User Management

この章は、次の内容で構成されています。

- Cisco UCS Central ユーザ アカウント，1 ページ
- ロールベース アクセス コントロール，16 ページ
- ユーザ ロケール，24 ページ
- ユーザ組織，29 ページ

Cisco UCS Central ユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。 最大で 128 個のユーザ アカウントを各 Cisco UCS Central ドメインで設定できます。 各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

ユーザ アカウントは、SSH 公開キーを付けて設定できます。 公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

管理者アカウント

Cisco UCS Central には、admin アカウントがあります。 管理者アカウントはデフォルト ユーザ アカウントで、変更や削除はできません。 このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。 管理者アカウントを非アクティブに設定することはできません。

ローカル admin ユーザは、認証がリモートに設定されている場合でも、フェールオーバーのためにログインできます。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザ アカウントは、Cisco UCS Central ユーザ データベースを介して認証され、admin 権限または aaa 権限を持つユーザがイネーブルまたはディセーブルにできます。 ローカル ユーザ アカウントがディセーブルになっている場合、ユーザはログインできません。 無効ローカル ユーザ アカウントの設定の詳細は、データベースによって削除されません。 無効ローカルユーザアカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存のコンフィギュレーションで再びアクティブになります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントは、LDAP を介して認証される Cisco UCS Central ユーザ アカウントです。 Cisco UCS ドメインは、LDAP、RADIUS および TACACS+ をサポートしています。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。 ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。

ユーザ名の作成に関するガイドライン

ユーザ名は、Cisco UCS Central のログイン ID としても使用されます。 Cisco UCS Central ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）

- ログイン ID は、Cisco UCS Central 内で一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。 数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワードの作成に関するガイドライン

それぞれのローカル認証されたユーザ アカウントにはパスワードが必要です。 admin、aaa、または domain-group-management 権限を持つユーザは、ユーザ パスワードについてパスワード強度のチェックを実行するように Cisco UCS Central を設定できます。 パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

シスコでは、各ユーザに強力なパスワードを設定することを推奨します。 ローカル認証されたユーザに対してパスワード強度のチェックを有効にした場合、Cisco UCS Central は、次の要件を満たさないパスワードを拒否します。

- 8 ～ 80 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、Cisco UCS ManagerCisco UCS Central のローカル認証されたユーザすべてのパスワード履歴やパスワード変更間隔プロパティが含まれます。 ローカル認証されたユーザのそれぞれに異なるパスワード プロファイルを指定することはできません。

（注） パスワードプロファイルプロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

（注） パスワード プロファイル プロパティを変更するには、admin、aaa、または domain-group-management 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティはこれらの管理権限を持つユーザには適用されません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。 このプロパティが設定されている場合、Cisco UCS ManagerCisco UCS Central は、ローカル認証されたユーザによって以前使用された最大 15 個のパスワードを保存します。 パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になる前に、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用する必要があります。 たとえば、パスワード履歴カウントを 8 に設定した場合、ローカル認証されたユーザは最初のパスワードを 9 番目のパスワードが期限切れになった後まで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。 この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザについてパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更回数を制限することができます。 次の表で、パスワード変更間隔の 2 つの設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更不許可	このオプションでは、ローカル認証されたユーザは、パスワードの変更後、指定された時間内にはパスワードを変更できません。 1 ～ 745 時間の変更禁止間隔を指定できます。 デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが 48 時間の間パスワードを変更できないようにする場合、次のように設定します。 • [Change During Interval] をディセーブルに • [No Change Interval] を 48 に

間隔の設定	説明	例
変更間隔内のパスワード変更許可	このオプションは、ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。 デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に最大1回の変更を許可する場合、次のように設定します。 • [Change During Interval] をイネーブルに • [Change Count] を 1 に • [Change Interval] を 24 に

変更間隔のパスワード変更の最大数の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、すべてのフィールドに入力します。

a) [Change During Interval] フィールド で、 をクリックします。

b) [Change Interval] フィールド で、[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数。 を入力します。
この値は、1 ～ 745 時間から自由に設定できます。

たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。

c) [Change Count] フィールド で、ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数 を入力します。
この値は、0 ～ 10 から自由に設定できます。

ステップ 5 [Save] をクリックします。

パスワードの変更禁止間隔の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、すべてのフィールドに入力します。

a) [Change During Interval] フィールド で、 をクリックします。

b) [No Change Interval] フィールド で、ローカル認証されたユーザが、新しく作成されたパスワードを変更する前に待機する時間の最小数 を入力します。
この値は、1 ～ 745 時間から自由に設定できます。

この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合、無視されます。

ステップ 5 [Save] をクリックします。

パスワード履歴カウントの設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、ローカル認証されたユーザが、以前 [History Count] フィールド で使用したパスワードを再使用できるようになる前に、作成する必要がある一意のパスワードの数を入力します。
この値は、0 ～ 15 から自由に設定できます。

デフォルトでは、[History Count] フィールドは 0 に設定されます。これは、履歴カウントをディセーブルにし、ユーザはいつでも前に使用されたパスワードを再使用できます。

ステップ 5 [Save] をクリックします。

ローカル認証されたユーザ アカウントの作成

少なくとも、次のユーザを作成することを推奨します。

- サーバ アドミニストレータ アカウント
- ネットワーク アドミニストレータ アカウント
- ストレージ アドミニストレータ

はじめる前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

- リモート認証サービス：ユーザがリモート認証サーバに存在すること、および適切なロールと権限を持っていることを確認します。
- 組織のマルチテナント機能：1 つ以上のロケールを作成します。 ロケールが 1 つもない場合、すべてのユーザはルートに作成され、すべての組織のロールと権限が割り当てられます。
- SSH 認証。SSH キーを取得します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Create Locally Authenticated User] をクリックします。

ステップ 5 [Create Locally Authenticated User] 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
[Login ID] フィールド	ローカルの Cisco UCS Central ユーザのユーザ名。 ログイン ID は次の制約事項を満たす必要があります。 • ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。 ◦ 任意の英字 ◦ 任意の数字 ◦ _（アンダースコア） ◦ -（ダッシュ） ◦ .（ドット） • ログイン ID は、Cisco UCS ManagerCisco UCS Central 内で一意である必要があります。 • ログイン ID は、英文字で開始する必要があります。 数字やアンダースコアなどの特殊文字からは開始できません。 • ログイン ID では、大文字と小文字が区別されます。 • すべて数字のログイン ID は作成できません。 • ユーザ アカウントの作成後は、ログイン ID を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。
[Description] フィールド	ユーザ アカウントの説明。 256 文字以下で入力します。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり記号）、<（小なり記号）、および'（一重引用符）以外のすべての文字またはスペースを使用できます。
[First Name] フィールド	ユーザの名。 32 文字までの文字またはスペースを入力します。
[Last Name] フィールド	ユーザの姓。 32 文字までの文字またはスペースを入力します。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone] フィールド	ユーザの電話番号。

名前	説明
[Password] フィールド	このアカウントに関連付けられているパスワード。 パスワード強度のチェックボックスをオンにした場合、ユーザ パスワードを強くする必要があります。 強力なパスワードは、次の要件を満たす必要があります。 • 8 ～ 80 文字を含む。 • 次の少なくとも 3 種類を含む。 ◦ 小文字 ◦ 大文字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • ユーザ名と同一、またはユーザ名を逆にしたものではない。 • パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。 • 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。
[Set] フィールド	このユーザにパスワードが設定済みかどうか。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Expiration] チェックボックス	オンにすると、このアカウントは期限切れになり、[Expiration Date] フィールドに指定した日付以降に使用できなくなります。
[Account Status] ドロップダウンリスト	ステータスが [Active] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Cisco UCS Central にログインできます。

