Exemplo de configuração de autenticação LDAP para UCS Central

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados **Conventions** Coletar informações Vincular detalhes do usuário Detalhes do DN base Detalhes do provedor Propriedade do filtro Adicionar e configurar atributos Adicionar atributo CiscoAVPair Atualizar atributo CiscoAVPair Atualizar atributo predefinido Configurar a autenticação LDAP no UCS Central Configurar provedor LDAP Configurar grupo de provedores LDAP Alterar regra de autenticação nativa Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento fornece uma configuração de exemplo para a autenticação LDAP (Lightweight Diretory Access Protocol) para o Cisco Unified Computing System (UCS) Central. Os procedimentos usam a interface gráfica de usuário (GUI) do UCS Central, um domínio de exemplo de bglucs.com, e um exemplo de nome de usuário do testuser.

Na versão 1.0 do software UCS Central, o LDAP é o único protocolo de autenticação remota suportado. A versão 1.0 tem suporte muito limitado para autenticação remota e configuração LDAP para o próprio UCS Central. No entanto, você pode usar o UCS Central para configurar todas as opções para os domínios do UCS Manager gerenciados pelo UCS Central.

As limitações da autenticação remota central do UCS incluem:

• RADIUS e TACACS não são suportados.

- Não há suporte para mapeamento de associação de grupo LDAP para atribuição de função e grupos de provedores LDAP para vários controladores de domínio.
- O LDAP usa apenas o atributo CiscoAVPair ou qualquer atributo não utilizado para passar a função. A função passada é uma das funções predefinidas no banco de dados local do UCS Central.
- Não há suporte para vários domínios/protocolos de autenticação.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O UCS Central é implantado.
- O Microsoft Ative Diretory está implantado.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- UCS Central versão 1.0
- Microsoft Ative Diretory

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.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Coletar informações

Esta seção resume as informações que você precisa coletar antes de iniciar a configuração.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Vincular detalhes do usuário

Vincular usuário pode ser qualquer usuário LDAP no domínio que tenha acesso de leitura ao domínio; um usuário de associação é necessário para a configuração LDAP. O UCS Central usa o nome de usuário e a senha do usuário de associação para conectar e consultar o Ative Diretory (AD) para autenticação de usuário e assim por diante. Este exemplo usa a conta de Administrador como o usuário de associação.

Este procedimento descreve como um administrador LDAP pode usar o ADSI (Ative Diretory Service Interfaces) para localizar o DN.

- 1. Abra o Editor ADSI.
- 2. Localize o usuário de associação. O usuário está no mesmo caminho do AD.
- 3. Clique com o botão direito do mouse no usuário e escolha Propriedades.
- 4. Na caixa de diálogo Propriedades, clique duas vezes em DistinguityName.
- 5. Copie o DN do campo



6. Clique em **Cancelar** para fechar todas as janelas.

Para obter a senha do usuário de associação, entre em contato com o administrador do AD.

Detalhes do DN base

O DN base é o DN da unidade organizacional (OU) ou do contêiner onde a pesquisa de detalhes do usuário e do usuário começa. Você pode usar o DN de uma OU criada no AD para o UCS ou o UCS Central. No entanto, você pode achar mais simples usar o DN para a própria raiz do domínio.

Este procedimento descreve como um administrador LDAP pode usar o ADSI Editor para localizar o DN base.

- 1. Abra o Editor ADSI.
- 2. Localize a OU ou o contêiner a ser usado como o DN base.
- 3. Clique com o botão direito do mouse na OU ou no contêiner e escolha Propriedades.

