UCS Central的LDAP身份驗證配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 收集資訊 繫結使用者詳細資訊 基礎DN詳細資訊 提供商詳細資訊 篩選器屬性 新增和配置屬性 新增CiscoAVPair屬性 更新CiscoAVPair屬性 更新預定義屬性 在UCS Central上配置LDAP身份驗證 配置LDAP提供程式 配置LDAP提供程式組 更改本機身份驗證規則 驗證 疑難排解 相關資訊

<u> 簡介</u>

本文檔提供適用於思科統一計算系統(UCS)中心的輕量級目錄訪問協定(LDAP)身份驗證的示例配置 。這些過程使用UCS Central圖形使用者介面(GUI)、bglucs.com的示例域和testuser的示例使用者 名稱。

在UCS Central軟體的1.0版中,LDAP是唯一受支援的遠端身份驗證協定。1.0版對UCS中心本身的 遠端身份驗證和LDAP配置的支援非常有限。但是,您可以使用UCS Central為UCS Central管理的 UCS Manager域配置所有選項。

UCS Central遠端身份驗證的限制包括:

- 不支援RADIUS和TACACS。
- 不支援角色分配的LDAP組成員對映和多域控制器的LDAP提供程式組。
- LDAP僅使用CiscoAVPair屬性或任何未使用的屬性來傳遞角色。傳遞的角色是UCS中心本地資 料庫中的預定義角色之一。
- 不支援多個身份驗證域/協定。



<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 部署了UCS Central。
- 已部署Microsoft Active Directory。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- UCS Central版本1.0
- Microsoft Active Directory

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>收集資訊</u>

本節彙總了在開始配置之前需要收集的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

<u> 繁結使用者詳細資訊</u>

繫結使用者可以是域中對該域具有讀取訪問許可權的任何LDAP使用者;LDAP配置需要繫結使用者 。UCS Central使用繫結使用者的使用者名稱和密碼來連線和查詢Active Directory(AD)以進行使用 者身份驗證等。此示例使用Administrator帳戶作為繫結使用者。

此過程描述LDAP管理員如何使用Active Directory服務介面(ADSI)編輯器查詢DN。

- 1. 開啟ADSI編輯器。
- 2. 查詢繫結使用者。使用者與AD中的使用者處於同一路徑。
- 3. 按一下右鍵使用者,然後選擇屬性。
- 4. 在「屬性」對話方塊中,按兩下distinguishedName。
- 5. 從值欄位中複製DN。



6. 按一下「Cancel」以關閉所有視窗。

要獲取繫結使用者的密碼,請與AD管理員聯絡。

基礎DN詳細資訊

基本DN是組織單位(OU)的DN或搜尋使用者和使用者詳細資訊的容器。您可以將在AD中建立的 OU的DN用於UCS或UCS Central。但是,您可能會發現對域根本身使用DN更簡單。

此過程描述LDAP管理員如何使用ADSI編輯器查詢基本DN。

- 1. 開啟ADSI編輯器。
- 2. 查詢要用作基本DN的OU或容器。
- 3. 按一下右鍵OU或容器,然後選擇**屬性**。
- 4. 在「屬性」對話方塊中,按兩下distinguishedName。
- 5. 從值欄位中複製DN,並記下所需的任何其他詳細資訊。



6. 按一下「Cancel」以關閉所有視窗。

提供商詳細資訊

在UCS中心的LDAP身份驗證和授權中,提供程式扮演著關鍵角色。提供程式是UCS中心查詢的 AD伺服器之一,用於搜尋和驗證使用者以及獲取使用者詳細資訊(如角色資訊)。請務必收集提供 商AD伺服器的主機名或IP地址。

<u>篩選器屬性</u>

過濾器欄位或屬性用於搜尋AD資料庫。在登入時輸入的使用者ID將傳回AD並與過濾器進行比較。

您可以使用sAMAccountName=\$userid作為篩選器值。sAMAccountName是AD中的一個屬性,其 值與AD使用者ID相同,ID用於登入到UCS Central GUI。

Show optional attribut	ies .	
Show only attributes t attri <u>b</u> utes:	hat have <u>v</u> alues	
Attribute	Syntax	Value 🔺
proxyAddresses pwdLastSet queryPolicyBL registeredAddress repIPropertyMetaData repIUpToDateVector repsFrom repsTo revision rid	Unicode String Large Integer/ Distinguished Octet String Octet String Octet String Octet String Octet String Integer Integer	<not set=""> 129723865322977500 <not set=""> Ox01 0x00 0x00 0x00 0x00 <not set=""> <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not>
sAMAccountName	Unicode String	testuser
sAMAccountTvbe ◀┃	Integer	805306368

