LDAP 認証

- LDAP プロバイダー，1 ページ
- UCS Central LDAP 設定の管理，4 ページ

LDAP プロバイダー

LDAP リモート ユーザを作成および設定し、Cisco UCS Central からロールとロケールを、Cisco UCS Manager と同じ要領で割り当てます。LDAP プロバイダーの作成は、常に Cisco UCS Central ドメイン グループ ルートから行ってください。

LDAP グループ マップ

複数の LDAP グループ マッピングを定義し、最大で Windows Active Directory が Cisco UCS Central のネストをサポートしているのと同じレベルまでそれらをネストできます。ネスト グループにプロバイダーを割り当てると、プロバイダーが異なる LDAP グループのメンバーであっても、親ネスト グループの認証メンバーになります。認証の際に、Cisco UCS Central は、プロバイダー グループ内のすべてのプロバイダーを順番に試行します。Cisco UCS Central は、設定されたサーバのいずれにもアクセスできない場合、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

LDAP グループの数は、Cisco UCS Manager のバージョンに応じて定義できます。サポートされる LDAP グループ マップ，（3 ページ）を参照してください。

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS が使用するプロバイダーのセットです。Cisco UCS Central では、最大 16 のプロバイダー グループを作成でき、グループごとに最大 8 つのプロバイダーを含めることができます。

認証の際には、プロバイダー グループ内のすべてのプロバイダーが順番に試行されます。設定されたすべてのサーバが使用できない場合、または到達不能な場合、Cisco UCS Central は、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

LDAP グループ マップ

LDAP データベースへのアクセス制限のために LDAP グループを使用している組織では、Cisco UCS ドメインで、グループ メンバーシップ情報を使用してログイン時に LDAP ユーザにロールやロケールを割り当てることができます。これにより、Cisco UCS Central を導入するときに、LDAP ユーザ オブジェクトでロールやロケール情報を定義する必要がなくなります。

Cisco UCS Central は、ユーザ ロールとロケールをリモート ユーザに割り当てるときに LDAP グループ ルールを使用して LDAP グループを決定します。ユーザがログインすると、Cisco UCS Centralはユーザのロールとロケールに関する情報を LDAP グループ マップから取得します。ロールとロケールの条件がポリシーの情報に一致すると、Cisco UCS Centralはそのユーザにアクセス権を提供します。

LDAP グループの数は、Cisco UCS Manager のバージョンに応じて定義できます。

最大で Windows Active Directory が Cisco UCS Central のネストをサポートしているのと同じレベルまでLDAP グループ マッピングをネストできます。ネスト グループにプロバイダーを割り当てると、プロバイダーが異なる LDAP グループのメンバーであっても、親ネスト グループの認証メンバーになります。認証の際に、Cisco UCS Central は、プロバイダー グループ内のすべてのプロバイダーを順番に試行します。Cisco UCS Central は、設定されたサーバのいずれにもアクセスできない場合、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

ロールとロケールの定義は Cisco UCS Central でローカルに設定され、LDAP ディレクトリに対する変更に基づいて自動的に更新されることはありません。LDAP ディレクトリで LDAP グループを削除または名前変更する場合、Cisco UCS Centralで変更を更新してください。

LDAP グループ マップは、次のロールとロケールのいずれかの組み合わせを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケール

たとえば、特定のロケーションのサーバ管理者グループを表す LDAP グループの認証を設定する場合は、その LDAP グループに対する server-profile や server-equipment などのユーザ ロールを含めることができます。特定のロケーションのサーバ管理者に対しアクセスを制限する場合は、特定のサイト名をロケールに指定できます。

（注） Cisco UCS Central にはすぐに使用できる多数のユーザ ロールが含まれていますが、ロケールは含まれていません。カスタム ロケールを作成して LDAP プロバイダー グループをロケールにマップする必要があります。

サポートされる LDAP グループ マップ

サポートされる LDAP グループ マップの数は、Cisco UCS Manager のバージョンによって異なります。

Cisco UCS Manager バージョン	LDAP グループ マップ サポート対象
Cisco UCS Manager リリース 3.1(2) 以降	160
Cisco UCS Manager リリース 3.1(1)	128
Cisco UCS Manager リリース 2.2(8) 以降	160
Cisco UCS Manager リリース 2.2(7) 以前	28

