Ejemplo de Configuración de Autenticación LDAP para UCS Central

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados **Convenciones** Recopilar información Enlazar detalles del usuario Detalles de DN base Detalles del proveedor Propiedad de filtro Agregar y configurar atributos Agregar atributo CiscoAVPair Actualizar atributo CiscoAVPair Actualizar atributo predefinido Configuración de la autenticación LDAP en UCS Central Configurar proveedor LDAP Configurar grupo de proveedores LDAP Cambiar regla de autenticación nativa Verificación **Troubleshoot** Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo para la autenticación LDAP (protocolo ligero de acceso a directorios) para Cisco Unified Computing System (UCS) Central. Los procedimientos utilizan la interfaz gráfica de usuario (GUI) de UCS Central, un dominio de ejemplo de bglucs.com y un nombre de usuario de ejemplo de testuser.

En la versión 1.0 del software UCS Central, LDAP es el único protocolo de autenticación remota admitido. La versión 1.0 tiene soporte muy limitado para la autenticación remota y la configuración LDAP para el propio UCS Central. Sin embargo, puede utilizar UCS Central para configurar todas las opciones para los dominios UCS Manager administrados por UCS Central.

Las limitaciones de la autenticación remota de UCS Central incluyen:

• RADIUS y TACACS no son compatibles.

- No se soporta la asignación de pertenencia a grupos LDAP para la asignación de roles y grupos de proveedores LDAP para múltiples controladores de dominio.
- LDAP utiliza solamente el atributo CiscoAVPair o cualquier atributo sin utilizar para pasar la función. La función pasada es una de las funciones predefinidas de la base de datos local de UCS Central.
- No se admiten varios dominios/protocolos de autenticación.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- UCS Central está implementado.
- Microsoft Active Directory está implementado.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCS Central versión 1.0
- Microsoft Active Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Recopilar información

Esta sección resume la información que necesita recopilar antes de iniciar la configuración.

<u>Nota:</u> Utilice la herramienta <u>Command Lookup</u> (sólo para clientes <u>registrados</u>) para obtener más información sobre los comandos utilizados en esta sección.

Enlazar detalles del usuario

El usuario de enlace puede ser cualquier usuario LDAP en el dominio que tenga acceso de lectura al dominio; se requiere un usuario de enlace para la configuración LDAP. UCS Central utiliza el nombre de usuario y la contraseña del usuario de enlace para conectar y consultar Active Directory (AD) para la autenticación de usuario, etc. En este ejemplo se utiliza la cuenta de administrador como usuario de enlace.

Este procedimiento describe cómo un administrador LDAP puede utilizar el Editor de interfaces de

servicio de Active Directory (ADSI) para encontrar el DN.

- 1. Abra el Editor ADSI.
- 2. Busque el usuario de enlace. El usuario se encuentra en la misma ruta que en AD.
- 3. Haga clic con el botón derecho del ratón en el usuario y elija Propiedades.
- 4. En el cuadro de diálogo Propiedades, haga doble clic en **nombre** distinguido.
- 5. Copie el DN del campo



6. Haga clic en Cancelar para cerrar todas las ventanas.

Para obtener la contraseña del usuario de enlace, póngase en contacto con el administrador de AD.

Detalles de DN base

DN base es el DN de la unidad organizativa (OU) o el contenedor donde comienza la búsqueda de los detalles del usuario y usuario. Puede utilizar el DN de una OU creada en AD para UCS o UCS Central. Sin embargo, puede que le resulte más sencillo utilizar el DN para la raíz del dominio en sí.

Este procedimiento describe cómo un administrador LDAP puede utilizar el Editor ADSI para encontrar el DN base.

1. Abra el Editor ADSI.

- 2. Busque la OU o el contenedor que se utilizará como DN base.
- 3. Haga clic con el botón derecho del ratón en la OU o en el contenedor y elija Propiedades.
- 4. En el cuadro de diálogo Propiedades, haga doble clic en **nombre** distinguido.
- 5. Copie el DN del campo de valor y observe cualquier otro detalle que

necesite.

