# Esempio di configurazione dell'autenticazione LDAP per UCS Central

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Raccogli informazioni Associa dettagli utente Dettagli DN di base Dettagli provider **Proprietà Filter** Aggiungi e configura attributi Aggiungi attributo CiscoAVPair Aggiorna attributo CiscoAVPair Aggiorna attributo predefinito Configura autenticazione LDAP su UCS Central Configura provider LDAP Configura gruppo di provider LDAP Modifica regola di autenticazione nativa Verifica Risoluzione dei problemi Informazioni correlate

# 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 <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

# 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 <u>strumento di</u> 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



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.

Show <u>o</u> ptional attribut	tes	
Show only attributes t	that have <u>v</u> alues	
Attributes:	Guntau	Value
nroxuAddresses	Unicode String	<not set=""></not>
pwdLastSet	Large Integer/	129723865322977500
auervPolicvBL	Distinguished	<not set=""></not>
reaisteredAddress	Octet String	<not set=""></not>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
replUpToDateVector	Octet String	<not set=""></not>
repsFrom	Octet String	<not set=""></not>
repsTo	Octet String	<not set=""></not>
revision	Integer	<not set=""></not>
rid	Integer	<not set=""></not>
roomNumber	Unicode String	<not set=""></not>
sAMAccountName	Unicode String	testuser
sAMAccountType	Integer	805306368
<u> </u>		<u> </u>

# 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 <u>strumento di</u> 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

n Console Root						
Console Root		Name				
1	Add/Remove Snap-in		? ×	There are no items to show in th	s view.	
	Standalone Extensions	move a stand-alone snap-in from the consol	e.			
	Snap-ins added to:	Console Root 💌	Add Star	dalone Snap-in		? ×
			Available	e standalone snap-ins:	Vandar	
	Description		Act Carlor Act Act Act Act Act Act Act Act Act Act	T Framework 1.1 Configuration ive Directory Domains and Trusts ive Directory Sthema ive Directory Sites and Services ive Directory Users and Compu iveX Control 51 Edit horization Manager tificates Telicates	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
	Add	ννε <u>Αβ</u> τυ;	Descrip View ar	oncases otion nd edit the Active Directory Schem	a	•
		CKC	a		Add Clos	× (

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

e <u>A</u> ction <u>V</u> iew →	Havorites Window He	ip ucs.dc01.balsuucs.com]\ 01
Console Root	y Schema [ucs-dc01.bglsvu ireate Attribute iew ▶ iew ₩indow from Here iew Taskpad View iefresh xport List ielp	Name   AccountExpires  AccountNameHistory  ACSAggregateTokenRa  ACSAllocableRSVPBand  ACSCacheTimeout  ACSDirection  ACSDSBMDeadTime  ACSDSBMPriority  ACSDSBMRefresh  ACSEnableACSService  ACSEnableRSVPAccoun  ACSEnableRSVPAccoun  ACSEnableRSVPMessag  ACSEventLogLevel  ACSIdentityName  ACSEVENTLogLevel  ACSIdentityName  ACSEVENTLogLevel  ACSIdentityName ACSEVENTLogLevel  ACSIdentityName ACSEVENTLogLevel  ACSIdentityName ACSEVENTLogLevel  ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSEVENTLogLevel ACSIdentityName ACSEVENTLogLevel ACSEVENTLOGLEVEN
d	Þ	<ul> <li>aCSMaxAggregatePeak</li> <li>aCSMaxDurationPerFlow</li> <li>aCSMaximumSDUSize</li> </ul>

#### attributo.

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

Identification	
Common <u>N</u> ame:	CiscoAVPair
LDAP Display Name:	CiscoAVPair
Unique X500 <u>O</u> bject ID:	1.3.6.1.4.1.9.287247.1
Description:	UCS role and locale
Syntax and Range	
<u>S</u> yntax:	Unicode String
Minimum:	
Mavimum:	<u> </u>

discesa

**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**.

🚡 Console 1			
File Action View Favgrites Window	Help		
The Console Root\Active Directory Schem	na [ucs-dc01.bglsvucs.com]\	Classes	
🔁 🥘 Classes	▲ Name	user Properties	? ×
	<ul> <li>ServiceConnectionPoint</li> <li>ServiceInstance</li> <li>ShadowAccount</li> <li>SimpleSecurityObject</li> <li>Site</li> </ul>	General Relationship Attributes Default Sec	sunity
addressTemplate applicationEntity applicationProcess applicationSettings applicationSiteSettings applicationVersion attributeSchema bootableDevice	<ul> <li>siteLink</li> <li>siteScontainer</li> <li>sitesContainer</li> <li>subnet</li> <li>subnetContainer</li> <li>subSchema</li> </ul>	Mandatory:	
CategoryRegistration     CategoryRegistration     CategoryRegistration     CategoryRegistration     CategoryRegistration     CategoryRegistration	Stop     StrustedDomain     StypeLibrary     Suser     Svolume	<u>Optional:</u> accountExpires aCSPolicyName adminCount audio badPasswordTime badPwdCount businessCategory carLicense CiscoAVPair	Add
		OK	Cancel <u>Apply</u>

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

<u>S</u> elect a schema object:			
builtinModifiedCount businessCategory bytesPerMinute c cACertificate cACertificateDN cAConnect canonicalName canUpgradeScript carLicense catalogs categories categories categoryld cAUsages cAWEBURL certificateAuthorityObject certificateRevocationList certificateTemplates DiscoAVPatr classDisplayName		OK Cancel	

- 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



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** 

🐗 ADAM-adsiedi	t - [ADAM ADSI Edit\Loca
🌏 File Action N	/iew Window Help
← → 1 1	
I ADAM ADSI Edit	Name
⊡ <mark>]] Localhost [loc</mark> ⊡ <b>⊡</b> DC=ucs + <b>⊡</b> CN=	Settings Remove
⊕ 🛄 CN=	Update Schema Now
	New
	View   New Window from Here
	Rename Refresh
	Export List
	Help
esso.	

# 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.				
🖏 ADSI Edit				
File Action View Window Help				
		Name	Class	Distinguished N
CN=Administrator			There are no	items to show in th
Image: Construction of the second	ty   attrib ibute es th	utes es nat have <u>v</u> alues	? ×	
Image: Control Access Rights         Image: Control Access Rights <t< td=""><td>- Mi</td><td>ulti-valued String Editor Attribute: CiscoAVPair Value to add: Values: shell:roles=''admin''</td><td></td><td>Add Remove</td></t<>	- Mi	ulti-valued String Editor Attribute: CiscoAVPair Value to add: Values: shell:roles=''admin''		Add Remove
			ОК	Cancel

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



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 >

UCS Central		8 10	▼ 4 1	▲ ▲ 8 17	
Equipment I Servers I Network I Storage I	Operations Management	Administration			
@ Images ■ Backup and Import ﷺ Domain Groups ↓ ∰ Backunftwort Policy	Operational Policie	s Manuan Group note Authentication I @ RAD	us i 🛉	TACACE+	1 LDAP
Backup/Export Policy      S Firmware Management      S Maintenance      Bemote Acce		K Fiter (off)	Properties		
- 🧐 Operational Policies ▶ 🛃 Schedules	SNMP     SNMP     Call Home     Securit     Securit     Securit     Securit     Securite	Authentication  Authenticatio		Timeout: 30, Atti Timeout: 5, Retr Timeout: 5	ibute: memberO(, Filter: sAMAscountName=Suse

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

# Configura provider LDAP

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

🗿 <u>Time Zone</u>	🔒 Authentication 🕴 🔒 RADIUS	🕴 🕆 TACACS+ 🕴 🕆 LDA
DNS	🕰 Filter (off)	
P Remote Access	Name	
SNMP	<ul> <li>Authentication</li> <li>Prusted Points</li> </ul>	
👁 <u>Debuq</u>	▶ 🎇 User Services	
🚯 <u>Call Home</u>	<ul> <li>LDAP</li> <li>Group Maps</li> </ul>	Timeout: 30, Attibute: mer
Security	🕨 🗎 Provider Groups	
Equipment	► ▲ RADIUS         E Create LDAP	Provider pout: 5, Retries: 1
S Identifier	► 🔒 TACACS+	Timeout: 5

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)

🚖 Create LDAP Provider				<b>×</b>
Create LDAP P	rovider			0
General				
- Properties		LDAP Group Rules		
Hostname (or IP Address):	10.10.10.10	Group Authorization:	disable	
Order:	lowest-available	Group Recursion:	non-recursive 🔻	
Bind DN:	CN=Administrator,CN=Users,DC=	Target Attribute:	memberOf	
Base DN:	DC=bglsvucs,DC=com			
Port:	389			
Enable SSL:				
Filter:	sAMAccountName=\$userid			
Attribute:	ciscoAVPair			
Password:	······			
Confirm Password:				
Timeout:	30			
			ОК Са	ncel

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



- 2. Nella finestra di dialogo Crea gruppo di provider LDAP, immettere il nome del gruppo nel campo Nome.
- 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

Create LDAP Provider Group									(
Properties									_
Name: Idap-dc									
Providers Available Providers	- As	sianed Prov	iders –						
Records: 1 Showing: 0	4	Filter (off)	Ŧ	*	+	*	Records:	1 Showing	ĸ
	≫ 10.	76.78.66							
	>								
	<								
	«								
									_

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).
- Selezionare Idap dall'elenco a discesa Realm. Il valore di Realm determina se l'origine dell'autenticazione è locale o LDAP.

🏯 Properties			≡ ×
Properties (Native	Authentication)		0
General Events			
- Default Authentication:			
Session Refresh Period (in secs): Session Timeout (in secs): Realm:	600 7200 Idap <b>Provider Group:</b>	Idap-dc 💌	
Console Authentication:			
Role Policy for Remote Users: as	sign-default-role 🔻		
		OK	Cancel

- 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 <u>Verifica</u>.

# **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.



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

cisco UCS Central					R	eterences LogOut A
Environant   Genere   Network   Storage   Or	er sliger Management 1. Administration	10 1 8 17				
	Library of Images     Library of Images	Name	Version	Source	State	Тура
User destucs)						System Time: 2013

# 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