ネストされた LDAP グループ

LDAP グループを他のグループのメンバーとしてネストすることにより、アカウントを統合して複製を減らすことができます。

デフォルトでは、LDAP グループを別のグループ内にネストすると、ユーザ権限が継承されます。たとえば、Group_2 のメンバーとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバーと同じ権限が与えられます。その結果、Group_1 のメンバーであるユーザを検索するときは、LDAP グループ マップで Group_2 だけを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

LDAP グループ マップで定義されたネストしたグループを検索できます。グループをネストすることによって、サブグループを作成する必要がなくなります。

（注） ネストした LDAP グループの検索は、Microsoft Active Directory サーバに対してのみサポートされます。サポートされているバージョンは Microsoft Windows 2003 SP3、Microsoft Windows 2008 R2、および Microsoft Windows 2012 です。

ネストしたグループ名に特殊文字を含めた場合は、次の例に示す構文を使用してそれらをエスケープする必要があります。

```
create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in
```

UCS Central LDAP 設定の管理

手順

ステップ 1 [Actions] バーから、「Managing UCS Central LDAP Configuration」と入力します。
これにより、[UCS Central LDAP Configuration Manage] ダイアログ ボックスが開きます。

ステップ 2 [LDAP]で、以下のタブで要求される情報を入力します。

a) [Basic] タブで、[Database Connection Timeout]、[Filter]、[Attribute]、および [Base DN] の値を入力します。

b) [Providers] タブで、[+] をクリックしてプロバイダーを追加し、[Basic] タブと [Group Rules] タブで必要な情報を入力します。

c) [Groups] タブで、[+] をクリックしてプロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

d) [Group Maps] タブで、[Provider Group Map DN] を入力します。オプションで、[Roles] と [Locales] を追加します。

（注） プロバイダー グループ マップの識別名に特殊文字を使用しないでください。

ステップ 3 [Authentication Domains] で、ネイティブまたはコンソール デフォルト ドメインを設定、追加、または削除します。

ステップ 4 [Native(Default)] をクリックして、次の手順を実行します。

a) [Default Behavior for Remote Users] を選択します。

b) [Web Session Refresh Period (Seconds)] に、更新要求間の最大許容時間を入力します。
Web セッションが時間制限を超えると、Cisco UCS Central は Web セッションを非アクティブと見なしますが、そのセッションを終了することはありません。

60 ～ 172800 秒の間で指定します。デフォルトは 600 秒です。

c) [Web Session Timeout (Seconds)] に、最後の更新要求後の最大経過時間を入力します。Web セッションが時間制限を超えると、Cisco Cisco UCS Central は、Web セッションが終了したと見なし、自動的に Web セッションを終了します。
60 ～ 172800 秒の間で指定します。デフォルト値は 7200 秒です。

d) [Enabled] または [Disabled] を、[Authentication] に選択します。

e) [Enabled] を選択した場合は、[Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

f) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[Provider Group] ドロップダウン リストから、関連するプロバイダー グループを選択できます。

ステップ 5 [Console (Default)] をクリックします。

a) [Enabled] または [Disabled] を、[Authentication] に選択します。

b) [Enabled] を選択した場合は、[Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

c) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[Provider Group] ドロップダウン リストから、関連するプロバイダー グループを選択できます。

ステップ 6 [+] をクリックして、新しい認証ドメインを追加します。

a) 認証ドメインの名前を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。スペースは使用できません。特殊文字では、-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）が使用できます。この名前は、いったん保存した後では変更できません。

RADIUS を使用したシステムでは、認証ドメイン名はユーザ名の一部と見なされます。したがって、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。Cisco UCS ではフォーマット用として 5 文字が予約されているため、ドメイン名とユーザ名を合わせて合計 27 文字を超える名前は使用できません。

b) [Web Session Refresh Period (Seconds)] を入力します。

c) [Web Session Timeout (Seconds)] を入力します。

d) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[Provider Group] ドロップダウン リストから、関連するプロバイダー グループを選択できます。

ステップ 7 [Save] をクリックします。
認証ドメインを作成したら、必要に応じて、設定を編集できます。また、ごみ箱をクリックして、選択した認証ドメインを削除することもできます。