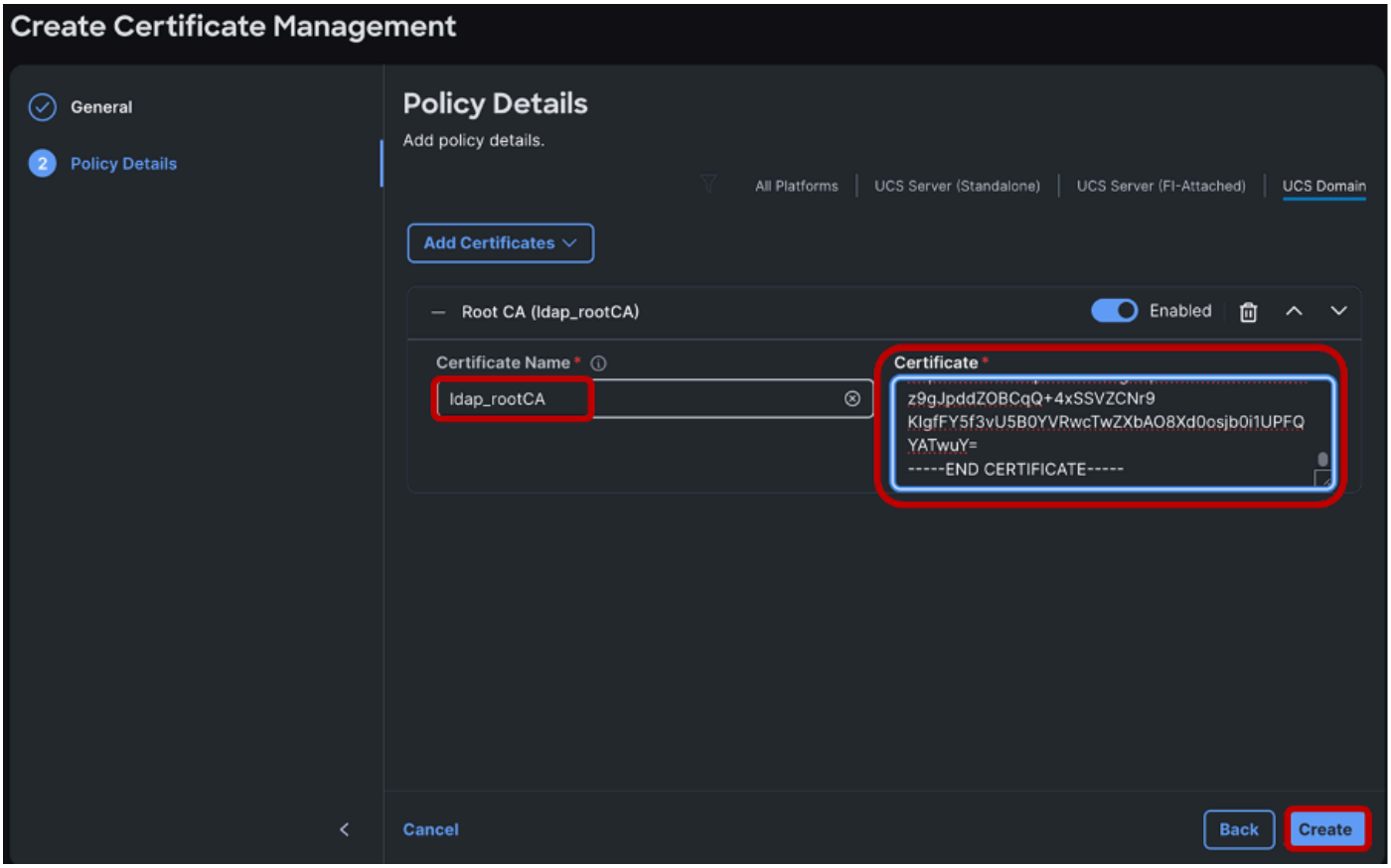


Klicken Sie auf Zertifikate hinzufügen.

