Exemple de configuration de l'authentification LDAP pour UCS Central

Contenu

Introduction Conditions préalables **Conditions requises Components Used Conventions Collecte d'informations** Détails de l'utilisateur lié Détails du DN de base Détails du fournisseur Filter, propriété Ajouter et configurer des attributs Ajouter un attribut CiscoAVPair Mettre à jour l'attribut CiscoAVPair Mettre à jour l'attribut prédéfini Configurer l'authentification LDAP sur UCS Central Configurer le fournisseur LDAP Configurer le groupe de fournisseurs LDAP Modifier la règle d'authentification native Vérification Dépannage Informations connexes

Introduction

Ce document fournit un exemple de configuration pour l'authentification LDAP (Lightweight Directory Access Protocol) pour Cisco Unified Computing System (UCS) Central. Les procédures utilisent l'interface utilisateur graphique (GUI) d'UCS Central, un exemple de domaine de bglucs.com et un exemple de nom d'utilisateur de testuser.

Dans la version 1.0 du logiciel UCS Central, LDAP est le seul protocole d'authentification à distance pris en charge. La version 1.0 ne prend en charge que très peu l'authentification à distance et la configuration LDAP pour UCS Central lui-même. Cependant, vous pouvez utiliser UCS Central afin de configurer toutes les options pour les domaines UCS Manager gérés par UCS Central.

Les limites de l'authentification distante UCS Central sont les suivantes :

- RADIUS et TACACS ne sont pas pris en charge.
- Le mappage d'appartenance de groupe LDAP pour l'attribution de rôle et les groupes de fournisseurs LDAP pour plusieurs contrôleurs de domaine ne sont pas pris en charge.
- LDAP utilise uniquement l'attribut CiscoAVPair ou tout attribut inutilisé afin de transmettre le rôle. Le rôle passé est l'un des rôles prédéfinis dans la base de données locale d'UCS Central.
- Plusieurs domaines/protocoles d'authentification ne sont pas pris en charge.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- UCS Central est déployé.
- Microsoft Active Directory est déployé.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- UCS Central version 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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Collecte d'informations

Cette section récapitule les informations à collecter avant de commencer la configuration.

Remarque : utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Détails de l'utilisateur lié

L'utilisateur de liaison peut être n'importe quel utilisateur LDAP du domaine qui a un accès en lecture au domaine ; un utilisateur de liaison est requis pour la configuration LDAP. UCS Central utilise le nom d'utilisateur et le mot de passe de l'utilisateur de liaison afin de se connecter et d'interroger Active Directory (AD) pour l'authentification des utilisateurs, etc. Cet exemple utilise le compte Administrateur comme utilisateur de liaison.

Cette procédure décrit comment un administrateur LDAP peut utiliser l'Éditeur ADSI (Active Directory Service Interfaces) afin de trouver le DN.

- 1. Ouvrez ADSI Editor.
- 2. Rechercher l'utilisateur de liaison. L'utilisateur se trouve dans le même chemin que dans l'AD.
- 3. Cliquez avec le bouton droit de la souris sur l'utilisateur, puis sélectionnez Propriétés.
- 4. Dans la boîte de dialogue Propriétés, double-cliquez sur nomunique.
- 5. Copiez le DN à partir du champ

6. Cliquez sur **Annuler** afin de fermer toutes les fenêtres.

Pour obtenir le mot de passe de l'utilisateur de liaison, contactez l'administrateur AD.

Détails du DN de base

Le DN de base est le DN de l'unité d'organisation (OU) ou le conteneur où commence la recherche des détails utilisateur et utilisateur. Vous pouvez utiliser le DN d'une unité d'organisation créée dans la AD pour UCS ou UCS Central. Cependant, vous pouvez trouver plus simple d'utiliser le DN pour la racine du domaine lui-même.

Cette procédure décrit comment un administrateur LDAP peut utiliser l'Éditeur ADSI afin de trouver le DN de base.

