Esempio di configurazione dell'autenticazione LDAP per UCS Central

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per l'autenticazione LDAP (Lightweight Directory Access Protocol) per Cisco Unified Computing System (UCS) Central. Nelle procedure vengono utilizzati l'interfaccia utente grafica (GUI) di UCS Central, un dominio di esempio bglucs.com e un nome utente di esempio testuser.

Nella versione 1.0 del software UCS Central, LDAP è l'unico protocollo di autenticazione remota supportato. La versione 1.0 offre un supporto molto limitato per l'autenticazione remota e la configurazione LDAP per UCS Central. Tuttavia, è possibile utilizzare UCS Central per configurare tutte le opzioni per i domini di UCS Manager gestiti da UCS Central.

Le limitazioni dell'autenticazione remota di UCS Central includono:

- RADIUS e TACACS non supportati.

- Il mapping dell'appartenenza ai gruppi LDAP per l'assegnazione dei ruoli e i gruppi di provider LDAP per più controller di dominio non sono supportati.
- Per passare il ruolo, LDAP utilizza solo l'attributo CiscoAVPair o qualsiasi attributo inutilizzato. Il ruolo passato è uno dei ruoli predefiniti nel database locale di UCS Central.
- Non sono supportati più domini/protocolli di autenticazione.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- UCS Central è distribuito.
- Microsoft Active Directory è stato distribuito.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- UCS Central versione 1.0
- 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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Raccogli informazioni

In questa sezione vengono riepilogate le informazioni da raccogliere prima di avviare la configurazione.

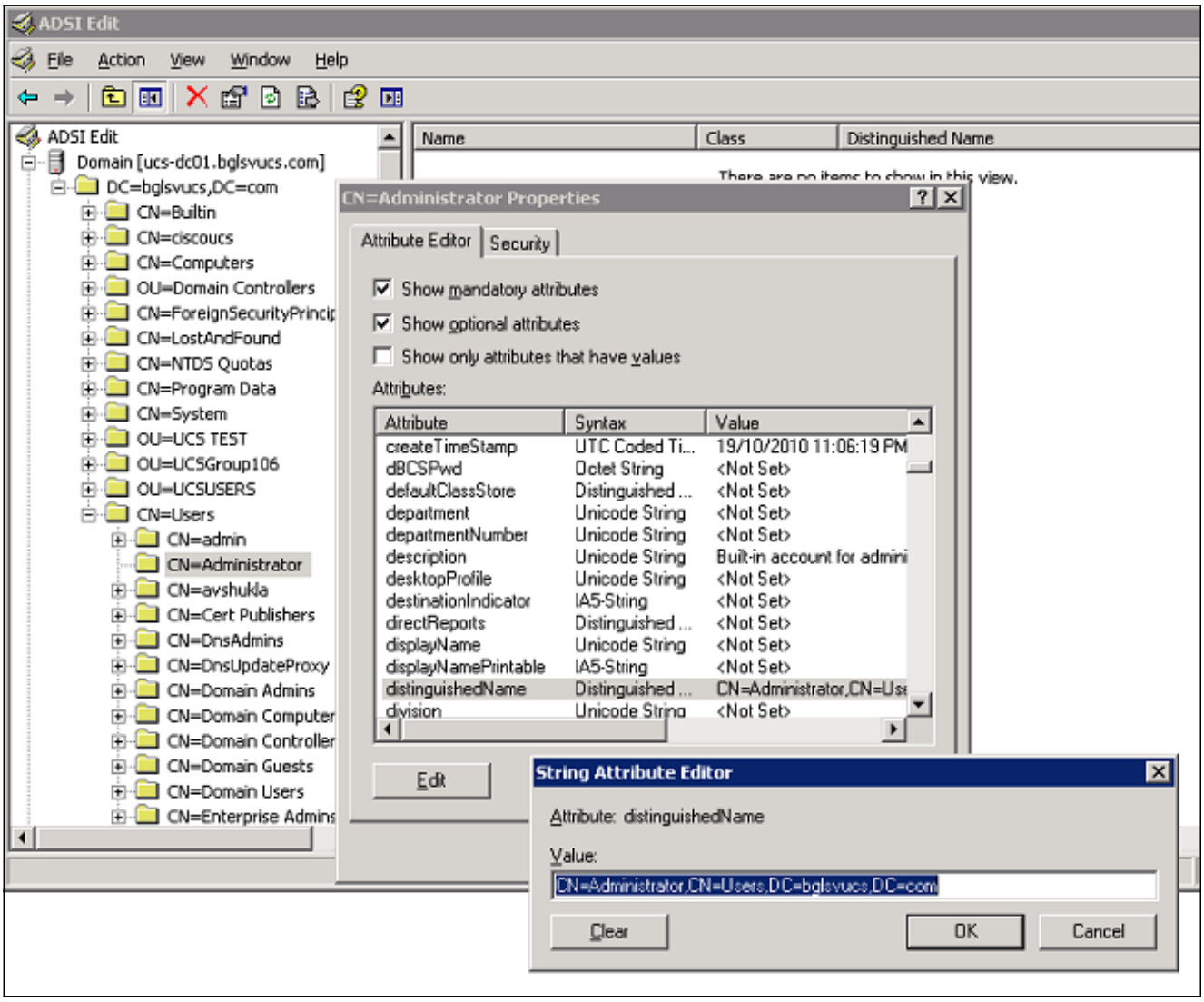
Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Associa dettagli utente

L'utente di binding può essere qualsiasi utente LDAP nel dominio che dispone dell'accesso in lettura al dominio. per la configurazione LDAP è necessario un utente di binding. UCS Central utilizza il nome utente e la password dell'utente associato per connettersi ad Active Directory (AD) ed eseguire query per l'autenticazione dell'utente e così via. In questo esempio viene utilizzato l'account Administrator come utente di binding.

In questa procedura viene descritto come un amministratore LDAP può utilizzare l'Editor ADSI (Active Directory Service Interfaces) per trovare il DN.

1. Aprire l'editor ADSI.
2. Trovare l'utente del binding. L'utente si trova nello stesso percorso di AD.
3. Fare clic con il pulsante destro del mouse sull'utente e scegliere **Proprietà**.
4. Nella finestra di dialogo Proprietà fare doppio clic su **distinguishedName**.
5. Copiare il DN dal campo
   Valore.



6. Per chiudere tutte le finestre, fare clic su **Annulla**.

Per ottenere la password per l'utente di binding, contattare l'amministratore di Active Directory.