<u>新增和配置屬性</u>

本節彙總了在啟動LDAP配置之前新增CiscoAVPair屬性(如果需要)並更新CiscoAVPair屬性或其 他預定義屬性所需的資訊。

屬性欄位指定AD屬性(在使用者屬性下),該屬性將回傳要分配給使用者的角色。在UCS Central軟體的1.0a版本中,可以統一自定義屬性CiscoAVPair或AD中任何其他未使用的屬性,以便 傳遞此角色。

註:使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

新增CiscoAVPair屬性

若要向域新增新屬性,請展開域的架構,並將屬性新增到類(在本例中為user)。

此過程介紹如何在Windows AD伺服器上展開架構並新增CiscoAVPair屬性。

1. 登入到AD伺服器。

2. 按一下Start > Run, 鍵入mmc, 然後按Enter開啟空的Microsoft管理控制檯(MMC)控制檯。

- 3. 在MMC中,按一下File > Add/Remove Snap-in > Add。
- 4. 在「新增獨立管理單元」對話方塊中,選擇Active Directory架構,然後按一下新增。

Console Root		Name				
1	Add/Remove Snap-in		? ×	There are no items to show in th	is view.	
	Standalone Extensions Use this page to add or res	nove a stand-alone snap-in from	the console.			
	Snap-ins added to:	onsole Root	Add Star	idalone Snap-in		? ×
			Available	a standalone snap-ins:		
			Snap-ir	1	Vendor	*
_	Description		Act Act Act Act Act Act Act Cer Cer	T Framework 1.1 Configuration ive Directory Domains and Trusts ive Directory Schema ive Directory Sites and Services ive Directory Users and Compu iveX 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	ve Absut	Descrip View ar	otion nd edit the Active Directory Schem	9	
		ОК	Ca	[Addlos	ie l

5. 在MMC中,展開Active Directory架構,按一下右鍵屬性,然後選擇建立屬性。

🚡 Console1				
Eile Action View	w Fav <u>o</u> rites <u>W</u> indow <u>H</u> el	þ		
🚡 Console Root	Active Directory Schema [ucs-dc01.bglsvucs.com]\Att		
🦲 Console Root		Name		
Active Dire	ctory Schema [ucs-dc01.bglsvu 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		
	Refresh Export List	 aCSEnableACSService aCSEnableRSVPAccoun aCSEnableRSVPMessag 		
	Help	aCSEventLogLevel		
		 aCSIdentityName aCSMaxAggregatePeak aCSMaxDurationPerFlow aCSMaximumSDUSize 		
Create a New Attrib	ute Object		<u></u> 挖出珇	「建

新屬性」對話方塊

 6. 在遠端身份驗證服務中建立名為CiscoAVPair的屬性。在Common Name和LDAP Display Name欄位中,輸入CiscoAVPair。在Unique 500 Object ID欄位中,輸入
 1.3.6.1.4.1.9.287247.1。在Description欄位中,輸入UCS角色和區域設定。在Syntax欄位中 ,從下拉選單中選擇Unicode String。

dentification		
Common <u>N</u> ame:	CiscoAVPair	
DAP Display Name:	CiscoAVPair	
Jnique X500 <u>O</u> bject ID:	1.3.6.1.4.1.9.287247.1	
escription:	UCS role and locale	
Syntax and Range		
jyntax:	Unicode String]
1 jinimum:		-
Aaximum:		~

並關閉對話方塊。將屬性新增到架構後,必須將其對映或包括在使用者類中。這允許您編輯使 用者屬性並指定要傳遞的角色的值。

7. 在用於AD架構擴展的相同MMC中,展開類,按一下右鍵user,然後選擇Properties。

8. 在使用者屬性對話方塊中,按一下**屬性**頁籤,然後按一下**新增**。

🚡 Console 1				
Eile Action View Favgrites Window E	<u>t</u> elp			
Console Root\Active Directory Schema	[ucs-dc01.bglsvucs.com]\	Classes		
Classes	Name	user Properties		? ×
account	serviceConnectionPoint	General Relation	onship Attributes Default Security	
acSResourceLimits	ShadowAccount			
	simpleSecurityObject		user	
addressTemplate	SiteLink	Mandatory		
	siteLinkBridge	Hansard).		
applicationSettings	storage			
applicationStesecongs	Subnet			
	Subschema			
	■# top	Optional:	accountExpires	
	trustedDomain	T	aCSPolicyName	<u></u>
	■ a cypebbrary		auto	ve
	• volume		badPwdCount	
			carLicense	
			CiscoAVPair 💌	- 11
			1	
			OK Cancel	yoply