- 1. Ouvrez ADSI Editor.
- 2. Recherchez l'unité d'organisation ou le conteneur à utiliser comme DN de base.
- 3. Cliquez avec le bouton droit sur l'unité d'organisation ou le conteneur, puis sélectionnez **Propriétés**.
- 4. Dans la boîte de dialogue Propriétés, double-cliquez sur nomunique.
- 5. Copiez le DN dans le champ de valeur et notez tous les autres détails dont vous avez



6. Cliquez sur Annuler afin de fermer toutes les fenêtres.

Détails du fournisseur

Le fournisseur joue un rôle clé dans l'authentification et l'autorisation LDAP dans UCS Central. Le fournisseur est l'un des serveurs AD que UCS Central interroge afin de rechercher et d'authentifier l'utilisateur et afin d'obtenir des détails utilisateur tels que des informations de rôle. Veillez à collecter le nom d'hôte ou l'adresse IP du serveur AD du fournisseur.

Filter, propriété

Le champ ou la propriété de filtre est utilisé afin de rechercher la base de données AD. L'ID utilisateur saisi lors de la connexion est renvoyé à l'AD et comparé au filtre.

Vous pouvez utiliser sAMAccountName=\$userid comme valeur de filtre. sAMAccountName est un attribut dans la AD et a la même valeur que l'ID utilisateur AD, qui est utilisé pour se connecter à l'interface utilisateur graphique d'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 •

Ajouter et configurer des attributs

Cette section résume les informations dont vous avez besoin pour ajouter l'attribut CiscoAVPair (si nécessaire) et mettre à jour l'attribut CiscoAVPair ou un autre attribut prédéfini avant de démarrer la configuration LDAP.

Le champ d'attribut spécifie l'attribut AD (sous la propriété utilisateur), qui renvoie le rôle à attribuer à l'utilisateur. Dans la version 1.0a du logiciel UCS Central, l'attribut personnalisé CiscoAVPair ou tout autre attribut inutilisé dans la AD peut être unifié afin de passer ce rôle.

Remarque : utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Ajouter un attribut CiscoAVPair

Afin d'ajouter un nouvel attribut au domaine, développez le schéma du domaine et ajoutez l'attribut à la classe (qui, dans cet exemple, est utilisateur).

Cette procédure décrit comment développer le schéma sur un serveur Windows AD et ajouter l'attribut CiscoAVPair.

- 1. Connectez-vous à un serveur AD.
- 2. Cliquez sur **Démarrer > Exécuter**, tapez **mmc** et appuyez sur **Entrée** pour ouvrir une console Microsoft Management Console (MMC) vide.
- 3. Dans MMC, cliquez sur Fichier > Ajouter/Supprimer un composant logiciel enfichable > Ajouter.
- 4. Dans la boîte de dialogue Ajouter un composant logiciel enfichable autonome, sélectionnez le **schéma Active Directory**, puis cliquez sur **Ajouter**.

0	dd/Remove Snap-in	r	? ×	There are no items to show in th	is view.	
	Standalone Extensions	move a stand-alone snap-in from	the console.			
	Snap-ins added to:	Console Root	Add Sta	ndalone Snap-in		?
			Availab	le standalone snap-ins:		
			Snap	'n	Vendor	
			日本 (1) (1) (1) (1) (1) (1) (1) (1)	ET Framework 1.1 Configuration trive Directory Schema trive Directory Schema trive Directory Sites and Services trive Directory Users and Compu triveX Control 251 Edit Educization Manager	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
	Description			ertificate Templates ertificates	Microsoft Corporation Microsoft Corporation	•
	Add	we Absut	View -	iption and edit the Active Directory Schem	9	
		OK	Ca			

5. Dans MMC, développez Schéma Active Directory, cliquez avec le bouton droit sur Attributs, puis choisissez Créer un

= ⇒ 🔁 💷	Active Directory Schema I	ucs-dc01 balsvucs com]\0
Console Root	ectory Schema [ucs-dc01.bglsvu s Create Attribute <u>New</u> <u>View</u> New <u>W</u> indow from Here New <u>Taskpad View</u> Refresh Export List <u>H</u> elp	Name accountExpires accountNameHistory aCSAggregateTokenRa aCSAllocableRSVPBand aCSCacheTimeout aCSDirection aCSDSBMDeadTime aCSDSBMPriority aCSDSBMRefresh aCSEnableACSService aCSEnableRSVPAccoun aCSEnableRSVPMessag aCSEventLogLevel aCSMaxAggregatePeak aCSMaxDurationPerFlow

attribut.

boîte de dialogue Créer un attribut s'affiche.