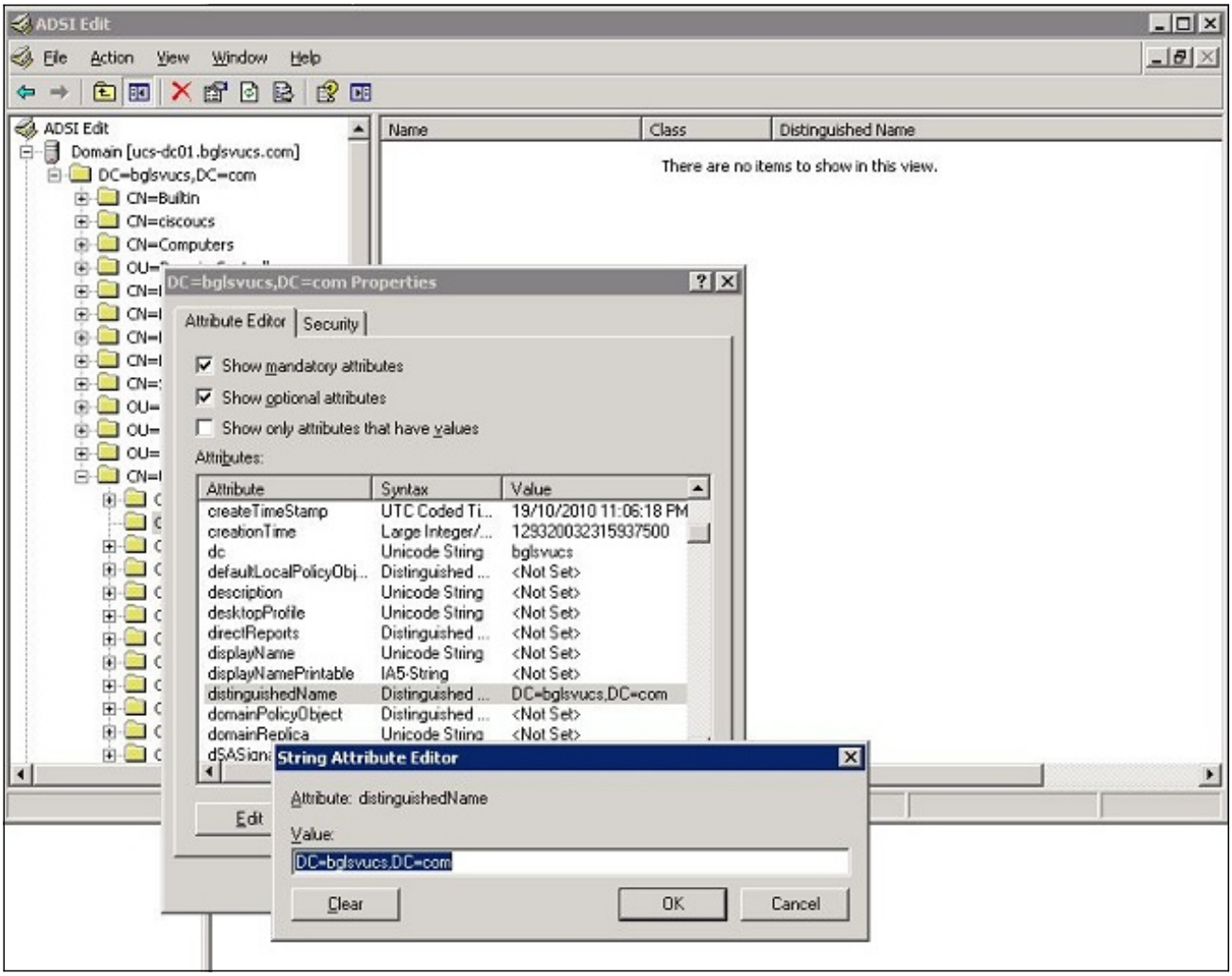
Dettagli DN di base

Il DN di base è il DN dell'unità organizzativa (OU, Organizational Unit) o il contenitore da cui ha inizio la ricerca dei dettagli utente e utente. È possibile utilizzare il DN di un'unità organizzativa creata in Active Directory per UCS o UCS Central. Tuttavia, potrebbe risultare più semplice utilizzare il DN per la radice del dominio.

In questa procedura viene descritto come un amministratore LDAP può utilizzare l'Editor ADSI per trovare il DN di base.

1. Aprire l'editor ADSI.

2. Individuare l'unità organizzativa o il contenitore da utilizzare come DN di base.
3. Fare clic con il pulsante destro del mouse sull'unità organizzativa o sul contenitore e scegliere **Proprietà**.
4. Nella finestra di dialogo Proprietà fare doppio clic su **distinguishedName**.
5. Copiare il DN dal campo del valore e prendere nota di tutti gli altri dettagli necessari.



6. Per chiudere tutte le finestre, fare clic su **Annulla**.

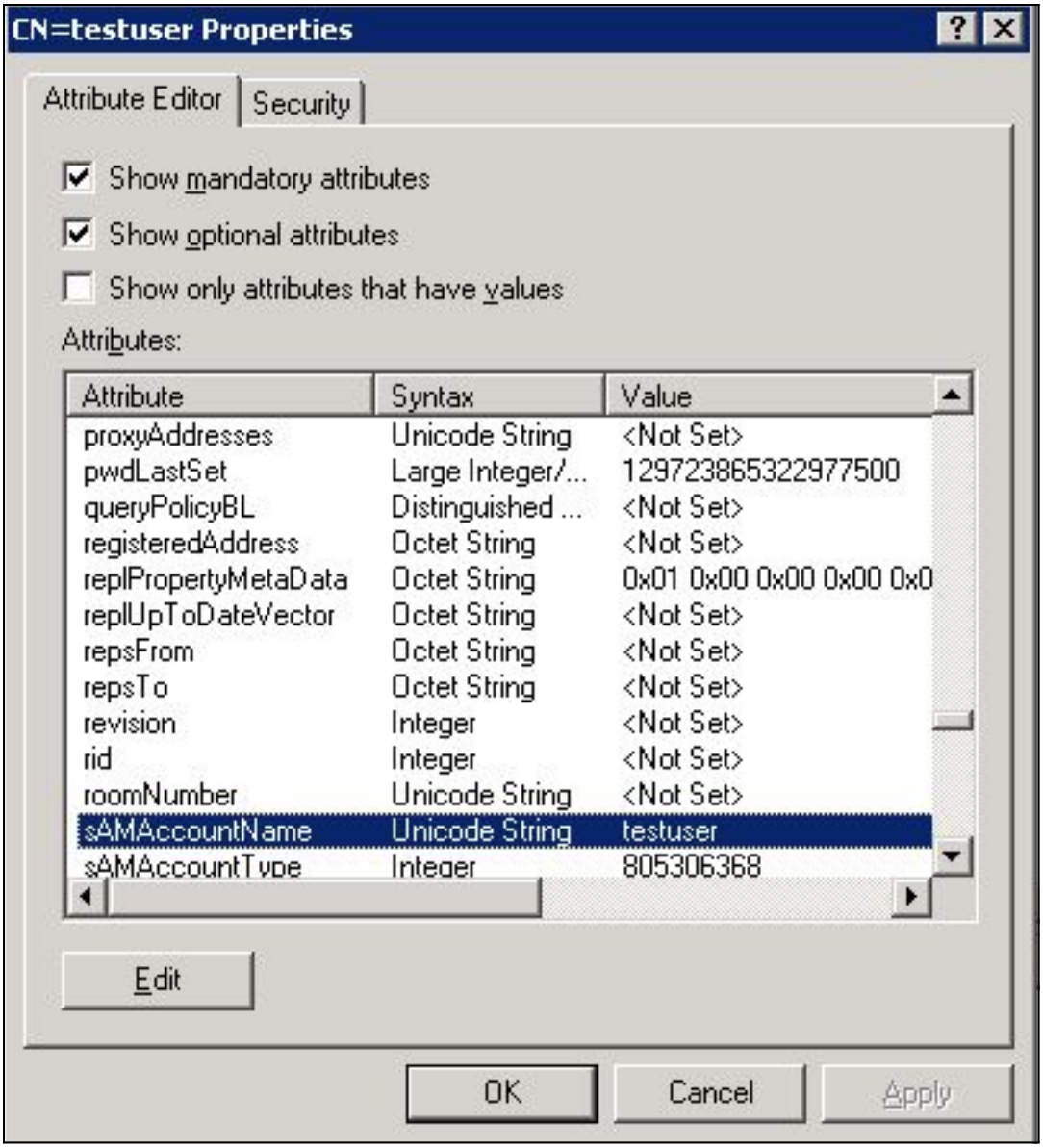
Dettagli provider

Il provider svolge un ruolo chiave nell'autenticazione e nell'autorizzazione LDAP in UCS Central. Il provider è uno dei server AD su cui UCS Central esegue query per cercare e autenticare l'utente e per ottenere i dettagli dell'utente, ad esempio le informazioni sul ruolo. Assicurarsi di raccogliere il nome host o l'indirizzo IP del server AD del provider.

Proprietà Filter

Il campo filtro o la proprietà viene utilizzato per eseguire ricerche nel database di Active Directory. L'ID utente immesso al momento dell'accesso viene restituito ad AD e confrontato con il filtro.

Èpossibile utilizzare sAMAccountName=$userid come valore di filtro. sAMAccountName è un attributo in Active Directory e ha lo stesso valore dell'ID utente di Active Directory, utilizzato per accedere all'interfaccia utente centrale di UCS.



Aggiungi e configura attributi

In questa sezione vengono riepilogate le informazioni necessarie per aggiungere l'attributo CiscoAVPair (se necessario) e aggiornare l'attributo CiscoAVPair o un altro attributo predefinito prima di avviare la configurazione LDAP.

Il campo attributo specifica l'attributo AD (sotto la proprietà utente), che restituisce il ruolo da assegnare all'utente. Nella release 1.0a del software UCS Central, è possibile unificare l'attributo personalizzato CiscoAVPair o qualsiasi altro attributo non utilizzato in Active Directory per passare questo ruolo.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

