ロールベース アクセスの設定

ロールベース アクセス コントロールの概要

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、適切なロールとロケールを割り当てることによって個々のユーザ権限を管理できます。

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の管理者ロールを与えられたユーザは、エンジニアリング組織のサーバ設定を更新できます。ただし、そのユーザに割り当てられたロケールに財務部門が含まれている場合を除いて、財務部門内のサーバ設定を更新することはできません。

ユーザ アカウント Cisco UCS

ユーザ アカウントは、システムへのアクセスに使用します。Cisco UCS Manager ドメインごとに最大 48 個の ローカル ユーザ アカウントを構成できます。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 ドメイン にはそれぞれ、1 つの管理者アカウントが付随しています。管理者アカウントはデフォルト ユーザ アカウントであり、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、ファブリック インターコネクトのを介して直接認証され、admin または aaa 権限の所有者によって有効または無効にできます。ローカル ユーザ アカウントを無効にすると、そのユーザはログインできなくなります。しかし無効になったローカル ユーザ アカウントの構成の詳細はデータベースから削除されません。無効にされた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、既存の構成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 アカウントとは、LDAP、RADIUS、または TACACS+ で認証されたユーザ アカウントです。

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により、リモート ユーザ アカウントに保持された値が上書きされます。

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 アカウントは無効になります。

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。

Note ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、そのアカウントの有効期限切れになる日付を更新して設定することは可能です。

予約語：ローカル認証されたユーザ アカウント

次の語は Cisco UCS でローカル ユーザ アカウントを作成するときに使用できません。

- root
- bin
- daemon

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

ユーザ アカウントの Web セッション制限

Cisco UCS Manager は、Web セッション制限を使用して、あるユーザ アカウントに対してある時点で許容される Web セッション数（GUI と XML の両方）を制限します。

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 セッション数はユーザ 1 人あたり 32 に設定されます。ただし、この値を最大でシステム上限の 256 まで構成できます。

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。ユーザごとに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 には、デフォルトのユーザ ロールを含めて最大 48 個のユーザ ロールを含めることができます。48 個目のユーザ ロールが許可された後に設定されたユーザ ロールは、障害が発生して無効になります。

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のユーザは、システム状態を変更することはできません。

ユーザは権限を作成したり、既存の権限を変更または削除したり、ロールを削除したりできます。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、権限を自由に組み合わせ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管理者ロールとストレージ管理者ロールには、異なる組み合わせの権限が付与されています。しかし、両方のロールの権限を持つサーバおよびストレージ管理者ロールを作成することができます。

Note ロールをユーザに割り当てた後で削除すると、そのロールはそれらのユーザ 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 プロファイルを、そのユーザに付与される権限に対応したロールを追加するように変更します。属性にはロール情報が保存されます。AAA サーバでは、要求とともにこの属性が返され、それを解析することで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。

Note ローカル ユーザ アカウントとリモート ユーザ アカウントが同じユーザ名である場合、Cisco UCS Manager は、リモート ユーザに割り当てられたロールをローカル ユーザに割り当てられたロールで上書きします。

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。その他のシステムに対する読み取りアクセス。

アドミニストレータ

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。このロールは、デフォルトで管理者アカウントに割り当てられます。変更することはできません。

ファシリティ マネージャ

power management 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。その他のシステムに対する読み取りアクセス。

ネットワーク管理者

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。その他のシステムに対する読み取りアクセス。

オペレーション

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。その他のシステムに対する読み取りアクセス。

読み取り専用

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。

サーバ計算

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。その他のシステムに対する読み取りアクセス。

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。その他のシステムに対する読み取りアクセス。

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。その他のシステムに対する読み取りアクセス。

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。その他のシステムに対する読み取りアクセス。

予約語：ユーザ ロール

次の語は、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。

- ネットワーク管理者

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

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 リソースにアクセスしたり、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。

Tip 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、次の *URL* から入手可能な『 Privileges in Cisco UCS http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html

Table 1: ユーザの権限

権限	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	アドミニストレータ
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

権限	説明	デフォルトのロール割り当て
fault	アラームおよびアラーム ポリシー	オペレーション
operations	ログおよび Smart Call Home	オペレーション
org-management	組織管理	オペレーション
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
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および書き込みアクセス権	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。	読み取り専用
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

権限	説明	デフォルトのロール割り当て
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
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

ユーザ ロールの作成

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]** > **[User Services]の順に展開します。**

ステップ 3 [User Services] を右クリックし、[Create Role] を選択します。

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 4 [Create Role] 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] フィールド	このユーザ ロールのユーザ定義名。 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。
[Privileges] リスト ボックス	システムに定義されている権限のリスト。 その権限の説明を表示するには、権限をクリックします。チェックボックスをオンにすると、選択したユーザにその権限が割り当てられます。
[Help] セクション	
[Description] フィールド	[Privileges] リスト ボックス内で最後にクリックした権限の説明。

