リモート認証

認証サービス

Cisco UCS では、ユーザ ログインを認証するための次の 2 つの方法をサポートしています。

- ローカル ユーザ認証：ローカルの Cisco UCS Manager に存在するユーザ アカウントを使用します。
- リモート ユーザ認証：次のプロトコルのいずれかを使用します。
  - LDAP
  - RADIUS
  - TACACS+

リモート認証プロバイダに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダを作成して、Cisco UCS Manager がそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Manager にローカルに設定したり、リモート認証サーバに設定することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Manager GUIと Cisco UCS Manager CLIで表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Cisco UCS Manager で作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を Cisco UCS Manager で使用される名前と一致させることが必要です。ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

リモート認証プロバイダのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Cisco UCS Manager へのログインに使用する各リモート認証プロバイダに Cisco UCS 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

（注） この手順は、LDAP グループ マッピングを使用してロールとロケールを割り当てる LDAP 設定では必要ありません。

ユーザがログインすると、Cisco UCS Manager は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが有効である場合は、そのユーザに割り当てられているロールとロケールをチェックします。

次の表は、Cisco UCS でサポートしているリモート認証プロバイダのユーザ属性要件を比較したものです。

表 *1*: リモート認証プロバイダによるユーザ属性の比較

認証プロバイダ	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	グループ マッピング使用時は不要 グループ マッピング不使用時は任意	オプション。次のいずれかを実行するよう選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定する。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成する。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します サンプルの OID が次のセクションに示されています。
RADIUS	任意	オプション。次のいずれかを実行するよう選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用する。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成する。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダ	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	必須です。スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。 `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。 cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコ デバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

Two-Factor Authentication

Cisco UCS Manager では、リモート ユーザのログインに二要素認証を使用して、アカウントのログインのセキュリティ レベルを高めています。二要素認証のログインでは、パスワード

フィールドでユーザ名、トークン、パスワードの組み合わせが必要です。PIN、証明書、またはトークンを指定できます。

二要素認証では、認証アプリケーションを使用します。このアプリケーションはトークン サーバを保持して、ログイン プロセス中にユーザ用のワンタイム トークンを生成し、パスワードを AAA サーバに保存します。ベンダー固有の属性を取得する要求がトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバが AAA サーバと統合されていることを想定するので、AAA サーバに要求を転送します。パスワードとトークンは、AAA サーバによって同時に検証されます。ユーザは、AAA サーバで設定されているのと同じ順序で、トークンとパスワードを入力する必要があります。

二要素認証は、RADIUS または TACACS+ プロバイダ グループを指定認証ドメインに関連付け、それらのドメインで二要素認証を有効にすることによってサポートされます。二要素認証では IPM をサポートしておらず、また認証レルムが LDAP、local、または none に設定されている場合はサポートされません。

Web セッションの更新および Web セッションのタイムアウト期限

[Web Session Refresh Period] は、Cisco UCS Manager GUI の Web セッションに対する更新要求間隔に許容される最大時間です。[Web Session Timeout] は、最後の更新要求後から Cisco UCS Manager GUI の Web セッションが非アクティブになるまでの最大経過時間です。

[Web Session Refresh Period] を 60 秒より長く、最大で 172800 秒まで長くすると、トークンとパスワードを繰り返し生成および再入力する必要があるセッション タイムアウトが頻繁に起きるのを避けることができます。デフォルト値は、二要素認証が有効の場合は 7200 秒、二要素認証が有効でない場合は 600 秒です。

[Web Session Timeout Period] には 300 から 172800 の間の値を指定できます。デフォルト値は、二要素認証が有効の場合は 8000 秒、二要素認証が有効でない場合は 7200 秒です。

LDAP プロバイダとグループ

ネストされた LDAP グループ

LDAP グループを別のグループのメンバーとして追加し、グループをネストすることで、グループ メンバーのアカウントを統合してレプリケーション トラフィックを削減できます。Cisco UCS Manager リリース 2.1(2) 以降では、LDAP グループ マップで定義されている別のグループに含まれるネストされた LDAP グループを検索できます。