6. Créez un attribut appelé CiscoAVPair dans le service d'authentification à distance.Dans les champs Common Name et LDAP Display Name, saisissez CiscoAVPair.Dans le champ Unique 500 Object ID, saisissez 1.3.6.1.4.1.9.287247.1.Dans le champ Description, saisissez le rôle et les paramètres régionaux UCS.Dans le champ Syntaxe, sélectionnez Chaîne Unicode dans la liste

Identification	N
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
Mjnimum:	
Maximum:	

déroulante.

sur **OK** pour enregistrer l'attribut et fermer la boîte de dialogue.Une fois l'attribut ajouté au schéma, il doit être mappé ou inclus dans la classe utilisateur. Cela vous permet de modifier la propriété utilisateur et de spécifier la valeur du rôle à passer.

- 7. Dans le MMC utilisé pour l'extension du schéma AD, développez **Classes**, cliquez avec le bouton droit sur **utilisateur**, puis choisissez **Propriétés**.
- 8. Dans la boîte de dialogue Propriétés de l'utilisateur, cliquez sur l'onglet **Attributs**, puis sur **Ajouter**.

🚡 Console1			
Eile Action View Favorites Window	Help		
The Console Root\Active Directory Schem	a [ucs-dc01.bglsvucs.com]\	Classes	
Classes Classe	Name ServiceConnectionPoint ServiceInstance ShadowAccount SimpleSecurityObject Site Site SiteUnk SiteUnkBridge SiteContainer	General Relationship Attributes Default Sec	? X
	subsection can be subset subnet subschema subSchema stop trustedDomain stypeLibrary suser syolume	Delional: accountExpires aCSPolicyName adminCount audio badPasswordTime badPwdCount businessCateconu	Add
		CiscoAVPair	 Cancel

9. Dans la boîte de dialogue Sélectionner un objet de schéma, cliquez sur CiscoAVPair, puis

<u>S</u> elect a schema object:	
builtinModifiedCount	ОК
bytesPerMinute	Cancel
cACertificate cACertificateDN	
cAConnect	
canUpgradeScript	
carLicense catalogs	
categories categoruld	
cAUsages	
certificateAuthorityObject	
certificateRevocationList	
CiscoAVPair	
classDisplayName	

10. Dans la boîte de dialogue Propriétés de l'utilisateur, cliquez sur Appliquer.

11. Cliquez avec le bouton droit sur **Schéma Active Directory**, puis sélectionnez **Recharger le schéma** afin d'inclure les nouvelles



12. Si nécessaire, utilisez ADSI Editor pour mettre à jour le schéma. Cliquez avec le bouton droit sur **Localhost**, puis sélectionnez **Mettre à jour le schéma**

🤣 ADAM-adsiedi	it - [ADAM ADSI Ed	lit\Loca
🤣 File Action	View Window Hel	lp 🛛
⇐ ⇒ 🗈 💽	1 🗟 😫	
🦂 ADAM ADSI Edit		Name
⊡ <mark>] Localhost [lo</mark> ⊡ ⊡ DC=ucs ⊕ ⊡ CN=	Settings Remove	<u>l</u> @
🗄 🧰 CN=	Update Schema No	W
⊕ 🛄 CN=	New	8 .
	View New Window from I	► Here
	Rename	
	Refresh	
	Export List	
	Helo	

Mettre à jour l'attribut CiscoAVPair

Cette procédure décrit comment mettre à jour l'attribut CiscoAVPair. La syntaxe est shell : rôles="<rôle>".

1. Dans la boîte de dialogue Modifier ADSI, recherchez l'utilisateur qui a besoin d'accéder à

UCS Central.