9. 在「選擇架構對象」對話方塊中,按一下CiscoAVPair,然後按一下確定。

Select a schema object:			
builtinModifiedCount businessCategory	-)K
bytesPerMinute		Ca	ncel
C oACortificato			
CACertificateDN			
cAConnect			
canonicalName			
canUpgradeScript			
carLicense			
catalogs			
categories			
categoryld			
CAUsages			
CAWEBURL			
certificateAuthorityUbject			
certificateTemplates			
DiscoAVPair			
classDisplayName			
an a	1001		

- 10. 在使用者屬性對話方塊中,按一下**應用**。
- 11. 按一下右鍵Active Directory架構,然後選擇**重新載入架構**以包含新更改。

Console Root	▲ Name
Active Directory Sch	ema fucs-dc01 bolsvucs.com
🖻 🦲 Classes	⊆hange Domain Controller
account	Operations Master
	Permissions
	<u>R</u> eload the Schema
	View
	New <u>W</u> indow from Here
	New Tackpad View
	New Tastbad New
	Refresh
	Export List
	Help
	vice

12. 如有必要,請使用ADSI編輯器更新架構。按一下右鍵Localhost,然後選擇Update Schema

Sile Action	View Window Help
🗢 🔶 🔁 💽	
I ADAM ADSI Edit	Na
E-Calhost [les E-Calhost [les E-Calhost [les	Settings Remove
⊕ 🛄 CN=	Update Schema Now
+ 🛄 CN=	New
	View
	New Window from Here
	Rename
	Refresh
	Export List
-	Help

更新CiscoAVPair屬性

o

以下過程介紹了如何更新CiscoAVPair屬性。語法是shell:roles="<role>"。

- 1. 在ADSI Edit對話方塊中,找到需要訪問UCS Central的使用者。
- 2. 按一下右鍵使用者,然後選擇**屬性**。
- 3. 在「屬性」對話方塊中,按一下**屬性編輯器**頁籤,按一下**CiscoAVPair**,然後按一下**編輯**。
- 4. 在多值字串編輯器對話方塊中,在「值」欄位中輸入值shell:roles="admin",然後按一下確定



5. 按一下「OK」以儲存變更並關閉「屬性」對話方塊。

更新預定義屬性

此過程介紹如何更新預定義屬性,其中角色是UCS Central中的預定義使用者角色之一。此示例使用屬性*company*來傳遞角色。語法是shell:roles="<role>"。

- 1. 在ADSI Edit對話方塊中,找到需要訪問UCS Central的使用者。
- 2. 按一下右鍵使用者,然後選擇屬性。
- 3. 在「屬性」對話方塊中,按一下屬性編輯器頁籤,按一下company,然後按一下編輯。
- 4. 在「字串屬性編輯器」對話方塊的「值」欄位中輸入值shell:roles="admin", 然後按一下確定

🖏 ADSI Edit					
🍕 Eile Action View Windo	w <u>H</u> elp				
🗢 🔿 🗈 💽 🗙 😭 🖉	1 🗟 🖸	1			
0U=UCSGroup106		Name		Class	Distinguished Name
OU=UCSUSERS OU=UCSUSERS OU= CN=admin On=Administra On=Administra On=Administra On=Administra On=Administra	ator			There are no	items to show in this view.
E-CN=testus	er Properties			? ×	
	ditor Security v mandatory att v only attribu s: e ssCategory calName ense vPair	ibutes utes tring Attribute Ed Attribute: company Value: shell:roles=''admin' Qlear Unicode String Unicode String Integer	itor testuser <not set=""> 0</not>		X Cancel
Comme compa control country create	nt ny AccessRights Code TimeStamp	Unicode String Unicode String Octet String Integer UTC Coded Ti	<not set=""> <not set=""> <not set=""> 0 30/01/2012 8:2 Cancel</not></not></not>	27:04 AM	

5. 按一下「OK」以儲存變更並關閉「屬性」對話方塊。

在UCS Central上配置LDAP身份驗證

UCS Central中的LDAP配置在操作管理下完成。

- 1. 以本地帳戶登入到UCS Central。
- 2. 按一下Operations Management,展開Domain Groups,然後按一下Operational Policies > Security。



3. 要配置LDAP身份驗證,請執行以下步驟:<u>配置LDAP提供程式。配置LDAP提供程式</u>組(版本 1.0a中不可用)。<u>更改本機身份驗證規則。</u>

配置LDAP提供程式

)

