Configurazione dell'accesso LDAP sicuro per le interconnessioni fabric in modalità Intersight Manager (console del dispositivo HTTP e SSH)

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione LDAP del dominio in un'istanza SaaS Intersight utilizzando il criterio LDAP.

Prerequisiti

Requisiti

Conoscenza di questi argomenti:

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

Componenti usati

- Istanza SaaS Cisco Intersight
- Microsoft Active Directory
- Server DNS
- Servizi certificati Microsoft Active Directory

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

LDAP è un protocollo noto utilizzato per accedere alle risorse da una directory sulla rete. In queste directory vengono memorizzate informazioni su utenti, organizzazioni e risorse. LDAP fornisce un processo standard per l'accesso e la gestione delle informazioni che possono essere utilizzate per i processi di autenticazione e autorizzazione.

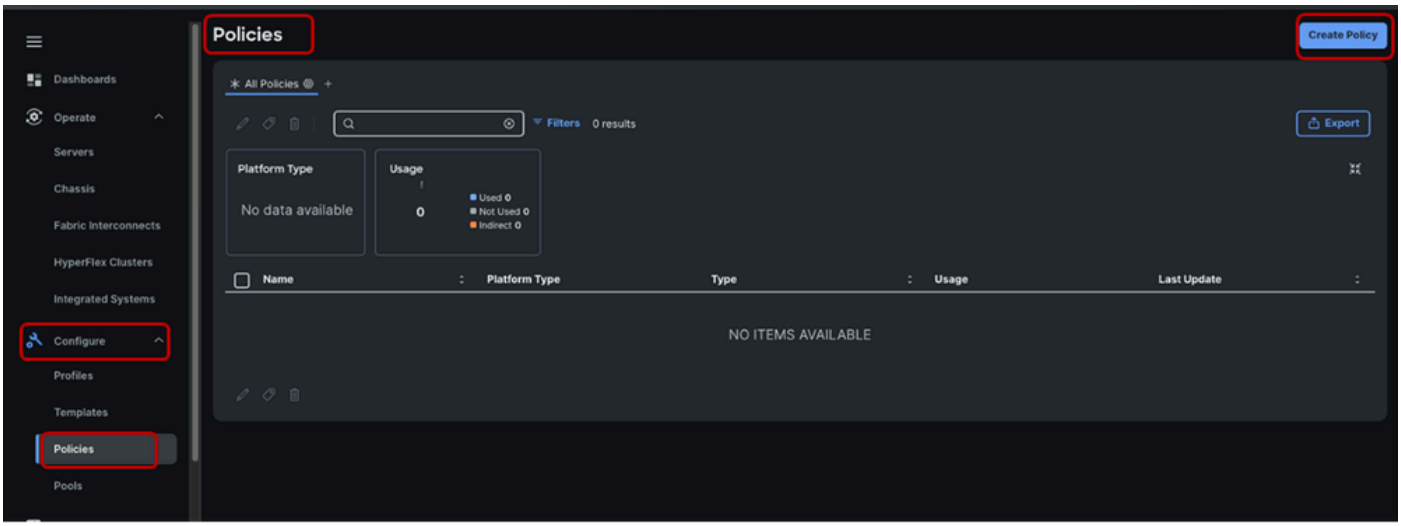
In questo documento viene descritto il processo di configurazione per l'autenticazione remota tramite il protocollo LDAP sicuro alla console del dispositivo o alla CLI (rispettivamente HTTP o SSH) di un peer di interconnessioni Fabric in modalità Intersight Managed.

Configurazione

Configurare il criterio LDAP

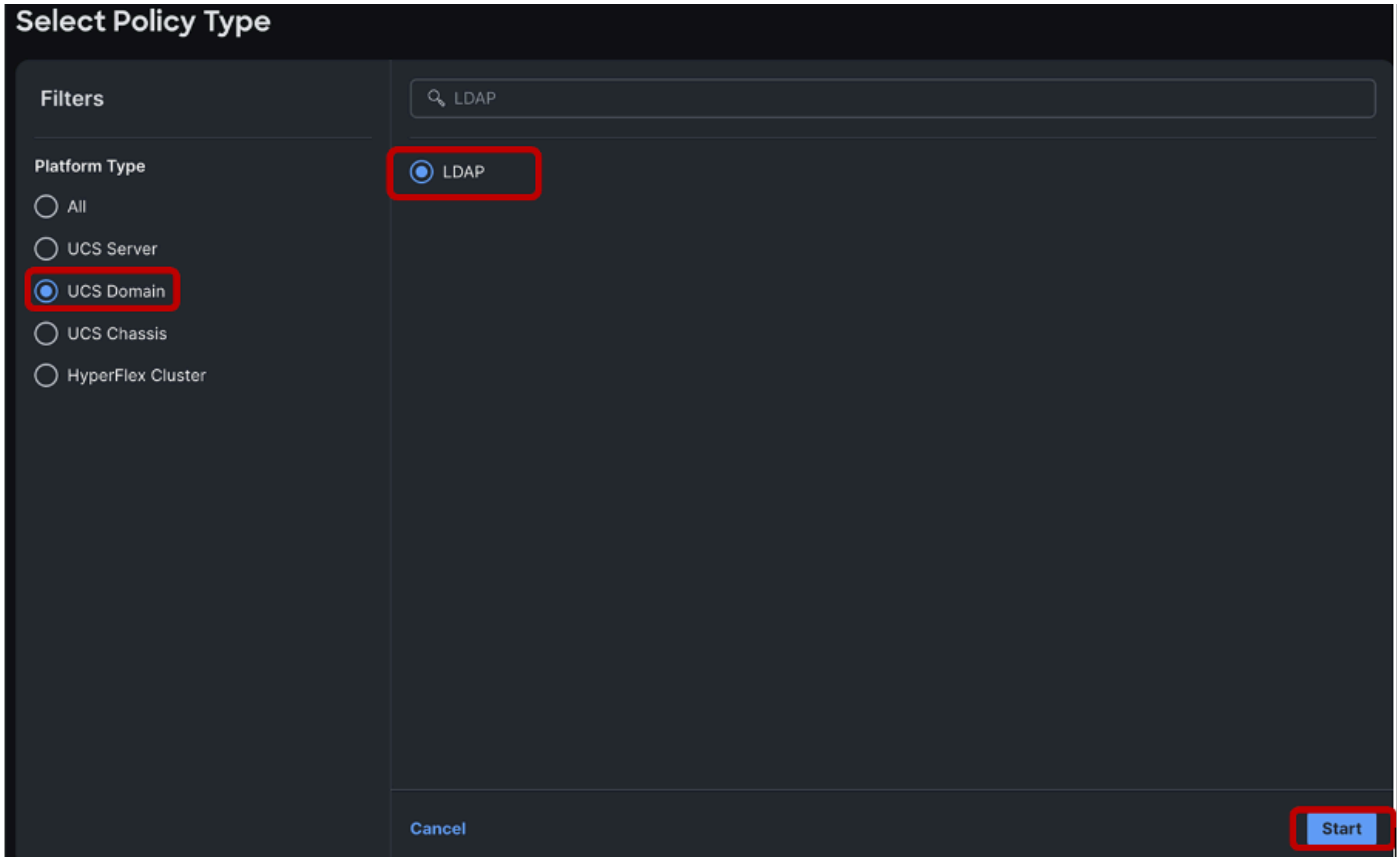
Per configurare il criterio LDAP, accedere all'istanza SaaS Intersight.

Passare alla sezione Configura > Fare clic su Criteri.
Passare alla finestra Criteri > Seleziona Crea criterio.