- 2. Cliquez avec le bouton droit de la souris sur l'utilisateur, puis sélectionnez Propriétés.
- 3. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **Éditeur d'attributs**, cliquez sur **CiscoAVPair**, puis sur **Modifier**.
- 4. Dans la boîte de dialogue Éditeur de chaînes à valeurs multiples, entrez la valeur shell : rôles=« admin » dans le champ Valeurs et cliquez sur

OK.				
🖏 ADSI Edit				
🥪 Eile Action View Window Help				
← → 🗈 🖪 🗙 😭 🗟 ।	3 🖬			
OU=UC5Group106		Name	Class	Distinguished N
Image: Construction of the second	stries curity ory attribute ibutes the y	utes es hat have yalues ulti-valued String Editor Attribute: CiscoAVPair Yalue to add: Values: shell:roles=''admin''	There are no il	Distinguished N tems to show in th
			ОК	Cancel

5. Cliquez sur **OK** pour enregistrer les modifications et fermer la boîte de dialogue Propriétés.

Mettre à jour l'attribut prédéfini

Cette procédure décrit comment mettre à jour un attribut prédéfini, où le rôle est l'un des rôles

utilisateur prédéfinis dans UCS Central. Cet exemple utilise l'attribut *company* afin de passer le rôle. La syntaxe est shell : rôles="<rôle>".

- 1. Dans la boîte de dialogue Modifier ADSI, recherchez l'utilisateur qui a besoin d'accéder à UCS Central.
- 2. Cliquez avec le bouton droit de la souris sur l'utilisateur, puis sélectionnez Propriétés.
- 3. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **Éditeur d'attributs**, cliquez sur **société**, puis sur **Modifier**.
- 4. Dans la boîte de dialogue Éditeur d'attributs de chaîne, entrez la valeur shell : rôles=« admin » dans le champ Valeur, puis cliquez sur





5. Cliquez sur OK pour enregistrer les modifications et fermer la boîte de dialogue Propriétés.

Configurer l'authentification LDAP sur UCS Central

La configuration LDAP dans UCS Central est terminée sous Gestion des opérations.

- 1. Connectez-vous à UCS Central sous un compte local.
- 2. Cliquez sur Gestion des opérations, développez Groupes de domaines, puis cliquez sur

Stratégies opérationnelles >

Sécurité.

Equipment Servers Network Storage	Operations Management	Administration	⊘ ' 10	1	8	17
	<mark>≇ torrein Groups</mark> ▶ # Operational Policie ∰ <u>Time Zone</u>	[®] <u>Constn Group rost</u> → S 1 Authentication 1 1	RADIUS	1 6	Y TACA	ics+ 🕴 🛅 LDAP
Backgrephone Points Software Management Software Management Software Management Software Management Software Management		A Filter (off) Name Authentication P A Authentication P Trusted Points B User Services LOAP B ADUS B ADUS B ACCS+			Timeo	Properties nut: 30, Attibute: memberO(, Filter: sAMAccountName=\$userid nut: 5, Robries: 1 nut: 5
	Security Security Security Security Security Security Security	P III INCINOT			Timeo	ur ə

 Afin de configurer l'authentification LDAP, procédez comme suit :<u>Configurez le fournisseur</u> <u>LDAP.Configurez le groupe de fournisseurs LDAP</u> (non disponible dans la version 1.0a).<u>Modifiez la règle d'authentification native.</u>

Configurer le fournisseur LDAP

1. Cliquez sur LDAP, cliquez avec le bouton droit sur Fournisseurs, puis choisissez Créer un fournisseur

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

2. Dans la boîte de dialogue Créer un fournisseur LDAP, ajoutez ces détails, qui ont été

recueillis précédemment.Nom d'hôte ou adresse IP du fournisseurDN de liaisonDN de baseFiltreAttribut (CiscoAVPair ou attribut prédéfini tel que company)Mot de passe (mot de passe de l'utilisateur utilisé dans le DN de

reate LDAP PI	rovider			
eral				
roperties		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			

3. Cliquez sur **OK** pour enregistrer la configuration et fermer la boîte de dialogue.

Remarque : aucune autre valeur ne doit être modifiée dans cet écran. Les règles de groupe LDAP ne sont pas prises en charge pour l'authentification UCS Central dans cette version.

