UCS Central 向け LDAP 認証の設定例

内容

概要 前提条件 要件 使用するコンポーネント 表記法 情報の収集 バインド ユーザの詳細 ベース DN の詳細 <u>プロバイダーの詳細</u> フィルタのプロパティ 属性の追加と設定 CiscoAVPair 属性の追加 CiscoAVPair 属性の更新 事前設定された属性の更新 UCS Central での LDAP 認証の設定 LDAP プロバイダーの設定 LDAP プロバイダー グループの設定 ネイティブ認証ルールの変更 確認 トラブルシュート 関連情報

<u>概要</u>

このドキュメントでは、Cisco Unified Computing System(UCS)Central 用の Lightweight Directory Access Protocol(LDAP)認証の設定例を示します。この設定手順では、UCS Central の GUI を使用し、ドメインを bglucs.com、ユーザ名を testuser としています。

LDAP は、UCS Central ソフトウェアのバージョン 1.0 がサポートする唯一のリモート認証プロ トコルです。バージョン 1.0 では、UCS Central 自身に対するリモート認証と LDAP 設定へのサ ポートが、ごく限られたものになっています。それでも UCS Central を使用すれば、UCS Central が管理する UCS Manager ドメイン用のすべてのオプションを設定することが可能です。

UCS Central のリモート認証へのサポートは、以下の点で制限されています。

- RADIUS と TACACS がサポートされていない。
- ・複数のドメイン コントローラに対してロールの割り当てと LDAP プロバイダー グループの マッピングを行う LDAP のグループ メンバシップがサポートされていない。
- ロールを割り当てる際、LDAP は CiscoAVPair の属性または未使用の属性しか使用できない

。割り当てるロールは、UCS Central のローカル データベースで事前に設定されたロールの うちの 1 つである。

複数の認証ドメインと認証プロトコルがサポートされていない。

<u>前提条件</u>

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- UCS が導入されている。
- Microsoft Active Directory が導入されている。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- UCS Central バージョン 1.0
- Microsoft Active Directory

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

情報の収集

このセクションでは、設定を行う前に知っておくべき情報についてまとめています。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登 録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセス できない場合がありますことをご了承ください。

<u>バインド ユーザの詳細</u>

バインド ユーザは、ドメインへの読み取りアクセス権を持つドメイン内のすべての LDAP ユーザ に対して指定できます。LDAP 設定にはバインド ユーザが必要です。UCS Central はバインド ユ ーザのユーザ名とパスワードを使用して、ユーザ認証などの情報について Active Directory (AD)に接続してクエリを行うことができます。ここでは、バインド ユーザに管理者 アカウントを使用しています。

この手順では、LDAP 管理者が Active Directory Service Interfaces(ADSI)エディタを使用して DN を検出する方法について説明します。

1. ADSI エディタを開きます。

- 2. バインド ユーザを検出します。ユーザのパスは、AD のパスと同じです。
- 3. ユーザを右クリックして [Properties] を選択します。
- 4. [Properties] ダイアログ ボックスで、[distinguishedName] をダブルクリックします。
- 5. [Value] フィールドの DN をコピーします。



6. [Cancel] をクリックし、すべてのウィンドウを閉じます。

バインド ユーザのパスワードを取得する際は、AD 管理者に連絡してください。

<u>ベース DN の詳細</u>

ベース DN は、ユーザとユーザの詳細情報の検索が開始される Organizational Unit(OU)または コンテナの DN です。UCS または UCS Central 用の AD に作成された OU の DN を使用できます 。ただし、ドメイン ルートの DN を使用した方が簡単な場合もあります。

この手順では、LDAP 管理者が(ADSI)エディタを使用してベース DN を検出する方法について 説明します。

1. ADSI エディタを開きます。

- 2. ベース DN として使用する OU またはコンテナを検出します。
- 3. OU またはコンテナを右クリックして [Properties] を選択します。
- 4. [Properties] ダイアログ ボックスで、[distinguishedName] をダブルクリックします。
- 5. [Value] フィールドの DN をコピーし、他の必要な詳細情報を記録します。



6. [Cancel] をクリックし、すべてのウィンドウを閉じます。

<u>プロバイダーの詳細</u>

プロバイダーの情報は、LDAP 認証や UCS Central での認証を行う際に非常に重要です。プロバ イダーは、ユーザの検索や認証を行ったり、ロール情報などのユーザの詳細情報を取得したりす るために UCS Central がクエリを行う AD サーバの 1 つです。プロバイダー AD サーバのホスト 名や IP アドレスを確実に取得してください。

<u>フィルタのプロパティ</u>

フィルタのフィールドやプロパティは、AD データベースの検索を行う際に使用します。ログイン時に入力されたユーザ ID は AD に返され、フィルタ値と照合されます。

フィルタ値には、sAMAccountName=\$userid を使用します。sAMAccountName は AD の属性で、UCS Central GUI へのログイン時に使用する AD のユーザ ID と同じ値になります。

Show <u>o</u> ptional attribu	tes	
Show only attributes	that have <u>v</u> alues	
Attribute	Syntax	Value 🔺
proxyAddresses	Unicode String	<not set=""></not>
pwdLastSet	Large Integer/	129723865322977500
queryPolicyBL	Distinguished	<not set=""></not>
registeredAddress	Uctet String	<not set=""></not>
replPropertyMetaData	Uctet String	
repiUp I oDateVector	Uctet String	<not set=""></not>
repsriom	Octet String	(Not Set)
reuision	listeder	<not set<="" td=""></not>
rid	Integer	<not sets<="" td=""></not>
roomNumber	Unicode String	<not set=""></not>
sAMAccountName	Unicode String	testuser
sAMAccountType	Integer	805306368

属性の追加と設定

このセクションでは、CiscoAVPair 属性の追加(必要な場合)や更新、または LDAP 設定を行う 前の事前設定された属性を更新する際に必要な情報についてまとめています。

属性フィールドでは、ユーザ プロパティ配下にある、ユーザに割り当てるロールを返す AD 属性 を指定します。UCS Central ソフトウェアのリリース 1.0a では、カスタムの CiscoAVPair 属性か 、AD の未使用属性を統合して、当該ロールを割り当てることができます。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

<u>CiscoAVPair 属性の追加</u>

ドメインに新規の属性を追加する場合は、ドメインのスキーマを展開して、属性をクラス(ここではユーザ)に追加します。

この手順では、Windows AD サーバのスキーマを展開し、CiscoAVPair 属性を追加する方法について説明します。

- 1. AD サーバにログインします。
- 2. [Start] > [Run] をクリックして mmc と入力し、Enter キーを押して空の Microsoft Management Console (MMC)を開きます。
- 3. MMC で、[File] > [Add/Remove Snap-in] > [Add] の順でクリックします。
- 4. [Add Standalone Snap-in] ダイアログボックスで [Active Directory Schema] を選択し、[Add] をクリックします。

Console Root					
Console Root		Name			
Ac	Add/Remove Snap-in Standalone Extensions Use this page to add or re	move a stand-alone snap-in from the consol	There are no items to show in the sho	is view.	
	Snap-ins added to:	Console Root 💌	Add Standalone Snap-in		? ×
			Available standalone snap-ins:		
	Description		Active Directory Jomains and Trusts Active Directory Jomains and Trusts Active Directory Schema Active Directory Stes and Services Active Directory Users and Compu Active X Control ADSI Edit Authorization Manager Certificate Templates Certificates	Version Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
	Add	ove About	Description View and edit the Active Directory Scher	na Add Slos	e

5. MMC で [Active Directory Schema] を展開し、[Attributes] を右クリックして [Create Attribute] を選択します。

∃ile <u>A</u> ction ⊻ie ⊨ → 🔁 🚺	w Favorites <u>W</u> indow <u>H</u> e	elp
Console Root	Active Directory Schema	[ucs-dc01.bglsvucs.com]\Att
Attribu	ctory Schema [ucs-dc01.bglsvu s	
	Create Attribute	 aCSAggregate Tokenka aCSAllocableRSVPBand aCSCacheTimeout
	View New Window from Here	 aCSDirection aCSDSBMDeadTime aCSDSBMPriority
	New <u>T</u> askpad View	• aCSDSBMRefresh
	Refresh Export List	 aCSEnableACSService aCSEnableRSVPAccoun aCSEnableRSVPMessag
	Help	 aCSEventLogLevel aCSIdentityName
		 aCSMaxAggregatePeak aCSMaxDurationPerFlow

Create New

Attribute] ダイアログボックスが表示されます。

6. リモート認証サービスで、CiscoAVPair という属性を作成します。[Common Name] フィー ルドと [LDAP Display Name] フィールドで、**CiscoAVPair** と入力します。[Unique 500 Object ID] フィールドで、**1.3.6.1.4.1.9.287247.1** と入力します。[Description] フィールドで 、**UCS role and locale** と入力します。[Syntax] フィールドで、ドロップダウン リストから [Unicode String] を選択します。

dentification		
Common <u>N</u> ame:	CiscoAVPair	
DAP Display Name:	CiscoAVPair	
Inique X500 <u>O</u> bject ID:	1.3.6.1.4.1.9.287247.1	
escription:	UCS role and locale	
iyntax and Range	wi wa ay	
iyntax:	Unicode String	
1jnimum:		
faximum:		

属性を保存してダイアログボックスを閉じます。属性がスキーマに追加されたら、この属性 の対応付けを行うか、この属性をユーザ クラスに追加する必要があります。こうすること で、ユーザ プロパティを編集し、割り当てるロールの値を指定できるようになります。

- 7. AD スキーマの展開に使用された MMC で [Classes] を展開し、**ユーザ**を右クリックして [Properties] を選択します。
- 8. [user Properties] ダイアログボックスで [Attributes] タブをクリックし、[Add] をクリックし ます。

📸 Console1			
Eile Action View Favorites Window	Help		
Console Root\Active Directory Schem	a [ucs-dc01.bglsvucs.com]\	Classes	
Classes Class		User Properties General Relationship Attributes Default Security Image: Comparison of the security user Mandatory: Image: Comparison of the security Image: Comparison of the security of the s	? X / Add. Bemove
	•5 volume	badPwdCount businessCategory carLicense CiscoAVPair	▼ Cancel <u>A</u> pply

9. [Select Schema Object] ダイアログボックスで [CiscoAVPair] > [OK] の順にクリックします

<u>5</u> elect a schema object:		
builtinModifiedCount	- T	ок
businessCategory		
bytesPerMinute		Cancel
c		Cancer
cACertificate		
cACertificateDN		
cAConnect		
canonicalName		
canUpgradeScript		
carLicense		
catalogs		
categories		
categoryld		
cAUsages		
cAWEBURL		
certificateAuthorityObject		
certificateRevocationList		
certificateTemplates		
CiscoAVPair		
classDisplayName	NUMBER OF STREET	
on		

10. [user Properties] ダイアログボックスで [Apply] をクリックします。

o

11. [Active Directory Schema] を右クリックし、[Reload the Schema] を選択して新たな変更を

🛛 🛄 Console Root	 Name
Active Directory Sch	pema fucs-dc01 bolsvucs.com]
E Classes	
account	Operations Master
	Permissions
	<u>R</u> eload the Schema
	18
	View
	New Window from Here
	New Taskpad View
	Refresh
	Export List
	uala .
	Ūeih

12. 必要に応じて、ADSI エディタを使用してスキーマを更新することもできます。[Localhost] を右クリックして [Update Schema Now] を選択します。



<u>CiscoAVPair 属性の更新</u>

この手順では、CiscoAVPair 属性の更新方法について説明します。入力する値は shell:roles="<role>" です。

- 1. [ADSI Edit] ダイアログボックスで、UCS Central へのアクセス権が必要なユーザを検索します。
- 2. ユーザを右クリックして [Properties] を選択します。
- 3. [Properties] ダイアログボックスで [Attribute Editor] タブをクリックし、[CiscoAVPair] > [Edit] の順にクリックします。
- 4. [Multi-valued String Editor] ダイアログボックスで、[Values] フィールドに shell:roles="admin" と入力して [OK] をクリックします。



5. [OK] をクリックし、変更を保存して [Properties] ダイアログボックスを閉じます。

事前設定された属性の更新

この手順では、事前設定された属性の更新方法について説明します。この属性のロールは、UCS Central で事前設定された複数のユーザ ロールのうちの 1 つです。ここでは、属性を *company* と してロールの割り当てを行います。入力する値は shell:roles="<role>" です。

- 1. [ADSI Edit] ダイアログボックスで、UCS Central へのアクセス権が必要なユーザを検索します。
- 2. ユーザを右クリックして [Properties] を選択します。
- 3. [Properties] ダイアログボックスで [Attribute Editor] タブをクリックし、[company] > [Edit]

の順にクリックします。

4. [String Attribute Editor] ダイアログボックスで、[Values] フィールドに shell:roles="admin" と入力して [OK] をクリックします。

nd SI Edit				
⇐ ⇒ 🗈 📧 🗙 🖀 🗟 😫				
OU=UCSGroup106	▲ Name		Class	Distinguished Name
OU=UCSGroup106 OU=UCSUSERS ON=users ON=admin ON=Administrator ON=avshukla ON=avshukla ON=avshukla ON=avshukla ON=testuser Propertie ON=C ON=C ON mandatory attribute ON only att	▲ Name Nam	litor testuser <not set=""> 0 <not set=""> <not set=""> <not set=""> <not set=""> 0</not></not></not></not></not>	Class There are no	Distinguished Name items to show in this view.
Configuration	UTC Coded Ti	30/01/2012 8:27:0		
<u>E</u> dit				
	ОК	Cancel		

5. [OK] をクリックし、変更を保存して [Properties] ダイアログボックスを閉じます。

<u>UCS Central での LDAP 認証の設定</u>

UCS Central での LDAP 設定は、[Operations Management] 内で完結できます。

- 1. ローカル アカウントで UCS Central にログインします。
- 2. [Operations Management] をクリックし、[Domain Groups] を展開して [Operational Policies] > [Security] の順にクリックします。

CISCO UCS Central	Operations Management	Administration	8 1 0	7 A 1 8	▲ 17	
 ▶ (@) Images ▶ (@) Backup and Import ♥ (\$\$ Domain Groups ♥ -(\$\$ Domain Group root 	양 <u>terrein Groups</u> 》 밝 Operational Policie 예 Time Zone	S <u>Queste Group rost</u> ≯ S	PADUIS		CACR+	Me i Dap
Backup/Export Policy Sirrware Management Si Maintenance Si Operational Policies	P DNS	Fiter (off) Name Mathematication				Properties
🖌 🔂 Schedules	<u>SNMP</u> Debug <u>Call Home</u>	P Trusted Points SUser Services B LOAP A RADIUS		Tim	eout: 30, Atti eout: 5, Retr	ibute: memberO(, Filter: sAMAccountName=\$userid
	Security Security Statestifier	► A TACACS+		Tim	eout 5	

3. LDAP 認証の設定手順は以下のとおりです。LDAP プロバイダーの設定LDAP プロバイダー グループの設定(リリース 1.0a ではサポート対象外)<u>ネイティブ認証ルールの変更</u>

LDAP プロバイダーの設定

1. [LDAP] をクリックし、[Providers] を右クリックして [Create LDAP Provider] を選択します

🗃 <u>Time Zone</u>	🕆 Authentication 🗍 🕆 RAD	dius 🖶 tacacs+ 📇 Lda
M DNS	🕰 Filter (off)	
<u> </u>	Name	
SNMP	Authentication P Trusted Points	
👁 Debuq	User Services	
🚳 <u>Call Home</u>	 LDAP Group Maps 	Timeout: 30, Attibute: mer
Security	🕨 🚔 Provider Groups	
Equipment	Providers ADIUS Create I	LDAP Provider pout: 5, Retries: 1
) Identifier	► 🚔 TACACS+	Timeout: 5

2. [Create LDAP Provider] ダイアログボックスで、事前に収集されたこれらの詳細情報を追加 します。プロバイダーのホスト名または IP アドレスバインド DNベース DNフィルタ属性 (CiscoAVPair、または company などの事前設定された属性) パスワード(バインド DN で 使用されているユーザのパスワード

Teale LDAF FI	ovider			0
eral Froperties Hostname (or IP Address): Order: Bind DN: Base DN: Port: Enable SSL: Filter: Attribute: Password:	10.10.10.10 lowest-available CN=Administrator,CN=Users,DC= DC=bglsvucs,DC=com 389 sAMAccountName=\$userid ciscoAVPair	LDAP Group Rules Group Authorization: Group Recursion: Target Attribute:	disable non-recursive memberOf	
Confirm Password: Timeout:	30			

3. [OK] をクリックし、設定を保存してダイアログボックスを閉じます。

注:この画面では、他の値を変更する必要はありません。このリリースでは、UCS Central の認 証用の LDAP グループ ルールはサポートされていません。

LDAP プロバイダー グループの設定

注:リリース1.0aでは、プロバイダーグループはサポートされていません。この手順では、後の 設定で使用するダミーのプロバイダー グループの設定方法について説明します。

1. [LDAP] をクリックし、[Provider Group] を右クリックして [Create LDAP Provider Group] を 選択します。

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

- 2. [Create LDAP Provider Group] ダイアログボックスで、[Name] フィールドにグループ名を 入力します。
- 3. 左下の [Available Providers] のリストで対象プロバイダーを選択し、[>] をクリックしてこの プロバイダーを右下の [Assigned Providers] に移動します。

🚖 Create LDAP Provider Group	
Create LDAP Provider Group	0
Name:	
Providers	Assigned Providers Assigned Providers Assigned Providers Assigned Providers Records: 1 Showing: 1 10.76.78.66
	OK Cancel

4. [OK] をクリックして変更を保存し、画面を閉じます。

<u>ネイティブ認証ルールの変更</u>

UCS Manager の場合と同様、リリース 1.0a では複数の認証ドメインをサポートしていません。 この問題を回避するには、ネイティブ認証ルールを変更する必要があります。

ネイティブ認証には、デフォルトのログインまたはコンソールのログインの認証を変更するオプ ションが備わっています。複数のドメインがサポートされていないため、ローカル アカウントま たは LDAP アカウントのどちらか一方のみを使用できます。レルムの値を変更し、ローカル アカ ウントか LDAP アカウントを認証用の元データとして使用します。

- 1. [Authentication] をクリックし、[Native Authentication] を右クリックして [Properties] を選択 します。
- デフォルト認証とコンソール認証のどちらを変更するのか、またはその両方を変更するのか を決めます。GUI と CLI(コマンド ライン インターフェイス)向けには、デフォルト認証 を使用します。 VM(仮想マシン)や KVM(カーネル ベースの仮想マシン)の表示には、 コンソール認証を使用します。
- 3. [Realm] ドロップダウン リストで [Idap] を選択します。認証元データにローカル アカウントを使用するか LDAP アカウントを使用するかは、レルムの値に基づいて決定されます。

🏯 Properties			∎ ×
Properties (Native	Authentication)		0
General Events			
- Default Authentication:			
Session Refresh Period (in secs):	600		
Session Timeout (in secs):	7200	7	
Realm:	Idap	Idap-dc 💌	
Console Authentication:			
Role Policy for Remote Users: as	sign-default-role 💌		
		OK	Cancel

4. [OK] をクリックしてウィンドウを閉じます。

5. 必要に応じて [Policies] ページで [Save] をクリックし、変更内容を保存します。

注:LDAP認証が正しく動作することを確認するまで、現在のセッションからログアウトしたり 、コンソール認証を変更したりしないでください。コンソール認証では、以前の設定に戻す方法 が表示されます。「<u>確認</u>」セクションを参照してください。

確認

この手順では、LDAP 認証のテスト方法について説明します。

UCS Central の新規セッションを開き、ユーザ名とパスワードを入力します。ユーザ名の前に、ドメインや文字を含める必要はありません。ここでは、ドメインのユーザ名を testucs としています。

uluulu cisco	UCS Central Version 1.0(14)	Usemame:	testucs
		Password	
			Log In
	사람들은 방법은 방법은 방법을 위해 가장 물건을 받았다. 방법은 감독 가장		

2. UCS Central ダッシュボードが表示されれば、LDAP 認証は成功です。ページの左下隅にユ ーザ名が表示されます。

altalta		UCS Faults				Batarances Lon Ort M
cisco UCS Central						
Equipment Servers Network Storage 0	perations Management Administration		_		_	
D Imates						
Backup and Import	Library of Images					
🔻 🎊 Domain Groups	country or enages					
	K Filter (off) Hide Show Hidden					
- SFirmware Management		Name	Version	Source	State	Туре
- S Maintenance						
- 50 Operational Policies	► @ t-series-bundle					
P-00 CONDERS	► @ catalog					
	In the second secon					
User (testucs)						System Time: 2013

<u>トラブルシュート</u>

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

・<u>テクニカル サポートとドキュメント – Cisco Systems</u>