ユーザ 管理

ユーザーとロール

Cisco ACI マルチサイト では、ロールベース アクセス コントロール（RBAC）を介してユーザのロールに従ってアクセスが提供されます。ロールは、ローカルと外部認証の両方に使用されます。次のユーザー ロールが Cisco ACI マルチサイト で使用可能です。

- 電源ユーザー；電源ユーザーは 管理者 ユーザーとしてすべての操作を実行できます。
- サイトおよびテナント マネージャ： サイトおよびテナント マネージャはサイト、テナント、関連付けを管理できます。
- スキーマ マネージャ；スキーマ マネージャは、テナントの関連付けに関係なくすべてのスキーマを管理できます。
- スキーマ マネージャ - 制限：制限スキーマ マネージャはユーザーが明示的に関連付けられるテナントを少なくとも 1 個含むスキーマを管理できます。
- ユーザーおよびとロールマネージャ：ユーザーおよびロールマネージャは、すべてのユーザー、そのロール、およびパスワードを管理できます。

管理者ユーザー

初期の設定スクリプトで、管理者アカウントが設定され、管理者はシステム起動時の唯一のユーザーとなります。管理者 ユーザーの最初のパスワードは、システムによって設定されます。最初のログイン中に、管理者 パスワードを変更する必要があります。

- 管理者 ユーザーは、電力ユーザーのロールが割り当てられます。

- 管理者ユーザーを使用して、ほかのユーザーを作成しその他すべてのDay-0設定を実行します。
- 管理者 ユーザーのアカウント ステータスは、**[非アクティブ]** に設定できません。

ユーザのロールと機能

次の表は、ユーザ ロールごとに利用可能な Cisco ACI マルチサイト の機能の一覧表示です。

表 *1*:

ユーザ ロール	マルチサイト の機能	マルチサイト av ペア
パワー ユーザ	• ダッシュボード • サイト（Sites） • スキーマ • テナント • ユーザ • レポートのトラブルシューティング	shell:msc-roles=powerUser
サイトとテナント マネージャ	• ダッシュ ボード—サイト • サイト • テナント	shell:msc-roles=siteManager
スキーマ マネージャ	• ダッシュ ボード—サイトとスキーマの健全性 • スキーマ	shell:msc-roles=schemaManager
スキーマ マネージャー - 制限あり	• ダッシュ ボード—サイトとスキーマの健全性 • スキーマ	shell:msc-roles=schemaEditor
ユーザとロール マネージャ	• ユーザ	shell:msc-roles=userManager

注意事項と制約事項

- ユーザー認証と認可は、ローカルまたは外部を指定できます（RADIUS または TACACS + を使用）。外部認証の詳細については、外部認証について （4 ページ）を参照してください。
- ローカルおよび外部認証の両方で、すべてのユーザ ^ に少なくとも 1 つのロールを関連付ける必要があります。ユーザーは複数のロールに関連付けることができます。複数のロールにユーザーに関連付けると、ユーザーがアクセスする機能の組み合わせが用意されます。
- スキーマのテナントを使用する前に、ユーザーがテナントに関連付けられている必要があります。

ユーザの作成

手順

ステップ 1 Cisco ACI マルチサイト にログインします。

ステップ 2 **[メイン メニュー]** で、**[ユーザー]** をクリックします。

ステップ 3 **[ユーザーの追加]** をクリックします。

ステップ 4 **[ユーザーの追加]** ページで、次の手順に従います。

a) **USERNAME** フィールドに、ユーザー名を入力します。

b) **[パスワード]** フィールドではパスワードを入力します。

パスワードは最少 6 文字以上で、少なくとも 1 個の文字、数字、および特殊文字を含める必要があります。スペースと * は使用できません。

c) **[パスワードの確認]** フィールドに、パスワードを再度入力します。

d) **[名]** フィールドに、ユーザーの名を入力します。

e) **[姓]** フィールドに、ユーザーの姓を入力します。

f) **[電子メール]** フィールドに、ユーザーの電子メール アドレスを入力します。

g) **[電話番号]** フィールドに、ユーザーの電話番号を入力します。

h) **[アカウント ステータス]** フィールドで、アカウント ステータスを選択します。

アクティブなユーザーのみが マルチサイト で認証さえます。

ステップ 5 **[ユーザー ロール]** ボタンをクリックし、ユーザーにロールを割り当てます。

すべてのユーザーに少なくとも 1 つのロールを関連付ける必要があります。ユーザーは複数のロールに関連付けることができます。複数のロールにユーザーに関連付けると、ユーザーがア

クセスする機能の組み合わせが用意されます。詳細については、「ユーザーとロール（1 ページ）」を参照してください。

ステップ 6 [送信（Submit）] をクリックします。

ユーザの管理

手順

ステップ 1 Cisco ACI マルチサイト。

ステップ 2 **Main menu** で、**Users** をクリックします。

ステップ 3 ユーザを選択し、**Actions** をクリックして、次の手順に従います。

a) ユーザを削除するには、**Actions** メニューから **Delete** を選択します。

admin ユーザは削除できません。

b) ユーザを編集するには、**Actions** メニューから **Edit** を選択します。

admin ユーザの名前、アカウント ステータス、およびロールは更新できません。

ステップ 4 ユーザのパスワードを更新するには、**Welcome** *username* をクリックします。

admin ユーザまたはユーザ ロール **Power User** または **User and Role Manager** に関連付けられているユーザは、エンド ユーザのパスワードを更新できます。エンド ユーザは、初回のログイン時に、自分のパスワードを更新する必要があります。

