「Configuring Authentication」

この章は、次の項で構成されています。

- 認証プロトコルと方法，1 ページ
- リモート認証プロバイダーに関するガイドラインおよび推奨事項，2 ページ
- リモート認証プロバイダーにおけるユーザ属性，2 ページ
- 二要素認証，4 ページ
- LDAP グループ ルール，5 ページ
- ネストされた LDAP グループ，5 ページ
- LDAP プロバイダーの設定，6 ページ
- RADIUS プロバイダーの設定，13 ページ
- TACACS+ プロバイダーの設定，15 ページ
- マルチ認証サービスの設定，17 ページ
- プライマリ認証サービスの選択，24 ページ

認証プロトコルと方法

Cisco UCS では、ユーザ ログインを認証するための次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ーに関するガイドラインおよび推奨事項

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ーを作成して、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 にローカルに存在するか、またはリモート認証サーバに存在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ーにおけるユーザ属性

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ーに 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. ユーザが検証されると、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。

次の表に、Cisco UCS によってサポートされるリモート認証プロバイダーのユーザ属性要件の比較を示します。

表 *1*：リモート認証プロバイダーによるユーザ属性の比較

認証プロバイダー	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します。 • 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は、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。

認証プロバイダー	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
```

二要素認証

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ために、リクエストがトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバがリクエストを AAA サーバに転送できるように、トークン サーバを AAA サーバと統合することを要求します。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+ プロバイダー 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、二要素認証がイネーブルの場合は 7200 秒、二要素認証がイネーブルでない場合は 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、二要素認証がイネーブルの場合は 8000 秒、二要素認証がイネーブルでない場合は 7200 秒です。

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。

ネストされた LDAP グループ

LDAP グループを他のグループおよびネスト グループのメンバーとして追加し、メンバー アカウントを統合してトラフィックの重複を減らすことができます。Cisco UCS Manager のリリース 2.1(2) 以降では、LDAP グループ マップで定義された他のグループ内にネストされた 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 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。

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 プロバイダーの設定

LDAP プロバイダー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。

はじめる前に

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Cisco UCS Manager では、最大 16 の LDAP プロバイダーがサポートされます。

はじめる前に

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をユーザに対して設定します。 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は、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 により使用されている仮想 IPv4 または IPv6 アドレスではありません。
- セキュアな通信を使用する場合は、LDAP サーバのルート認証局（CA）の証明書が格納されたトラスト ポイントを Cisco UCS Manager で作成します。
- 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。
- Active Directory バインド識別名の属性を定義する際に次の表にある特殊文字を使用する場合、対応する文字の 16 進数値の後にバックスラッシュ（\）を使用して、特殊文字をエスケープ文字で置き換える必要があります。

特殊文字	説明	16 進数値
,	カンマ	0x2C
+	プラス記号	0x2B

特殊文字	説明	16 進数値
"	二重引用符	0x22
\	バックスラッシュ	0x5C
<	左角ブラケット	0x3C
>	右角ブラケット	0x3E
;	セミコロン	0x3B
LF	改行	0x0A
CR	復帰	0x0D
=	等号	0x3D
/	スラッシュ	0x2F

https://msdn.microsoft.com/en-us/library/aa366101 に特殊文字をエスケープ文字と 16 進数値に置き換える方法についての説明があります。

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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。

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。

次の作業

単一の LDAP データベースが関係する実装の場合は、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は、LDAP プロバイダー グループを設定します。

LDAP プロバイダーの LDAP グループ ルールの変更

手順

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

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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	Cisco UCS が、ユーザ ロールとロケールを認証してリモート ユーザに割り当てるときに、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 UCS は LDAP グループにアクセスしません。 • [Enable]：Cisco UCS は、この Cisco UCS ドメインに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 ユーザが検出されると、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属している場合や LDAP 属性で指定されたロールまたはロケールを持っている場合、Cisco UCS は、それらのグループまたは属性のいずれかにマップされているすべてのロールとロケールをそのユーザに割り当てます。

名前	説明
[Group Recursion] フィールド	Cisco UCS が、マッピングされたグループとそれらの親グループの両方を検索するかどうか。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。ユーザが属するいずれのグループでもユーザの認証プロパティが明示的に設定されていない場合、Cisco UCS はデフォルトの設定を使用します。 • [Recursive]：Cisco UCS は、マップされた各グループおよびそのすべて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あるため、Cisco UCS は、明示的な認証プロパティ設定を備えたグループを検出すると、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 データベース内のグループ メンバーシップを判別するために使用する属性。 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。
[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 プロバイダーの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。
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 マッピングにより、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 にログインする際、LDAP グループ マップはユーザのロールとロケールに関する情報を取り出します。ロールとロケールの基準がポリシーの情報と一致する場合、アクセスが許可されます。Cisco UCS Manager は、リリース バージョンに応じて、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。

Cisco UCS Manager でローカルに設定したロールとロケール定義に対しては、LDAP ディレクトリに対する変更に基づいた自動更新は行われません。LDAP ディレクトリ内の LDAP グループの削除や名前変更を行う場合は、その変更に合わせて 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 にはすぐに使用できるユーザ 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 プロバイダー 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

はじめる前に

- 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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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][LDAP Group DN] フィールド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させる必要があります。

（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。

次の作業

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] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。
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 プロバイダーの設定

RADIUS プロバイダー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。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[User Management] > [RADIUS] を展開します。
ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。
ステップ 4 [Save Changes] をクリックします。

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Cisco UCS Manager では、最大 16 の RADIUS プロバイダーがサポートされます。

はじめる前に

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をユーザに対して設定します。 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 により使用されている仮想 IP アドレスではありません。

手順

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

ステップ 2 [Admin] タブの [All] > [User Management] > [RADIUS] を展開します。

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。

（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 [Save Changes] をクリックします。

次の作業

単一の RADIUS データベースが関係する実装の場合は、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は、RADIUS プロバイダー グループを設定します。