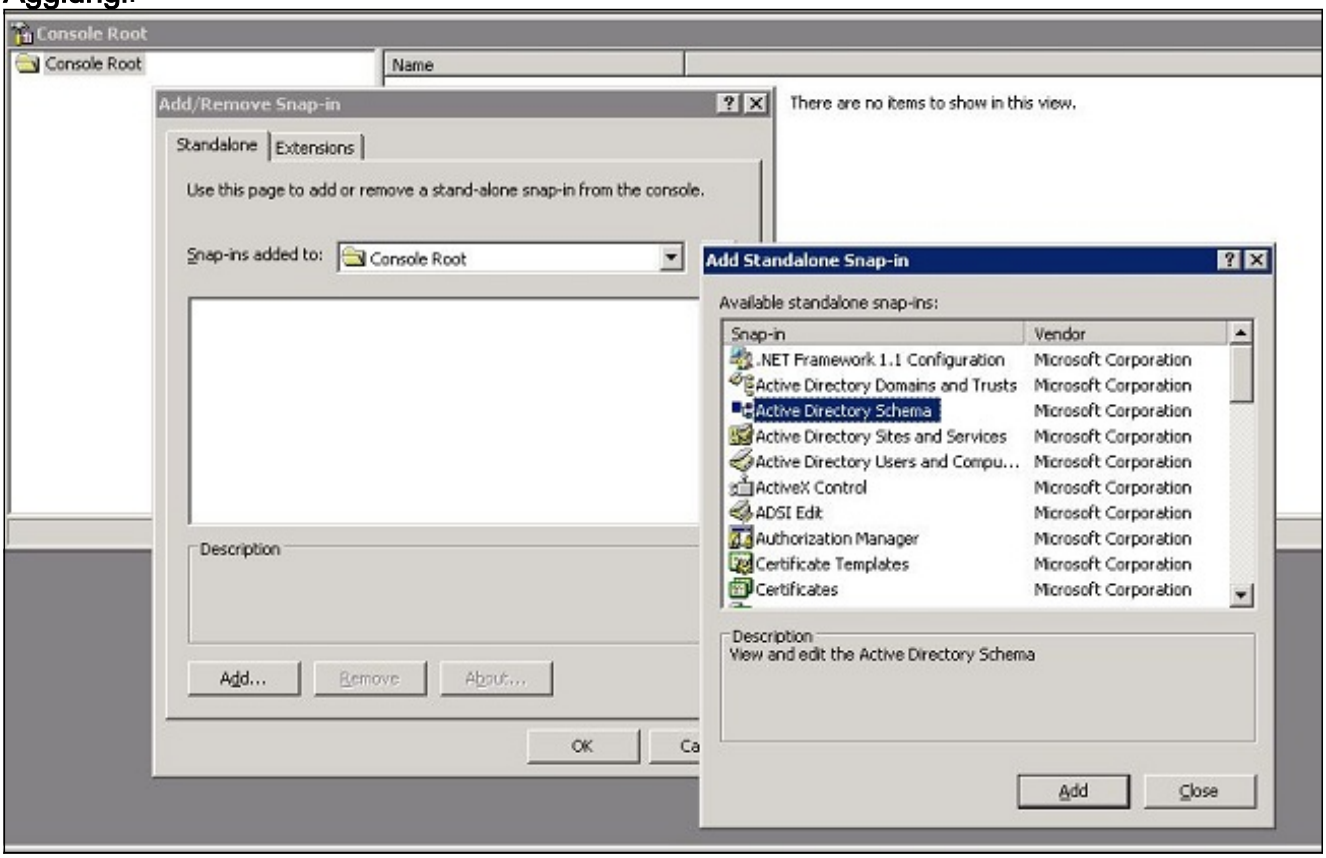
Aggiungi attributo CiscoAVPair

Per aggiungere un nuovo attributo al dominio, espandere lo schema del dominio e aggiungere l'attributo alla classe (che in questo esempio è user).

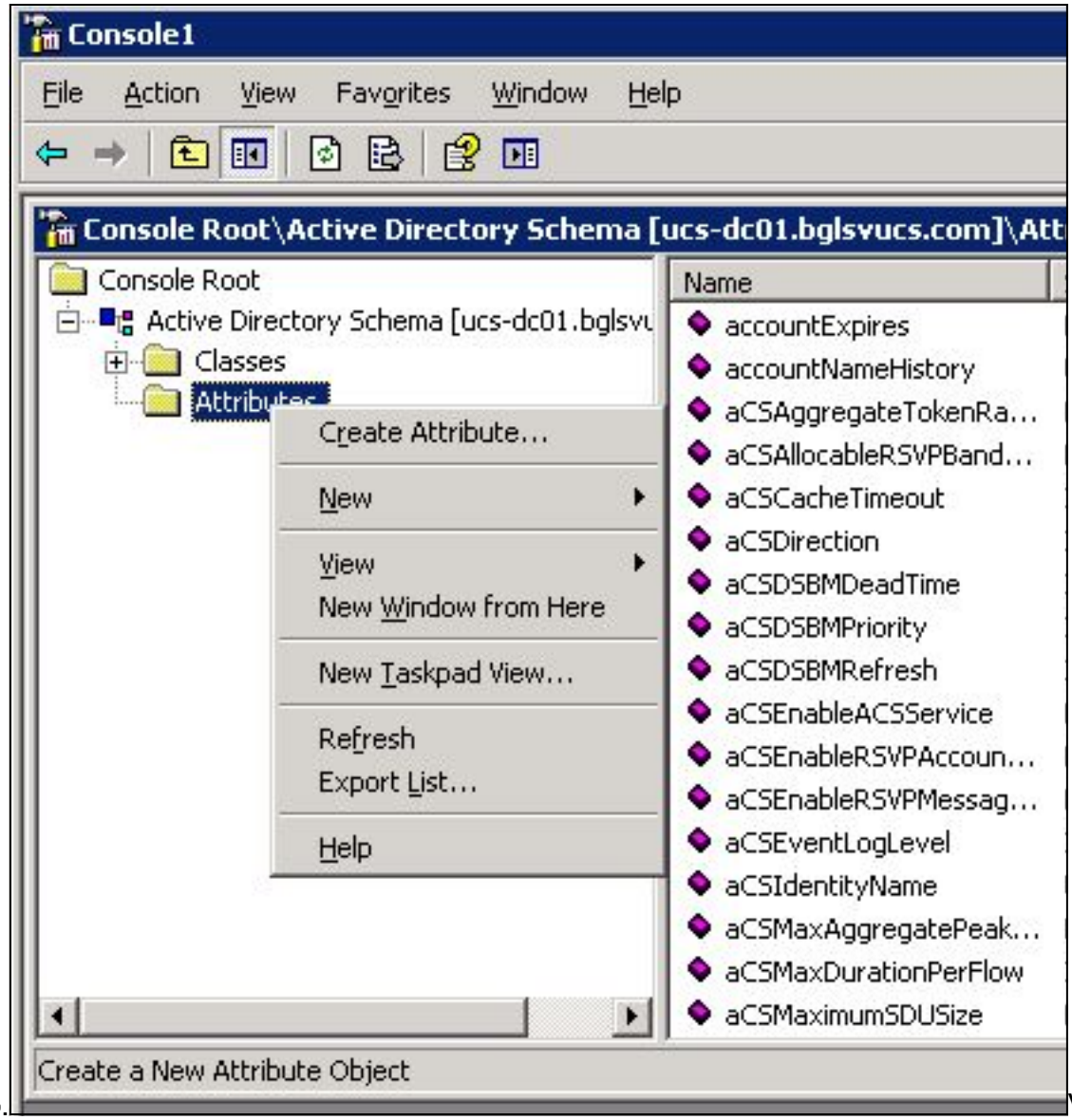
In questa procedura viene descritto come espandere lo schema in un server AD di Windows e

aggiungere l'attributo CiscoAVPair.

1. Accedere a un server AD.
2. Per aprire una console MMC vuota, fare clic su **Start > Esegui**, digitare **mmc** e premere **Invio**.
3. In MMC fare clic su **File > Aggiungi/Rimuovi snap-in > Aggiungi**.
4. Nella finestra di dialogo Aggiungi snap-in autonomo selezionare **Schema di Active Directory** e fare clic su
   Aggiungi.

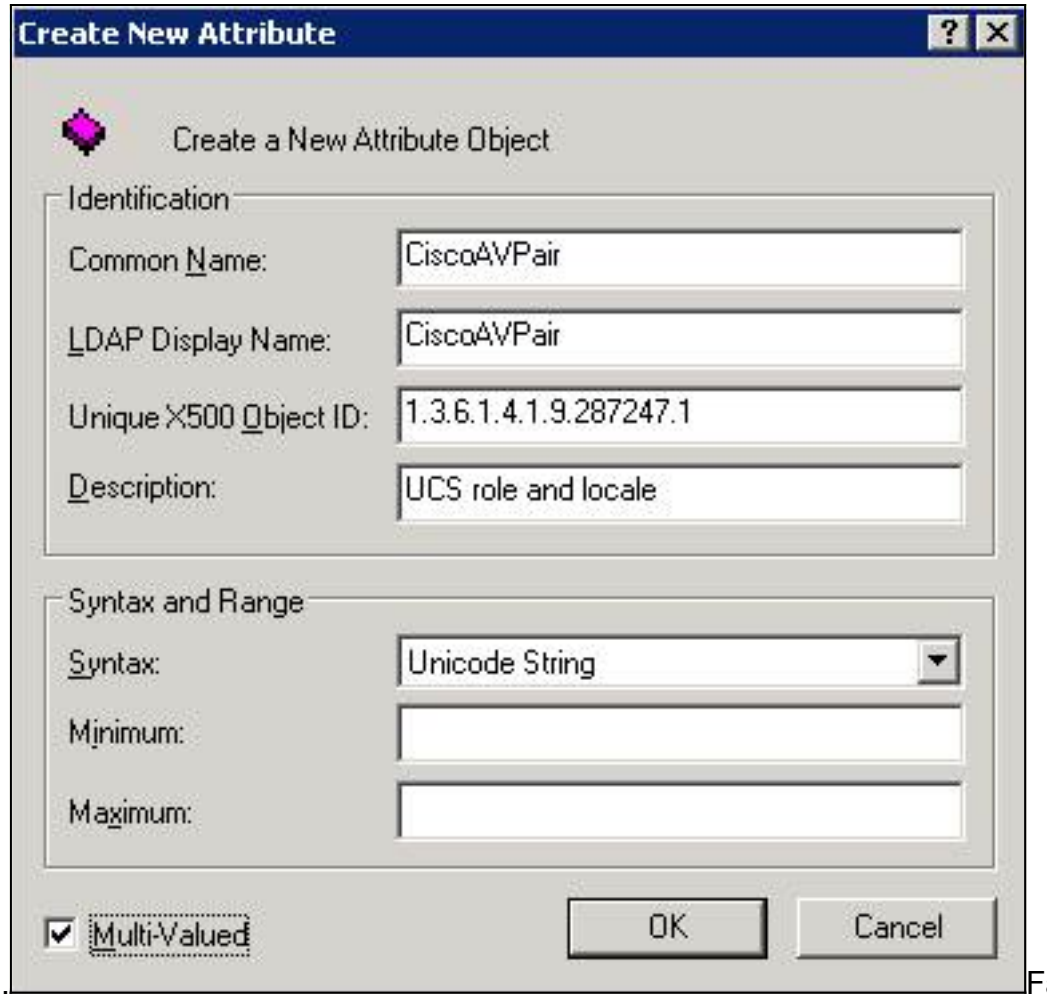


5. In MMC espandere **Schema di Active Directory**, fare clic con il pulsante destro del mouse su **Attributi** e scegliere **Crea**