外部認証および許可の設定

外部認証について

Cisco ACI マルチサイト リリース 1.1(x) 以降では、RADIUS または TACACS + を使用して、ユーザのために外部認証と承認を設定することができます。

マルチサイト 管理者は、次のものをを設定できます:

- RADIUS または TACACS+ プロバイダー冗長性のために、少なくとも 2 つの RADIUS または TACACS + プロバイダーを設定することをお勧めします。
- ログイン ドメインをプロバイダーに関連付けます。

  デフォルト ドメインは、ローカル認証のためのローカル ドメインです。

- ユーザをドメインに割り当てます。

ドメインを作成した後、ドメインの編集、非アクティブ化または削除を行えます。ローカル ドメインを削除することはできませんが、非アクティブにすることはできます。

監査ログは、外部認証と承認をサポートします。

RADIUS および TACACS+ サーバでのユーザ設定の注意事項

リモート認証を行うユーザを設定するには、RADIUS および TACACS + サーバでユーザごとに設定を行う必要があります。

ユーザを設定するには、 Cisco ACI マルチサイト 属性を、`cisco-av-pair=shell:msc-roles=role1,role2` の形式で追加します。

たとえば、`cisco-av-pair=shell:msc-roles=siteManager,schemaManager` のようになります。

各ロールは、マルチサイト のいずれかになります。 ユーザのロールと機能 （2 ページ） に記載されています。

RADIUS または TACACS + プロバイダーの作成

マルチサイトにおいて、次の手順に従い、ユーザの認証と許可を行う RADIUS または TACACS+ プロバイダーを追加します。

手順

ステップ 1 **Admin** > **Providers** をクリックします。

ステップ 2 **ADD PROVIDER** をクリックします。

ステップ 3 RADIUS または TACACS+ サーバのホスト名または IP アドレスを入力します。

ステップ 4 プロバイダーの説明を入力します。

ステップ 5 必要に応じて、**RADIUS** または **TACACS+** をクリックします。

ステップ 6 **KEY** フィールドにキーを入力し、**CONFIRM KEY** フィールドでも繰り返します。

ステップ 7 オプション。**Additional Settings** をクリックして、デフォルトの **PORT**、認証プロトコル (CHAP または PAP)、**TIMEOUT (SEC)**、または **RETRIES (MAX 5 ALLOWED)** を変更します。

次のタスク

プロバイダーをさらに設定するには、この手順を繰り返します。

ログインドメインの作成

ログイン ドメインは、ユーザの認証ドメインを定義します。ログイン ドメインには、ローカル、LDAP、RADIUS、または TACACS+ 認証メカニズムを設定できます。REST API または GUI からシステムにアクセスすると、マルチサイトによりユーザは正しい認証ドメインを選択できます。

たとえば、REST API を使用する場合、ユーザ名にプレフィックスとして文字列が付くため、完全なログイン ユーザ名は次の例のようになります:

```
https://<host>:<port>/api/v1/auth/login
"username": "bob", "password": "we1come!", "domainid": "59d5b5978d0000d000909f65",
```

システムに GUI からアクセスする場合、マルチサイト からユーザのドメインのドロップダウンリストが表示されるので、それから選択することができます。ドメインが指定されなかった場合は、ローカル ドメインがユーザ名の検索のために使用されます。

ログイン ドメインを設定する複数のサイトでは、次の手順を実行します。

手順

ステップ 1 をクリックして **Admin** > **ドメイン** 。

ステップ 2 **ADD DOMAIN** をクリックします。

ステップ 3 ドメイン名を入力します。

ステップ 4 ドメインの説明を入力します。

ステップ 5 **レルム** フィールドで、をクリックして **RADIUS** または **TACACS +** 適切です。

ステップ 6 で、 **プロバイダーに割り当てる** フィールドで、ドメインを 1 つ以上の RADIUS または TACACS + プロバイダーに割り当てるプロバイダーをクリックします。

次のタスク

ドメインをさらに作成するには、この手順を繰り返します。

これらの作成後は編集、削除、またはドメインを非アクティブ化] をクリックして **Admin** > **ドメイン** 。右クリックして **アクション** ドメインで] を選択します **編集** 、 **削除** 、または **非アクティブ化** 。

ローカルのドメインを削除することはできませんが、非アクティブ化することができます。

リモート ユーザのログイン

外部認証がで有効になって Cisco ACI マルチサイト 、にログオンできます マルチサイト として次のとおりです。

手順

ステップ 1 入力のブラウザを使用して、 マルチサイト URL し、ユーザ名を入力します。

ステップ 2 ドロップダウン リストから、自分が割り当てられているドメインを選択します。

ステップ 3 割り当てられたパスワードを入力します。

ステップ 4 [Submit] をクリックします。`
権限が認証に合格していて、マルチサイト GUI が表示されに割り当てられているロールに応じて特権があります。パスワードは、初回ログオン時に変更する必要があります。