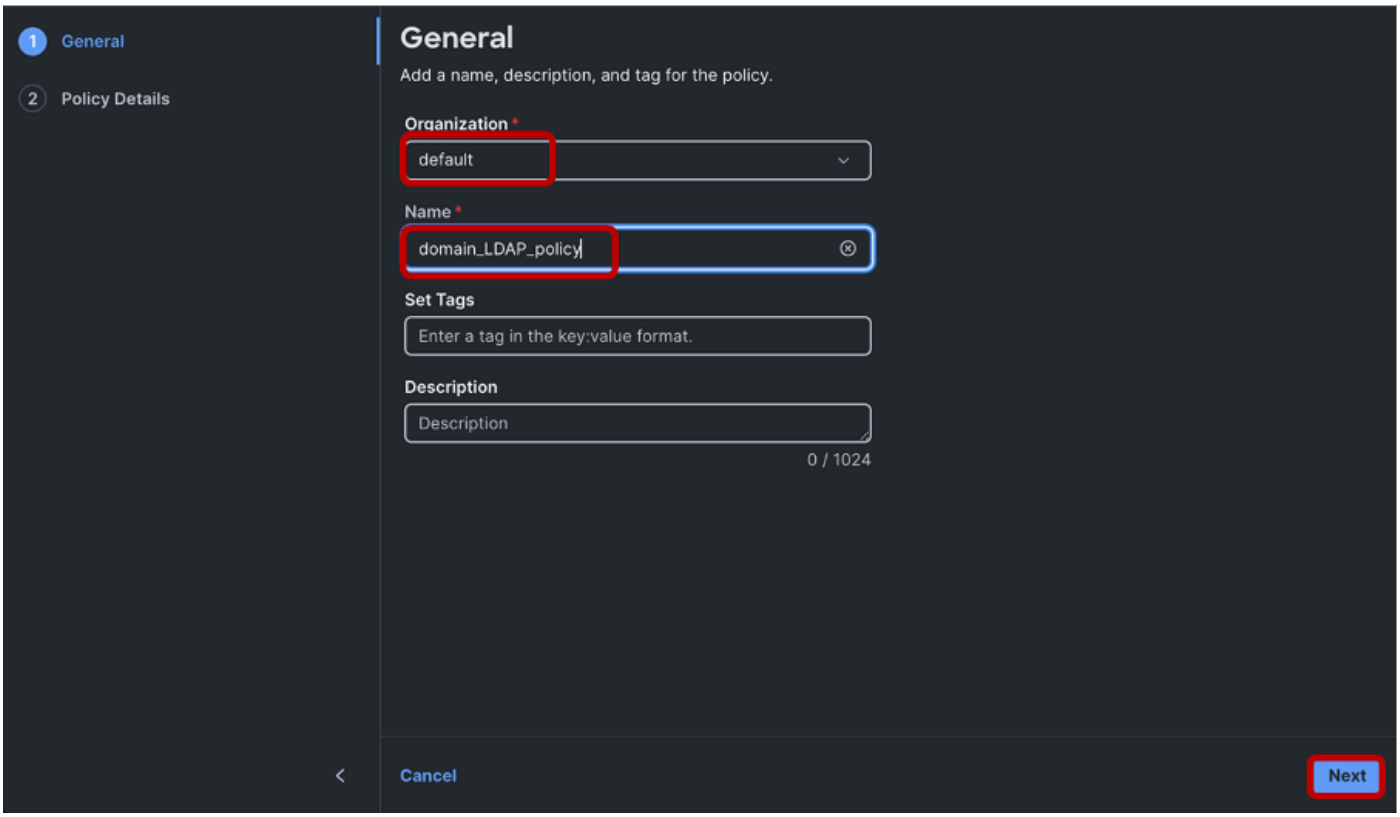


Nella barra di ricerca, cercare "LDAP".

Selezionare il pulsante di scelta LDAP > Fare clic su Start.

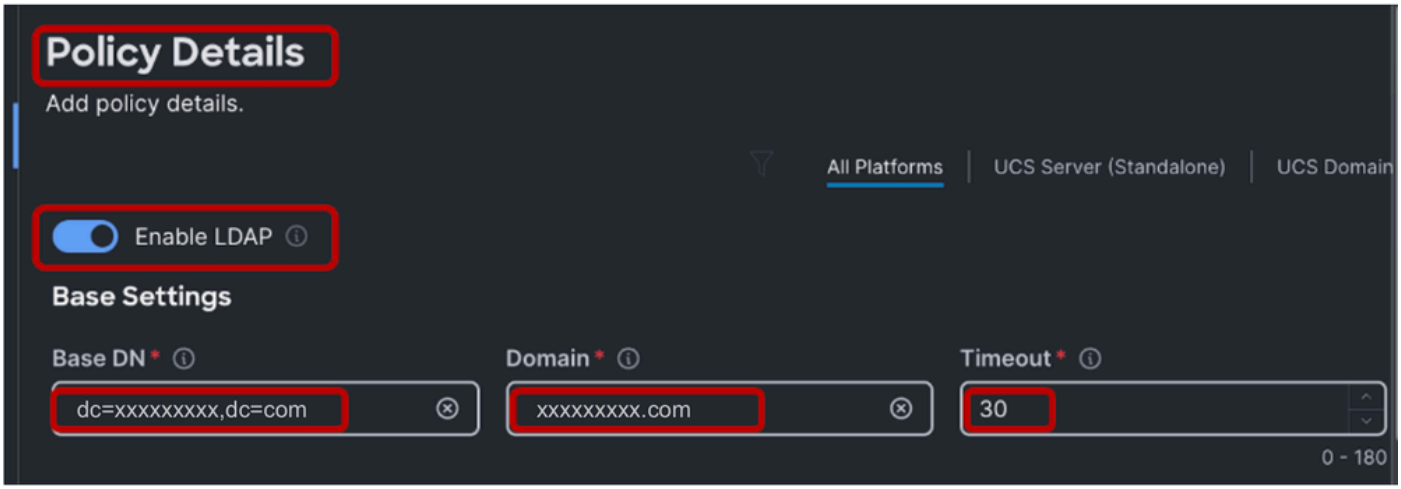


Nella finestra Crea > Scegliere l'organizzazione desiderata > Nome criterio LDAP > Fare clic su Avanti:



Nella sezione Dettagli criterio > Selezionare il dispositivo di scorrimento Abilita LDAP > Popolare i valori di DN di base, Dominio e Timeout.

I valori di Timeout, se impostati su un valore compreso tra 0 e 29, vengono automaticamente impostati su 30 secondi. Per questa dimostrazione, "xxxxxxxxx.com" è il dominio desiderato già configurato sul server LDAP ed è stato specificato un valore di timeout di 30 secondi.

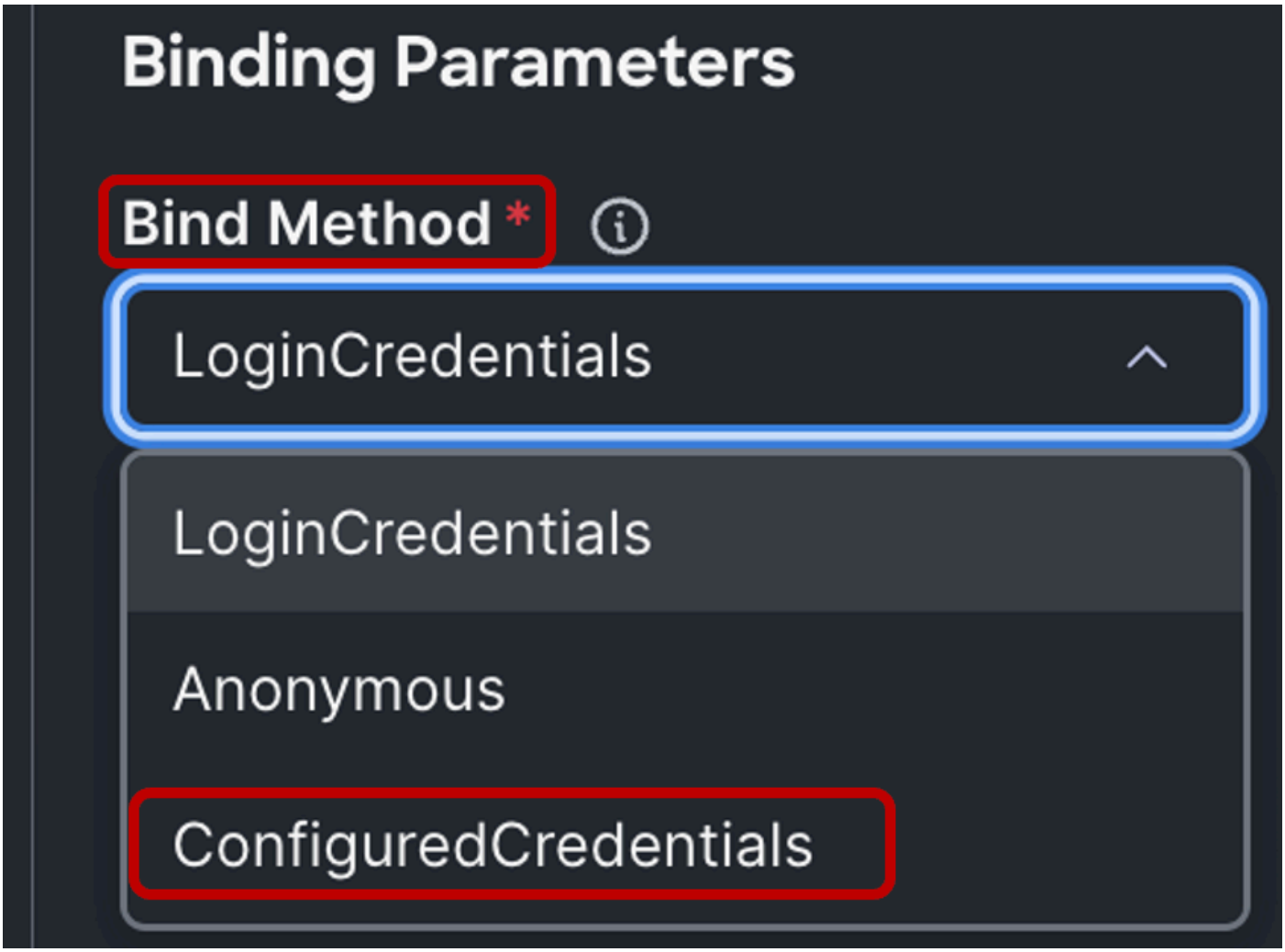


Per configurare Secure LDAP, attivare il pulsante di scelta Abilita crittografia.