名前	説明
[Expiration Date] フィールド	アカウントの期限が切れる日付。 日付の形式は yyyy-mm-dd です。 このフィールドの終端にあるカレンダーアイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 6 [Create Locally Authenticated User] ダイアログボックスで、[Roles/Locales] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[Assigned Roles] リスト ボックス	Cisco UCS Central に定義されているユーザ ロールのリスト。 選択したユーザに割り当てられているユーザ ロールは、関連付けられたチェックボックスがオンになっています。
[Assigned Locales] リスト ボックス	Cisco UCS Central に定義されているロケールのリスト。 選択したユーザに割り当てられているロケールは、関連付けられたチェックボックスがオンになっています。

ステップ 7 （任意） システムに組織が含まれている場合は、[Assigned Role(s)] ペインの 1 つ以上のチェックボックスをオンにして、ユーザを適切なロケールに割り当てます。

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

ステップ 8 [Create Locally Authenticated User] ダイアログボックスで、[SSH] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[Type] フィールド	次のいずれかになります。 • [Key]：このユーザがログインするときに、SSH 暗号化が使用されます。 • [Password]：ユーザはログイン時にパスワードを入力する必要があります。
[SSH Data] フィールド	[Type] を [Key] に設定すると、関連付けられた SSH キーがこのフィールドに表示されます。

ステップ 9 [OK] をクリックします。

予約語：ローカル認証されたユーザ アカウント

Cisco UCS および Cisco UCS Central でローカル ユーザ アカウントを作成する場合は、次の単語を使用できません。

- root
- bin
- daemon
- adm
- ip
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

ローカルに認証されたユーザ アカウントの削除

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。
ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。
ステップ 4 削除する [User] を右クリックし、[Delete] を選択します。
ステップ 5 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザ アカウントのイネーブル化

ローカルユーザ アカウントを有効または無効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。

はじめる前に

ローカル ユーザ アカウントを作成します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。
ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。
ステップ 4 修正するユーザ アカウントをクリックします。
ステップ 5 [Work] ペインの [General] タブをクリックします。
ステップ 6 [Account Status] フィールドで、[active] オプション ボタンをクリックします。
ステップ 7 [Save] をクリックします。

ローカル認証されたユーザ アカウントのディセーブル化

ローカルユーザ アカウントを有効または無効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。

（注） Cisco UCS Manager GUICisco UCS Central GUI を介してディセーブル化されたアカウントのパスワードを変更した場合、アカウントをイネーブルにしてアクティブ化した後、ユーザはこの変更されたパスワードを使用できません。 アカウントをイネーブル化してアクティブ化した後に、必要なパスワードを再び入力する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Account Status] フィールドで、[inactive] オプション ボタンをクリックします。
admin ユーザ アカウントは常にアクティブに設定されます。 変更はできません。

ステップ 7 [Save] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロールの変更

ユーザ ロールと権限の変更は、次回ユーザがログインするまで有効になりません。 ユーザ アカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Role(s)] 領域で、ロールの割り当ておよび削除を行います。

- ユーザ アカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。

- ユーザ アカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ローカル認証されたユーザへのパスワード強度チェックのイネーブル化

パスワードの強度の確認を有効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。 パスワードの強度の確認が有効になっている場合、Cisco UCS ManagerCisco UCS Central では、強力なパスワードのガイドラインを満たしていないパスワードを選択できません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Work] ペインで、[Properties] 領域の [Password Strength Check] チェックボックスをオンにします。

ステップ 5 [Save] をクリックします。

ローカル認証されたユーザのパスワード履歴のクリア

パスワードプロファイルプロパティを変更するには、admin、aaa、または domain-group-management 権限を持っている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域に、ローカルで認証されたユーザが [History Count][History Count] フィールドフィールドで以前に使用したパスワードを再利用するために作成する必要がある一意のパスワードの数として 0 を入力します。
[History Count] フィールドを 0（デフォルト設定）に設定すると、履歴カウントがディセーブルになり、ユーザは以前に使用したパスワードをいつでも再使用できるようになります。