RADIUS プロバイダーの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[User Management] > [RADIUS] を展開します。
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+ プロバイダーの設定

TACACS+ プロバイダー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。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[User Management] > [TACACS+] を展開します。
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。

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Cisco UCS Manager では、最大 16 の TACACS+ プロバイダーがサポートされます。

はじめる前に

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 により使用されている仮想 IP アドレスではありません。

手順

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

ステップ 2 [Admin] タブの [All] > [User Management] > [TACACS+] を展開します。

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。

（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。

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。

次の作業

単一の TACACS+ データベースが関係する実装の場合は、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は、TACACS+ プロバイダー グループを設定します。

TACACS+ プロバイダーの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[User Management] > [TACACS+] を展開します。
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。

マルチ認証サービスの設定

マルチ認証サービス

次の機能を実装して、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。

- プロバイダー グループ
- 認証ドメイン

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 がアクセスするプロバイダーのセットです。プロバイダー グループ内のすべてのプロバイダーが、ユーザの認証に Cisco UCS プロバイダー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、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。

LDAP プロバイダー 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。

（注） 単一の LDAP データベースを使用した認証では、LDAP プロバイダー グループを設定する必要はありません。

はじめる前に

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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。

次の作業

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 プロバイダー グループの削除

はじめる前に

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [LDAP] を展開します。

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 プロバイダー 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。

（注） 単一の RADIUS データベースを使用した認証では、RADIUS プロバイダー グループを設定する必要はありません。

はじめる前に

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [RADIUS] を展開します。

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 Providers] 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削除できます。

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。

次の作業

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 プロバイダー グループの削除

認証設定で使用されているプロバイダー グループは削除できません。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [RADIUS] を展開します。
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。

（注） 単一の TACACS+ データベースを使用した認証では、TACACS+ プロバイダー グループを設定する必要はありません。

はじめる前に

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] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [TACACS+] を展開します。
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

認証設定で使用されているプロバイダー グループは削除できません。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [TACACS+] を展開します。
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 内のプロバイダー グループと領域に関連付けられています。プロバイダー 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] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [User Management] > [Authentication] を展開します。
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
名前	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。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（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 はフォーマットに 5 文字を挿入するため、ドメイン名とユーザ名を合わせた合計が 27 文字を超えると、認証は失敗します。
Web Session Refresh Period (sec)	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、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、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 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。
Web Session Timeout (sec)	最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 8000 秒です。

名前	説明
レルム	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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに対して指定された LDAP サーバで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 プロバイダー 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。
二要素認証	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 Session Refresh Period] が期限切れになるまでに 60 秒ある場合は、ユーザ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。

プライマリ認証サービスの選択

コンソール認証サービスの選択

はじめる前に

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、最初にプロバイダーを作成する必要はありません。

手順

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

ステップ 2 [Admin] タブの [All] > [User Management] > [Authentication] を展開します。

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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに対して指定された LDAP サーバで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 ドメインに対してローカルである場合は、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。

名前	説明
[Provider Group] ドロップダウン リスト	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。 （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。
二要素認証	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

はじめる前に

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、最初にプロバイダーを作成する必要はありません。

手順

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

ステップ 2 [Admin] タブの [All] > [User Management] > [Authentication] を展開します。

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	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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された LDAP サーバで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 ドメインに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。
[Provider Group] ドロップダウン リスト	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。
Web Session Refresh Period (sec)	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、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、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 7200 秒です。

名前	説明
Web Session Timeout (sec)	最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 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 Session Refresh Period] が期限切れになるまでに 60 秒ある場合は、ユーザ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） 二要素認証をイネーブルにして設定を保存した後、デフォルトの Web Session Refresh Period (sec) は 7200 に、デフォルトの Web Session Timeout (sec)は 8000 に変わります。

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] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [User Management] > [Authentication] を展開します。

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。