Nota: La normale configurazione LDAP può utilizzare un indirizzo IP o un FQDN, ma un certificato firmato non è un requisito. Pertanto, quando si configura il protocollo LDAP standard, è possibile ignorare l'opzione Abilita crittografia, il criterio di connettività di rete del server DNS e un certificato nelle configurazioni del criterio di gestione dei certificati. LDAP protetto richiede un server DNS configurato per la risoluzione dei nomi dei server LDAP e un certificato radice.

Nella sezione Parametri di binding, l'impostazione predefinita è LoginCredentials, che utilizza la singola autenticazione delle credenziali LDAP dell'utente per l'operazione di binding. In questo modo non è più necessario configurare un utente di binding dedicato.

Per questa dimostrazione, è configurato un utente di binding. Pertanto, il "Metodo Bind" viene modificato in "ConfiguredCredentials".

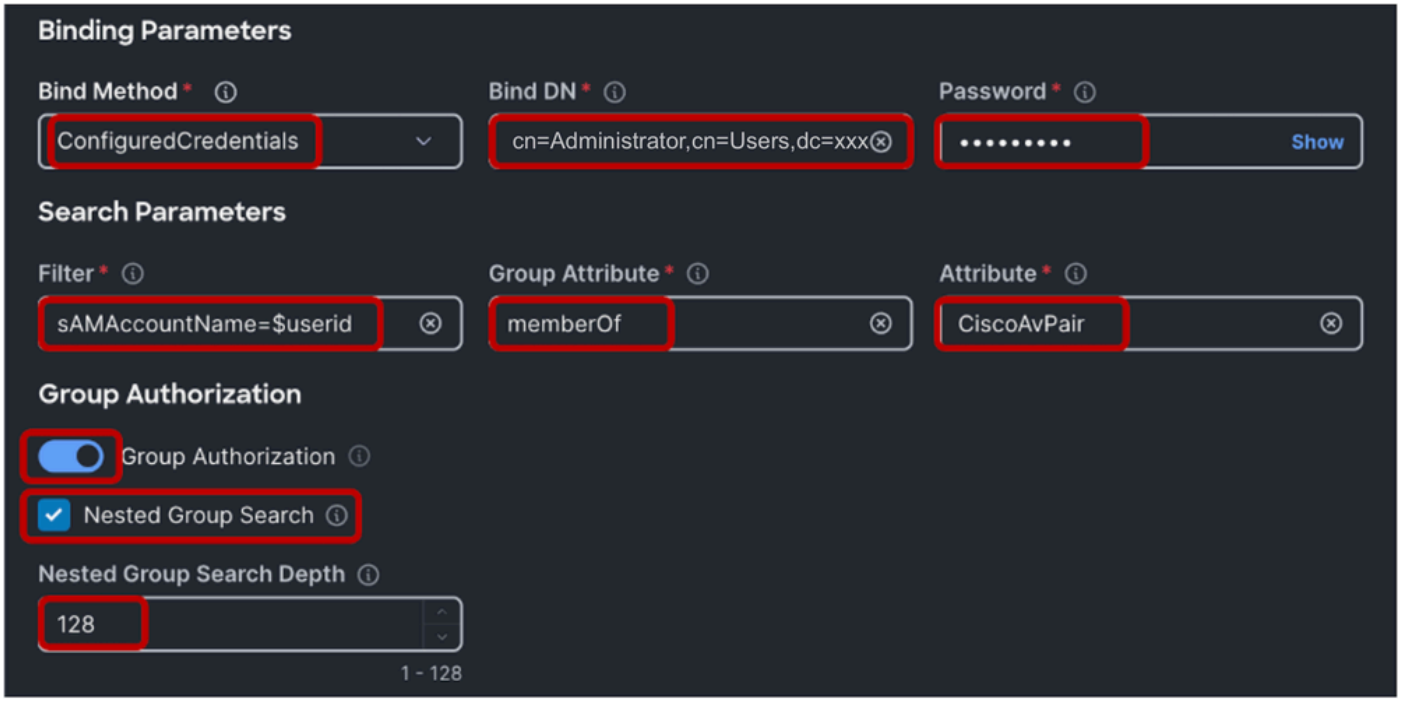


Aggiungere quindi un DN di binding (un utente di binding) e la password utente di binding. Può corrispondere a qualsiasi utente configurato in Windows Active Directory. In questa dimostrazione viene utilizzato l'utente Amministratore.

‘cn=Administrator,cn=Users,dc=xxxxxxxxx,dc=com’.

Nella sezione Parametri di ricerca, in Filtro, immettere "sAMAccountName=$userid".

Per Attributi gruppo aggiungere "memberOf" e nel campo Attributo aggiungere "CiscoAvPair". A seconda della configurazione del server LDAP, è possibile attivare Autorizzazione gruppo e Ricerca gruppo nidificato. Per questa dimostrazione viene utilizzata la profondità di ricerca del gruppo nidificato di default pari a 128.



Nella sezione "Configurazione server LDAP" > Immettere l'indirizzo IP o il nome FQDN del server LDAP (richiesto per Secure LDAP) e il numero di porta (389).

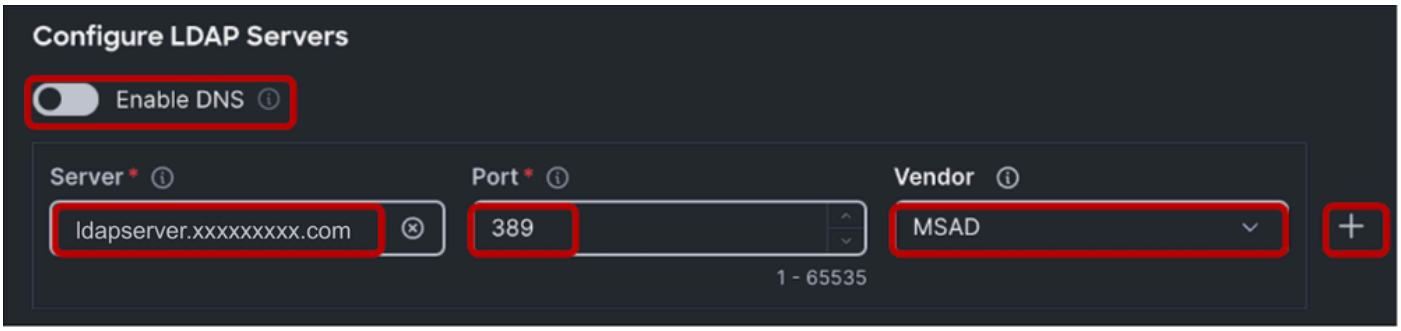
Secure LDAP in UCS utilizza STARTTLS per abilitare la comunicazione crittografata tramite la porta 389.

La modifica della porta da 389 a 636 può causare errori di autenticazione. Cisco UCS esegue la negoziazione TLS sulla porta 636 per SSL; tuttavia, la connessione iniziale viene sempre stabilita in modalità non crittografata sulla porta 389.

Selezionare il fornitore del server LDAP. Le opzioni del fornitore disponibili sono OpenLDAP e MSAD (Microsoft Active Directory). Per questa dimostrazione, poiché il server LDAP in uso è Windows Server 2019, viene utilizzato MSAD.

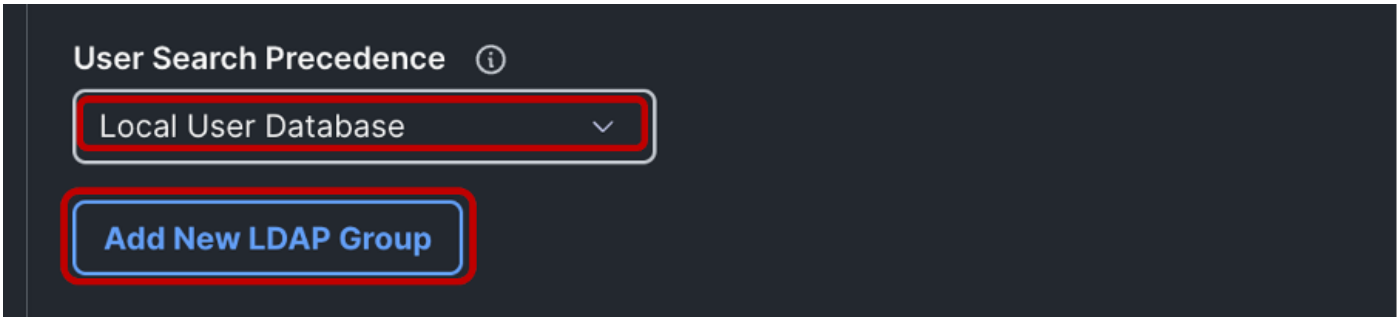
Lasciare il pulsante Abilita DNS disattivato in quanto questa opzione non è applicabile alla configurazione LDAP nel dominio UCS.