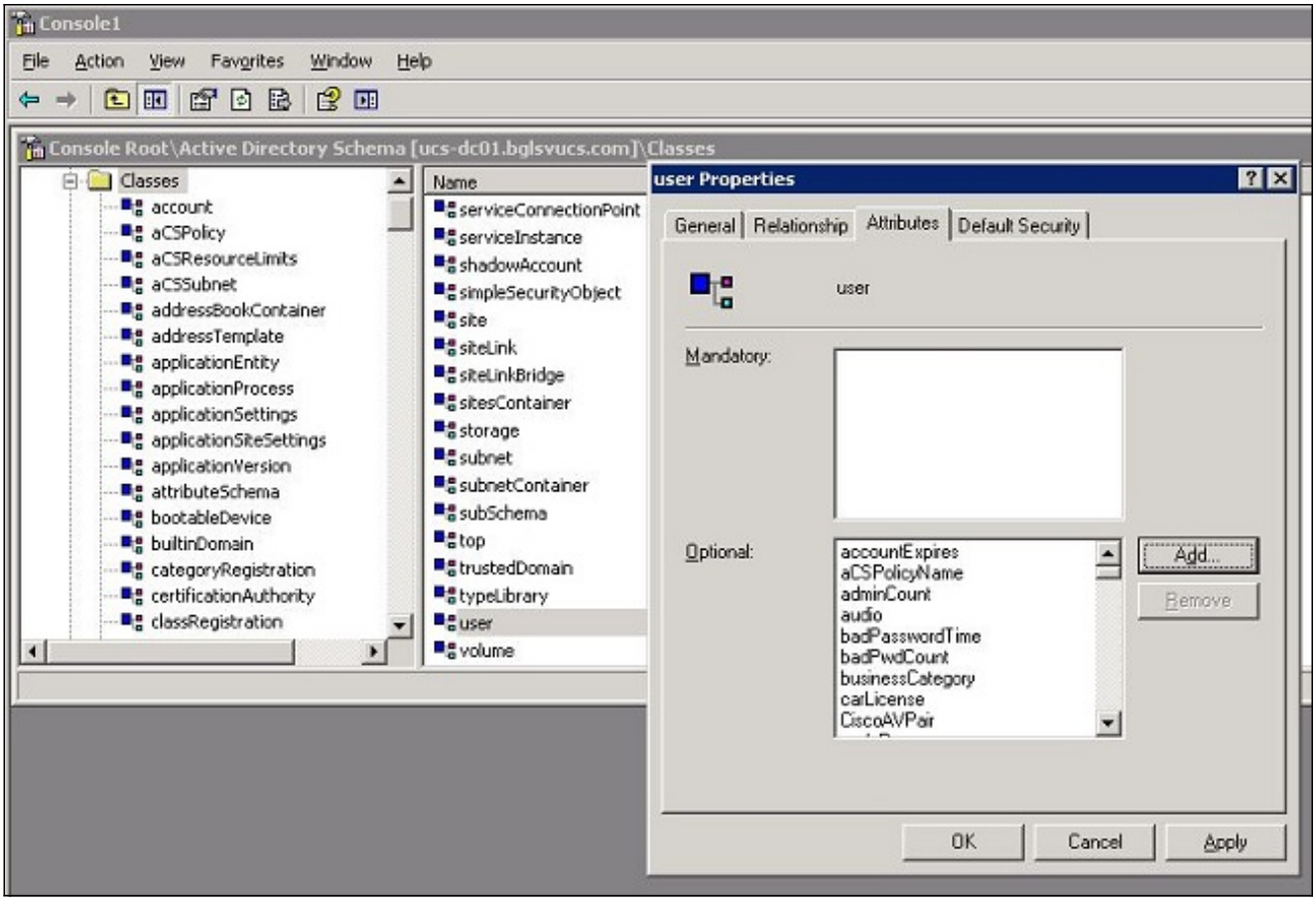
attributo.Verrà visualizzata la finestra di dialogo Crea nuovo attributo

6. Creare un attributo denominato CiscoAVPair nel servizio di autenticazione remota.Nei campi Nome comune e Nome visualizzato LDAP, immettere **CiscoAVPair**.Nel campo ID oggetto univoco 500, immettere **1.3.6.1.4.1.9.287247.1**.Nel campo Description (Descrizione), immettere **UCS role and locale (Ruolo UCS e impostazioni internazionali)**.Nel campo Sintassi selezionare **Stringa Unicode** dall'elenco a

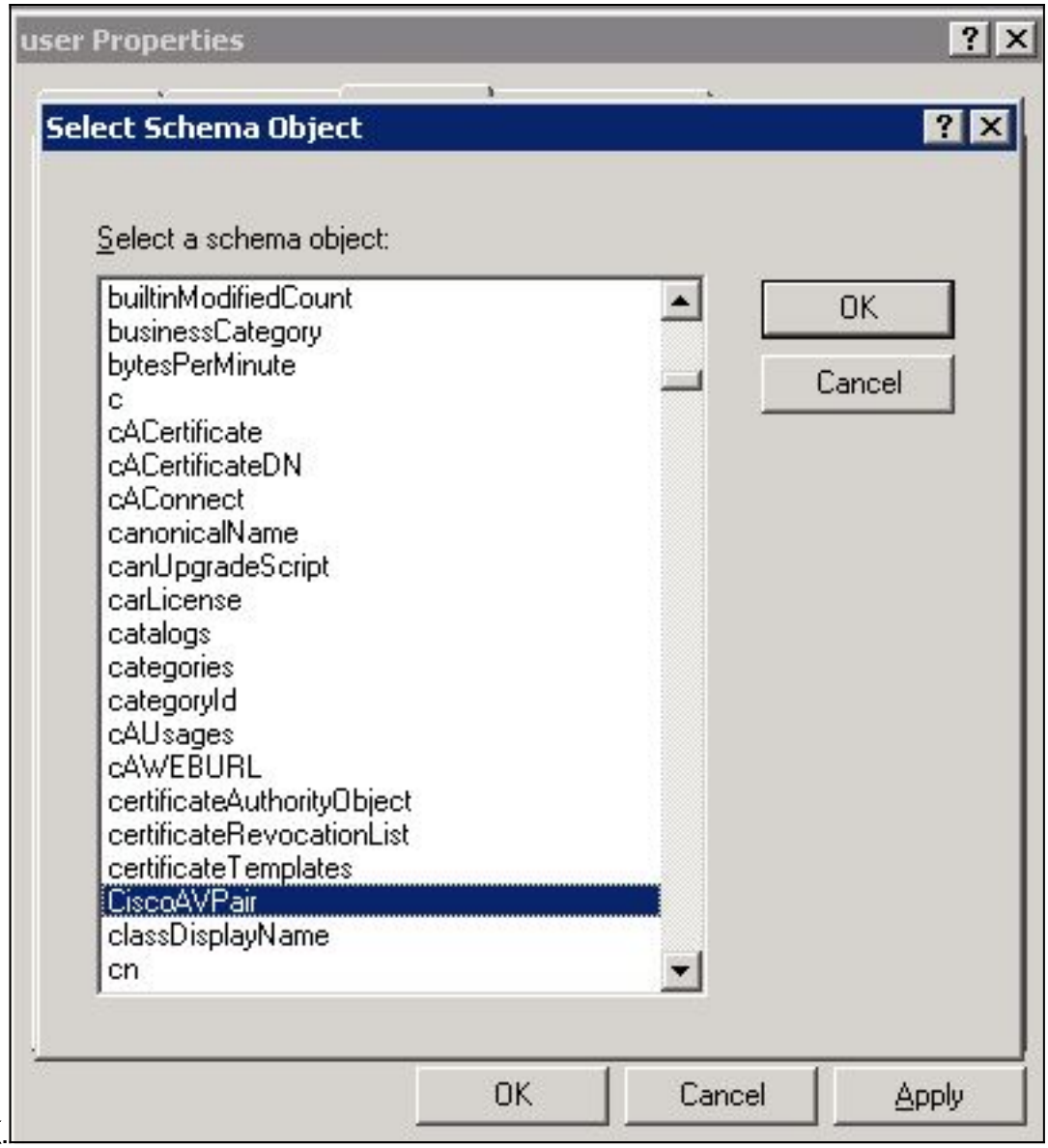


discesa. Fare clic su **OK** per salvare l'attributo e chiudere la finestra di dialogo.Una volta aggiunto allo schema, l'attributo deve essere mappato o incluso nella classe utente. In questo modo è possibile modificare la proprietà utente e specificare il valore del ruolo da passare.