- 4. Na caixa de diálogo Propriedades, clique duas vezes em DistinguityName.
- 5. Copie o DN do campo de valor e anote quaisquer outros detalhes
 - necessários.

n AD51 Edit					_ 🗆 ×
S Elle Action Yiew Window Help					<u>_8×</u>
ADSI Edit	Vame		Class	Distinguished Name	
ADSI Edit Domain [ucs-dc01.bg/svucs.com] CN=bg/svucs.DC=com CN=Bultin CN=Computers CN=CON=CON=CON=CON CN=CON=CON=CON=CON=CON=CON=CON=CON=CON=C	Vame Provide String Provide String Pricede String	Value 19/10/2010 11:06 129320032315937 bglsvucs <not set=""> <not set=""> <no< td=""><td>Class There are no its ? X (18 PM /500</td><td>Distinguished Name ems to show in this view.</td><td></td></no<></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	Class There are no its ? X (18 PM /500	Distinguished Name ems to show in this view.	

6. Clique em **Cancelar** para fechar todas as janelas.

Detalhes do provedor

O provedor desempenha um papel importante na autenticação e autorização LDAP no UCS Central. O provedor é um dos servidores AD que o UCS Central consulta para pesquisar e autenticar o usuário e para obter detalhes do usuário, como informações de função. Certifique-se de coletar o nome do host ou o endereço IP do servidor do provedor AD.

Propriedade do filtro

O campo de filtro ou a propriedade é usada para pesquisar o banco de dados do AD. A ID de usuário inserida no login é passada de volta para o AD e comparada com o filtro.

Você pode usar sAMAccountName=\$userid como o valor do filtro. sAMAccountName é um atributo no AD e tem o mesmo valor que o ID de usuário do AD, que é usado para fazer login na GUI do 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
•		F
		003306366 •

Adicionar e configurar atributos

Esta seção resume as informações necessárias para adicionar o atributo CiscoAVPair (se necessário) e atualizar o atributo CiscoAVPair ou outro atributo predefinido antes de iniciar a configuração LDAP.

O campo do atributo especifica o atributo do AD (sob a propriedade do usuário), que retorna a função a ser atribuída ao usuário. Na versão 1.0a do software UCS Central, o atributo personalizado CiscoAVPair ou qualquer outro atributo não utilizado no AD pode ser desabilitado para passar essa função.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Adicionar atributo CiscoAVPair

Para adicionar um novo atributo ao domínio, expanda o esquema do domínio e adicione o atributo à classe (que, neste exemplo, é usuário).

Este procedimento descreve como expandir o esquema em um servidor do Windows AD e

adicionar o atributo CiscoAVPair.

- 1. Efetue login em um servidor AD.
- 2. Clique em **Iniciar > Executar**, digite **mmc** e pressione **Enter** para abrir um console vazio do Microsoft Management Console (MMC).
- 3. No MMC, clique em File > Add/Remove Snap-in > Add.
- 4. Na caixa de diálogo Adicionar Snap-in independente, selecione o **Esquema do Ative Diretory** e clique em

Console Root						
Console Root		Name				
1	Add/Remove Snap-in		? ×	There are no items to show in thi	s view.	
	Standalone Extensions	remove a stand-alone snap-in from the conso	le.			
	Snap-ins added to:	Console Root	Add Star	dalone Snap-in		? ×
			Available	standalone snap-ins:		
_	Description		Act Second	T Framework 1.1 Configuration ive Directory Domains and Trusts we Directory Schema We Directory Sites and Services ive Directory Users and Compu WeX Control 51 Edit horization Manager tificate Templates tificates	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	_
	Add	emove About	Descrip View ar	otion d edit the Active Directory Schem	a	

5. No MMC, expanda **Esquema do Ative Diretory**, clique com o botão direito do mouse em **Atributos** e escolha **Criar**

⊨ → € [
🚡 Console Roa	t\Active Directory Schema [ucs-dc01.bglsvucs.com]\A
🚞 Console Rool	:	Name
Active Di Class	rectory Schema [ucs-dc01.bglsvu ies	 accountExpires accountNameHistory aCSAggregateTokenRa
	Create Attribute	aCSAllocableRSVPBand
	New •	aCSCacheTimeout
	View	aCSDirection
	New Window from Here	aCSDSBMDeadTime
	New <u>T</u> askpad View	 aCSDSBMPriority aCSDSBMRefresh
	Refresh Export List	aCSEnableACSService aCSEnableRSVPAccoun
		 aCSEnableRSVPMessag aCSEventLogLevel
		aCSIdentityName
		aCSMaxAggregatePeak
		aCSMaxDurationPerFlow

atributo.

caixa de diálogo Criar novo atributo é exibida

6. Crie um atributo chamado CiscoAVPair no serviço de autenticação remota.Nos campos Nome comum e Nome de exibição LDAP, insira CiscoAVPair.No campo ID de objeto exclusivo 500, insira 1.3.6.1.4.1.9.287247.1.No campo Descrição, insira a função e a localização do UCS.No campo Sintaxe, selecione Sequência de caracteres Unicode na lista

Identification	
Common <u>N</u> ame:	CiscoAVPair
LDAP Display Name:	CiscoAVPair
Unique ×500 <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
Mjnimum:	
Ma <u>x</u> imum:	

OK para salvar o atributo e fechar a caixa de diálogo.Depois que o atributo é adicionado ao esquema, ele deve ser mapeado ou incluído na classe de usuário. Isso permite editar a propriedade do usuário e especificar o valor da função a ser passada.

- 7. No mesmo MMC usado para a expansão do esquema do AD, expanda **Classes**, clique com o botão direito do mouse em **usuário** e escolha **Propriedades**.
- 8. Na caixa de diálogo Propriedades do usuário, clique na guia **Atributos** e clique em **Adicionar**.

🛗 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. Na caixa de diálogo Selecionar objeto de esquema, clique em CiscoAVPair e clique em

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

- 10. Na caixa de diálogo Propriedades do usuário, clique em Aplicar.
- 11. Clique com o botão direito do mouse em **Esquema do Ative Diretory** e escolha **Recarregar o Esquema** para incluir as novas



12. Se necessário, use o Editor ADSI para atualizar o esquema. Clique com o botão direito do mouse em Localhost e escolha Atualizar esquema

	- Parana araan 10	in al ois
🍕 File Action N	view Window Help	P .
🗢 🔶 🗈 💽		
I ADAM ADSI Edit		Nam
E- DC=ucs	Settings Remove	10-
🗄 🧰 CN=	Update Schema Nov	N
⊕ 🛄 CN= OU=	New	÷
	View New Window from H	Here 🕨
	Rename Refresh	
	Export List	
	Help	

Atualizar atributo CiscoAVPair

Este procedimento descreve como atualizar o atributo CiscoAVPair. A sintaxe é shell:role="<role>".

1. Na caixa de diálogo Editar ADSI, localize o usuário que precisa acessar o UCS Central.

- 2. Clique com o botão direito do mouse no usuário e escolha Propriedades.
- 3. Na caixa de diálogo Propriedades, clique na guia **Editor de atributos**, clique em **CiscoAVPair** e clique em **Editar**.
- 4. Na caixa de diálogo Editor de string multivalorizado, digite o valor **shell:role="admin"** no campo Valores e clique em

OK.			
🍕 ADSI Edit			
Sele Action View Window Help A → A T T Y ™ A P A	19		
		[chara	Distinguished A
		There are no) items to show in th
⊡			
CN=testuser Properties CN=testuser Properties CON=testuser Properties CON=testuser Properties CON=testuser Properties CON=testuser Properties	s /	? X	
 Brind C Brind C Brind C Brind C C F Show optional attributes: Brind C C C C Show only attributes: 	tributes outes s that have <u>v</u> alues		
Image: Construction Image: Construction Image: Construction Image: Construction	Multi-valued String Editor Attribute: CiscoAVPair Value to add: Values: shell:roles="admin"		Add <u>R</u> emove
		OK	Cancel

5. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo Propriedades.

Atualizar atributo predefinido

Este procedimento descreve como atualizar um atributo predefinido, em que a função é uma das funções de usuário predefinidas no UCS Central. Este exemplo usa o atributo *company* para

passar a função. A sintaxe é shell:role="<role>".

- 1. Na caixa de diálogo Editar ADSI, localize o usuário que precisa acessar o UCS Central.
- 2. Clique com o botão direito do mouse no usuário e escolha Propriedades.
- 3. Na caixa de diálogo Propriedades, clique na guia **Editor de atributos**, clique em **empresa** e clique em **Editar**.
- 4. Na caixa de diálogo Editor de atributos de cadeia de caracteres, digite o valor **shell:role="admin"** no campo Valor e clique em

ADSI Edit			
, Eile Action View Window Help			
· → 🗈 🖬 🗙 😭 🐼 😫	P		
DU=UCSGroup106	Name	Class	Distinguished Name
 OU=UCSUSERS CN=Users CN=Administrator CN=avshukla CN=avshukla CN=testuser Propertie CN=testuser Properties CN=testuser Properties<	es ity attributes ributes ributes String Attribute Editor Attribute: company Yalue: shell:roles="admin" Clear Unicode String testuser Unicode String (Not Se Integer 0 UTC Coded Ti 30/01/2	There are no ? × ? × 01 01 02 012 8:27:04 AM	c items to show in this view.

5. Clique em OK para salvar as alterações e fechar a caixa de diálogo Propriedades.

Configurar a autenticação LDAP no UCS Central

A configuração LDAP no UCS Central é concluída em Gerenciamento de operações.

- 1. Faça login no UCS Central em uma conta local.
- Clique em Operations Management, expanda Domain Groups e clique em Operational Policies > Security.

Equipment Servers Network Storage	Operations Management	Administration	8 10	1	8	A 17				
	Convin Groups	⁶ <u>Consin Group root</u> ▶ S	RADIUS		1 TAC	ACS+ 😁 L	DAP			
Software Management S	DNS Bemate Access SNMP Debue Cell Home Security Security Security Security Security Security Security	Authentication Name Authentication P Authentication P Outroated Points Bounds Bactures DaP B BACTURS D TACACS+			Time Time Time	out: 30, Attibute: out: 5, Retries: 1 out: 5	member0(, Filte	r. sAMArcount	Propertie:	s.

3. Para configurar a autenticação LDAP, faça o seguinte: <u>Configure o provedor LDAP.Configure</u> <u>o grupo do provedor LDAP</u> (não disponível na versão 1.0a).<u>Alterar a regra de autenticação</u> <u>nativa.</u>

Configurar provedor LDAP

1. Clique em LDAP, clique com o botão direito em Providers e escolha Create LDAP Provider.

🟥 Domain Groups 🕨 🚊	Domain Group root 🕨	
Operational Policie	S	
🗿 <u>Time Zone</u>	🕆 Authentication 🛛 🕆 RADIUS	🕆 TACACS+ 🕆 LDAI
🔗 Remote Access	Name	
	Authentication Prusted Points	
👁 <u>Debuq</u>	▶ 繼 User Services	
🛞 <u>Call Home</u>	 LDAP Group Maps 	Timeout: 30, Attibute: mer
Security	🕨 🚔 Provider Groups	
音音 <u>Equipment</u> ⑤ <u>Identifier</u>	 Providers RADIUS TACACS+ 	ider pout: 5, Retries: 1 Timeout: 5

 Na caixa de diálogo Criar provedor LDAP, adicione esses detalhes, que foram obtidos anteriormente.Nome de host ou IP do provedorVincular DNDN baseFiltrarAtributo (CiscoAVPair ou um atributo predefinido como empresaSenha (senha do usuário usada no DN de

reate LDAP Pr	rovider		
eral Properties Hostname (or IP Address): Order:	10.10.10.10 lowest-available	LDAP Group Rules Group Authorization: Group Recursion:	disable 💌 non-recursive 💌
Bind DN: Base DN: Port:	CN=Administrator,CN=Users,DC= DC=bglsvucs,DC=com	Target Attribute:	memberOf
Enable SSL: Filter: Attribute:	sAMAccountName=\$userid		
Password: Confirm Password: Timeout:	30		

3. Clique em OK para salvar a configuração e fechar a caixa de diálogo.

Observação: nenhum outro valor precisa ser modificado nesta tela. As regras do grupo LDAP não são suportadas para a autenticação UCS Central nesta versão.