È possibile configurare più server LDAP facendo clic sull'icona "+" all'estrema destra del server LDAP configurato.

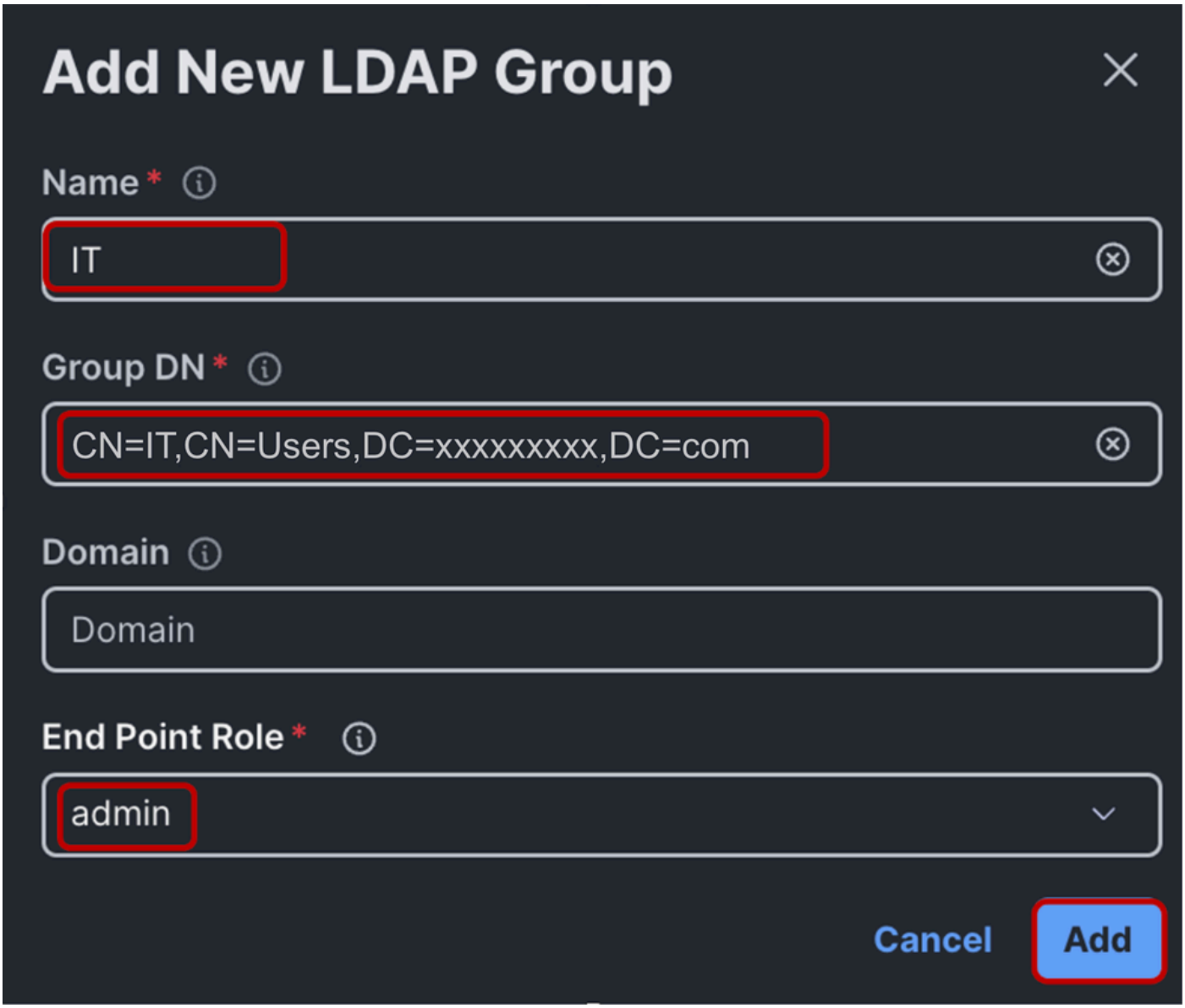


Nota: È possibile mantenere la precedenza della ricerca utente come database utenti locale o modificarla in database utenti LDAP a seconda dello Use Case.

Procedere quindi per aggiungere un DN gruppo corrispondente al gruppo configurato nel server LDAP, facendo clic sul pulsante Aggiungi nuovo gruppo LDAP.



Assegnare un nome al gruppo, aggiungere il DN gruppo ricevuto dal server LDAP e selezionare il ruolo di endpoint desiderato.