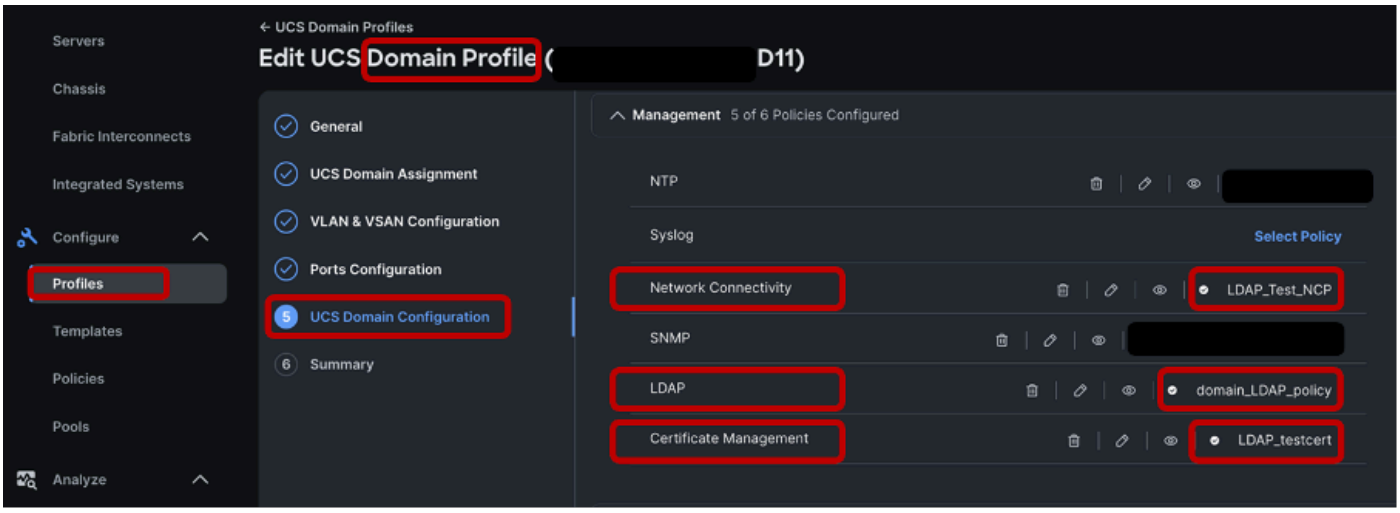


Nennen Sie das Zertifikat, und fügen Sie es aus den Microsoft Active Directory-Zertifikatdiensten in das Stammzertifikat ein.

Klicken Sie auf Erstellen.



Verweisen Sie nach dem Erstellen der Richtlinien für LDAP, Netzwerkkonnektivität und Zertifikatsverwaltung im Abschnitt "UCS-Domänenkonfiguration" auf die neu erstellten Richtlinien im gewünschten Domänenprofil (siehe Abbildung).



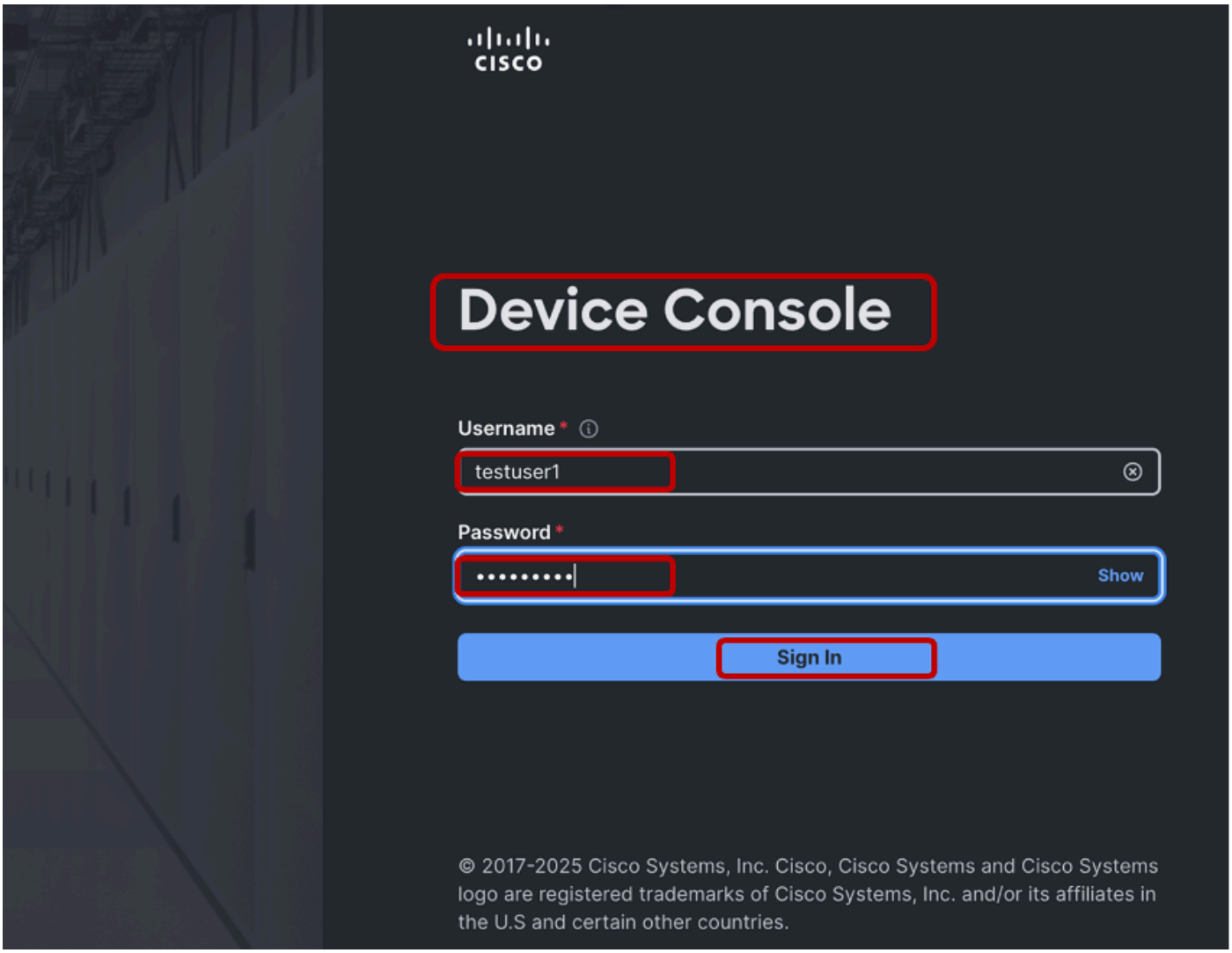
Klicken Sie auf Weiter, Speichern und Bereitstellen des Domänenprofils.