ステップ 5 [OK] をクリックします。

ユーザ ロールへの権限の追加

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]** > **[User Services]**の順に展開します。
ステップ 3 [Roles] ノードを展開します。
ステップ 4 権限を追加するロールを選択します。
ステップ 5 [General] タブで、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 6 [Save Changes] をクリックします。

ユーザ ロールからの権限の削除

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]** > **[User Services]**の順に展開します。

ステップ 3 [Roles] ノードを展開します。
ステップ 4 権限を削除するロールを選択します。
ステップ 5 [General] タブで、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 6 [Save Changes] をクリックします。

ユーザ ロールの削除

あるユーザー ロールを削除すると、Cisco UCS Managerにより、このロールは割り当て先のすべてのユーザー アカウントから削除されます。

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]** > **[User Services]の順に展開します。**
ステップ 3 [Roles] ノードを展開します。
ステップ 4 削除するロールを右クリックし、[Delete] を選択します。
ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

ロケール

ユーザ ロケール

ユーザは、1 つ以上のロケールに割り当てることができます。各ロケールでは、ユーザがアクセスできる1つ以上の組織（ドメイン）を定義します。アクセスは通常、ロケールで指定された部門のみに限定されます。ただし、部門をまったく含まないロケールは例外です。このようなロケールは、全部門のシステム リソースへの無制限のアクセスを提供します。

1 つの Cisco UCS ドメイン には、最大 48 個のユーザ ロケールを含めることができます。48 個目のユーザ ロールが許可された後に設定されたユーザ ロケールは、障害が発生して無効になります。

admin または aaa 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のみに制限されます。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。

Note 次の権限の 1 つ以上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。

- 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 エンジニアリング部門のみを含むロケールでは、その部門内のシステム リソースにのみアクセスできます。しかし、エンジニアリング部門を含むロケールでは、ソフトウェア エンジニアリング部門とハードウェア エンジニアリング部門の両方のリソースにアクセスできます。

ロケールへの組織の割り当て

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]** > **[User Services]の順に展開します。**
ステップ 3 [Locales] ノードを展開し、組織を追加するロケールをクリックします。
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 [Organizations] 領域のテーブル アイコン バーで [+] をクリックします。
ステップ 6 [Assign Organizations] ダイアログボックスで、次の手順を実行します。
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 7 [OK] をクリックします。

ロケールの作成

始める前に

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 [Navigation] ペインで [Admin] をクリックします。

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

ステップ 3 [Locales] を右クリックし、[Create a Locale] を選択します。

ステップ 4 [Create Locale] ページで、次の手順を実行します。

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 ～ 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。

b) [Next] をクリックします。

ステップ 5 [Assign Organizations] ダイアログボックスで、次の手順を実行します。

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 6 [Finish] をクリックします。

次のタスク

ロケールを 1 つまたは複数のユーザ アカウントに追加します。詳細については、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 （18 ページ）を参照してください。

ロケールからの組織の削除

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]** > **[User Services]の順に展開します。**

ステップ 3 [Locales] ノードを展開し、組織を削除するロケールをクリックします。

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 [Organizations] 領域で、ロケールから削除する組織を右クリックし、[Delete] を選択します。

ステップ 6 [Save Changes] をクリックします。

ロケールの削除

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]** > **[User Services]の順に展開します。**
ステップ 3 [Locales] ノードを展開します。
ステップ 4 削除するロケールを右クリックし、[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。

ローカル認証されたユーザ アカウント

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

Note ユーザ アカウントの作成後、Cisco UCS Manager GUIからユーザ アカウントのフィールドのいずれかを変更する場合は、パスワードをもう一度入力する必要があります。

Before you begin

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。

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]** > **[User Services]の順に展開します。**

ステップ 3 [User Services] を右クリックし、[Create User] を選択して [User Properties] ダイアログボックスを開きます。

[Locally Authenticated Users] の右クリックでもそのオプションにアクセスできます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明

[Login ID] フィールド	このアカウントにログインするときに使用されるアカウント名。このアカウントは固有である必要があり、しかも Cisco UCS Manager ユーザ アカウントに関する次のガイドラインと制約事項を満たしている必要があります。
	• 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 Manager 内で一意である必要があります。
	• ログインIDは、英文字から始まる必要があります。アンダースコアなどの特殊文字や数字から始めることはできません。
	• ログイン ID では、大文字と小文字が区別されます。
	• すべてが数字のログイン 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。
	ユーザを保存した後は、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。

名前	説明
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[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。
[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。パスワード強度チェックが有効にされている場合は、ユーザ パスワードを強固なものにする必要があります。Cisco UCS Manager は次の要件を満たしていないパスワードを拒否します。 • 8 ～ 80 文字を含む。 • パスワードの強度の確認が有効になっている場合はパスワード長は可変で、6 ～ 80 文字の間で設定できます。 **Note** デフォルトは 8 文字です。 • 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。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[Account Status] フィールド	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 Manager にログインできます。
[Account Expires] 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。 **Note** ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、そのアカウントの有効期限切れになる日付を更新して設定することは可能です。
[Expiration Date] フィールド	アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。 このフィールドの終端にある下矢印をクリックするとカレンダーが表示されるので、それを使用して期限日を選択できます。 **Note** **[Account Expires]** チェックボックスをオンにすると、Cisco UCS Manager GUI が表示されます。

ステップ 5 [Roles] 領域で 1 つ以上のボックスをオンにして、ユーザ アカウントにロールと権限を割り当てます。

Note 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 6 (Optional) システムに組織が含まれる場合、[Locales] 領域の 1 つ以上のチェックボックスをオンにして、適切なロケールをユーザに割り当てます。

ステップ 7 [SSH] 領域で、次のフィールドに値を入力します。

a) [Type] フィールドで、次をクリックします。

- [Password Required]：ユーザはログインするときにパスワードを入力する必要があります。
- [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。

b) [Key] を選択する場合、[SSH data] フィールドに SSH キーを入力します。

ステップ 8 [OK] 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有効化

パスワードの強度確認を有効にするには、admin または aaa 権限が必要です。有効になっている場合、Cisco UCS Manager では、強力なパスワードのガイドラインを満たさないパスワードを選択できません。

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]** > **[User Services]の順に展開します。**

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

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 Changes] をクリックします。

Web セッション制限の設定

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]** > **[Communication Management]** > **[Communication Services] の順に展開します。**

ステップ 3 [Communication Services] タブをクリックします。

ステップ 4 [Web Session Limits] 領域で、次のフィールドに入力します。

（注） HTML-5インターフェイスではブラウザごとにユーザセッションを1つサポートします。

名前	説明
Maximum Sessions Per User	各ユーザに許可される HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。
Maximum Sessions	システム内のすべてのユーザに許可される HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。

名前	説明
[Maximum Event Interval (in seconds)]	2 つのイベント間の最大時間間隔。UI からのユーザ要求に対する応答など、さまざまなタイプのイベント変更通知を追跡します。時間間隔が経過すると、UI セッションは終了します。 120 ～ 3600 の整数を入力します。

ステップ 5 [Save Changes] 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 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブの **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]** を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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 [Locales] 領域で、次の手順を実行します。

- 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 6 [Save Changes] 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 ロールおよび権限の変更は次回のユーザ ログイン時に有効になります。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 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブの **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]** を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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 [Roles] 領域で、次の手順を実行します。

- 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 6 [Save Changes] をクリックします。

ユーザ アカウントの有効化

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、admin または aaa 権限が必要です。

始める前に

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 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]の順に展開します。**

ステップ 3 有効にするユーザをクリックします。

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 [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 6 [Save Changes] をクリックします。

ユーザ アカウントの無効化

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、admin または aaa 権限が必要です。

（注） Cisco UCS Manager GUI を介して無効化されたアカウントのパスワードを変更した場合、アカウントを有効化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。アカウントを有効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 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]**の順に展開します。
ステップ 3 無効にするユーザをクリックします。
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 [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 6 [Save Changes] 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

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]** > **[User Services]** > **[Locally Authenticated Users]**の順に展開します。
ステップ 3 パスワード履歴をクリアするユーザをクリックします。
ステップ 4 [Actions] 領域で、[Clear Password History] をクリックします。
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。

ローカルに認証されたユーザ アカウントの削除

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]** > **[User Services]**の順に展開します。
ステップ 3 [Locally Authenticated Users] ノードを展開します。

ステップ 4 削除するユーザ アカウントを右クリックし、[Delete] を選択します。
ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

ユーザ セッションのモニタリング

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 [Admin] タブで、[All] > [User Management] を展開します。
ステップ 3 [User Services] ノードをクリックします。
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
[Name] カラム	セッションの名前。
[User] カラム	セッションに参加しているユーザ名。
[Fabric ID] カラム	このセッションのためにユーザがログインしているファブリック インターコネクト。
[Login Time] カラム	セッションが開始された日時。
[Refresh Period] カラム	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。
[Session Timeout] カラム	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。
[Terminal Type] カラム	ユーザがログインするときに使用する端末の種類。
[Host] カラム	ユーザのログイン元である IP アドレス。

名前	説明
[Current Session] カラム	このカラムに [Y] が表示された場合は、関連するユーザ セッションが現在アクティブです。