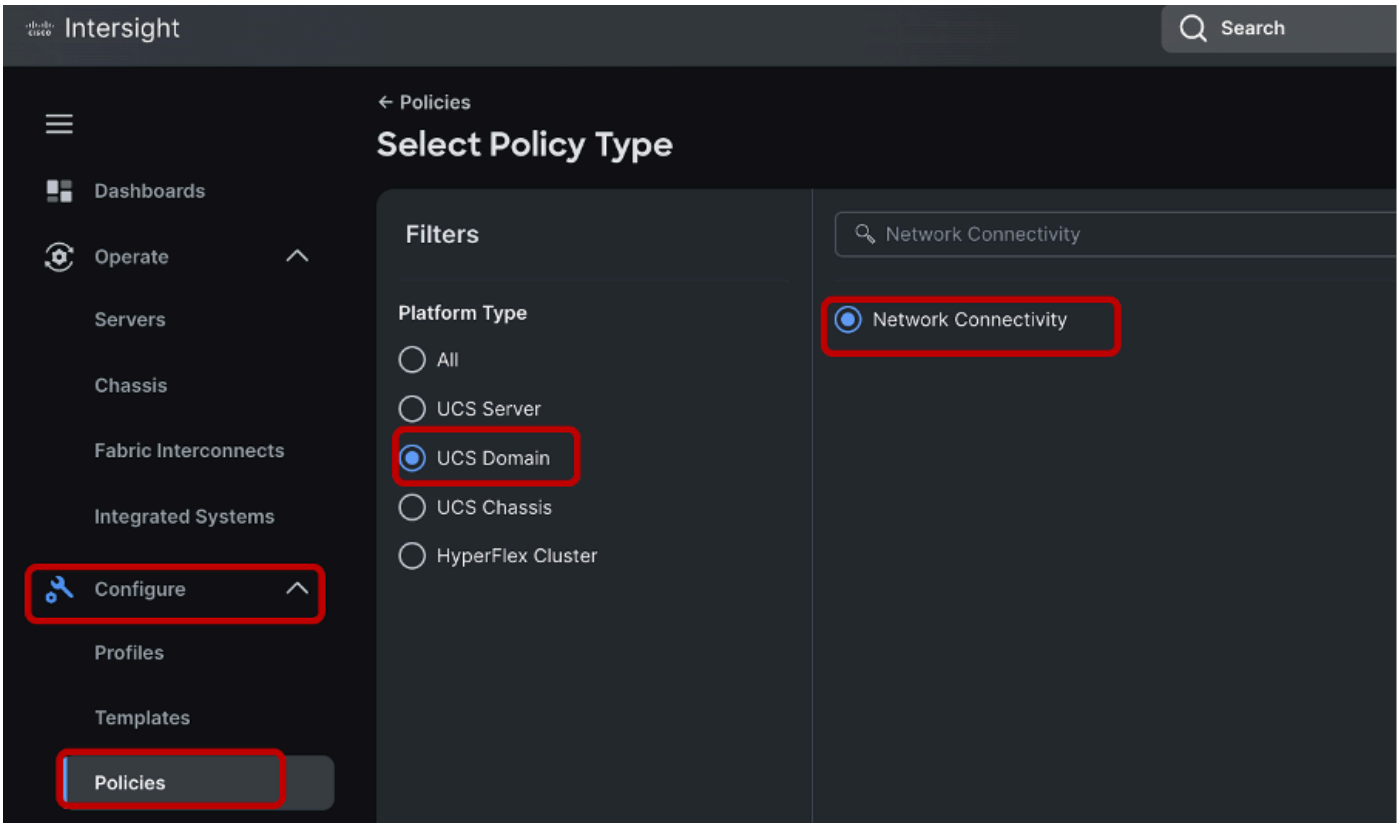


Fare clic su Aggiungi > Seleziona creazione per creare il criterio LDAP

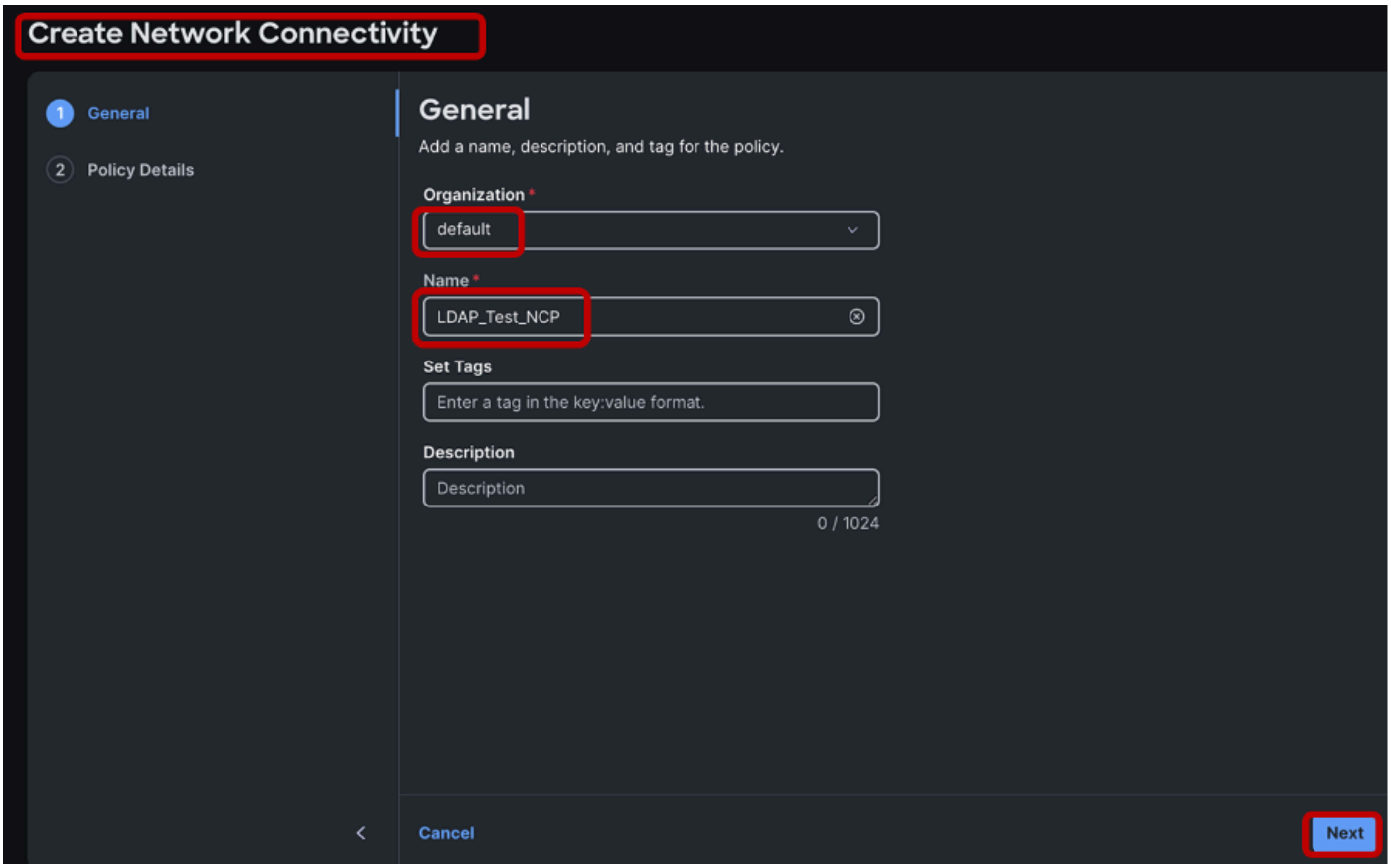
Nota: Per la configurazione dei criteri LDAP del dominio, l'unico ruolo di endpoint supportato è "admin" al momento della creazione del documento.

Configura criterio di connettività di rete

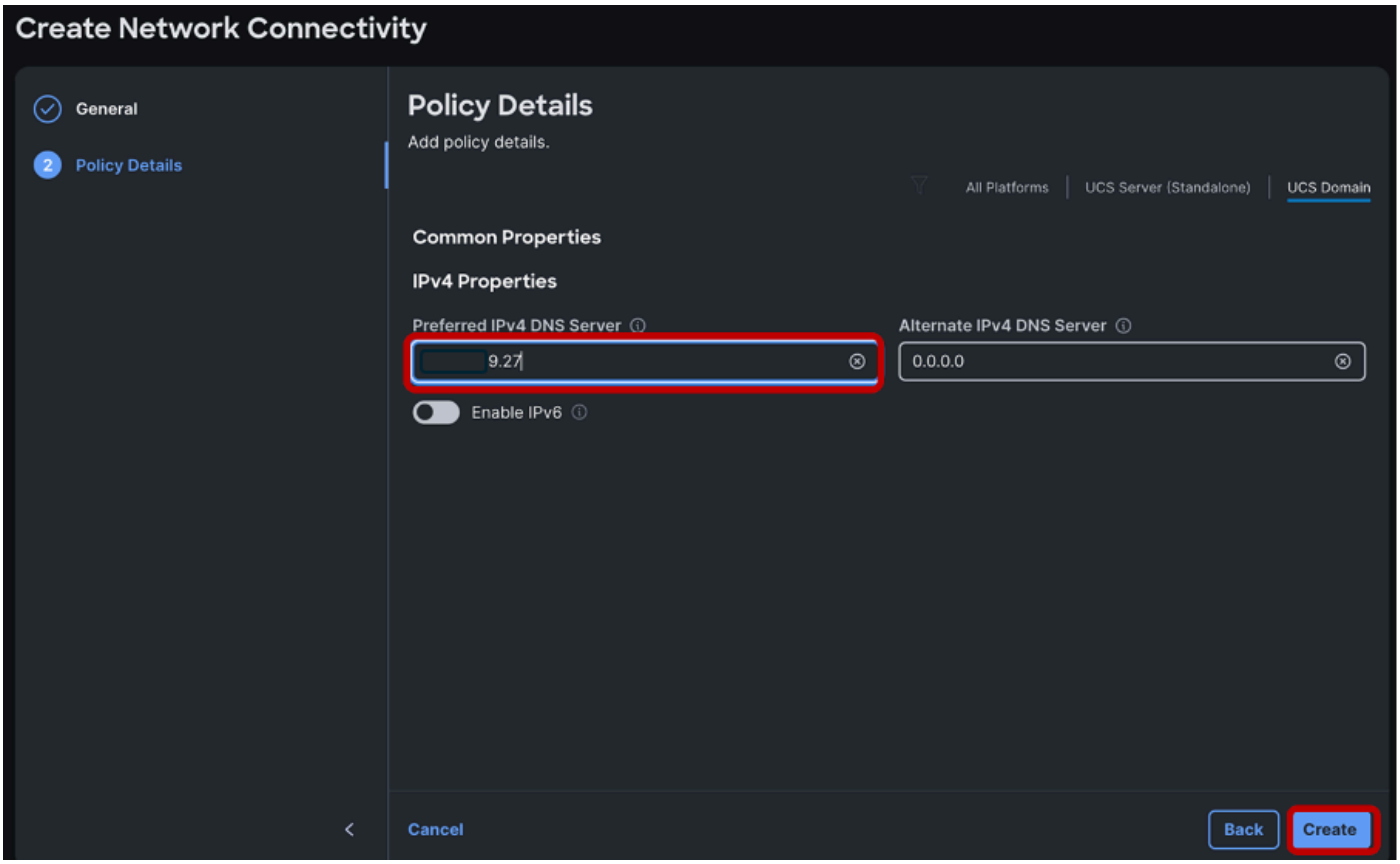
Configurare un server DNS per il dominio UCS creando un criterio di connettività di rete.



Selezionare l'organizzazione appropriata > Immettere il nome del criterio > Fare clic su Avanti.