（注） ネストされた LDAP の検索サポートは 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。

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きに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 のみを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

Cisco UCS Manager のグループ マップでサブグループを常に作成する必要がなくなります。

LDAP グループ ルール

LDAP グループ ルールによって、ユーザ ロールおよびロケールをリモート ユーザに割り当てるときに Cisco UCS が LDAP グループを使用するかどうかが決まります。

LDAP プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。

（注） ユーザ ログインは LDAP ユーザの userDn が 255 文字を超えると失敗します。

ステップ 4 [Save Changes] をクリックします。

次のタスク

LDAP プロバイダを作成します。

LDAP プロバイダの作成

Cisco UCS Manager は最大 16 の LDAP プロバイダーをサポートします。

始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

- LDAP サーバで、次のいずれかの設定を行います。
  - LDAP グループを設定します。LDAP グループには、ユーザのロールとロケール情報が含まれています。
  - Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性についてLDAPスキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、CiscoAVPair 属性などのカスタム属性を作成します。

    シスコの LDAP の実装では、Unicode タイプの属性が必要です。

    CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します
  - クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが2つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager で使用される仮想 IPv4 または IPv6 アドレスからではありません。
- セキュア通信を使用するには、Cisco UCS Manager で LDAP サーバのルート認証局（CA）の証明書を含むトラスト ポイントを作成します。
- LDAP プロバイダーを変更したり、追加または削除したりする必要がある場合は、ドメイン認証レルムをローカルに変更し、プロバイダーに変更を加えた後、ドメイン認証レルムを LDAP に戻します。

注目 特殊文字が含まれる LDAP リモート ユーザ名では、バージョン 2.2(3a) 以降を実行しているシステムにログインできません。ユーザがログインできない理由は、Nexus OS では特殊文字 !、%、^ をユーザ名に対してサポートしていないという制限があるためです。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] エリアで、[Create LDAP Provider] をクリックします。

ステップ 5 ウィザードの [Create LDAP Provider] ページで、すべてのフィールドに適切な LDAP サービス情報を入力します。

a) 使用する LDAP サービスに関する情報を使用して、次のフィールドに値を入力します。

名前	説明
[Hostname/FDQN (or IP Address)] フィールド	LDAP プロバイダが存在するホスト名または IP アドレス（IPv4 または IPv6）。SSL が有効の場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていない、または DNS 管理が**ローカル**に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Order] フィールド	Cisco UCS でユーザーの認証にこのプロバイダーを使用する順序。 1 ～ 16 の範囲の整数を入力します。または、この Cisco UCS ドメインで定義されている他のプロバイダーに基づいて、次に使用できる順序を Cisco UCS で自動的に割り当てる場合には、**[lowest-available]** または **[0]**（ゼロ）を入力します。
[Bind DN] フィールド	ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
[Base DN] フィールド	リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から CN=username の長さを差し引いた長さに設定することができます。ここで、username は、LDAP 認証を使用して Cisco UCS Manager へアクセスしようとしているリモート ユーザの識別に使用されます。 デフォルトのベース DN が LDAP の [General] タブで設定されていない場合は、この値が必要です。

名前	説明
[Port] フィールド	Cisco UCS が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリアテキストで送信されます。 LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。 オンにした場合、ポートを 636 に変更せずに、389 のままにしてください。Cisco UCS は SSL 用のポート 636 で TLS セッションのネゴシエーションを行いますが、最初の接続は暗号化されずに 389 で開始されます。
[Filter] フィールド	LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。 デフォルトのフィルタが LDAP の [General] タブで設定されていない場合は、この値が必要です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP スキーマを拡張しない場合、既存の未使用 LDAP 属性を Cisco UCS ロールとロケールに設定できます。あるいは、属性 ID「**1.3.6.1.4.1.9.287247.1**」を持つ、CiscoAVPair という名前の属性をリモート認証サービスに作成できます。 デフォルトの属性が LDAP の [General] タブで設定されていない場合は、この値が必要です。
[Password] フィールド	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Password] フィールド	確認のための LDAP データベース パスワードの再入力。