ステップ 5 [Save] をクリックします。

ユーザ アカウントの Web セッション制限

Web セッション制限は、指定されたユーザ アカウントに対してある 1 つの時点で許容される Web セッション数（GUI と XML の両方）の制限のため Cisco UCS Manager に使用されます。

各 Cisco UCS Manager ドメインは、ユーザ 1 人につき同時 Web セッションを最大 32 件、合計 256 件のユーザ セッションをサポートします。 デフォルトでは、Cisco UCS Manager が許容する同時 Web セッションはユーザ 1 人あたり 32 に設定されます。ただし、この値は最大でシステム上限である 256 まで設定できます。

Cisco UCS Central は、この時点では、複数の同時 Web セッションの管理をサポートしていません。 Cisco UCS Central ユーザに対して 32 個の同時 Web セッションをサポートし、またすべてのユーザでは合計 256 個の同時セッションをサポートします。

ユーザ セッションのモニタリング

CLI と GUI のどちらでログインしているかに関係なく、ローカル認証されたユーザとリモート認証されたユーザの両方について、Cisco UCS Central セッションをモニタできます。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Access Control] タブで、[Locally Authenticated Users] または [Remotely Authenticated Users] をクリックします。

ステップ 3 ユーザ セッションは、[Navigation] ペインで、すべてのユーザまたは各ユーザに関して [Locally Authenticated Users] 下でモニタされます。

- [Navigation] ペインで、[Locally Authenticated Users] をクリックして、すべてのユーザ セッションをモニタします。
- [Navigation] ペインで、[Locally Authenticated Users] ノードを展開し、ユーザ名をクリックして個々のユーザをモニタします。

ステップ 4 [Work] ペインで [Sessions] タブをクリックします。
このタブには、ユーザ セッションに関する次の詳細情報が表示されます。

名前	説明
[Filter] ボタン	テーブル内のデータをフィルタリングできます。 フィルタを適用すると、このボタン名は [Filter (on)] に変わります。

名前	説明
[Terminate Session] ボタン	選択したユーザのセッションを終了します。
[Host] カラム	ユーザのログイン元である IP アドレス。
[Login Time] カラム	ユーザがログインした日時。
[Terminal Type] カラム	ユーザのログイン元であるターミナルのタイプ
[Current Session] カラム	セッションが現在アクティブかどうか。

ロールベース アクセス コントロール

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステムアクセスを制限または許可する方法です。 ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。 権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールとロケールを割り当てることが主な作業になります。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。 たとえば、エンジニアリング組織内のサーバ管理者ロールを持つユーザは、エンジニアリング組織内のサーバ設定を更新できますが、そのユーザに割り当てられたロケールに財務組織が含まれていなければ、財務組織内のサーバ設定を更新できません。

ユーザ ロール

ユーザ ロールには、ユーザに許可される操作を定義する 1 つ以上の権限が含まれます。 各ユーザに 1 つ以上のロールを割り当てることができます。 複数のロールを持つユーザは、割り当てられたすべてのロールを組み合わせた権限を持ちます。 たとえば、Role1 にストレージ関連の権限が含まれ、Role2 にサーバ関連の権限が含まれている場合、Role1 と Role2 の両方を持つユーザは、ストレージ関連の権限とサーバ関連の権限を持つことになります。

Cisco UCS ドメインは、デフォルトのユーザ ロールを含めて、最大 48 個のユーザ ロールを持つことができます。 最初の 48 個の後に設定されたユーザ ロールは受け入れられますが、非アクティブであり障害が上げられます。Cisco UCS Central の各ドメイン グループは、親ドメイン グループから継承したユーザ ロールを含めて、48 個のユーザ ロールを持つことができます。 ユーザ ロールが Cisco UCS Central からCisco UCS Manager にプッシュされると、最初の 48 個のロールだけがアクティブになります。 最初の 48 個より後のユーザ ロールは、非アクティブであり障害が上げられます。