7. Nello stesso MMC utilizzato per l'espansione dello schema di Active Directory espandere **Classi**, fare clic con il pulsante destro del mouse su **utente** e scegliere **Proprietà**.
8. Nella finestra di dialogo Proprietà dell'utente, fare clic sulla scheda **Attributi**, quindi su **Aggiungi**.

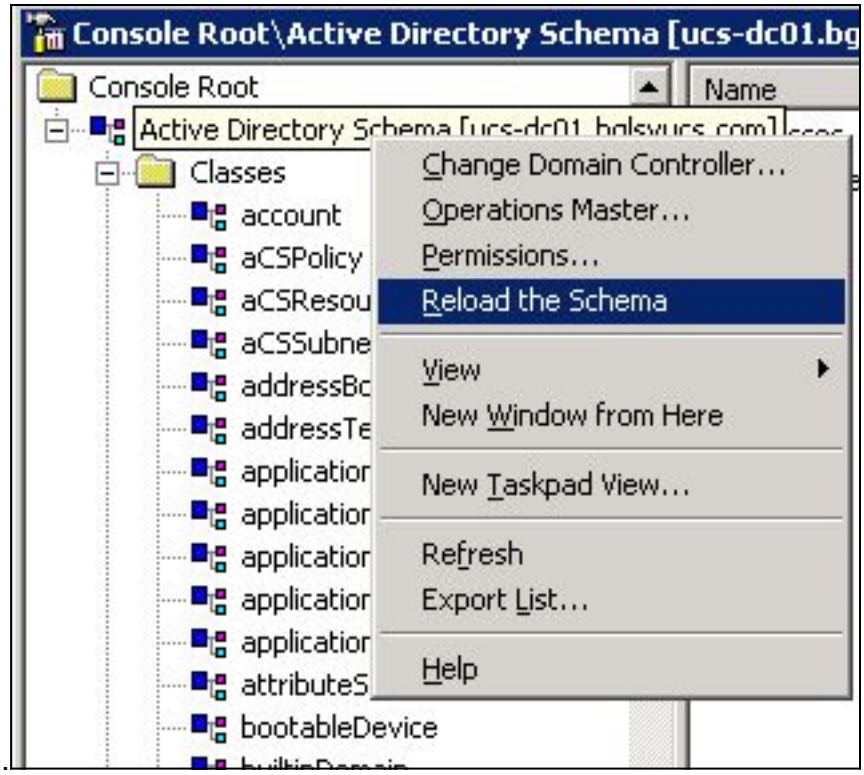


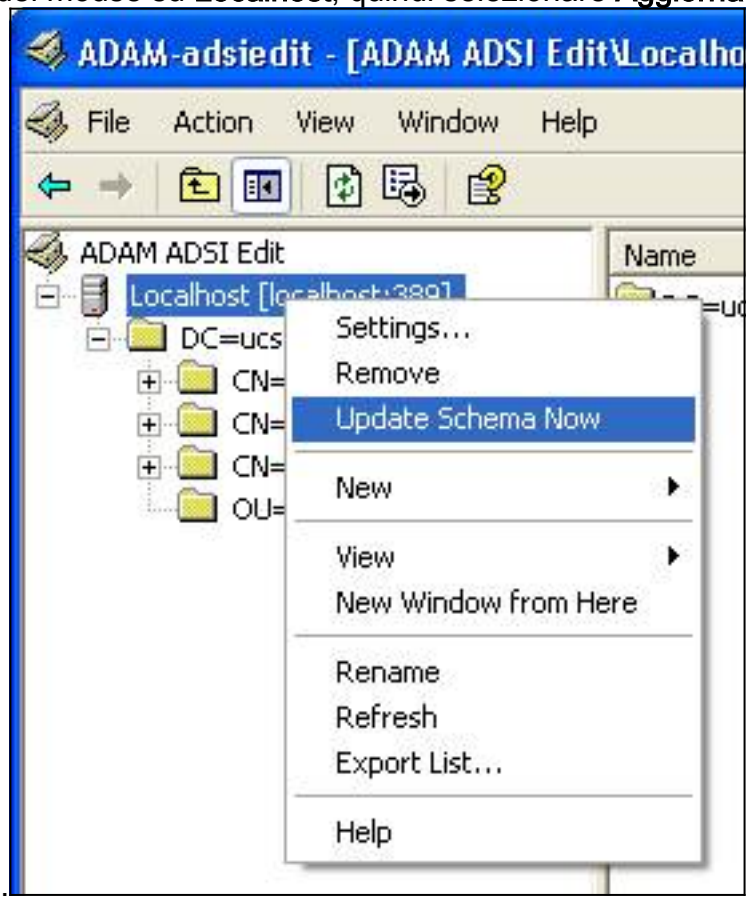
9. Nella finestra di dialogo Seleziona oggetto schema fare clic su **CiscoAVPair**, quindi su



OK.

10. Nella finestra di dialogo Proprietà dell'utente fare clic su **Applica**.
11. Fare clic con il pulsante destro del mouse su **Schema di Active Directory** e scegliere **Ricarica schema** per includere le nuove

modifiche. 

12. Se necessario, utilizzare l'editor ADSI per aggiornare lo schema. Fare clic con il pulsante destro del mouse su **Localhost**, quindi selezionare **Aggiorna schema adesso**. 

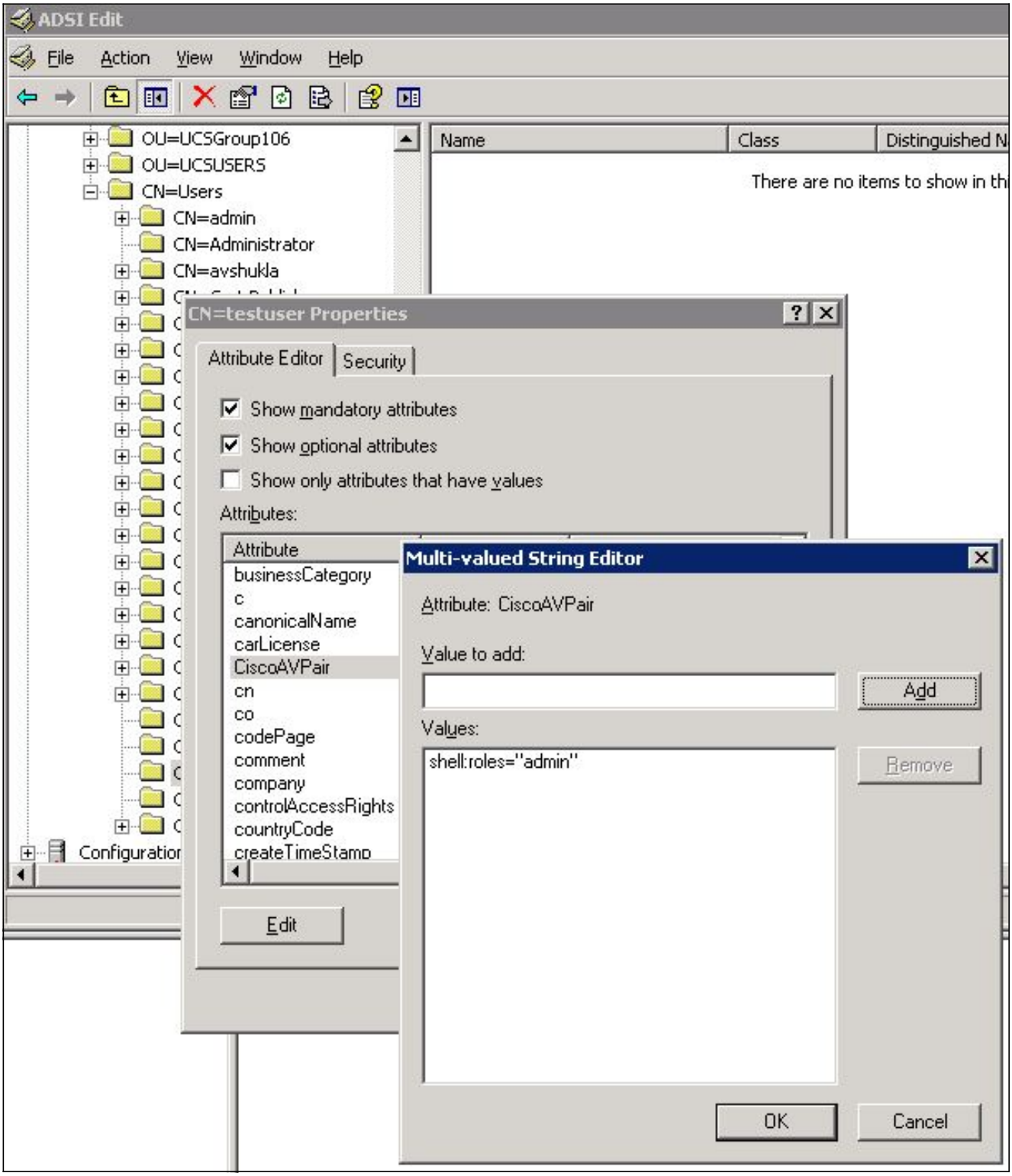
Aggiorna attributo CiscoAVPair

In questa procedura viene descritto come aggiornare l'attributo CiscoAVPair. La sintassi è `shell:roles="<role>"`.