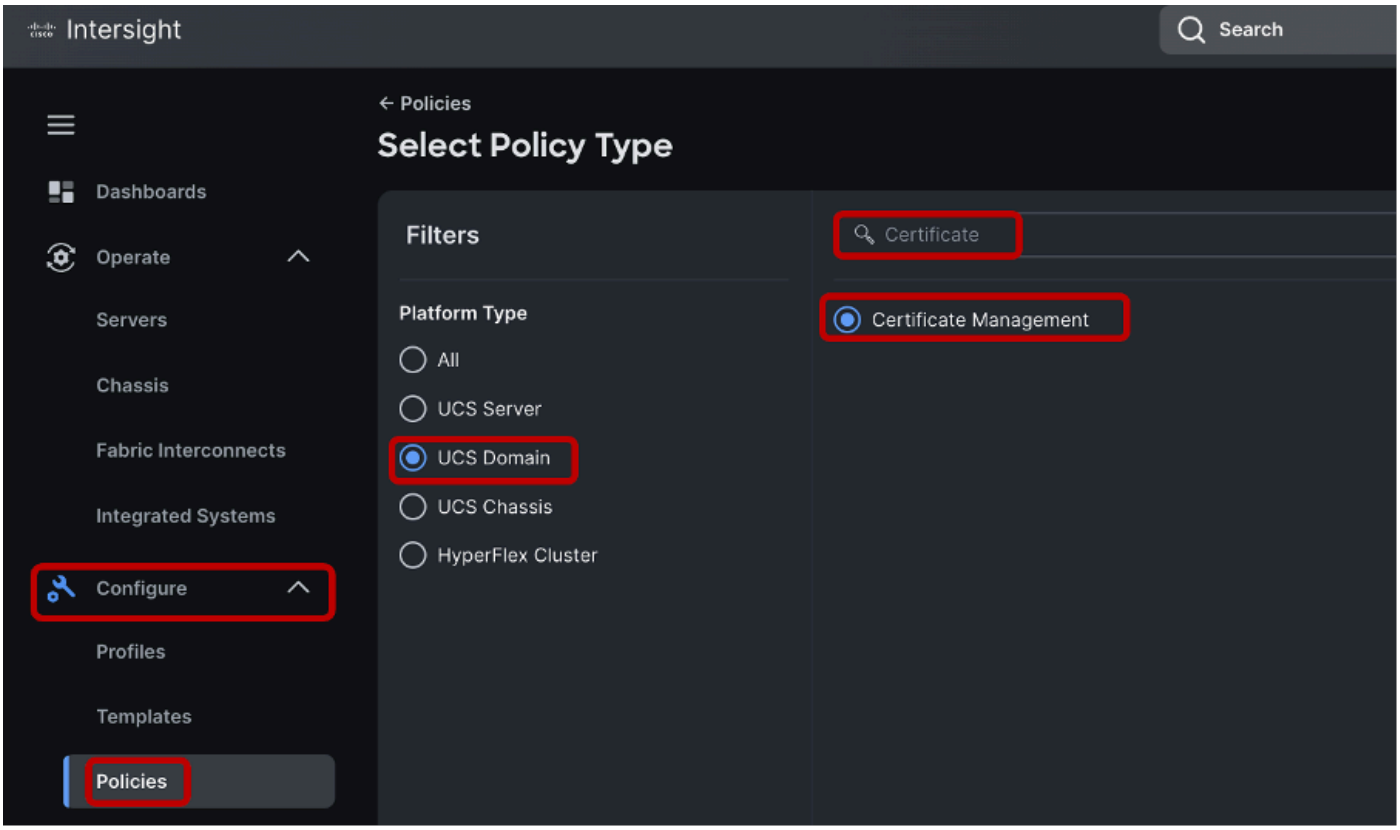
Definire un indirizzo IPv4 del server DNS preferito e fare clic su Crea per salvare il criterio.



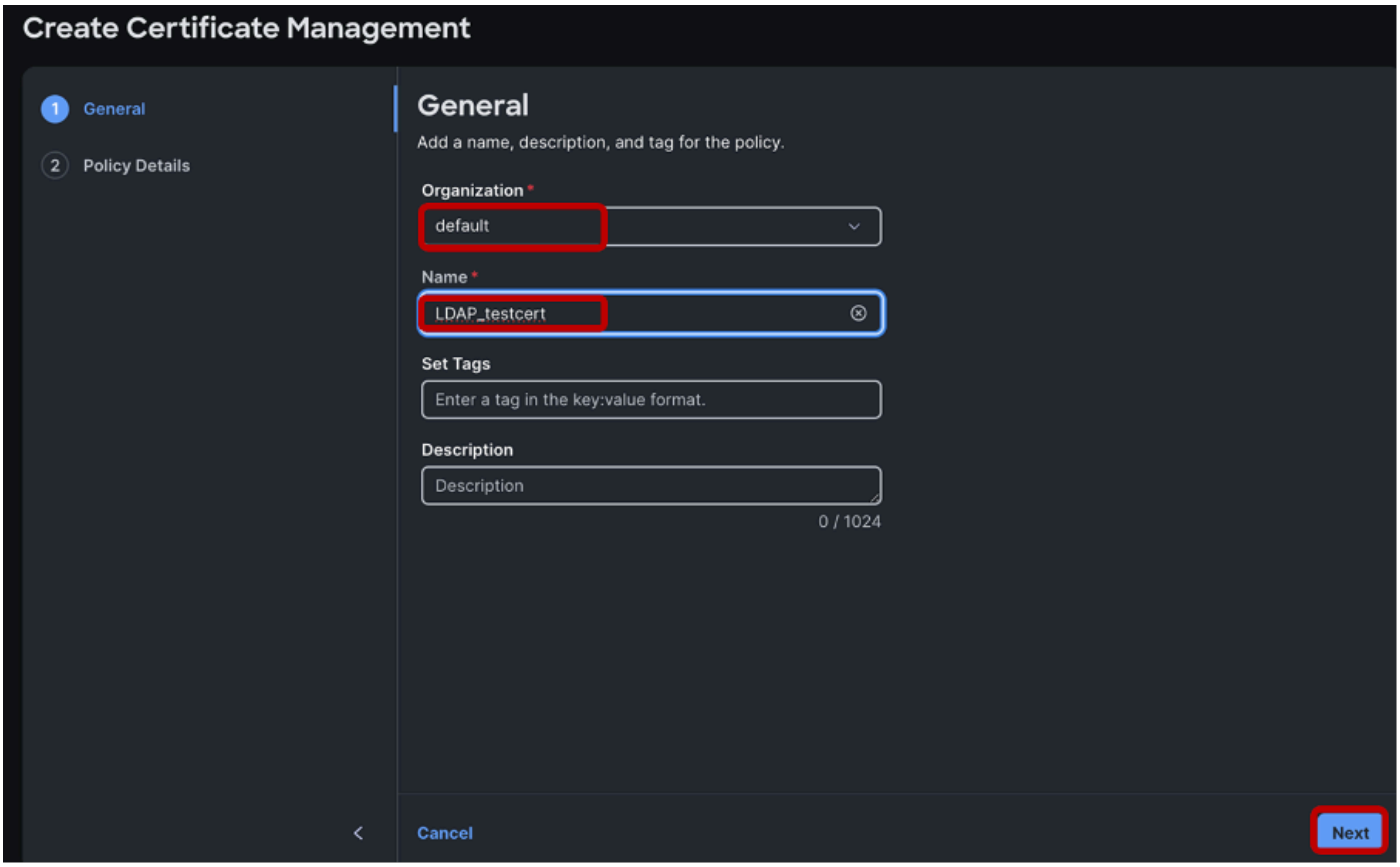
Verificare che l'indirizzo IP di un server DNS sia configurato e raggiungibile per la risoluzione dei nomi. Verificare che la risoluzione dei nomi sia funzionale per il server LDAP e le interconnessioni di infrastruttura all'interno del dominio. Per questa dimostrazione, il server DNS si trova nella stessa istanza del computer Windows del server LDAP.

Configura criteri di gestione dei certificati

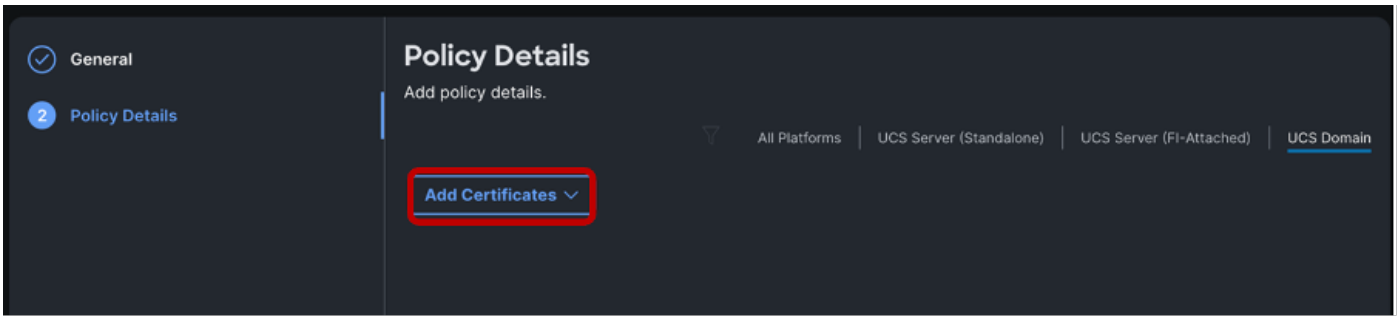
Configurare quindi un criterio di gestione dei certificati. Questa operazione è necessaria per il funzionamento della crittografia LDAP.



