Secret Rotation

- Secret Rotation （1 ページ）
- Cisco Nexus Top of Rack Switch の Rotating Secrets （2 ページ）
- Rotating Secrets of Cisco UCS Manager の Rotating Secrets （2 ページ）

Secret Rotation

Azure Stack Hub は、内部および外部の Secret を使用して、Azure Stack Hub インフラストラクチャ リソースとサービス間のセキュアな通信を維持します。Azure Stack Hub 固有の Secret Rotation の詳細については、https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets?view=azs-2002 を参照してください。

すべてのユーザーアカウントに強力なパスワードを使用することを推奨します。この章では、ハードウェア管理ユーザー アカウントの Secret をローテーションする手順について説明します。

Cisco Azure Stack Hub には、インストール時に次のデフォルトのユーザー アカウントが作成されます。ユーザー アカウントは、インストール時に顧客が指定したパスワードで設定されます。

デバイス	アカウント	目的
Cisco UCS	admin	Cisco UCS Manager の管理者ロールを持つデフォルトの管理者アカウント
	UCSAzSAdmin	UCS Manager の管理者ロールを持つ追加の管理者アカウント
	IpmiUser	ベースボード管理コントローラ（BMC）ユーザー アカウント。

デバイス	アカウント	目的
Nexus	admin	ネットワーク管理者ロールを持つデフォルトの管理者アカウント
	azsadmin-<5 character random string>	network-administrator ロールを持つ追加の管理者アカウント

Cisco Nexus Top of Rack Switch の Rotating Secrets

Cisco Nexus Top of Rack スイッチの各ユーザー アカウントのパスワードを変更するには、次のコマンドを実行します。

```
n9k-1# conf t
n9k-1(config)# username <username> password <new password>
```

（注） Cisco Nexus Top of Rack スイッチは、強力なパスワードのみを許可するように設定されています。既存のパスワードを、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「パスワード強度のチェックを有効化」の項に記載されている要件を満たす強力なパスワードに置き換えてください。

Rotating Secrets of Cisco UCS Manager の Rotating Secrets

Cisco UCS Manager は、UCS サーバインフラストラクチャのコントロールセンターです。Cisco UCS Manager は、Azure Stack Hub アウトオブバンド管理ネットワークにアクセスできる任意のコンピュータ上のサポートされているブラウザを使用してアクセスできます。

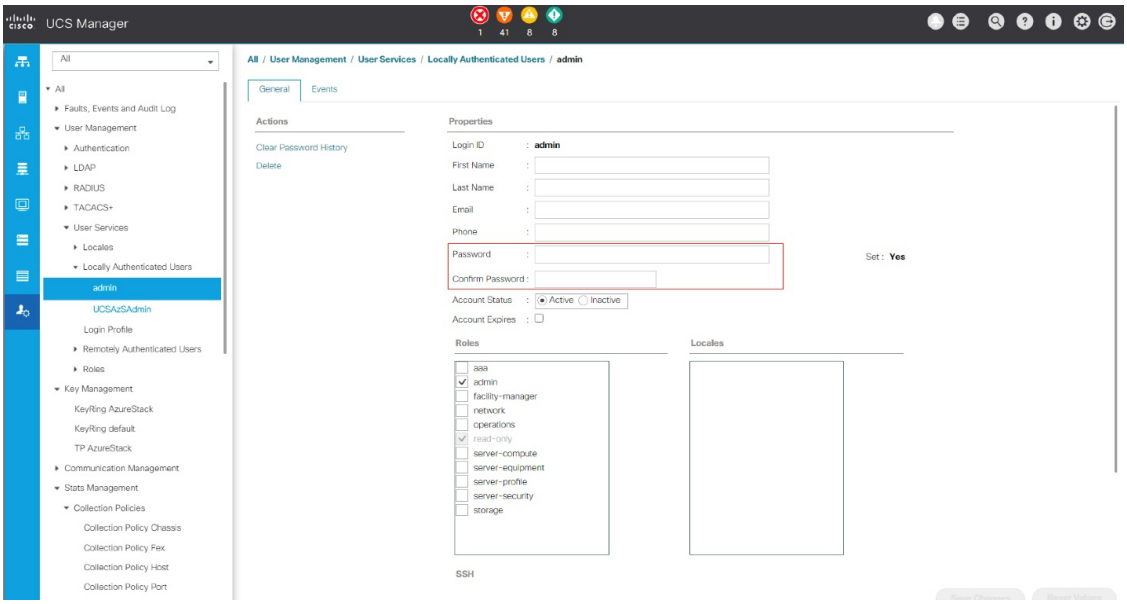
（注） シスコのサポート技術者から要求された場合を除き、Cisco UCS Manager を使用してサーバやその他のコンポーネントを再起動しないでください。Cisco UCS Manager からの再起動操作によって、一時的または永続的なデータが失われる可能性があります。

表に示すように、Cisco UCS Manager には 3 つのユーザー アカウントがあります。ユーザー アカウントのパスワードを変更するには、次のタスクを実行します。