Configurer le groupe de fournisseurs LDAP

Remarque : Dans la version 1.0a, les groupes de fournisseurs ne sont pas pris en charge. Cette procédure décrit comment configurer un groupe de fournisseurs fictifs à utiliser ultérieurement dans la configuration.

1. Cliquez sur LDAP, cliquez avec le bouton droit sur Groupe de fournisseurs, puis choisissez Créer un groupe de fournisseurs

LDAP.	
User Services	
LDAP Groun Mans	Timeout: 30, Attibute: memberot, Fliter: sAMAccountivame=\$userid
Provider Groups	
🔒 Idap-dc	Create LDAP Provider Group
🔻 🔒 Providers	

- 2. Dans la boîte de dialogue Créer un groupe de fournisseurs LDAP, saisissez le nom du groupe dans le champ Nom.
- Dans la liste des fournisseurs disponibles à gauche, sélectionnez le fournisseur et cliquez sur le symbole supérieur à (>) afin de déplacer ce fournisseur vers les fournisseurs affectés

à

Create LDAP Provider Group								
Create LDAP Provider Group								
neral								
Name: Jdap-dc								
Providers - Available Providers - Records: 1 Showing 0	ſ	Assigned Prov	iders T	*	+	+	Records:	1 Showing
	>>	10.76.78.66		-		-		
	>							
	<							
	< «							

4. Cliquez sur OK pour enregistrer les modifications et fermer l'écran.

Modifier la règle d'authentification native

La version 1.0a ne prend pas en charge plusieurs domaines d'authentification comme dans UCS Manager. Pour contourner ce problème, vous devez modifier la règle d'authentification native.

L'authentification native a la possibilité de modifier l'authentification pour les connexions par défaut ou les connexions de console. Comme plusieurs domaines ne sont pas pris en charge, vous pouvez utiliser le compte local ou un compte LDAP, mais pas les deux. Modifiez la valeur de Realm afin d'utiliser local ou LDAP comme source d'authentification.

- 1. Cliquez sur **Authentification**, cliquez avec le bouton droit sur **Authentification native**, puis sélectionnez **Propriétés**.
- Déterminez si vous souhaitez l'authentification par défaut, l'authentification de la console ou les deux. Utilisez l'authentification par défaut pour l'interface utilisateur graphique et l'interface de ligne de commande (CLI). Utilisez l'authentification de console pour la vue KVM (Virtual Machine) basée sur le noyau de la machine virtuelle.
- Choisissez Idap dans la liste déroulante Domaine. La valeur de domaine détermine si local ou LDAP est la source de l'authentification.

🏯 Properties			⊐ ×
Properties (Native	Authentication)		0
General Events			
- Default Authentication:			
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. Cliquez sur **OK** pour fermer la page.
- 5. Sur la page Stratégies, cliquez sur **Enregistrer** si nécessaire afin d'enregistrer les modifications.

Remarque : Ne vous déconnectez pas de votre session actuelle ou ne modifiez pas l'authentification de la console tant que vous n'avez pas vérifié que l'authentification LDAP fonctionne correctement. L'authentification par console permet de revenir à la configuration précédente. Reportez-vous à la section <u>Vérifier</u>.

Vérification

Cette procédure décrit comment tester l'authentification LDAP.

 Ouvrez une nouvelle session dans UCS Central, puis saisissez le nom d'utilisateur et le mot de passe. Vous n'avez pas besoin d'inclure un domaine ou un caractère avant le nom d'utilisateur. Cet exemple utilise des testucs comme utilisateur à partir du domaine.

cisco	UCS Central	Usemame:	testucs
		Passwort	********
			Log In

 L'authentification LDAP réussit si vous voyez le tableau de bord UCS Central. L'utilisateur s'affiche en bas de la page.

allulu LICS Control						Preterences Log Out A	
		10 1 8	17				
Equipment I Servers I Network I Storage I Op	erations Management			_			
Commin Groups Demain Groups Backup and Import Backup and Import Backup/Export Policy Soft Proving Management Soft Proving Management Soft Policy Soft Pol	Ubrary of Images	Name		Version	Source	State	Тура
User (testucs)							System Time: 2013

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

Support et documentation techniques - Cisco Systems