1. 按一下LDAP,按一下右鍵Providers,然後選擇Create LDAP Provider。

🗿 <u>Time Zone</u>	🕆 Authentication 🕴 🖶 RAE	dius 🕆 tacacs+ 🕆 Lda
DNS	🕰 Filter (off)	
P Remote Access	Name	
SNMP	Authentication P Trusted Points	
👁 <u>Debuq</u>	▶ 🎇 User Services	
🚯 <u>Call Home</u>	 LDAP Group Maps 	Timeout: 30, Attibute: me
Security	🕨 🗎 Provider Groups	
計量 <u>Equipment</u>	 Providers RADIUS Create I 	_DAP Providereout: 5, Retries: 1
<u>Identifier</u>	► 🚔 TACACS+	Timeout: 5

2. 在「建立LDAP提供程式」對話方塊中,新增之前收集到的這些詳細資訊。提供程式的主機名或IP繫結DN基本DN篩選條件屬性(CiscoAVPair或預定義屬性,例如company密碼(繫結DN中使用的使用者的密碼)

create LDAP Pr	ovider			0
eral Properties Hostname (or IP Address): Order: Bind DN: Base DN: Port: Enable SSL:	10.10.10.10 lowest-available CN=Administrator,CN=Users,DC= DC=bglsvucs,DC=com 389	LDAP Group Rules Group Authorization: Group Recursion: Target Attribute:	disable non-recursive memberOf]
Filter: Attribute: Password: Confirm Password: Timeout:	ciscoAVPair			

3. 按一下「OK」以儲存組態並關閉對話方塊。

注意:在此螢幕上不需要修改其他值。此版本中的UCS中心身份驗證不支援LDAP組規則。

配置LDAP提供程式組

注意:在版本1.0a中,不支援提供程式組。以下過程介紹了如何配置虛擬提供程式組,以便以後在 配置中使用。

1. 按一下LDAP,按一下右鍵Provider Group,然後選擇Create LDAP Provider Group。

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

- 2. 在建立LDAP提供程式組對話方塊中,在名稱欄位中輸入組的名稱。
- 3. 從左側的可用提供程式清單中,選擇提供程式,然後按一下大於符號(>),以將該提供程式移 動到右側的已分配提供程式。

Create LDAP Provider Group										
Create LDAP Provider Group										C
neral										
Properties										_
Name: Jidap-dc										
•										
roviders										-
Available Providers		- Assigned Prov	Aders -				-			
Records: 1 Showing: 0		40.76.79.66	T	×	*	2	Records:	1	Showing:	_
	77	10.70.70.00								
	>									
	<									
	~									
										_
								UK	Car	ICE

4. 按一下「OK」以儲存變更並關閉畫面。

更改本機身份驗證規則

版本1.0a不支援多個身份驗證域,如UCS Manager中的那樣。為了解決此問題,您需要修改本機身 份驗證規則。

本地身份驗證可以選擇修改預設登入或控制檯登入的身份驗證。由於不支援多個域,您可以使用本 地帳戶或LDAP帳戶,但不能同時使用這兩個帳戶。更改Realm的值,以便使用本地或LDAP作為身 份驗證源。

- 1. 按一下Authentication,按一下右鍵Native Authentication,然後選擇Properties。
- 確定您是要使用Default Authentication、Console Authentication還是同時使用兩者。對GUI和 命令列介面(CLI)使用預設身份驗證。 對虛擬機器(VM)基於核心的虛擬機器(KVM)檢視使用控 制檯身份驗證。
- 3. 從Realm下拉選單中選擇Idap。Realm的值確定本地身份驗證源還是LDAP身份驗證源。

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

4. 按一下「OK」以關閉頁面。

5. 在Policies(策略)頁上,根據需要按一下Save以儲存更改。

注意:在驗證LDAP身份驗證是否正常工作之前,請勿從當前會話註銷或修改控制檯身份驗證。控 制檯身份驗證提供了一種還原到先前配置的方法。請參閱<u>驗證</u>部分。

<u>驗證</u>

以下過程介紹了如何測試LDAP身份驗證。

1. 在UCS Central中開啟一個新會話,然後輸入使用者名稱和密碼。您不需要在使用者名稱之前 包含域或字元。此示例使用testucs作為域中的使用者。

cisco Version 1.0(1a)		Usemame	testucs
		Passwort	
			Log In

2. 如果您看到UCS中心控制面板,則LDAP身份驗證成功。使用者顯示在頁面底部。

cisco UCS Central			A				Preferences Log Out Al
		10 1 8	17				
Equipment i Servers i Network i Storage i 📀	erations Management Administration						
Corran Groups Demain Groups Demain Groups Demain Groups Demain	Ubrary of Images	Narse		Versian	Source	State	Type
User destucs)							System Time: 2013

<u>疑難排解</u>

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

• 技術支援與文件 - Cisco Systems