Selezionare l'organizzazione appropriata, assegnare un nome al criterio > Fare clic su Avanti

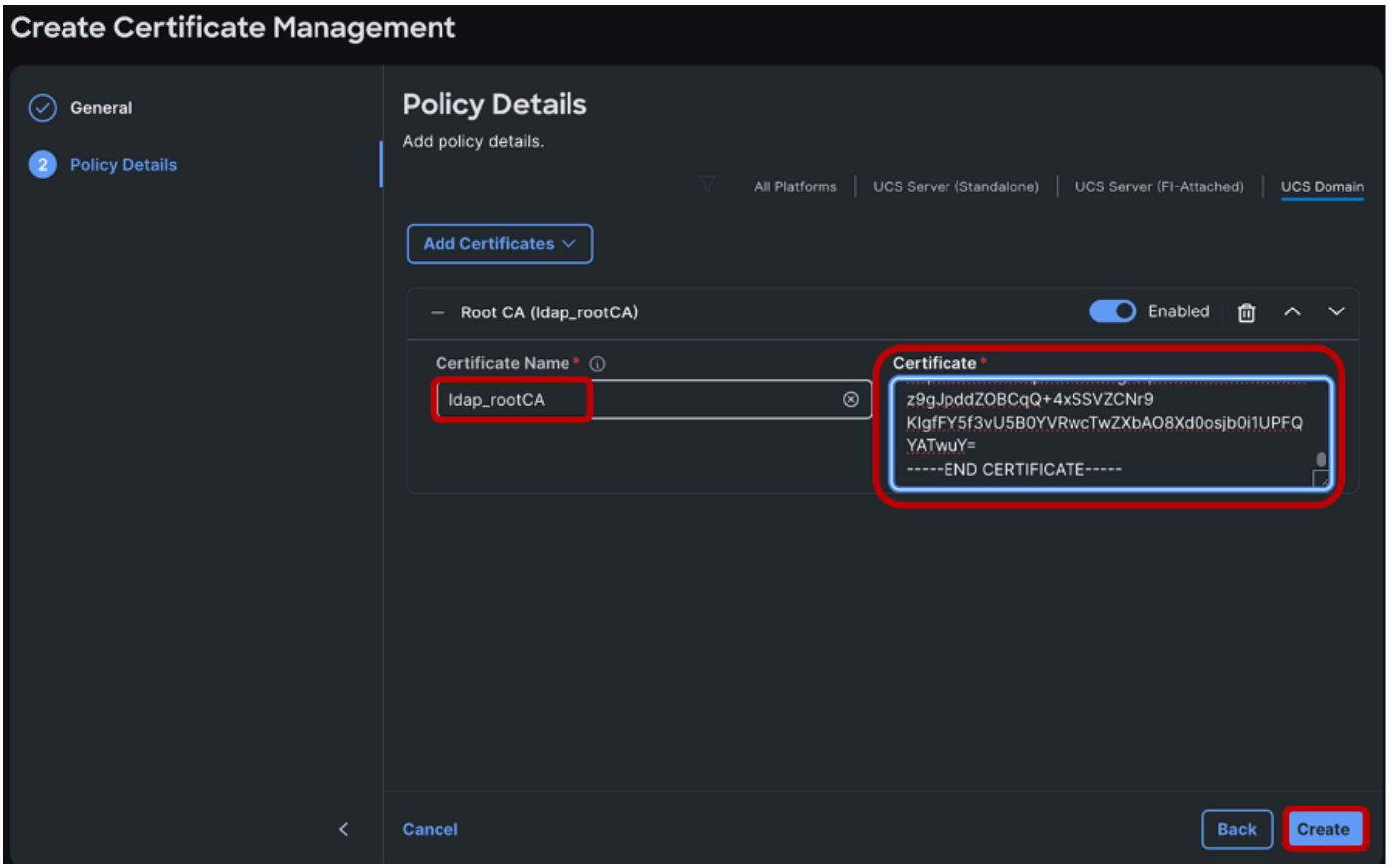


Fare clic su Aggiungi certificati.

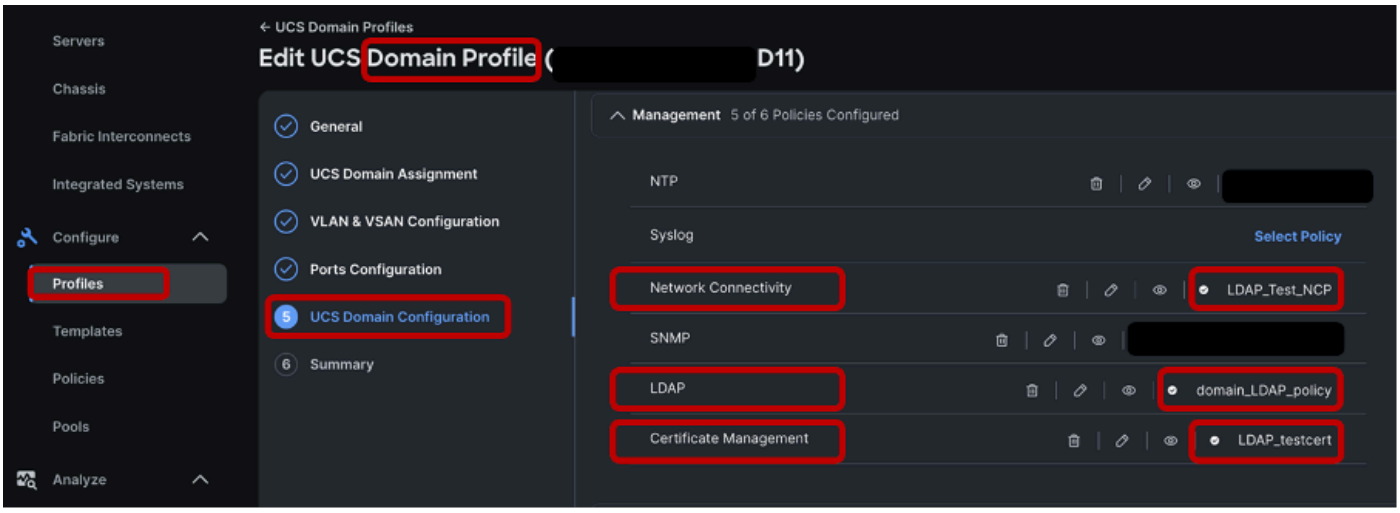


Assegnare un nome al certificato e incollarlo nel certificato radice da Servizi certificati Microsoft Active Directory.

Fare clic su Crea.



Dopo la creazione dei criteri LDAP, Connettività di rete e Gestione certificati, fare riferimento ai nuovi criteri creati nel profilo di dominio desiderato, nella sezione "Configurazione dominio UCS", come mostrato.



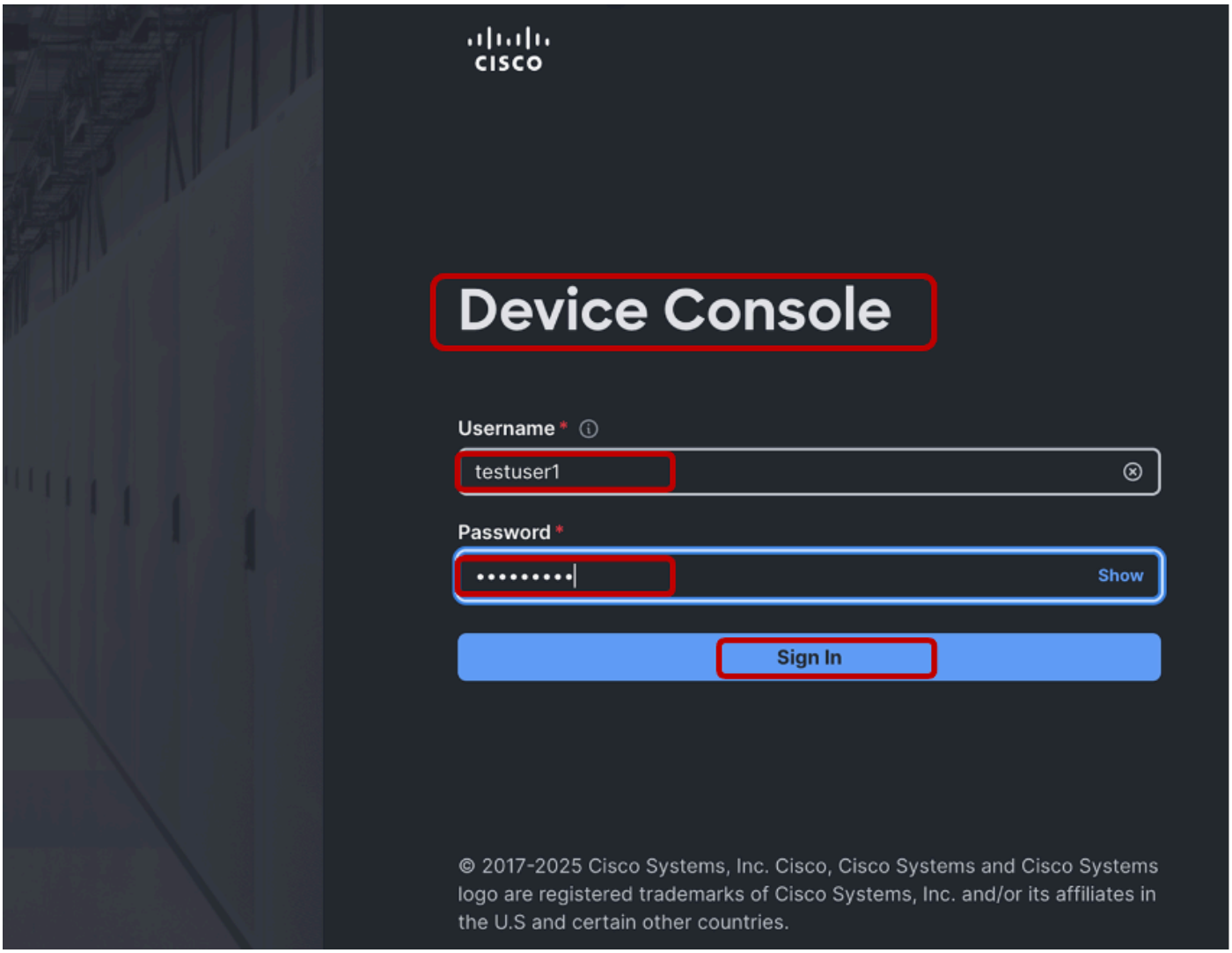
Fare clic su Avanti, Salva e distribuisci il profilo di dominio.