名前	説明
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して LDAP の [General] で指定したタイムアウト値を使用します。デフォルトは 30 秒です。
[Vendor] オプション ボタン	ユーザが使用する LDAP ベンダー。次のいずれかになります。 • [Open Ldap]：LDAP プロトコルのオープン ソース実装。 • [MS AD]：Microsoft Active Directory。

b) [Next] をクリックします。

ステップ 6 ウィザードの [LDAP Group Rule] ページで、すべてのフィールドに適切な LDAP グループ ルール情報を入力します。

（注） ロールとロケールの割り当ては累積されます。ユーザが複数のグループに含まれる、または LDAP 属性で指定されたロールやロケールがある場合、Cisco UCS はそのユーザに対し、それらのグループや属性のいずれかにマッピングされたすべてのロールとロケールを割り当てます。

次のタスク

単一の LDAP データベースが関係する実装の場合、認証サービスとして LDAP を選択します。

複数の LDAP データベースが関係する実装の場合、LDAP プロバイダー グループを設定します。

LDAP プロバイダの LDAP グループ ルールの変更

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [LDAP Providers] を展開し、グループ ルールを変更する LDAP プロバイダーを選択します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [LDAP Group Rules] 領域で、次のフィールドに値を入力します。

名前	説明
[Group Authorization] フィールド	リモートユーザを認証し、ユーザ ロールとロケールを割り当てる際に、Cisco UCS が LDAP グループも検索するかどうか。次のいずれかになります。 • [Disable]：Cisco UCS はどの LDAP グループにもアクセスしません。 • [Enable]：Cisco UCS はこの Cisco UCS ドメイン 内でマッピングされたすべての LDAP グループを検索します。リモート ユーザが見つかると、Cisco UCS は関連する LDAP グループ マップでその LDAP グループに対して定義されているユーザ ロールとロケールを割り当てます。 （注） ロールとロケールの割り当ては累積されます。ユーザが複数のグループに含まれる、または LDAP 属性で指定されたロールやロケールがある場合、Cisco UCS はそのユーザに対し、それらのグループや属性のいずれかにマッピングされたすべてのロールとロケールを割り当てます。
[Group Recursion] フィールド	マッピングされたグループとその親グループの両方を Cisco UCS が検索するかどうか。次のいずれかになります。 • [Non Recursive]：Cisco UCS はこの Cisco UCS ドメイン でマッピングされたグループだけを検索します。どのグループにもユーザの認証プロパティを明示的に設定するユーザが含まれない場合、Cisco UCS はデフォルト設定を使用します。 • [Recursive]：Cisco UCS はマッピングされた各グループとその親グループでユーザの認証プロパティを検索します。これらのプロパティは累積的です。したがって、Cisco UCS は明示的な認証プロパティ設定を検出した各グループについて、それらの設定を現在のユーザに適用します。それ以外の場合は、デフォルト設定が使用されます。
[Target Attribute] フィールド	Cisco UCS が LDAP データベースのグループ メンバーシップを決定するのに使用する属性。 サポートされるストリングの長さは 63 文字です。デフォルトの文字列は「**memberOf**」です。

名前	説明
[Use Primary Group] フィールド	メンバーシップの確認のための LDAP グループ マップとしてプライマリ グループを設定できるかどうかを判断するために、Cisco UCS で使用される属性。このオプションを使用すると、Cisco UCS Manager はユーザのプライマリグループ メンバーシップをダウンロードして検証できます。

ステップ 6 [Save Changes] をクリックします。

LDAP プロバイダの削除

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。
ステップ 3 [LDAP Providers] を展開します。
ステップ 4 削除する LDAP プロバイダーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

LDAP グループ マッピング

LDAP グループ マッピングを使用すると、LDAP ユーザ オブジェクトのロールまたはロケール情報を定義する必要がなくなります。LDAP データベースへのアクセスを制限する LDAP グループを使用している組織にログインする際、UCSM はグループ メンバーシップ情報を使用してロールとロケールを LDAP ユーザに割り当てます。

ユーザが Cisco UCS Manager にログインすると、LDAP グループ マップからそのユーザのロールとロケールに関する情報が取得されます。ロールとロケールの条件がポリシー内の情報と一致すれば、アクセス権が付与されます。リリース バージョンに応じて、Cisco UCS Manager では最大 28 個、128 個、または 160 個の LDAP グループ マップをサポートしています。

（注） Cisco UCS Manager リリース 3.1 (1) では最大 128 個の LDAP グループ マップ、リリース 3.1 (2) 以降では最大 160 個の LDAP グループ マップがサポートされます。

Cisco UCS Manager でローカルに構成したロールとロケールの定義が、LDAP ディレクトリの変更に応じて自動的に更新されることはありません。LDAP ディレクトリ内の LDAP グループを削除または名前変更するときには、その変更が反映されるよう Cisco UCS Manager も更新する必要があります。

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

- ロールのみ
- ロケールのみ
- ロールとロケールの両方

たとえば、特定の場所のサーバ管理者グループを表す LDAP グループがあるとします。LDAP グループ マップには、サーバ プロファイルやサーバ機器などのユーザ ロールが含まれていることもあります。特定の場所のサーバ管理者へのアクセスを制限するために、ロケールに特定のサイト名を設定することができます。

（注） Cisco UCS Manager には、すぐに使用可能な多くのユーザ 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。LDAP プロバイダ グループをロケールにマッピングするには、カスタム ロケールを作成する必要があります。

LDAP グループ マップの作成

始める前に

- LDAP サーバで LDAP グループを作成します。
- LDAP サーバで LDAP グループの識別名を設定します。
- Cisco UCS Manager でロケールを作成します（任意）。
- Cisco UCS Manager でカスタム ロールを作成します（任意）。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [LDAP Group Maps] を右クリックし、[Create LDAP Group Map] を選択します。

ステップ 4 [Create LDAP Group Map] ダイアログボックスで、必要に応じてすべての LDAP グループ マップ情報を指定します。

重要 **[LDAP Group DN] フィールド** で指定する名前は、LDAP データベース内の名前と一致する必要があります。

（注） [LDAP Group DN] フィールドに特殊文字を使用する場合は、特殊文字の前にエスケープ文字 \（シングル バックスラッシュ）を付ける必要があります。

次のタスク

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。
ステップ 3 [LDAP Group Maps] を展開します。
ステップ 4 削除する LDAP グループ マップを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

RADIUS プロバイダ

RADIUS プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

（注） RADIUS 認証では、Password Authentication Protocol（PAP）を使用します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[User Management]** > **[RADIUS]** の順に選択します。
ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。
ステップ 4 [Save Changes] をクリックします。

次のタスク

RADIUS プロバイダーを作成します。

RADIUS プロバイダの作成

Cisco UCS Manager は最大 16 の RADIUS プロバイダーをサポートします。

Before you begin

RADIUS サーバで、次の設定を行います。

- Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性について RADIUS スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の RADIUS 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、cisco-avpair 属性などのカスタム属性を作成します。

  シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。

  次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**

ステップ 3 [Create RADIUS Provider] ダイアログボックスで、該当するすべての RADIUS サービス情報を指定します。

Note IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 4 [Save Changes] をクリックします。

What to do next

単一の RADIUS データベースが関係する実装の場合、RADIUS をプライマリ認証サービスとして選択します。

複数の RADIUS データベースが関係する実装の場合、RADIUS プロバイダー グループを設定します。

RADIUS プロバイダの削除

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[User Management]** > **[RADIUS]** の順に選択します。
ステップ 3 削除する RADIUS プロバイダーを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

TACACS+ プロバイダ

TACACS+ プロバイダのプロパティの設定

（注） このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[User Management]** > **[TACACS+]** の順に選択します。
ステップ 3 [Properties] 領域で、**[Timeout]** フィールドに値を入力します。
ステップ 4 [Save Changes] をクリックします。

次のタスク

TACACS+ プロバイダを作成します。

TACACS+ プロバイダの作成

Cisco UCS Manager は最大 16 の TACACS+ プロバイダーをサポートします。

Before you begin

TACACS+ サーバで、次の設定を行います。

- cisco-av-pair 属性を作成します。既存の TACACS+ 属性は使用できません。

  cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。

  次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**

ステップ 3 [General] タブの [Actions] 領域で、[Create TACACS+ Provider] をクリックします。

ステップ 4 [Create TACACS+ Provider] ダイアログボックスで、次の手順を実行します。

a) 必要に応じてすべてのフィールドに TACACS+ サービス情報を入力します。

Note IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

b) [OK] をクリックします。

ステップ 5 [Save Changes] をクリックします。

What to do next

単一の TACACS+ データベースが関係する実装の場合、TACACS+ をプライマリ認証サービスとして選択します。

複数の TACACS+ データベースが関係する実装の場合、TACACS+ プロバイダー グループを設定します。

TACACS+ プロバイダの削除

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[User Management]** > **[TACACS+]** の順に選択します。
ステップ 3 削除する TACACS+ プロバイダーを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

プライマリ認証サービス

コンソール認証サービスの選択

Before you begin

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダを作成する必要はありません。

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**
ステップ 3 [Native Authentication] をクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Console Authentication] 領域で、次のフィールドに入力します。

名前	説明
[Realm] フィールド	コンソールにログインするユーザが認証される方法。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン内でローカルに定義する必要があります。 • [Radius]：この Cisco UCS ドメインに対して指定された Radius サーバでユーザを定義する必要があります。 • [Tacacs]：この Cisco UCS ドメインに対して指定された Tacacs サーバでユーザを定義する必要があります。 • [Ldap]：この Cisco UCS ドメインに対して指定された LDAP サーバでユーザを定義する必要があります。 • **[None]**：ユーザ アカウントがこの Cisco UCS ドメインにローカルである場合、ユーザがコンソールにログインするときにパスワードは必要ありません。
[Provider Group]	ユーザがコンソールにログインするときに認証に使用するプロバイダー グループ。 **Note** **[Provider Group]** は、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
Two Factor Authentication	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスをオンにすると、コンソールは、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするように求めます。

ステップ 6 [Save Changes] をクリックします。

デフォルト認証サービスの選択

始める前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダを作成する必要はありません。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

ステップ 3 [Native Authentication] をクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [Default Authentication] 領域で、次のフィールドに入力します。

名前	説明
[Realm] ドロップダウン リストt	リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン 内でローカルに定義する必要があります。 • **[Radius]**：この Cisco UCS ドメイン に関して指定された Radius サーバでユーザ アカウントを定義する必要があります。 • **[Tacacs]**—この Cisco UCS ドメインに関して指定された TACACS サーバでユーザ アカウントを定義する必要があります。 • **[Ldap]**—この Cisco UCS ドメイン に関して指定された LDAP サーバでユーザ アカウントを定義する必要があります。 • **[None]**—ユーザ アカウントがこの Cisco UCS ドメイン にローカルである場合、ユーザがリモートでログインするときにパスワードは必要ありません。
[Provider Group]	リモート ログイン中にユーザを認証するために使用するデフォルト プロバイダー グループ。 （注） [Provider Group] ドロップダウンは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。

名前	説明
Web Session Refresh Period (sec)	Web クライアントが Cisco UCS Manager に接続する際は、Web セッションをアクティブ状態に維持するために、クライアントは Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションを強制終了することはしません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 600 秒、二要素認証が有効の場合は 7200 秒です。
Web Session Timeout (sec)	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。
[Two Factor Authentication] チェックボックス	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスを選択すると、Cisco UCS Manager と KVM Launch Manager では、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするよう求めます。[Web セッションの更新期間（Web Session Refresh Period）] が期限切れになるまでに 60 秒ある場合は、新しいトークンを生成し、そのトークンとパスワードを入力してセッションを続行する必要があります。 （注） 二要素要素認証を有効にして、デフォルト設定を保存すると、デフォルトの **Web Session Refresh Period (sec)**が 7200 に、デフォルトの **Web Session Timeout (sec)** が 8000 に変更されます。

ステップ 6 [Save Changes] をクリックします。

リモート ユーザのロール ポリシー

デフォルトでは、Cisco UCS Manager でユーザ ロールが設定されていない場合は、LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Cisco UCS Manager にログインしているすべてのユーザに読み取り専用アクセス権が付与されます。セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致するユーザへのアクセスを制限するのが望ましい場合があります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限しません。その他のユーザ ロールが Cisco UCS Manager で定義されていない限り、読み取り専用アクセス権がすべてのユーザに付与されます。

これはデフォルトの動作です。

no-login

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限します。リモート認証システムにユーザ ロールが割り当てられていない場合、アクセスは拒否されます。

リモート ユーザのロール ポリシーの設定

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

ステップ 3 [Native Authentication] をクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 **[Role Policy for Remote Users]** フィールドでは、ユーザがログインを試行した際に、リモート認証プロバイダーが認証情報を伴うユーザ ロールを提供しない場合にどのように処理するかを決定するために、次のオプション ボタンのいずれかをクリックします。

- [No Login]：ユーザ名とパスワードが正しい場合でも、ユーザはシステムにログインできません。
- [Assign Default Role]：ユーザは、読み取り専用ユーザ ロールでログインできます。

ステップ 6 [Save Changes] をクリックします。

マルチ認証サービスの設定

マルチ認証サービス

次の機能の実装により、Cisco UCS が複数の認証サービスを使用するよう設定することができます。

- プロバイダ グループ
- 認証ドメイン

プロバイダ グループ

プロバイダ グループは、認証プロセス中に Cisco UCS がアクセスするプロバイダのセットです。プロバイダ グループ内のすべてのプロバイダが、ユーザの認証に Cisco UCS プロバイダが使用する順にアクセスされます。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 Manager 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。

Cisco UCS Manager では、最大 16 のプロバイダ グループを作成でき、グループごとに最大 8 つのプロバイダを含めることができます。

LDAP プロバイダ グループの作成

LDAP プロバイダー グループを作成すると、複数の LDAP データベースを使用して認証できます。

始める前に

1 つ以上の LDAP プロバイダーを作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [LDAP Provider Groups] を右クリックし、[Create LDAP Provider Group] を選択します。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 4 [Create LDAP Provider Group] ダイアログボックスで、適切なすべての LDAP プロバイダー グループ情報を指定します。

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

LDAP プロバイダ グループの削除

始める前に

認証設定からプロバイダー グループを削除します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**
ステップ 3 [LDAP Provider Groups] を展開します。
ステップ 4 削除する LDAP プロバイダー グループを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

RADIUS プロバイダ グループの作成

RADIUS プロバイダー グループを作成すると、複数の RADIUS データベースを使用して認証できます。

始める前に

1 つ以上の RADIUS プロバイダーを作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**
ステップ 3 [RADIUS Provider Groups] を右クリックし、[Create RADIUS Provider Group] を選択します。
ステップ 4 [Create RADIUS 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。

この名前には、1 ～ 127 の ASCII 文字を使用できます。

b) **[RADIUS プロバイダー]** テーブル で、グループに含める 1 つ以上のプロバイダーを選択します。
c) **[>>]** ボタン をクリックして、[Included Providers] テーブル にプロバイダーを追加します。

[<<] ボタン を使用して、グループからプロバイダーを排除できます。

d) （任意）RADIUS プロバイダーがプロバイダーを認証する順序を変更するには、[Included Providers] リストの [Move Up] または [Move Down] の矢印を使用します。
e) 必要なすべてのプロバイダーをプロバイダー グループに追加した後、[OK] をクリックします。

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

RADIUS プロバイダ グループの削除

別の認証設定がプロバイダー グループを使用している場合、そのプロバイダー グループを削除することはできません。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**
ステップ 3 [RADIUS Provider Groups] を展開します。
ステップ 4 削除する RADIUS プロバイダー グループを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

TACACS+ プロバイダー グループの作成

TACACS+ プロバイダー グループを作成すると、複数の TACACS+ データベースを使用して認証できます。

始める前に

1 つ以上の TACACS+ プロバイダーを作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**
ステップ 3 [TACACS+ Provider Groups] を右クリックし、[Create TACACS+ Provider Group] を選択します。
ステップ 4 [Create TACACS+ Provider Group] ダイアログボックスで、必要に応じてすべての TACACS+ プロバイダーのグループ情報を指定します。

TACACS+ プロバイダー グループの削除

別の認証設定がプロバイダー グループを使用している場合、そのプロバイダー グループを削除することはできません。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**
ステップ 3 [TACACS+ Provider Groups] を展開します。
ステップ 4 削除する TACACS+ プロバイダー グループを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

認証ドメイン

Cisco UCS Manager では、複数の認証システムを活用するために認証ドメインを使用しています。各認証ドメインはログイン時に指定および設定できます。これを行わない場合、Cisco UCS Manager はデフォルトの認証サービス設定を使用します。

最大 8 個の認証ドメインを作成できます。各認証ドメインは、Cisco UCS Manager 内のプロバイダ グループと領域に関連付けられています。プロバイダ グループを指定しないと、Cisco UCS Manager では領域内のすべてのサーバを使用します。

認証ドメインの作成

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**
ステップ 3 [Authentication Domains] を右クリックし、[Create a Domain] を選択します。
ステップ 4 [Create a Domain] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name]	ドメインの名前。 この名前には、1～16文字の英数字を使用できます。スペースや(ハイフン)、_(アンダースコア)以外の特殊文字は使用できません。（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。 （注） リモート認証プロトコルを使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、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に5文字が挿入されるため、ドメイン名とユーザ名の合計が27文字を超える場合には認証が失敗します。
Web Session Refresh Period (sec)	Webクライアントが Cisco UCS Manager に接続する際は、Webセッションをアクティブ状態に維持するために、クライアントはCisco UCS Managerに更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Managerは Webセッションを非アクティブであると見なしますが、セッションを強制終了することはしません。 60～172800の整数を指定します。デフォルト値は、二要素認証が有効でない場合は600秒、二要素認証が有効の場合は7200秒です。 （注） [Web Session Refresh Period] に設定する秒数は、[Web Session Timeout] に設定する秒数未満である必要があります。[Web Session Refresh Period] に [Web Session Timeout] と同じ値を設定しないでください。

名前	説明
Web Session Timeout (sec)	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。
Realm	このドメインのユーザに適用される認証プロトコル。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン内でローカルに定義する必要があります。 • [Radius]：この Cisco UCS ドメインに対して指定された Radius サーバでユーザを定義する必要があります。 • [Tacacs]：この Cisco UCS ドメインに対して指定された Tacacs サーバでユーザを定義する必要があります。 • [Ldap]：この Cisco UCS ドメインに対して指定された LDAP サーバでユーザを定義する必要があります。
Provider Group	リモート ログイン中にユーザを認証するために使用するデフォルト プロバイダ グループ。 （注） [Provider Group] ドロップダウン リストは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
Two Factor Authentication	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスを選択すると、Cisco UCS Manager と KVM Launch Manager では、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするよう求めます。[Web セッションの更新期間（Web Session Refresh Period）] が期限切れになるまでに 60 秒ある場合は、新しいトークンを生成し、そのトークンとパスワードを入力してセッションを続行する必要があります。

ステップ 5 [OK] をクリックします。