すべてのロールには、Cisco UCS ドメイン内のすべての設定に対する読み取りアクセス権限が含まれています。 読み取り専用ロールを持つユーザは、システム状態を変更できません。

ロールは、作成、変更（新しい権限の追加や既存の権限の削除）、および削除できます。 ロールを変更すると、そのロールを持つすべてのユーザに新しい権限が適用されます。 権限の割り当ては、デフォルトロールに定義されている権限に限定されません。 つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。 たとえば、デフォルトのサーバアドミニストレータ ロールとストレージ アドミニストレータ ロールの持つ権限の組み合わせは異なっていますが、両方のロールの権限を組み合わせた新しい 1 つのサーバおよびストレージ アドミニストレータ ロールを作成できます。

ロールがユーザへの割り当て後に削除されると、それらのユーザ アカウントからも削除されます。

AAA サーバ（RADIUS または TACACS+）上のユーザ プロファイルは、そのユーザに与える権限に対応したロールを追加するように変更する必要があります。 属性はロール情報を保存するために使用されます。 AAA サーバでは、要求とともにこの属性が返され、それを解析してロールが得られます。 LDAP サーバでは、ユーザ プロファイル属性内のロールが返されます。

（注） ローカル ユーザ アカウントとリモート ユーザ アカウントに同じユーザ名がある場合、リモート ユーザに割り当てられたすべての役割は、ローカル ユーザに割り当てられた内容で上書きされます。

デフォルト ユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。 デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

ファシリティ マネージャ

power-mgmt 権限による、電源管理操作に対する読み取りと書き込みのアクセス。 システムの残りの部分に対する読み取りアクセス権。

ネットワーク アドミニストレータ

ファブリック インターコネクト インフラストラクチャとネットワーク セキュリティ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

動作

システムのログ（syslogサーバを含む）と障害に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

Server Compute

サービス プロファイルのほとんどの側面に対する読み取りと書き込みのアクセス権。 ただし、ユーザは vNIC または vHBA を作成、変更、または削除できません。

サーバ機器アドミニストレータ

物理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ プロファイル アドミニストレータ

論理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ セキュリティ アドミニストレータ

サーバ セキュリティ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

ストレージ アドミニストレータ

ストレージ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。 次の表に、各権限と、その権限がデフォルトで与えられるユーザ ロールのリストを示します。

ヒント　これらの権限および権限によってユーザが実行できるようになるタスクの詳細情報は、『*Privileges in Cisco UCS*』は、次の URL で入手可能です。http://preview.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html で利用可能です。

表 *1*：ユーザの権限

特権	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	管理者
domain-group-management	ドメイン グループ管理	ドメイン グループ管理者
ext-lan-config	外部 LAN 設定	ネットワーク アドミニストレータ
ext-lan-policy	外部 LAN ポリシー	ネットワーク アドミニストレータ
ext-lan-qos	外部 LAN QoS	ネットワーク アドミニストレータ
ext-lan-security	外部 LAN セキュリティ	ネットワーク アドミニストレータ
ext-san-config	外部 SAN 設定	ストレージアドミニストレータ
ext-san-policy	外部 SAN ポリシー	ストレージアドミニストレータ
ext-san-qos	外部 SAN QoS	ストレージアドミニストレータ
ext-san-security	外部 SAN セキュリティ	ストレージアドミニストレータ
fault	アラームおよびアラーム ポリシー	動作
operations	ログおよび Smart Call Home	動作
org-management	組織管理	動作
pod-config	ポッド設定	ネットワーク アドミニストレータ
pod-policy	ポッド ポリシー	ネットワーク アドミニストレータ
pod-qos	ポッド QoS	ネットワーク アドミニストレータ