Al termine della distribuzione del profilo di dominio, la configurazione LDAP protetta per il dominio IMM è stata completata.

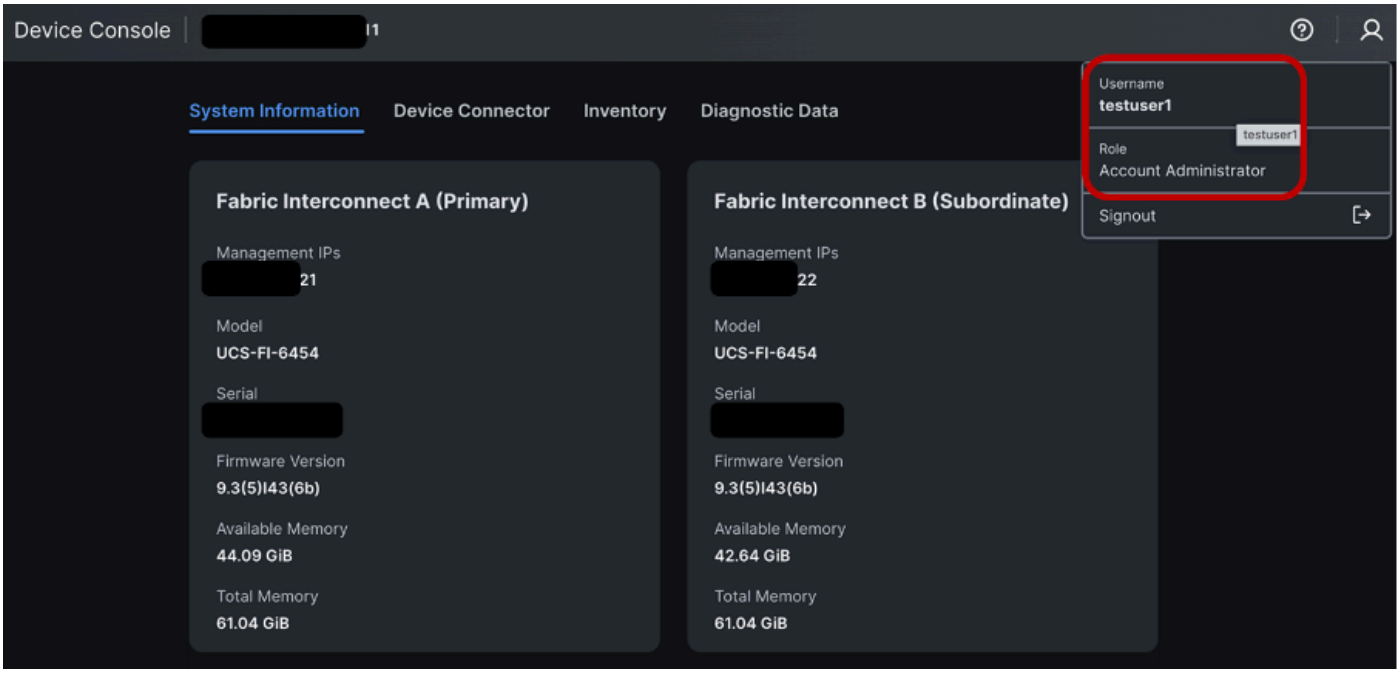
Verifica

Per verificare, tentare di accedere all'interfaccia GUI della console del dispositivo e all'interfaccia CLI di Fabric Interconnect utilizzando uno degli utenti LDAP/Active Directory configurati.

Verifica accesso console dispositivo

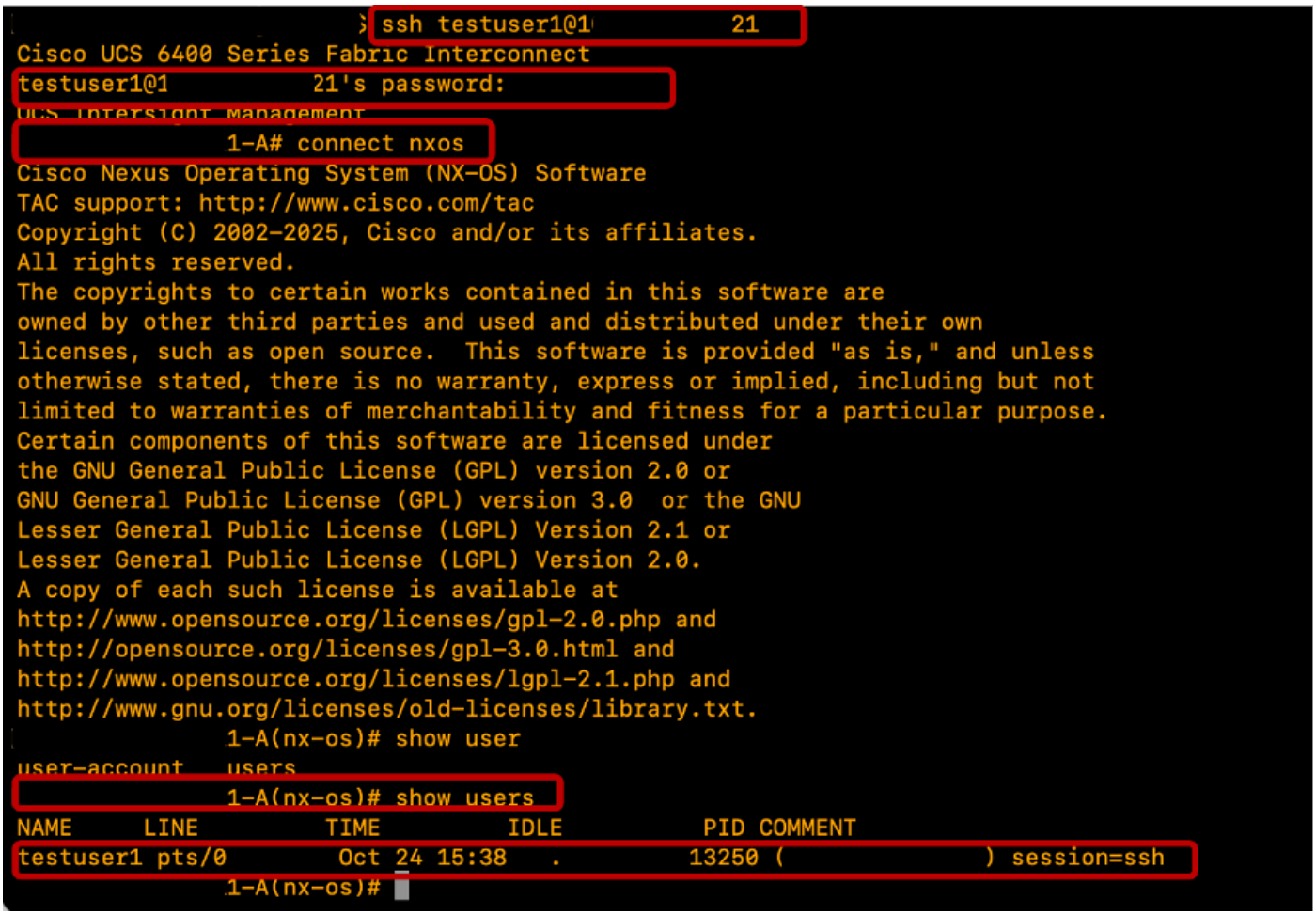


Accesso alla console del dispositivo Testuser1 riuscito.



Test di accesso FI SSH

L'accesso SSH Testuser1 è riuscito.



Informazioni correlate

- Intersight Help Center
- Guida per l'amministratore di Cisco Intersight Managed Mode Fabric Interconnect

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).