

Secret Rotation

- Secret Rotation $(1 \sim ::)$
- Cisco Nexus Top of Rack Switch \mathcal{O} Rotating Secrets $(2 \sim \vec{\mathcal{V}})$
- Rotating Secrets of Cisco UCS Manager \mathcal{O} Rotating Secrets $(2 \sim \vec{\mathcal{V}})$

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 \mathcal{O} 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 \mathcal{O} 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。

cisco.	UCS Manager		🔞 👽 🙆 🐠 1 41 8 8		• 🖨	999 0000
æ	All	All / User Management / User Service	s / Locally Authenticated Users / admin			
	* AI	General Events				
	 Faults, Events and Audit Log User Management 	Actions	Properties			
	Authentication	Clear Password History	Login ID : admin			
- E	RADIUS	L.C.L.C.	Last Name :			
Q	 TACACS+ User Services 		Email :			
=	Locales		Password :		Set: Yes	
	 Locally Autnenticated Users admin 		Confirm Password :			
*	UCSAzSAdmin Login Profile		Account Status : Accive inactive]		
	Remotely Authenticated Users		Roles	Locales		
	 Roles Key Management 		aaa admin facility-manager			
	KeyRing AzureStack KeyRing default		operations			
	TP AzureStack		server-compute			
	Communication Management Stats Management		server-equipment server-profile			1
	Collection Policies Collection Policy Chassis		storage			
	Collection Policy Fex					
	Collection Policy Host Collection Policy Port		SSH			

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。

	UCS Manager		🙁 👽 🕓 📀			0
			1 41 8 8			
R	All	All / User Management / User Ser	vices / Locally Authenticated Users / UCSAzSAd	min		
	▼ AI	General Events				
	 Faults, Events and Audit Log 					
		Actions	Properties			
	 Authentication 	Clear Password History	Login ID : UCSAzSAdmin			
	► LDAP	Delete	First Name : Azure Stack			
	RADIUS		Last Name : Administrator			
	▶ TACACS+		Email : azurestackadmi	in@azurestack.local		
	▼ User Services		Phone :			
	 Locales 		Password		Out Mar	
	▼ Locally Authenticated Users				Set: res	
2	admin		Confirm Password :			
6	UCSAzSAdmin		Account Status : Active Inac	stive		
	Login Profile		Account Expires :			
	 Remotely Authenticated Users 		Roles	Locales		
	 Roles 		aaa]		
	✓ Key Management		✓ admin			
	KeyRing AzureStack		network			
	KeyRing default		operations			
	TP AzureStack		read-only server-compute			
	 Communication Management 		server-equipment			
	 Stats Management 		server-profile			
			storage			
	Collection Policy Chassis					
	Collection Policy Fex					
	Collection Policy Host		SSH			
	Collection Policy Port		001			
	Collection Policy Server					

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。

cisco.	UCS Manager		🛞 👽 🙆 📀 1 41 8 8	•
æ	All	Servers / Policies / root / Sub-Organizations	RTAZS2 / IPMI/Redfish Acce / IPMI/Redfish Profi	
-	 Power Control Policies Power Sync Policies 	General Events		
器	 Scrub Policies Serial over LAN Policies 	Create User	Properties Name : Ipmild	
Ŧ	 Server Pool Policies Server Pool Policy Qualifications 	Delete Show Policy Usage	Description : Owner : Local	
	 Threshold Policies iSCSI Authentication Profiles 		IPMI/Redfish Over LAN : Disable Disable Enable	
	vMedia Policies vNIC/vHBA Placement Policies Sub Operations		+ - Ty Advanced Filter ↑ Export Print Name	Role
3 ₀	Sub-Organizations RTAZS2 Adapter Policies BIOS Policies		IpmiUser	Admin
	 Boot Policies Diagnostics Policies Graphics Card Policies Host Firmware Packages 			⊕ Add
	IPMI/Redfish Access Profiles IPMI/Redfish Profile Ipmild KVM Management Policies Local Disk Config Policies			

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。

Properties for: IpmiUser				×
General Events				
Actions	Properties			
Delete	Name :	IpmiUser	_	
	Password	:	Set: Yes	
	Confirm Password :			
	Role :	Read Only Admin	-	
	Description :			
			OK Apply	Cancel Help

- 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。

I

Rotating Secrets of Cisco UCS Manager \mathcal{O} Rotating Secrets