1. Nella finestra di dialogo Modifica ADSI individuare l'utente che deve accedere a UCS

Central.

2. Fare clic con il pulsante destro del mouse sull'utente e scegliere **Proprietà**.
3. Nella finestra di dialogo Proprietà fare clic sulla scheda **Editor attributi**, quindi su **CiscoAVPair** e infine su **Modifica**.
4. Nella finestra di dialogo Editor stringhe multivalore immettere il valore **shell:roles="admin"** nel campo Valori e fare clic su **OK**.



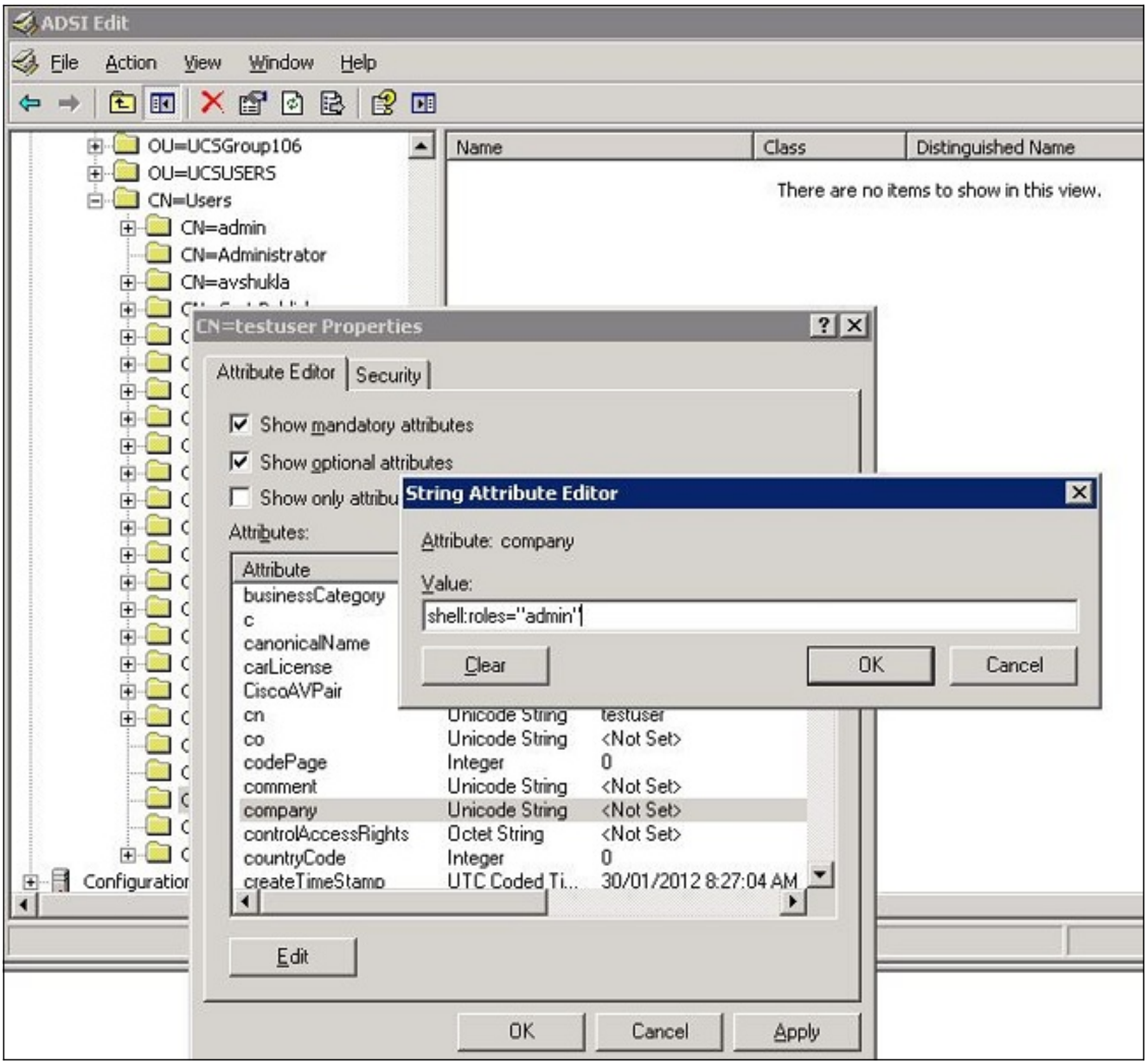
5. Fare clic su **OK** per salvare le modifiche e chiudere la finestra di dialogo Proprietà.

Aggiorna attributo predefinito

In questa procedura viene descritto come aggiornare un attributo predefinito, dove il ruolo è uno

dei ruoli utente predefiniti in UCS Central. In questo esempio viene utilizzato l'attributo *company* per passare il ruolo. La sintassi è `shell:roles="<role>"`.

1. Nella finestra di dialogo Modifica ADSI individuare l'utente che deve accedere a UCS Central.
2. Fare clic con il pulsante destro del mouse sull'utente e scegliere **Proprietà**.
3. Nella finestra di dialogo Proprietà fare clic sulla scheda **Editor attributi**, quindi su **società** e infine su **Modifica**.
4. Nella finestra di dialogo Editor attributi stringa immettere il valore **shell:roles="admin"** nel campo Valore e fare clic su **OK**.



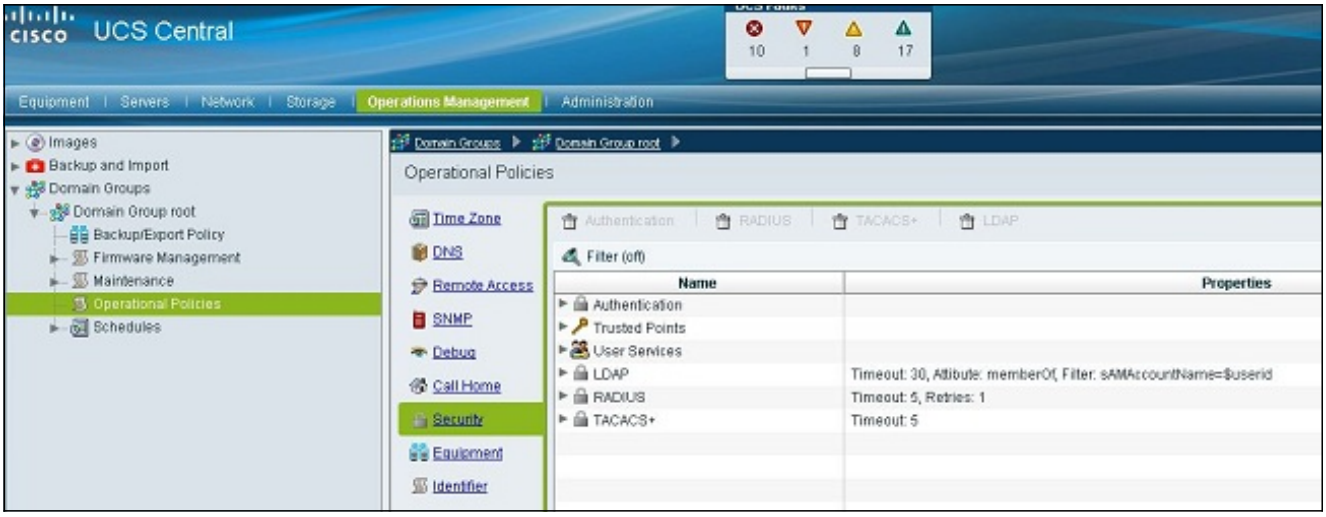
5. Fare clic su **OK** per salvare le modifiche e chiudere la finestra di dialogo Proprietà.

Configura autenticazione LDAP su UCS Central

La configurazione LDAP in UCS Central viene completata in Operations Management.