🧔 ADSI Edit					
Sele Action View Window Help					<u>_8</u> ×
← → È II × 2 2 2 3					
ADSI Edit	Name		Class	Distinguished Na	me
Domain [ucs-dc01.bg/svucs.com] DC-bg/svucs,DC=com ON=Bulkin ON=Computers OU= CN=I OU= DC=bg/svucs,DC=com Pro OU= CN=I Attribute Editor Security OU= V Show mandatory attribute OU= V Show only attributes the	utes ss hat have <u>v</u> alues		There are no i	items to show in this	view.
Attributes:					
Attribute	Syntax	Value	•		
CreateTimeStamp CreateTimeSta	UTC Coded Ti Large Integer/ Unicode String Distinguished Unicode String Distinguished Unicode String IA5-String Distinguished Distinguished Unicode Strina unice Strina	19/10/2010 11:06 129320032315937 bglsvucs <not set=""> <not set=""></not></not></not></not></not></not></not></not></not></not></not>	:18 PM 500	X	
	the second second				<u> </u>
Edit Value: Clear	conguishedName		OK _	Cancel	

6. Haga clic en Cancelar para cerrar todas las ventanas.

Detalles del proveedor

El proveedor desempeña un papel clave en la autenticación y autorización LDAP en UCS Central. El proveedor es uno de los servidores AD que UCS Central consulta para buscar y autenticar al usuario y para obtener detalles del usuario, como información de rol. Asegúrese de recopilar el nombre de host o la dirección IP del servidor de AD del proveedor.

Propiedad de filtro

El campo o la propiedad de filtro se utiliza para buscar la base de datos de AD. La ID de usuario ingresada al inicio de sesión se devuelve al AD y se compara con el filtro.

Puede utilizar sAMAccountName=\$userid como valor de filtro. sAMAccountName es un atributo en AD y tiene el mismo valor que el ID de usuario de AD, que se utiliza para iniciar sesión en la GUI de UCS Central.

Show mandatory attril Show optional attribut	butes tes	
Show only attributes t	hat have <u>v</u> alues	
.ttri <u>b</u> utes:		
Attribute	Syntax	Value 🔺
proxyAddresses	Unicode String	<not set=""></not>
pwdLastSet	Large Integer/	129723865322977500
queryPolicyBL	Distinguished	<not set=""></not>
registeredAddress	Octet String	<not set=""></not>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
repIUpToDateVector	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>N.</u>		

Agregar y configurar atributos

Esta sección resume la información que necesita para agregar el atributo CiscoAVPair (si es necesario) y actualizar el atributo CiscoAVPair u otro atributo predefinido antes de iniciar la configuración LDAP.

El campo de atributo especifica el atributo AD (en la propiedad de usuario), que devuelve la función que se va a asignar al usuario. En la versión 1.0a del software UCS Central, el atributo personalizado CiscoAVPair o cualquier otro atributo no utilizado en AD se puede unificar para pasar esta función.

<u>Nota:</u> Utilice la herramienta <u>Command Lookup</u> (sólo para clientes <u>registrados</u>) para obtener más información sobre los comandos utilizados en esta sección.

Agregar atributo CiscoAVPair

Para agregar un nuevo atributo al dominio, expanda el esquema del dominio y agregue el atributo a la clase (que, en este ejemplo, es usuario).

Este procedimiento describe cómo expandir el esquema en un servidor de Windows AD y agregar

el atributo CiscoAVPair.

- 1. Inicie sesión en un servidor AD.
- 2. Haga clic en **Inicio > Ejecutar**, escriba **mmc** y presione **Intro** para abrir una consola vacía de Microsoft Management Console (MMC).
- 3. En el MMC, haga clic en Archivo > Agregar o quitar complemento > Agregar.
- 4. En el cuadro de diálogo Agregar complemento independiente, seleccione el **esquema de** Active Directory y haga clic en

Console Root		Name	1				
COIDOIC ROOL		Indine		-			
	Add/Remove Snap-in			? ×	There are no items to show in thi	s view.	
Standalone	Standalone Extensions						
	Use this page to add or r	emove a stand-alone snap-in fr	om the console				
	Snap-ins added to: 🔄	Console Root	•	Add Stan	dalone Snap-in		? ×
			1000	Available	standalone snap-ins:		
				Snap-in		Vendor	*
				A NET	Framework 1.1 Configuration	Microsoft Corporation	
				4 gActi	ve Directory Domains and Trusts	Microsoft Corporation	
				CACIT	ve Directory Schema	Microsoft Corporation	
				Activ	ve Directory Sites and Services	Microsoft Corporation	
				Acti	ve Directory Users and Compu	Microsoft Corporation	
				3 Activ	veX Control	Microsoft Corporation	
				ADS	IEdt	Microsoft Corporation	
	Description				Iorization Manager	Microsoft Corporation	
				den Cert	ificate Templates	Microsoft Corporation	
				Cert	incates	Microsoft Corporation	-
				Descrip View ap	tion d edit the Active Directory Schem		
	Add	Absut					
		04					
					-		

5. En el MMC, expanda **Esquema de Active Directory**, haga clic con el botón derecho en **Atributos** y elija **Crear**

		<u>Teih</u>
n Console Root	Active Directory Schema	a [ucs-dc01.bglsvucs.com]\At
Console Root	New Colore Free deat being	Name
	ctory Schema Lucs-dc01.bglsv s Create Attribute	 AccountExpires AccountNameHistory ACSAggregateTokenRa ACSAllocableRSVPBand
	New	aCSCacheTimeout
	⊻iew New <u>W</u> indow from Here	aCSDirection aCSDSBMDeadTime aCSDSBMPriority
	New <u>T</u> askpad View	aCSDSBMRefresh
	Re <u>f</u> resh Export <u>L</u> ist	 aCSEnableACSService aCSEnableRSVPAccoun aCSEnableRSVPMessag
	Help	♦ aCSEventLogLevel
1	1	 aCSIdentityName aCSMaxAggregatePeak aCSMaxDurationPerFlow aCSMaximumSDUSize

atributo.

cerá el cuadro de diálogo Crear nuevo atributo

6. Cree un atributo denominado CiscoAVPair en el servicio de autenticación remota.En los campos Nombre común y Nombre de visualización LDAP, ingrese CiscoAVPair.En el campo Identificador de objeto único 500, introduzca 1.3.6.1.4.1.9.287247.1.En el campo Description (Descripción), introduzca UCS role and locale.En el campo Sintaxis, seleccione Cadena Unicode en la lista

- 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:	
Maximum:	

clic en **Aceptar** para guardar el atributo y cerrar el cuadro de diálogo.Una vez agregado el atributo al esquema, se debe asignar o incluir en la clase de usuario. Esto permite editar la propiedad de usuario y especificar el valor de la función que se va a pasar.

- 7. En el mismo MMC utilizado para la expansión del esquema de AD, expanda **Clases**, haga clic con el botón derecho en **usuario** y elija **Propiedades**.
- 8. En el cuadro de diálogo Propiedades del usuario, haga clic en la ficha Atributos y haga clic en

Agregar.

🛗 Console1			
Eile Action View Favorites Window	Help		
Console Root\Active Directory Schem	a [ucs-dc01.bglsvucs.com]\	Classes	
Classes	Name ReserviceConnectionPoint	user Properties	? ×
aCSPolicy aCSResourceLimits aCSSubnet addressBookContainer	ServiceInstance ShadowAccount SimpleSecurityObject Site	General Relationship Attributes Default	Security
addressTemplate applicationEntity applicationProcess applicationSettings applicationSiteSettings applicationVersion attributeSchema bootableDevice	SiteLink SiteLinkBridge SitesContainer SitesContainer SitesContainer SitesContainer SubnetContainer Subschema	Mandatory:	
BuiltinDomain CategoryRegistration CategoryRegistration CategoryRegistration CategoryRegistration CategoryRegistration	LippeLibrary User Volume	Qptional: accountExpires aCSPolicyName adminCount audio badPasswordTime badPwdCount businessCategory carLicense CiscoAVPoir	Add
		<u>ОК</u>	Cancel Apply

9. En el cuadro de diálogo Seleccionar objeto de esquema, haga clic en CiscoAVPair y haga

use	er Properties			?
S	elect Schema Object			? ×
	Select a schema object: builtinModifiedCount businessCategory bytesPerMinute c cACertificate cACertificateDN cAConnect canonicalName canUpgradeScript carLicense catalogs categories categoryId cAUsages cAWEBURL certificateRevocationList certificateRevocationList certificateTemplates CISCOAVPair classDisplayName cn			OK Cancel
· · ·		0K	Cancel	

- 10. En el cuadro de diálogo Propiedades del usuario, haga clic en Aplicar.
- 11. Haga clic con el botón derecho en **Esquema de Active Directory** y elija **Recargar el Esquema** para incluir los nuevos



12. Si es necesario, utilice el Editor ADSI para actualizar el esquema. Haga clic con el botón derecho del ratón en Localhost y elija Actualizar esquema

🌏 File Action \	/iew Window Help	
⇐ ⇒ 🗈 💽	🖻 🗟 😰	
I ADAM ADSI Edit		Nam
E DC=ucs	Settings Remove	<u>.</u>
⊡ (N=	Update Schema Now	
⊕ 🛄 CN=	New	8
	View New Window from He) ere
	Rename Refresh	
	Export List	
-	Help	

Actualizar atributo CiscoAVPair

Este procedimiento describe cómo actualizar el atributo CiscoAVPair. La sintaxis es shell:roles="<role>".

1. En el cuadro de diálogo Editar ADSI, busque el usuario que necesita acceso a UCS Central.

- 2. Haga clic con el botón derecho del ratón en el usuario y elija Propiedades.
- 3. En el cuadro de diálogo Propiedades, haga clic en la ficha **Editor de atributos**, haga clic en **CiscoAVPair** y haga clic en **Editar**.
- En el cuadro de diálogo Editor de cadenas multivaloradas, introduzca el valor shell:roles="admin" en el campo Valores y haga clic en Aceptar

🗳 ADSI Edit			
G Eile Action View Window Help			
	N E		
OU=UCSGroup106	Name	Class	Distinguished N
		There are no	items to show in thi
		incre are no	
CN=Administrator			
🕀 🧰 CN=avshukla			
CN=testuser Propertie	5	? ×	
	d .		
		1	
E International Enternation E	tributes		
😥 🧰 c 🛛 🗹 Show optional attrit	lutes		
E	s that have <u>v</u> alues		
Attribute businessCategory	Multi-valued String Editor		×
	<u>Attribute: CiscoAVPair</u>		
	Value to add:		
E CiscoAVPair			
	Values:		
codePage	shell:roles="admin"		Bemove 1
C company			1701101/2
E ControlAccessmights			
Configuration CreateTimeStamp			
			F
<u>E</u> dit			=
		ОК	Cancel

5. Haga clic en Aceptar para guardar los cambios y cerrar el cuadro de diálogo Propiedades.

Actualizar atributo predefinido

Este procedimiento describe cómo actualizar un atributo predefinido, donde la función es una de las funciones de usuario predefinidas en UCS Central. Este ejemplo utiliza la *compañía* de

atributos para pasar la función. La sintaxis es shell:roles="<role>".

- 1. En el cuadro de diálogo Editar ADSI, busque el usuario que necesita acceso a UCS Central.
- 2. Haga clic con el botón derecho del ratón en el usuario y elija Propiedades.
- 3. En el cuadro de diálogo Propiedades, haga clic en la ficha **Editor de atributos**, haga clic en **compañía** y haga clic en **Editar**.
- 4. En el cuadro de diálogo Editor de atributos de cadena, introduzca el valor **shell:roles="admin"** en el campo Valor y haga clic en

icopiai.				
🆏 ADSI Edit				
🍕 Eile Action Yiew Window Help				
← → 🗈 🖬 🗙 😭 🗟 😫				
DU=UCSGroup106	▲ Name		Class	Distinguished Name
OU=UCSUSERS OU=UCSUSERS ON=admin ON=Administrator ON=avshukla ON=testuser Propert ON=Construction ON=Constr	ies irity attributes tributes string Attribute Ed Attribute: company Value: shell:roles="admin" Unicode String Unicode String Unicode String Integer UTC Coded Ti	itor testuser <not set=""> 0 <not set=""> <not set=""> <not set=""> 0 30/01/2012 8:27:0</not></not></not></not>	There are no	items to show in this view.
	ОК	Cancel	Apply	

5. Haga clic en Aceptar para guardar los cambios y cerrar el cuadro de diálogo Propiedades.

Configuración de la autenticación LDAP en UCS Central

La configuración LDAP en UCS Central se completa en Operations Management.

- 1. Inicie sesión en UCS Central en una cuenta local.
- Haga clic en Operations Management, expanda Domain Groups y haga clic en Operational Policies > Security.

Equipment Servers Network Storage	Operations Management	Administration	8 10	1	8	▲ 17	
	Consin Groups Paratin Groups Operational Policie Ime Zone Pols	S Authentication	n RADIUS	B	â 140	AC8+	10 LDAP
 Schedules Schedules 	Bemate Access SNMP Call Home Security Security Security Security Security Security	Name Authentication Authentication Cuser Services Cuser Services Cuser Services Cuse Cuse Cuse Cuse Cuse Cuse Cuse Cu			Time Time Time	rout: 30, / rout: 5, R rout: 5	Properties Adjoute: memberO(, Filter: sAMAccountName=\$userid letries: 1

3. Para configurar la autenticación LDAP, siga estos pasos:<u>Configure el proveedor</u> <u>LDAP.Configure el grupo de proveedores LDAP</u> (no disponible en la versión 1.0a).<u>Cambie la</u> <u>regla de autenticación nativa.</u>

Configurar proveedor LDAP

1. Haga clic en LDAP, haga clic con el botón derecho en Proveedores y elija Crear proveedor LDAP.

📅 <u>Domain Groups</u> 🕨 🛱 Operational Policie	[≇] <u>Domain Group root</u> S	
Time Zone Image: DNS	🕆 Authentication 🕴 🕆 RADIUS	🖶 TACACS+ 🖶 LDAI
P Remote Access	Name	
SNMP	Authentication P Trusted Points	
👁 Debuq	▶ 🎇 User Services	
🚯 <u>Call Home</u>	LDAP Group Maps	Timeout: 30, Attibute: mer
Security	▶ 🚔 Provider Groups	
Equipment <u>S</u> Identifier	 Providers RADIUS TACACS+ 	rovider pout: 5, Retries: 1 Timeout: 5

 En el cuadro de diálogo Crear proveedor LDAP, agregue estos detalles, que se recopilaron anteriormente.Nombre de host o IP del proveedorEnlazar DNDN baseFiltroAtributo (CiscoAVPair o un atributo predefinido como la empresaContraseña (contraseña del usuario utilizada en el DN de

3. Haga clic en Aceptar para guardar la configuración y cerrar el cuadro de diálogo.

Nota: No es necesario modificar ningún otro valor en esta pantalla. Las reglas del grupo LDAP no son compatibles con la autenticación de UCS Central en esta versión.

Configurar grupo de proveedores LDAP

Nota: En la versión 1.0a, no se admiten grupos de proveedores. Este procedimiento describe cómo configurar un grupo de proveedores ficticio para que lo use más adelante en la configuración.

1. Haga clic en LDAP, haga clic con el botón derecho del mouse en Grupo de Proveedores y elija Crear Grupo de Proveedores

🖻 📇 User Services	
🖉 🚔 LDAP	Timeout: 30, Attibute: memberOf, Filter: sAMAccountName=\$userid
🕨 🔒 Group Maps	
🔻 🚔 Provider Groups	
🔒 Idap-dc	E Create LDAP Provider Group
🔻 🔒 Providers	

- 2. En el cuadro de diálogo Crear grupo de proveedores LDAP, introduzca el nombre del grupo en el campo Nombre.
- En la lista de proveedores disponibles a la izquierda, seleccione el proveedor y haga clic en el símbolo mayor que (>) para mover ese proveedor a Proveedores asignados a la derecha.

🚓 Create LDAP Provider Group	□ ×
Create LDAP Provider Group	0
Name: dap-dc Providers Available Providers Records: 1 Showing: 0	Assigned Providers Assigned Providers Filter (off) Records: 1 Showing: 1 10.76.78.66
	OK Cancel

4. Haga clic en Aceptar para guardar los cambios y cerrar la pantalla.

Cambiar regla de autenticación nativa

La versión 1.0a no admite varios dominios de autenticación como en UCS Manager. Para solucionar esto, debe modificar la regla de autenticación nativa.

La autenticación nativa tiene la opción de modificar la autenticación para los inicios de sesión o inicios de sesión de consola predeterminados. Dado que no se soportan varios dominios, puede utilizar la cuenta local o una cuenta LDAP, pero no ambos. Cambie el valor de rango para utilizar local o LDAP como origen de autenticación.

- 1. Haga clic en Authentication, haga clic con el botón derecho en Native Authentication y elija Properties.
- Determine si desea autenticación predeterminada, autenticación de consola o ambas. Utilice la autenticación predeterminada para la interfaz gráfica de usuario y la interfaz de línea de comandos (CLI). Utilice la autenticación de consola para la vista de máquina virtual (KVM) basada en kernel de máquina virtual (VM).
- 3. Elija **Idap** en la lista desplegable Rango. El valor de rango determina si local o LDAP es el origen de la autenticación.

🏯 Properties			⊟ ×
Properties (Native	Authentication)		0
General Events			
- Default Authentication:			1
Session Refresh Period (in secs): Session Timeout (in secs): Realm:	600 7200 Idap 👻 Provider Group:	Idap-dc 💌	
Console Authentication:			
Role Policy for Remote Users: as	sign-default-role 🔻		
		OK	Cancel

- 4. Haga clic en Aceptar para cerrar la página.
- 5. En la página Políticas, haga clic en **Guardar** si es necesario para guardar los cambios.

Nota: No cierre la sesión actual ni modifique la autenticación de la consola hasta que verifique que la autenticación LDAP funcione correctamente. La autenticación de consola proporciona una manera de volver a la configuración anterior. Consulte la sección <u>Verificación</u>.

Verificación

Este procedimiento describe cómo probar la autenticación LDAP.

1. Abra una nueva sesión en UCS Central e introduzca el nombre de usuario y la contraseña. No es necesario incluir un dominio o un carácter antes del nombre de usuario. En este ejemplo se utilizan los pasos como usuario del dominio.



 La autenticación LDAP es correcta si ve el panel de UCS Central. El usuario se muestra en la parte inferior de la página.

abab		UCS Faults				
cisco UCS Central					P0	Herenzes Log OLZ AL
		10 1 8 17				
Equipment Servers Network Storage	Operations Management Administration		_			
🖸 Images						
Backup and Import	Library of Images					
v 💏 Domain Groups						
Backup/Export Policy	K Filter (off) Hide Show Hidden					
- 55 Firmware Management		Name	Version	Source	State	Туре
- S Maintenance	mestructure bundle					
D Operational Policies	► @ t-series-bundle					
P Qu serres a	► @ catalog					
	► @ UCS Central bundle					
User destuca)						System Time: 2013

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems