コンフィギュレーションの例：Cisco UCS、LDAP、および Active Directory

初版：2011 年 03 月 24 日

最終更新：2012 年 05 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-24834-03-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

概要

この章の内容は、次のとおりです。

Active Directory を使用した LDAP および複数の認証サーバの設定

LDAP、および Active Directory（AD）などのさまざまなリモート認証プロバイダーを使用してユーザ ログインをリモートで認証するよう、Cisco UCS を設定することができます。

このサンプル設定は、AD サーバを使用して Cisco UCS LDAP および複数サーバの認証を実装するための完全な（最初から最後までの）プロセスを示すことを意図しています。 また、Cisco UCS Manager GUI および Cisco UCS Manager CLI で実装をテストするための手順も含まれています。

具体的には、この設定には AD サーバの以下のタスクが含まれています。

- 組織ユニットの作成とグループの追加，（3 ページ）
- admin にバインドされないユーザ アカウントの作成，（4 ページ）
- ユーザの作成と CiscoUCS OU への追加，（5 ページ）
- UCS LDAP 設定用の情報の収集，（5 ページ）

以下のタスクは Cisco UCS Manager で行います。

- ローカル認証ドメインの作成，（7 ページ）
- LDAP プロバイダーの作成，（8 ページ）
- LDAP グループのルールの設定，（9 ページ）
- LDAP プロバイダー グループの作成，（9 ページ）

前提条件

このサンプル設定を完成するには、以下のものが必要です。

- Cisco UCS システム
- Cisco UCS Manager バージョン 1.4(1) 以降
- Microsoft Active Directory server 2003 以降
- Active Directory サーバの管理者権限
- ADSI Edit

第 2 章

Active Directory サーバの設定

この章の内容は、次のとおりです。

組織ユニットの作成とグループの追加

AD サーバの組織ユニット（OU）には、Cisco UCS のユーザ ロールをマップする AD グループが含まれています。 AD で保持されているすべてのロールについては、Cisco UCS で同じロールを設定しておく必要があります。

（注） 統合するには、AD および Cisco UCS のロール名が一致している必要あります。

手順

ステップ 1 [Active Directory Users and Computers] を開きます。

ステップ 2 AD インスタンス sampledesign.com を右クリックし、[New] > [Organizational Unit]を選択します。

ステップ 3 [Name] に CiscoUCS と入力します。

ステップ 4 ucsaaa という新しいグループを作成し、新しく作成した CiscoUCS OU にそのグループを割り当てます。

a) 新しい [CiscoUCS] OU を右クリックし、[New] > [Group]を選択します。

b) [New Object - Group] ダイアログボックスで、[Group name] フィールドに ucsaaa と入力します。

c) [Group scope] エリアで、[Global] オプション ボタンをクリックします。

d) [Group type] エリアで [Security] オプション ボタンをクリックし、[OK] をクリックします。

ステップ 5 以下のロールについて、ステップ 4 を繰り返します。

- ucsaaa
- ucsadmin
- ucsnetwork
- ucsoperation
- ucsecurity
- ucstorage

次の作業

admin にバインドされないユーザを作成し、それを CiscoUCS OU に追加します。

admin にバインドされないユーザ アカウントの作成

Cisco UCS は admin にバインドされないユーザ アカウントを使用して、AD サーバの中でユーザがどのグループに含まれているかを定期的にチェックします。

（注） 不要な認証エラーを防止するため、このアカウントには、有効期限のないパスワードを設定することをお勧めします。

AD サーバ内で、Cisco UCS がユーザを認証するために使用可能な admin 以外のユーザ アカウントがすでに存在している場合は、新しい admin にバインドされないユーザ アカウントを作成する必要がありません。 このタスクを省略し、サンプル ユーザを作成して、これらのユーザを Cisco UCS OU へ追加することができます。

手順

ステップ 1 [CiscoUCS] OU を右クリックして、[New] > [User]を選択します。

ステップ 2 [First name] に ucs と入力します。

ステップ 3 [Initials] フィールドはブランクのままにします。

ステップ 4 [Last name] に binduser と入力します。

ステップ 5 [User logon name] に ucsbind と入力し、ドロップダウン リストで [UPN suffix] を選択して [Next] をクリックします。

CiscoUCS OU に、ucsbind というユーザ アカウントが表示されます。

次の作業

サンプル ユーザを作成し、そのユーザを CiscoUCS OU に追加します。

ユーザの作成と CiscoUCS OU への追加

手順

ステップ 1 [CiscoUCS] を右クリックし、[New] > [User]を選択します。

ステップ 2 [First name] に sample と入力します。

ステップ 3 [Last name] に admin と入力します。

ステップ 4 [Full name] に sampleadmin と入力します。

ステップ 5 [User logon name] に sampleadmin と入力し、ドロップダウン リストから [UPN suffix] を選択して [Next] をクリックします。

ステップ 6 作業ペインで sampleadmin を右クリックして [Properties] をクリックします。

ステップ 7 [MemberOf] タブをクリックして [Add] をクリックします。

ステップ 8 [Select Groups] ダイアログボックスの [Enter the object names to select] フィールドで ucsadmin と入力して [OK] をクリックします。

ステップ 9 もう一度 [OK] をクリックして [Sample Admin Properties] ダイアログボックスを閉じます。

ステップ 10 （任意） ステップ 1 ～ 9 を繰り返して次のユーザを作成します。

- sampleaaa
- samplenetwork
- sampleoperation
- samplesecurity
- samplestorage

次の作業

Cisco UCS LDAP の設定に必要な情報を収集します。

UCS LDAP 設定用の情報の収集

LDAP、および Cisco UCS Manager の複数の同時承認を設定するには、AD サーバのいくつかの値にアクセスする必要があります。この例では、サードパーティのユーティリティである ADSI Edit を使用して、必要な値を検索します。

はじめる前に

ADSI Edit をインストールし、編集します。

手順

ステップ 1 ADSI Edit を開いて DC=sampledesign,DC=com に移動します。
これは BaseDN フォルダです。

ステップ 2 LDAP 認証を設定するために Cisco UCS Manager で必要な BaseDN の値を検索するには、次の手順を実行します。

a) DC=sampledesign,DC=com インスタンスを右クリックして [Properties] を選択します。
b) [Attribute Editor] タブで、distinguishedName を選択します。
c) [String Attribute Editor] ダイアログボックスで、文字列を選択して [Value] フィールドにコピーします。
BaseDN の値は、DC=sampledesign,DC=com の形式に従っています。
d) BaseDN の値の文字列は、後で使用できるようテキスト ファイルに貼り付けます。

ステップ 3 DN で、AD の CiscoUCS OU に追加した各ロールを検索するには、次の手順を実行します。

a) CiscoUCS OU を展開し、CN=ucsadmin ロールを右クリックして [Properties] を選択します。
b) [Attribute Editor] タブで、distinguishedName を選択します。
c) [String Attribute Editor] ダイアログボックスで、文字列を選択して [Value] フィールドにコピーします。
これは、CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com の形式に従っている必要があります。
d) DN の値の文字列は、後で使用できるようテキスト ファイルに貼り付けます。
e) CiscoUCS OU 内の各 AD グループについてこれらの手順を繰り返します。

ステップ 4 BindDN で admin にバインドされないユーザ アカウントを検索するには、次の手順を実行します。

a) ucsbind というユーザ アカウントにナビゲートします。
b) CiscoUCS OU で ucsbind というユーザ アカウントを右クリックし、[Properties] を選択します。
c) [Attribute Editor] タブで、distinguishedName を選択します。
d) [String Attribute Editor] ダイアログボックスで、文字列を選択して [Value] フィールドにコピーします。
BindDN は、CN=ucsbind,OU=CiscoUCS,DC=sampledesign,DC=com の形式に従っている必要があります。
e) BindDN の値の文字列は、後で使用できるようテキスト ファイルに貼り付けます。

ステップ 5 [Attribute Editor] タブで、sAMAccountName 属性が存在することを確認します。

次の作業

これらの値を使用して Cisco UCS を設定します。

第 3 章

Cisco UCS の設定

この章の内容は、次のとおりです。

ローカル認証ドメインの作成

このサンプル設定では、Cisco UCS Manager で LDAP の設定を行う前に、ローカル認証ドメインを作成することを推奨します。 ローカルな admin ユーザとしてログインすると、この方法の手順の完了に必要なアクセス権を持っていることが保証され、誤った設定をすぐに修正できます。

はじめる前に

Cisco UCS Manager GUI に admin ユーザとしてログインします。

手順

ステップ 1 [Authentication Domains] を右クリックし、[Create a Domain] を選択します。

ステップ 2 [Name] フィールドに local と入力します。

ステップ 3 [Realm] で、[local] オプション ボタンをクリックします。

次の作業

Cisco UCS Manager で LDAP のプロパティを設定します。

LDAP プロバイダーの作成

このサンプル設定には、SSL を使用して LDAP を設定する手順は含まれていません。

手順

ステップ 1 [Actions] エリアで、[Create LDAP Provider] をクリックします。

ステップ 2 ウィザードの [Create LDAP Provider] ページで、次を実行します。

a) [Hostname] フィールドに、AD サーバの IP アドレスを入力します。

b) [Order] フィールドに lowest-available と入力します。

c) [BindDN] フィールドに、AD 設定の BindDN をコピーして貼り付けます。
このサンプル設定では、BindDN の値は CN=ucsbind,OU=CiscoUCS,DC=sampledesign,DC=com です。

d) [BaseDN] フィールドに、AD 設定の BaseDN をコピーして貼り付けます。
このサンプル設定では、BaseDN の値は DC=sampledesign,DC=com です。

e) [Enable SSL] チェックボックスはオフのままにします。

f) [Port] フィールドに 389 と入力します。

g) [Filter] フィールドに、AD 設定のフィルタ属性をコピーして貼り付けます。
Cisco UCS は、このフィルタ値を使用して、ログオン画面に Cisco UCS Manager から与えられたユーザ名が AD に含まれているかどうかを判別します。

このサンプル設定では、フィルタ値は sAMAccountName=*$userid* です。ここで、*$userid* は Cisco UCS Manager ログオン画面に入力するユーザ名です。

h) [Attribute] フィールドはブランクのままにします。

i) [Password] フィールドに、AD で設定した ucsbind アカウントのパスワードを入力します。
[Create LDAP Provider] ウィザードに戻ってパスワードをリセットする必要がある場合、パスワード フィールドがブランクでも警告は発生しません。「Set: yes」メッセージがパスワード フィールドの横に表示された場合は、パスワードが設定されたことを示しています。

j) [Confirm Password] フィールドに、AD で設定した ucsbind アカウントのパスワードをもう一度入力します。

k) [Timeout] フィールドに 30 と入力します。

ステップ 3 [Next] をクリックします。

次の作業

LDAP グループ ルールを設定します。

LDAP グループのルールの設定

手順

ステップ 1 ウィザードの [LDAP Group Rule] ページで、以下のフィールドを設定します。

a) [Group Authentication] フィールドで、[enable] オプション ボタンをクリックします。
グループ認証を有効にすると、認証しようとしているユーザが ucsaaa などのグループ内にいるかどうかを確認するために、ターゲット属性（この例では memberOf）を使用することが UCSM に示されます。

b) [Group Recursion] フィールドで [recursive] オプション ボタンをクリックします。
再帰に対してグループの再帰を設定すると、該当するユーザが見つかるまで、システムが 1 レベルずつ調べられるようになります。 グループの再帰を非再帰に設定すると、該当するユーザが検索で見つからなかった場合も、UCS の検索が最初のレベルに制限されます。

c) [Target Attribute] フィールドで、memberOf と入力します。

ステップ 2 [Finish] をクリックします。

（注） 実際のシナリオでは、ほとんどの場合に複数の LDAP プロバイダーがあるはずです。 複数の LDAP プロバイダーに対して、設定で保証されている順序を変更して、各 LDAP プロバイダーの LDAP Group Rule を設定します。 ただし、このサンプル設定では LDAP プロバイダーが 1 つだけのため、この処理は不要です。

[LDAP] > [LDAP Providers] を選択して表示される [Navigation] ペインに、AD サーバの IP アドレスが示されます。

次の作業

LDAP プロバイダー グループを作成します。

LDAP プロバイダー グループの作成

手順

ステップ 1 [Navigation] ペインで、[LDAP Provider Groups] を右クリックし、[Create LDAP Provider Group] を選択します。

ステップ 2 [Create LDAP Provider Group] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、グループの一意の名前を入力します。

b) [LDAP Providers] テーブルで、AD サーバの IP アドレスを選択します。

c) [>>] ボタンをクリックして AD サーバを [Included Providers] テーブルに追加します。

ステップ 3 [OK] をクリックします。

プロバイダー グループが [LDAP Provider Groups] フォルダに表示されます。

次の作業

LDAP グループ マップを設定します。

LDAP グループ マップの作成

手順

ステップ 1 [Work] ペインで、[Create LDAP Group Map] をクリックします。

ステップ 2 [Create LDAP Group Map] ダイアログボックスで、次を実行します。

a) [LDAP Group DN] フィールドに、LDAP グループに関する AD サーバ設定セクションに保存した値をコピーして貼り付けます。
この手順で要求された LDAP Group DN 値が、AD で UCS Groups の下に作成した各グループの識別名にマップされます。 このため、Cisco UCS Manager に入力する Group DN 値は、AD サーバの Group DN 値と正確に一致している必要があります。 このサンプル設定では、この値は CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com です。

b) [Roles] テーブルで、[admin] チェックボックスをクリックし、[OK] をクリックします。
ロールのチェックボックスをクリックすると、admin 権限をグループ マップに含まれている全ユーザに割り当てることになります。

ステップ 3 テストする AD サーバの他の各ロールについて、新規の LDAP グループ マップを作成します（前に AD から記録しておいた情報を使用します）。

次の作業

LDAP 認証ドメインを作成します。

LDAP 認証ドメインの作成

手順

ステップ 1 [Authentication Domains] を右クリックし、[Create a Domain] を選択します。

ステップ 2 [Create a Domain] ダイアログボックスで、次の情報を入力します。

a) [Name] フィールドに、ドメインの名前を入力します。
b) [Realm] 領域で、[ldap] オプション ボタンをクリックします。
c) [Provider Group] ドロップダウン リストからプロバイダー グループを選択して [OK] をクリックします。

[Authentication Domains] の下に認証ドメインが表示されます。

次の作業

Cisco UCS Manager GUI を使用して LDAP の設定をテストします。

第 4 章

コンフィギュレーションのテスト

この章の内容は、次のとおりです。

UCS Manager CLI を使用した設定のテスト

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco UCS Manager CLI にログインします。	
ステップ 2	UCS-A# **scope nxos**	NXOS モードを開始します。
ステップ 3	UCS-A (nxos)# **test aaa server ldap** *ip-address username password*	設定したすべてのユーザ用の LDAP 設定をテストします。

次に、LDAP 設定をテストする例を示します。

```
UCS-A# scope nxos
UCS-A (nxos) # test aaa server ldap 10.29.96.77 sampleaaa password
user has been authenticated
Attributes downloaded from remote server:
User Groups:
     CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com
Roles:
     admin
```

UCS Manager GUI を使用した設定のテスト

手順

ステップ 1 Cisco UCS Manager GUI を起動します。

ステップ 2 [User Name] フィールドに sampleaaa と入力します。

ステップ 3 [Password] フィールドに、sampleaaa の AD パスワードを入力します。

ステップ 4 [Domain] ドロップダウン リストから、LDAP のプロバイダーを選択して [OK] をクリックします。

ステップ 5 [All] > [User Management] > [User Services] > [Remotely Authenticated Users] に移動し、認証ドメインおよび AD ユーザ名がリストされていることを確認します。
この値は、*AuthenticationDomain\ADUserName* の形式になります。

付 録 A

よくある質問

Q 再帰検索が有効な場合、どのレベルの深さまで再帰しますか。

A 最初に、ユーザが直接メンバになっているすべてのグループが検索されます。次に、これらの各グループについて、その先祖のグループがトラバースされます。最上位レベルのグループに到達するまで、再帰が繰り返されます。

Q AD 統合と Cisco UCS Manager は、AD の証明書を使用した 2 要素認証をサポートしますか。

A いいえ。Cisco UCS Manager はパスワードベースの認証のみサポートしています。

Q Cisco UCS Manager と AD の統合で既知の制限は何ですか。（たとえば、AD のトラバースの結果、検索されるグループの最大数、最大の AD オブジェクトなど）。

A
- 現在は、プレーン ユーザ認証の AD インスタンス サイズに関する既知の制限はありません。ただし、フィルタの値によって、検索結果は 1 つまたは 2 つに制限されます。Cisco UCS Manager, versions 1.3(x) 以前ではランダム フィルタが許可されていたため、検索結果が膨大になっていました。バージョン 1.4(1) では、この問題を防止する検証が導入されました。
- ユーザが、最初のレベルの膨大な数のグループに属している場合、これらのグループの検索は、UCS Manager LDAP クライアントで使用できるメモリによって制限されます。UCS Manager はロールまたはロケール（あるいはその両方）で設定されているグループのみ処理し、その他のグループは破棄します。

ユーザがメンバになることができるグループの最大数は 32 です。これは、UCS Manager で許可されているグループとロールのマッピング数と一致しています。

Q テストされ、確認されている最大 AD 構造はどのようなものですか。

A 当社では、ユーザ認証が AD サイズに依存しないことを確認しています。グループ名が 100 文字で、120 を超えるグループに属しているユーザとの AD 統合がテスト済みです。