特権	説明	デフォルトのロール割り当て
pod-security	ポッド セキュリティ	ネットワーク アドミニストレータ
power-mgmt	電源管理操作に対する読み取りと書き込みのアクセス	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	Read-Only
server-equipment	サーバ ハードウェア管理	サーバ機器アドミニストレータ
server-maintenance	サーバ メンテナンス	サーバ機器アドミニストレータ
server-policy	サーバ ポリシー	サーバ機器アドミニストレータ
server-security	サーバ セキュリティ	サーバセキュリティ アドミニストレータ
service-profile-compute	サービス プロファイルの計算	サーバ計算アドミニストレータ
service-profile-config	サービス プロファイル設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービス プロファイル エンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク アドミニストレータ
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク アドミニストレータ
service-profile-qos	サービス プロファイル QoS	ネットワーク アドミニストレータ
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク アドミニストレータ

特権	説明	デフォルトのロール割り当て
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プールポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージアドミニストレータ
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージアドミニストレータ
stats	統計情報管理	統計情報の管理者

ユーザ ロールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。

b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Roles] に移動します。

a) [Security] をクリックします。

b) [User Services] ノードを展開します。

c) [Roles] をクリックします。

ステップ 5 [Create Role] をクリックします。
また、[Roles] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Create Role] ダイアログボックスで、ロールを割り当てる [Name] を入力します。

ステップ 7 ロールのすべての [Privileges] を選択します。

ステップ 8 [OK] をクリックします。

予約語：ユーザ ロール

次の単語は、Cisco UCS でカスタム ロールを作成するときに使用できません。

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

ユーザ ロールの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 削除するロールをクリックします。

ステップ 6 [Delete] をクリックします。

また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ユーザ ロールへの権限の追加

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 権限を追加するロールを選択します。

ステップ 6 [Properties] をクリックします。
また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Properties] ダイアログボックスで、ロールに追加する権限に対応するチェックボックスをオンにします。

ステップ 8 [Save Changes] をクリックします。

ユーザ ロールからの権限の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 権限を削除するロールを選択します。

ステップ 6 [Properties] をクリックします。
また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Properties] ダイアログボックスで、ロールから削除する権限に対応するボックスをオフにします。

ステップ 8 [Save Changes] をクリックします。

ユーザ ロケール

ユーザには、ロケールを 1 つ以上割り当てることができます。 各ロケールには、ユーザからのアクセスを許可する 1 つ以上の組織（ドメイン）を定義します。アクセスは、このロケールで指定された組織の範囲内に制限されます。 このルールの 1 つの例外として、組織が指定されていないロケールがあります。この場合、すべての組織内のシステム リソースに対して無制限のアクセスが可能になります。

Cisco UCS ドメインは、最大 48 個のユーザ ロケールを持つことができます。 最初の 48 個より後に設定されたユーザ ロケールは、非アクティブであり障害が上げられます。 Cisco UCS Central の各ドメイン グループは、親ドメイン グループから継承されたユーザ ロケールを含めて、48 個のユーザ ロケールを持つことができます。 Cisco UCS Central からユーザ ロケールが Cisco UCS Manager にプッシュされると、最初の 48 個のロケールだけがアクティブになります。 最初の 48 個より後のユーザ ロケールは、非アクティブであり障害が上げられます。

admin または aaaadmin、aaa、または domain-group-management の権限を持つユーザは、組織をその他のユーザのロケールに割り当てることができます。 組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。 たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） admin 権限を持つユーザにロケールを割り当てることはできません。

（注） ロケールを次の権限の 1 つ以上を持つユーザに割り当てることはできません。

- aaa
- admin
- fault
- operations

組織は階層的に管理できます。トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。たとえば、エンジニアリング組織が、ソフトウェアエンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。 ソフトウェアエンジニアリング組織のみを含むロケールでは、その組織内のシステムリソースにしかアクセスできません。一方、エンジニアリング組織が含まれるロケールでは、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織の両方のリソースにアクセスできます。

ユーザ ロケールの作成

はじめる前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Locales] に移動します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Locales] をクリックします。