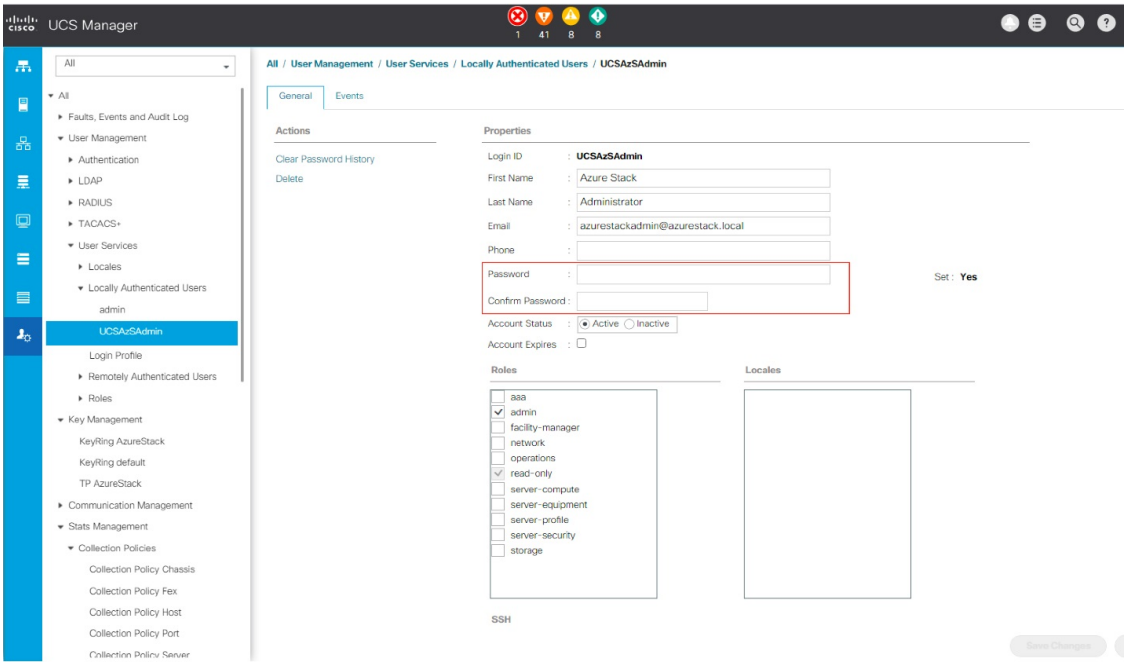
手順

ステップ 1 サポートされているブラウザで、`https://<UCS Manager IP>` と入力し、管理者クレデンシャルを使用して Cisco UCS Manager にログインします。

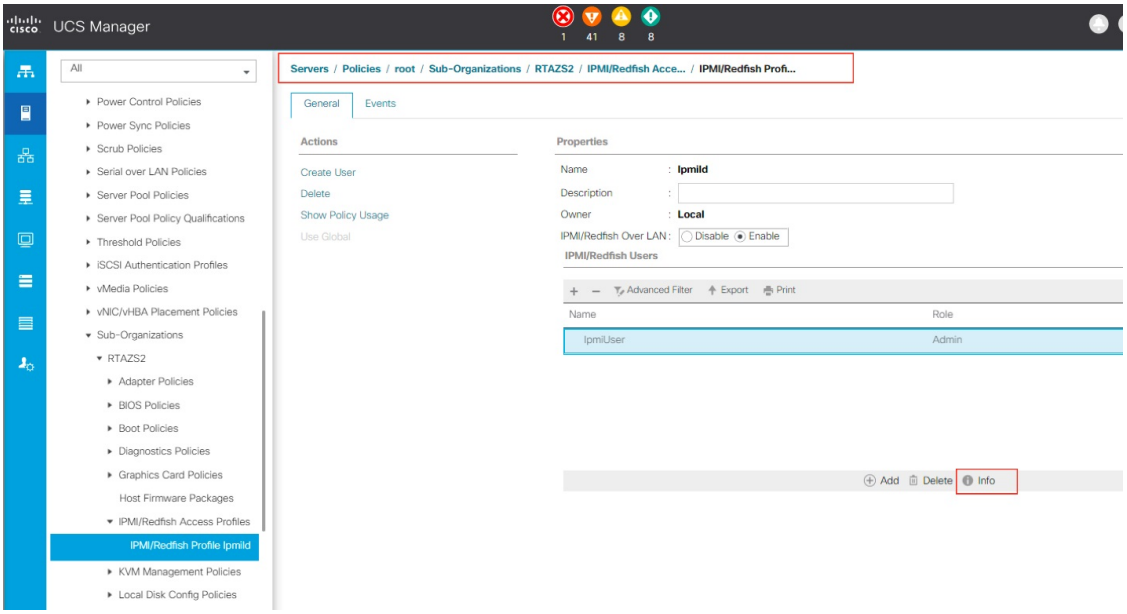
ステップ 2 [Navigation] ペインで [Admin] をクリックします。**[すべて（All）]** > **[ユーザー管理（User Management）]** > **[ユーザー サービス（User Services）]** > **[ローカル認証ユーザー（Locally Authenticated Users）]** の順に展開し、**[管理（Admin）]** ユーザーを選択します。右の **[プロパティ（Properties）]** 領域で、**[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