Nach erfolgreicher Bereitstellung des Domänenprofils ist die sichere LDAP-Konfiguration für die IMM-Domäne abgeschlossen.

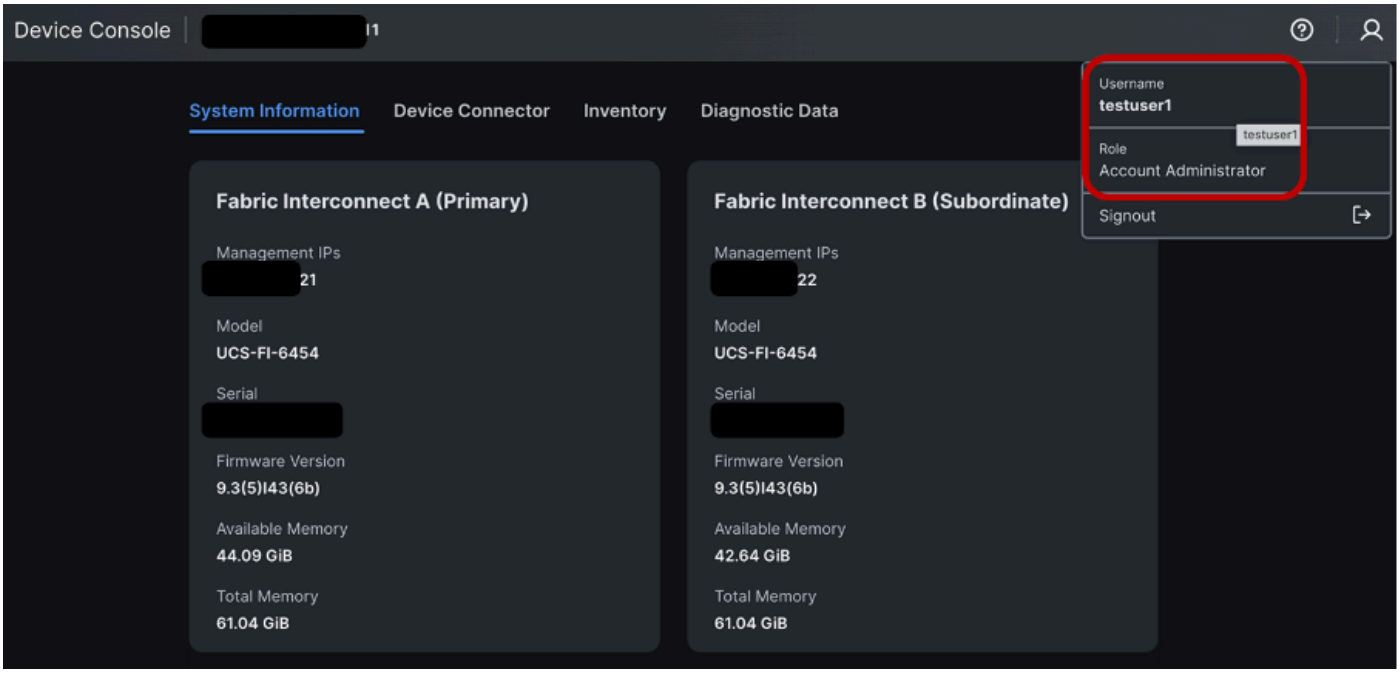
Verifizierung

Versuchen Sie, sich mithilfe eines der konfigurierten LDAP-/Active Directory-Benutzer bei der grafischen Benutzeroberfläche der Gerätekonsole und der CLI von Fabric Interconnects anzumelden.