Configurar grupo de provedores LDAP

Observação: na versão 1.0a, os grupos de provedores não são suportados. Este procedimento descreve como configurar um grupo de provedores fictícios para usar na configuração posteriormente.

1. Clique em LDAP, clique com o botão direito em Grupo de provedores e escolha Criar grupo de provedores

DAP.	
LDAP	Timeout: 30, Attibute: memberOf, Filter: sAMAccountName=\$userid
🕨 🇰 Group Maps	
🔻 🔓 Provider Groups	
🔒 Idap-dc	E Create LDAP Provider Group
🔻 🔒 Providers	

- 2. Na caixa de diálogo Criar grupo de provedores LDAP, digite o nome do grupo no campo Nome.
- Na lista de provedores disponíveis à esquerda, selecione o provedor e clique no símbolo maior que (>) para mover esse provedor para os provedores atribuídos à direita.

🚔 Create LDAP Provider Group	□ ×
Create LDAP Provider Group	0
Properties Name:	
Providers Available Providers Records: 1 Showing: 0	Assigned Providers Assigned Providers Records: 1 Showing: 1 10.76.78.66
	OK Cancel

4. Clique em **OK** para salvar as alterações e fechar a tela.

Alterar regra de autenticação nativa

A versão 1.0a não suporta vários domínios de autenticação como no UCS Manager. Para contornar isso, é necessário modificar a regra de autenticação nativa.

A autenticação nativa tem a opção de modificar a autenticação para logins padrão ou logins de console. Como vários domínios não são suportados, você pode usar a conta local ou uma conta LDAP, mas não ambos. Altere o valor do território para usar local ou LDAP como origem de autenticação.

- 1. Clique em Authentication, clique com o botão direito do mouse em Native Authentication e escolha Properties.
- 2. Determine se você deseja a autenticação padrão, a autenticação do console ou ambos. Use a autenticação padrão para a GUI e a interface de linha de comando (CLI). Use a autenticação de console para a exibição de máquina virtual (KVM) baseada em kernel.
- Escolha Idap na lista suspensa Território. O valor do território determina se local ou LDAP é a origem da autenticação.

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

- 4. Clique em **OK** para fechar a página.
- 5. Na página Políticas, clique em **Salvar** se necessário para salvar as alterações.

Observação: não faça logoff da sessão atual ou modifique a autenticação do console até verificar se a autenticação LDAP funciona corretamente. A autenticação do console fornece uma forma de reverter para a configuração anterior. Consulte a seção <u>Verificar</u>.

Verificar

Este procedimento descreve como testar a autenticação LDAP.

1. Abra uma nova sessão no UCS Central e insira o nome de usuário e a senha. Você não precisa incluir um domínio ou caractere antes do nome de usuário. Este exemplo usa testucs como o usuário do domínio.



 A autenticação LDAP é bem-sucedida se você vir o painel do UCS Central. O usuário é exibido na parte inferior da página.

cisco UCS Central		005131113			Pro	iterences LogOut Al
Equipment i Servers i Network i Storage i O	perations Management Administration					
Compare Import Backup and Import Backup and Import Demain Groups set Backup Export Policy G Firmwire Wasigement S Maintenance G Operational Policies G Operational Policies G Schedules	Library of Images	Namo	Version	Source	State	Туре
User: destucs)						System Time: 2013

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

<u>Suporte Técnico e Documentação - Cisco Systems</u>