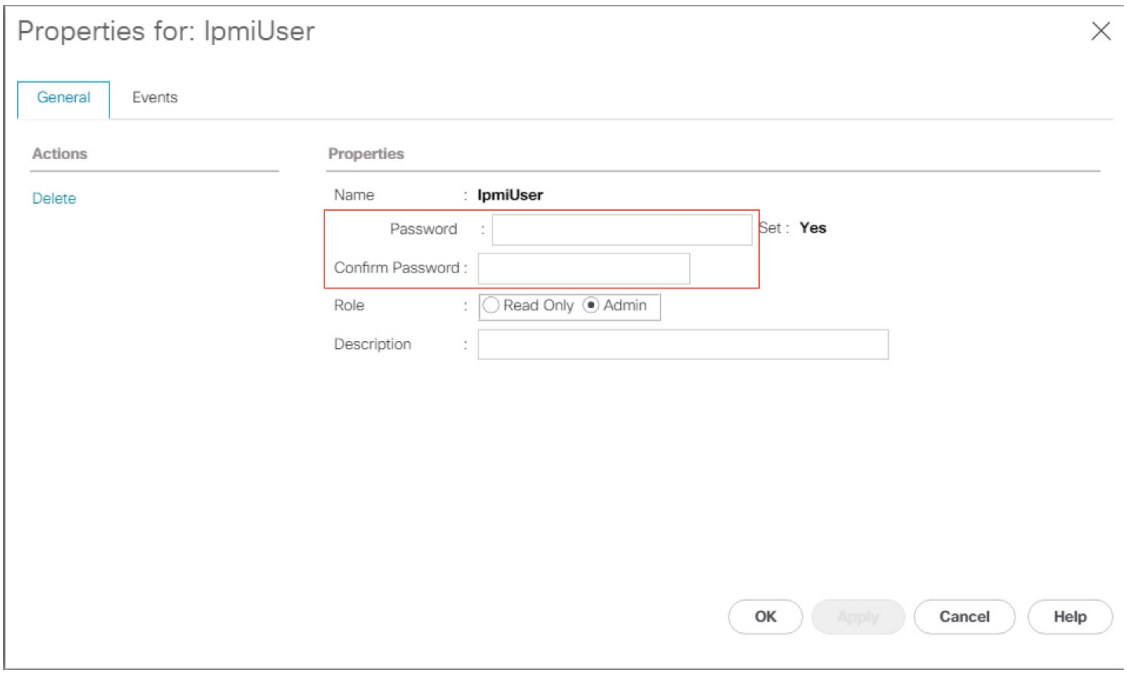
ステップ 3 **[すべて（All）]** > **[ユーザー管理（User Management）]** > **[ユーザー サービス（User Services）]** > **[ローカル認証ユーザー（Locally Authenticated Users）]** の下にある **[UCSAzSadmin]** ユーザーを選択します。右の **[プロパティ（Properties）]** 領域で、**[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



ステップ 4 [Navigation] ペインで [Servers] をクリックします。**[サーバ > ポリシー > ルート > サブ組織 > [展開中に提供された組織名（IPMI / Redfish Access Profiles）] > [IPMI/Redfish アクセス プロファイル（IPMI/Redfish Access Profiles）]** を展開し、**[IPMI / Redfish profile IpmiId]** を選択します。右側の **[プロパティ（Properties）]** 領域の **[IPMI / Redfish ユーザー（IPMI / Redfish Users）]** サブ領域で、**[IpmiUser]** を選択し、**[情報（info)]** をクリックします。



ステップ 5 **[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに新しいパスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



ステップ 6 Elevated PowerShell ウィンドウを開き、「Cloudadmin」アカウントを使用して Azure Stack Hub Emergency Recovery コンソールに接続します。`-BypassBMCUpdate` フラグを指定して `set-bmccredential` コマンドを実行し、ベースボード管理コントローラ（BMC）クレデンシャルを更新します。

（注） 順序は、まず Cisco UCS Manager から各サーバの BMC クレデンシャルを更新し（ステップ 4 と 5）、次に `set-bmccredential` コマンドを実行します（ステップ 6）。詳細については、Microsoft 社のドキュメントを参照してください。

汎用 Azure Stack Hub では、`set-bmccredential` コマンドを使用して、各サーバの BMC コントローラの BMC クレデンシャルを内部クレデンシャルストアの更新とともに更新できます。ただし、Cisco Azure Stack Hub では、サーバ BMC コントローラは Cisco UCS Manager を使用して制御されるため、各サーバでのクレデンシャルの更新はできません。したがって、Cisco UCS Manager を使用して BMC コントローラで新しいクレデンシャルを設定し、`set-bmccredential` コマンドを使用して Azure Stack Hub の内部クレデンシャル ストアを更新します。