Anmeldung an der Gerätekonsole testen

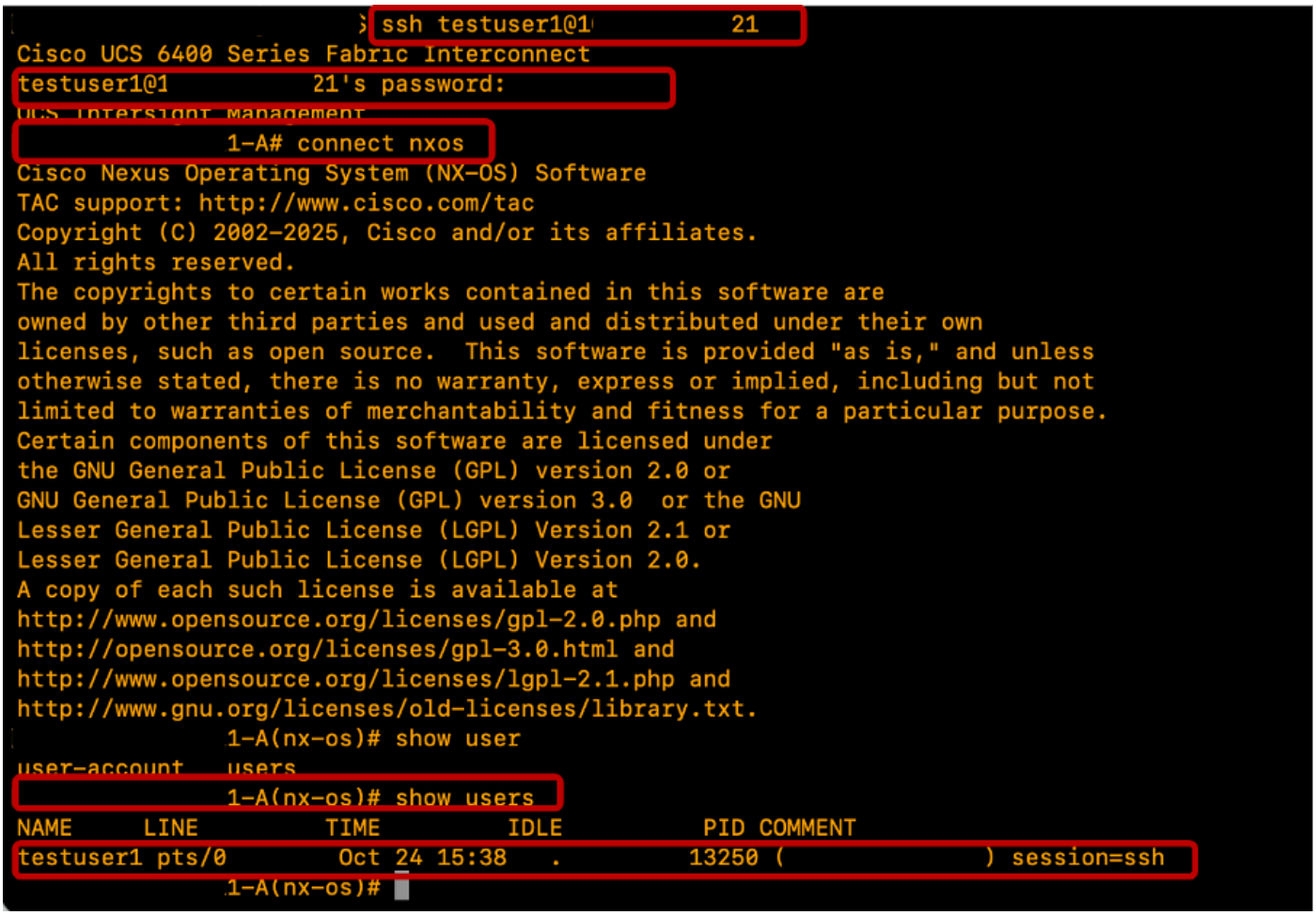


Die Anmeldung an der Testuser1-Gerätekonsole war erfolgreich.



FIs SSH-Anmeldung testen

Testuser1 SSH-Anmeldung erfolgreich.



Zugehörige Informationen

- Interview-Helpcenter
- Administratorhandbuch für Cisco Intersight Managed Mode Fabric Interconnect

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.