1. Accedere a UCS Central con un account locale.
2. Fare clic su **Operations Management**, espandere **Gruppi di dominio** e fare clic su **Criteri**

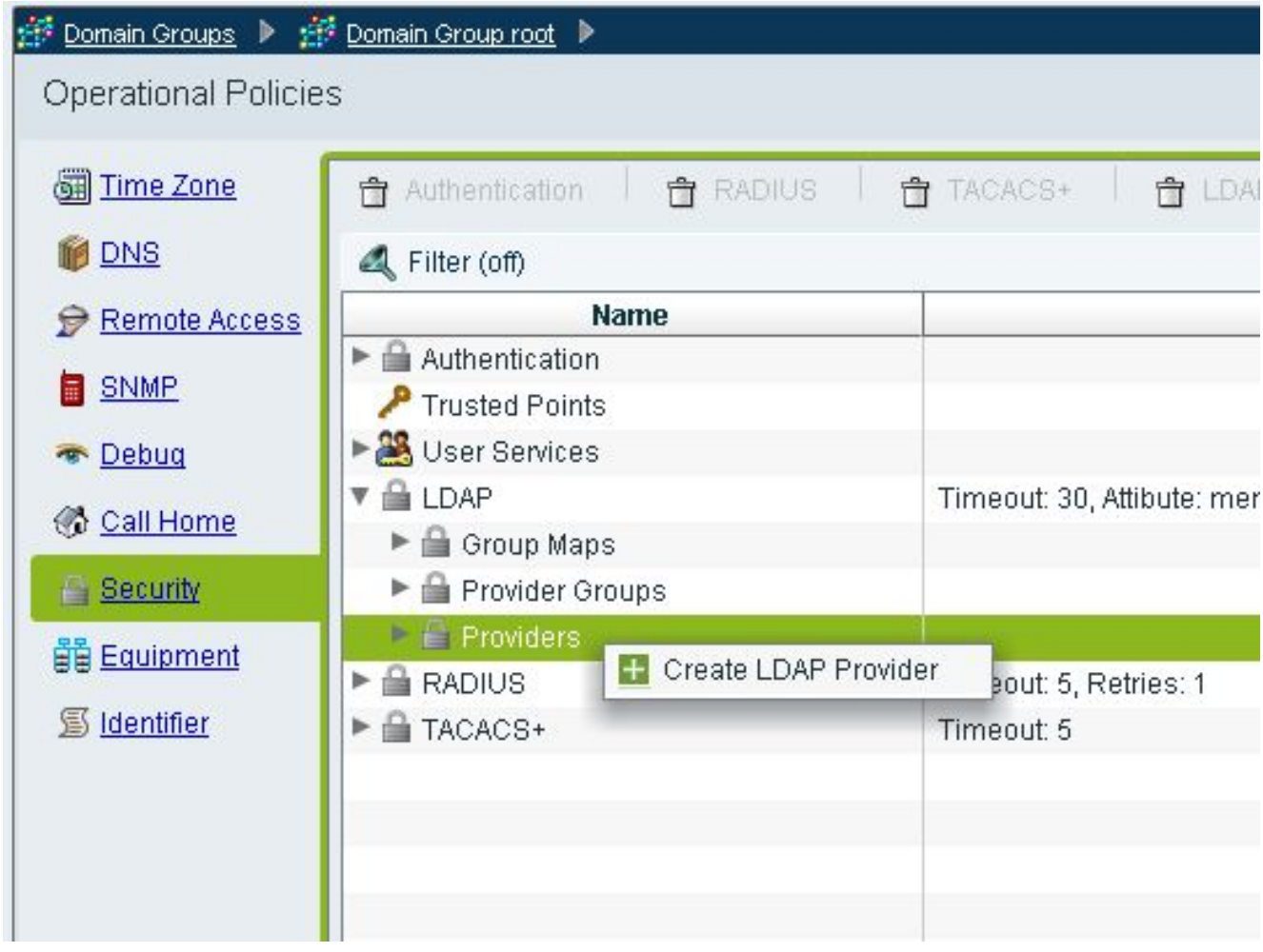
operativi >
Protezione.



3. Per configurare l'autenticazione LDAP, procedere come segue:Configurare il provider LDAP.Configurare il gruppo di provider LDAP (non disponibile nella release 1.0a).Modificare la regola di autenticazione nativa.

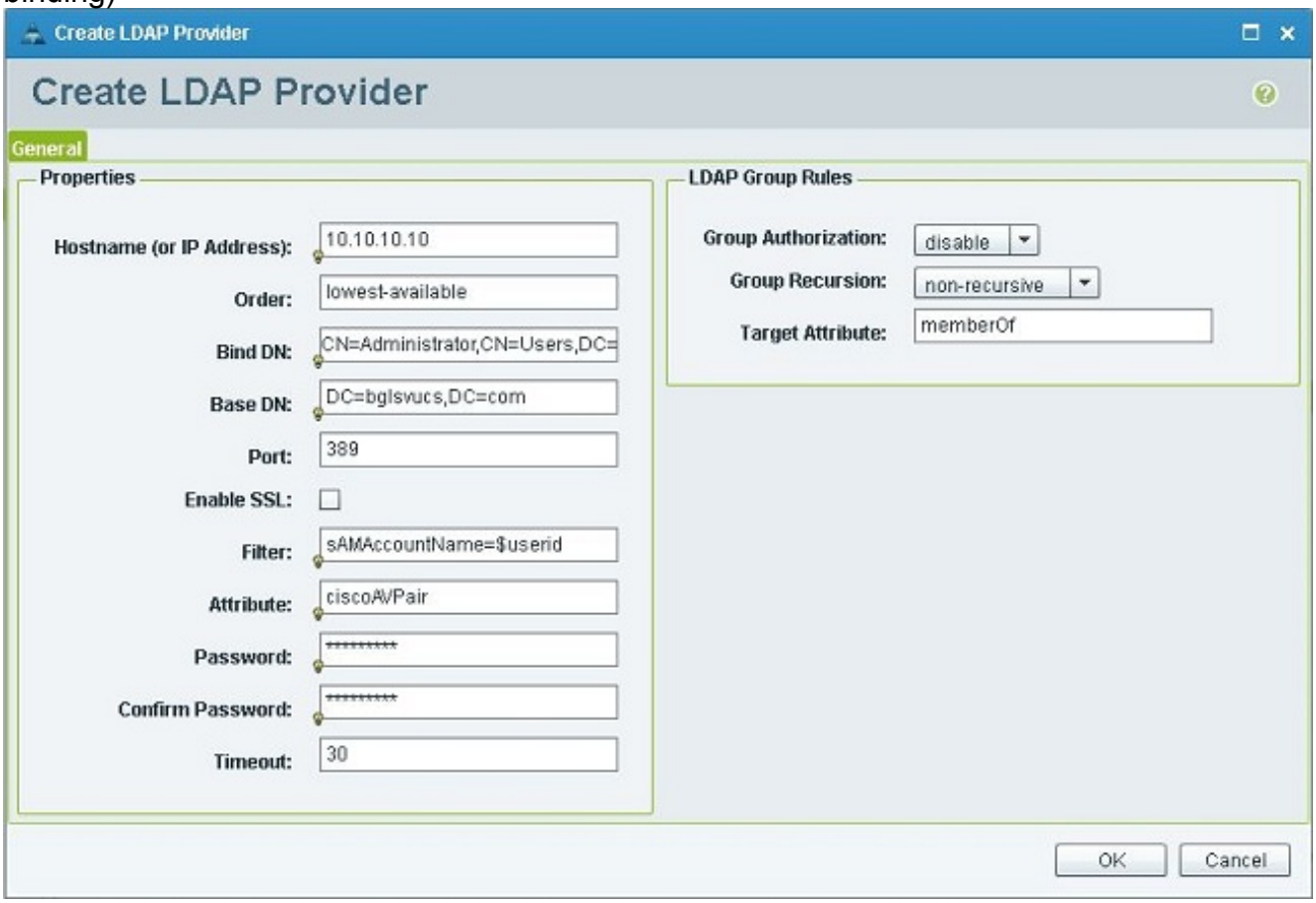
Configura provider LDAP

1. Fare clic su **LDAP**, fare clic con il pulsante destro del mouse su **Provider** e scegliere **Crea provider LDAP**.



2. Nella finestra di dialogo Crea provider LDAP aggiungere i dettagli raccolti in

precedenza.Nome host o indirizzo IP del providerDN bindingDN di baseFiltroAttributo (CiscoAVPair o un attributo predefinito come companyPassword (password dell'utente utilizzata nel DN di
binding)



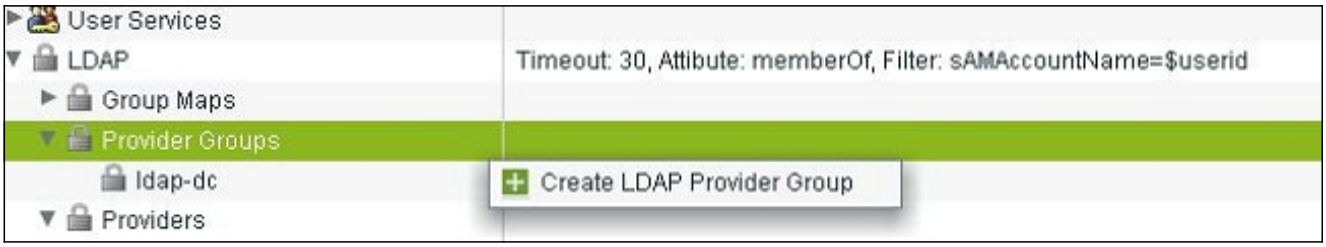
3. Per salvare la configurazione e chiudere la finestra di dialogo, fare clic su **OK**.