ステップ 5 [Create Locales] をクリックします。
また、[Locales] を右クリックしてそのオプションにアクセスすることもできます。

ステップ 6 [Create Locale] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、ロケールの一意の名前を入力します。
この名前には、1～32 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で、この名前を変更することはできません。

b) [Description] フィールドにロケールの説明を入力します。

ステップ 7 [Filter] をクリックします。

ステップ 8 [Table Filter] ダイアログボックスで、要求された情報を入力します。

a) [Assigned Organization] フィルタを選択します。
b) [Assigned Organization] フィルタの値を入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Assign Organization] をクリックします。

ステップ 11 [Assign Organizations] ダイアログボックスで、組織をロケールに割り当てます。

a) [Organizations] 領域を展開して、Cisco UCS ドメイン内の組織を表示します。
b) [root] ノードを展開して、サブ組織を表示します。
c) ロケールを割り当てる組織をクリックします。
d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。
e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 12 [OK] をクリックして組織を割り当てます。

ステップ 13 [OK] をクリックしてロケールを作成します。

ユーザ ロケールの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロケールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。

c) [Locales] ノードを展開します。

ステップ 5 削除するロケールをクリックします。

ステップ 6 [Delete] をクリックします。
また、削除する [Locale] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ユーザ ロケールへの組織の割り当て

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインでロケールを選択します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Locales] ノードを展開します。

ステップ 5 組織を追加するロケールをクリックします。

ステップ 6 [Assign Organization] をクリックします。
また、[Locale] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Assign Organizations] ダイアログボックスで、[Organization] を入力します。

ステップ 8 [OK] をクリックします。

ユーザ ロケールからの組織の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロケールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Locales] ノードを展開します。

ステップ 5 削除する組織が割り当てられたロケールをクリックします。

ステップ 6 [Properties] をクリックします。

ステップ 7 [Work] ペインで、削除する [Organization] をクリックします。

ステップ 8 [Delete] をクリックします。
また、削除する [Organization] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 9 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロケールの変更

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Locale(s)] 領域で、ロケールの割り当ておよび削除を行います。

- ユーザ アカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ユーザ組織

ユーザは、1 つ以上の組織を作成できます。 各組織では、サブ組織、障害、イベント、UUID 接尾辞プール、および UUID のブロックが定義されます。

Cisco UCS 組織 は、ユーザによって階層的に管理されます。 ルート レベルの組織に割り当てられたユーザは、自動的にすべての組織およびその下にあるドメイン グループにアクセスできます。

ユーザ組織の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を作成します。

a) [Pools] ノードを展開します。

b) [root] をクリックします。

c) [Work] ペインで、[Create Organization] をクリックします。

ステップ 3 [Create Organization] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、組織の一意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。-（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で、この名前を変更することはできません。

b) [Description] フィールドに、組織の説明を入力します。

ステップ 4 [OK] をクリックして組織を作成します。

ユーザ組織の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を選択します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。
d) [Sub-Organizations] ペインで、削除する [Organization] をクリックします。

ステップ 3 [Delete] をクリックします。
また、削除する [Organization] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 4 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ユーザのサブ組織の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、サブ組織を作成します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。

ステップ 3 [Sub-Organizations] ペインで、該当する割り当てられた組織名をクリックします。

ステップ 4 [Work] ペインで、[Create Organization] をクリックします。

ステップ 5 [Create Organization] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、組織の一意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。-（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で、この名前を変更することはできません。

b) [Description] フィールドに、組織の説明を入力します。

ステップ 6 [OK] をクリックしてサブ組織を作成します。

ユーザのサブ組織の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を選択します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。
d) [Sub-Organizations] ペインで、該当する割り当てられた組織ノードを展開します。
e) [Sub-Organizations] ペインで、削除する [Organization] をクリックします。
該当する組織名に到達するまで、該当する割り当てられた組織ノードを展開します。

ステップ 3 [Delete] をクリックします。
また、削除するターゲットに到達するまで [Organizations] を展開し、[Organization] を右クリックしてそのオプションにアクセスすることもできます。

ステップ 4 [Confirm] ダイアログボックスで、[Yes] をクリックします。