Nota: non è necessario modificare altri valori in questa schermata. Le regole di gruppo LDAP non sono supportate per l'autenticazione UCS Central in questa release.

Configura gruppo di provider LDAP

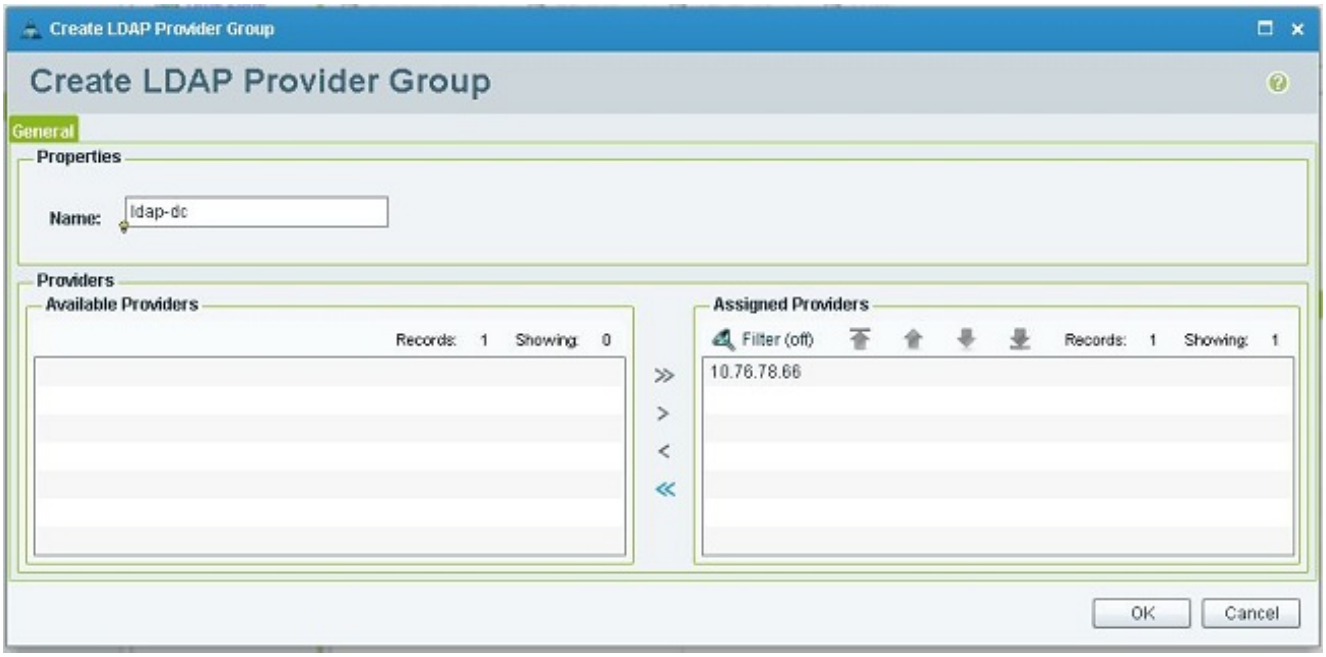
Nota: nella release 1.0a, i gruppi di provider non sono supportati. In questa procedura viene descritto come configurare un gruppo di provider fittizi da utilizzare nella configurazione in un secondo momento.

1. Fare clic su **LDAP**, fare clic con il pulsante destro del mouse su **Gruppo provider** e scegliere **Crea gruppo provider**
LDAP.



2. Nella finestra di dialogo Crea gruppo di provider LDAP, immettere il nome del gruppo nel campo Nome.
3. Dall'elenco dei provider disponibili a sinistra, selezionare il provider e fare clic sul simbolo maggiore di (**>**) per spostare il provider in Provider assegnati a

destra.



4. Fare clic su **OK** per salvare le modifiche e chiudere la schermata.

Modifica regola di autenticazione nativa

La release 1.0a non supporta più domini di autenticazione come in UCS Manager. Per risolvere questo problema, è necessario modificare la regola di autenticazione nativa.

L'autenticazione nativa consente di modificare l'autenticazione degli accessi predefiniti o della console. Poiché non sono supportati più domini, è possibile utilizzare l'account locale o un account LDAP, ma non entrambi. Modificare il valore del realm in modo da utilizzare locale o LDAP come origine dell'autenticazione.

1. Fare clic su **Autenticazione**, fare clic con il pulsante destro del mouse su **Autenticazione nativa** e scegliere **Proprietà**.
2. Determinare se si desidera l'autenticazione predefinita, l'autenticazione della console o entrambe. Utilizzare l'autenticazione predefinita per la GUI e l'interfaccia della riga di comando (CLI). Utilizzare l'autenticazione della console per la visualizzazione della macchina virtuale (KVM) basata su kernel della macchina virtuale (VM).
3. Selezionare **ldap** dall'elenco a discesa Realm. Il valore di Realm determina se l'origine dell'autenticazione è locale o
   LDAP.

4. Per chiudere la pagina, fare clic su **OK**.
5. Nella pagina Criteri, fare clic su **Salva** se necessario per salvare le modifiche.

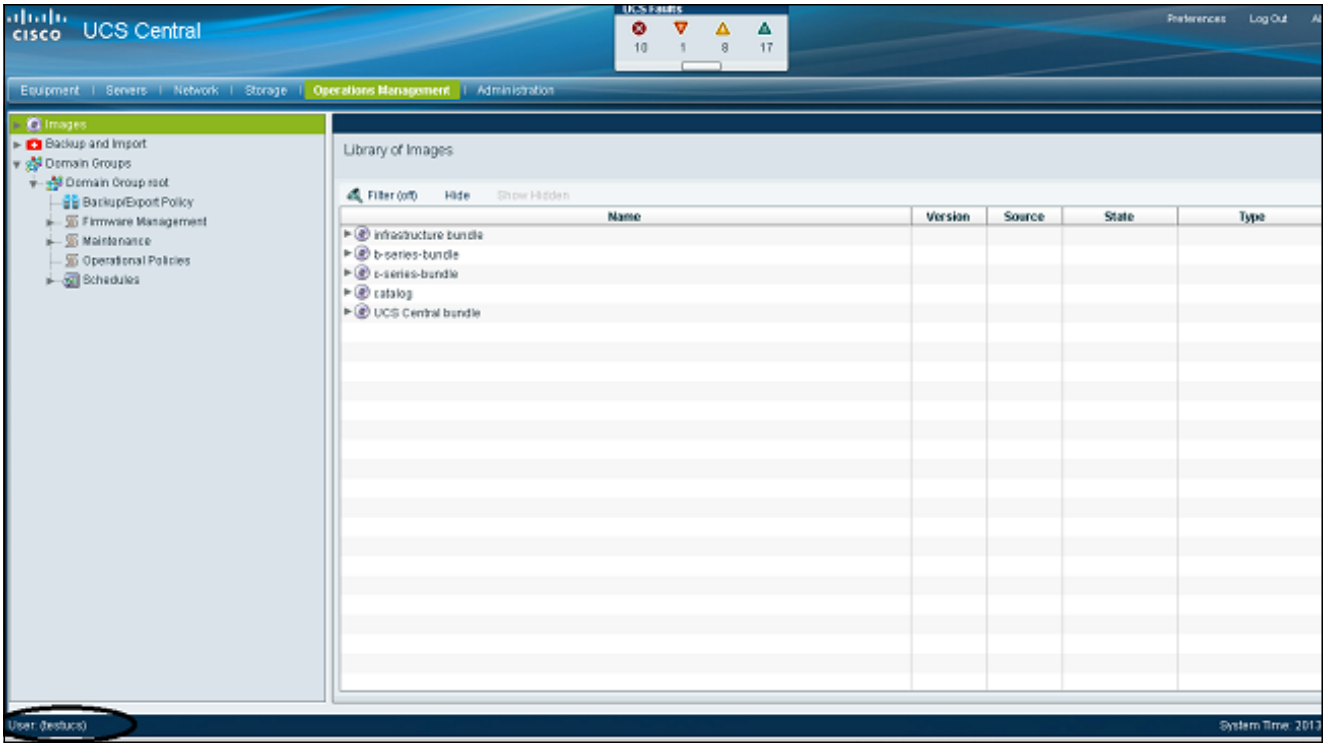
Nota: non disconnettersi dalla sessione corrente o modificare l'autenticazione della console fino a quando non si verifica che l'autenticazione LDAP funzioni correttamente. L'autenticazione della console consente di ripristinare la configurazione precedente. Consultare la sezione Verifica.

Verifica

In questa procedura viene descritto come verificare l'autenticazione LDAP.

1. Aprire una nuova sessione in UCS Central e immettere il nome utente e la password. Non è necessario includere un dominio o un carattere prima del nome utente. In questo esempio viene utilizzato testucs come utente del dominio.

2. L'autenticazione LDAP ha esito positivo se viene visualizzato il dashboard UCS Central. L'utente viene visualizzato nella parte inferiore della
pagina.



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems