HX Data Platform インターフェイスへのログイン

HyperFlex クラスタ インターフェイスの概要

それぞれの HyperFlex インターフェイスから、HX ストレージ クラスタに関する情報にアクセスし、アクションを実行することができますHX。HXストレージクラスタのインターフェイスは次のとおりです。

- HX Connect—モニタリング、パフォーマンス チャート、およびアップグレード、暗号化、複製、データストア、ノード、ディスク、VM ready clones のタスク。
- HX Data Platform プラグイン—モニタリング、パフォーマンス チャート、データストア、ホスト（ノード）、ディスクのタスク。
- Admin Shellコマンドライン：HX Data Platform の `hxcli` コマンドを実行します。
- HyperFlex システム RESTful API—オンデマンドのステートレス プロトコルにより、HyperFlex システムの認証、レプリケーション、暗号化、モニタリング、および管理を可能にします。

- パフォーマンスを最も正確に読み取るには、HX Connect クラスタ レベルのパフォーマンスチャートを参照してください。他のグラフでは、HyperFlexのストレージを分散し、データストアを介してVMが消費するという方法が原因で、全体像が把握しづらい場合があります。

他にも次のインターフェイスがあります。

- HX Data Platform インストーラ：HX Data Platform のインストール、HX ストレージ クラスタの展開と拡張、ストレッチ クラスタの展開、Hyper-V クラスタの展開。
- Cisco UCS Manager — HX ストレージ クラスタのネットワーク、ストレージとストレージアクセス、およびリソースの管理のタスク。
- VMware vSphere Webクライアントおよびvsphereクライアント：vCenterクラスタ内のすべてのVMware ESXiサーバを管理します。
- VMware ESXi — ホスト コマンド ラインを提供する個々の ESXi ホストの管理。

HX Data Platform ログイン クレデンシャルに関するガイドライン

`hxcli` コマンドは、ログイン クレデンシャルを要求します。

HX Data Platform インストーラの実行時に、事前定義された `admin` および `root` ユーザの管理シェルパスワードが指定されます。インストール後は、`hxcli` コマンドラインを使用してパスワードを変更できます。

ユーザーが 10 回連続で間違ったクレデンシャルでログインしようとした場合、アカウントは 2 分間ロックされます。SSH でログインの試行が失敗した場合、アカウントがロックされたことを示すエラー メッセージが表示されます。HX Connect または REST API でログインの試行が失敗した場合、10 回の試行中にアカウントがロックされたことを示すエラー メッセージが表示されます。

コンポーネント	権限レベル	ユーザ名（Username）	パスワード（Password）	注記
HX Data Platform インストーラ VM	root	root	Cisco123	**重要** システム出荷時のデフォルト パスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。
HX 接続	管理者または読み取り専用	vCenter で定義されたユーザ。	vCenter で定義されたユーザ。	
		事前定義された `admin` または `root` ユーザ。	HX のインストール時に指定。	
管理シェル		HX のインストール時に定義されたユーザ。 事前定義された `admin` ユーザー。	HX のインストール時に指定。 強力なパスワードが必要です。	ストレージ クラスタ内のすべてのノードで一致している必要があります。 安全な admin シェルへの SSH のサポートは、ユーザー admin に制限されています。 インストール後、パスワードを変更するときは `hxcli` コマンドを使用します。

コンポーネント	権限レベル	ユーザ名（Username）	パスワード（Password）	注記
vCenter	admin	デフォルト：administrator@vsphere.local SSO 対応。 設定どおり（MYDOMAIN\name または name@mydomain.com）	SSO 対応。 設定どおり。	読み取り専用ユーザーは、HX Data Platform プラグインにアクセスできません。
ESXi サーバ	root	SSO 対応。 設定どおり。	SSO 対応。 設定どおり。	ストレージ クラスタ内のすべての ESX サーバで一致している必要があります。
ハイパーバイザ	root	root	HX のインストール時に指定。	HX のインストール後にパスワードを変更するには、vCenter または `esxcli` コマンドを使用します。
UCS Manager	admin	設定どおり。	設定どおり。	
ファブリック インターコネクト	admin	設定どおり。	設定どおり。	

HX Data Platform の名前、パスワード、文字

ほとんどの印刷可能 ASCII 文字と拡張 ASCII 文字を名前とパスワードに使用できます。ただし一部の文字は、HX Data Platform のユーザ名、パスワード、仮想マシン名、ストレージ コントローラ VM 名、およびデータストア名に使用できません。フォルダとリソース プールには、使用できない文字はありません。

パスワードは、少なくとも 1 つの小文字、1 つの大文字、1 つの数字、および次のうち 1 つの特殊文字を含む、10 文字以上で指定する必要があります。

アンパサンド（&）、アポストロフィ（'）、アスタリスク（*）、アット マーク（@）、バック スラッシュ（\）、コロン（:）、カンマ（,）、ドル記号（$）、感嘆符（!）、スラッシュ（/）、小なり記号（<）、大なり記号（>）、パーセント（%）、パイプ（|）、シャープ（#）、疑問符（?）、セミコロン（;）

特殊文字を入力するときは、使用するシェルを考慮してください。シェルによって、注意が必要な文字が異なります。名前またはパスワードに特殊文字がある場合は、引用符で囲んでください（例：'speci@lword!'）。フィールドから HyperFlex Installer パスワードの単一引用符内で、パスワードを入力する必要はありません。

HX ストレージ クラスタの名前

HX クラスタ名の最大文字数は 50 文字です。

HX ストレージ クラスタのホスト名

HX クラスタ ホスト名は 80 文字以内です。

仮想マシンとデータストアの名前

仮想マシン名、コントローラ VM 名、またはデータストア名の作成時にはほとんどの文字を使用できます。エスケープされた文字を、仮想マシン名、コントローラ VM 名、またはデータストア名に使用できます。

最大文字数：仮想マシン名には 80 文字まで使用できます。

除外される文字：スナップショットの対象となるユーザ仮想マシン名やデータストア名には、次の文字を使用しないでください。

- アクセント（`）

特殊文字：次の特殊文字を、ユーザの仮想マシンまたはデータストア名で使用できます。

- アンパサンド（&）、アポストロフィ（'）、アスタリスク（*）、アットマーク（@）、バック スラッシュ（\）、サーカムフレクス（^）、コロン（:）、カンマ（,）、ドル記号（$）、ドット（.）、二重引用符（"）、等号（=）、感嘆符（!）、スラッシュ（/）、ハイフン（-）、左波カッコ（{）、左丸カッコ（(）、左角カッコ（[）、小なり記号（<）、大なり記号（>）、パーセント（%）、パイプ（|）、プラス記号（+）、シャープ（#）、疑問符（?）、右波カッコ（}）、右丸カッコ（)）、右角カッコ（]）、セミコロン（;）、ティルダ（~）、アンダースコア（_）

ユーザ名の要件

ユーザ名として HX Data Platform のコンポーネントに固有のものを指定でき、UCS Manager のユーザ名要件を満たす必要があります。

UCS Manager ユーザ名の要件。

- 文字数：6 ～ 32 文字
- Cisco UCS Manager 内で一意である必要があります。
- 英文字から始まる必要があります。
- 英文字（大文字または小文字）が必要です。
- 数字を含めることができます。すべて数字にすることはできません。
- 特殊文字：アンダースコア（_）、ダッシュ（-）、およびドット（.）に限定

コントローラ VM パスワードの要件

コントローラ VM の root ユーザ/admin ユーザのパスワードには、次の規則が適用されます。

（注） パスワードに関する一般的な規則：コマンド文字列にパスワードを含めないでください。コマンドがパスワードの入力を求めることができる状態にします。

- 最小長：10
- 最小 1 大文字
- 最小で 1 つの大文字
- 最小で 1 つの数字
- 最小で 1 つの特殊文字
- 最大 3 回の再試行で新しいパスワードを設定

コントローラ VM パスワードを変更するには、常に `stcli` コマンドを使用します。Unix パスワード コマンドなどの他のパスワード変更コマンドを使用しないでください。

1. 管理コントローラ VM にログインします。
2. `stcli` コマンドを実行します。

   stcli security password set [-h] [--user USER]

   変更は、HX クラスタですべてのコントローラ Vm に伝達されます。

UCS Manager および ESX のパスワード形式と文字の要件

UCS Manager と VMware ESXi のパスワードの形式と文字の要件の概要は次のとおりです。詳細については、Cisco UCS Manager および VMware ESX のドキュメントを参照してください。

- **文字クラス**：小文字、大文字、数字、特殊文字。

  パスワードは大文字と小文字が区別されます。

- **文字長**：最小 6、最大 80

  4 つすべての文字クラスの文字が含まれる場合は、6 文字以上が必要です。

  3 つ以上の文字クラスの文字が含まれる場合は、7 文字以上が必要です。

  1 つまたは 2 つの文字クラスの文字しか含まれない場合は、8 文字以上が必要です。

- **開始文字と終了文字**：パスワードの先頭の大文字またはパスワードの末尾の数字は文字数の合計に含まれません。

  パスワードが大文字で始まる場合は、2 つの大文字が必要です。パスワードが数字で終わる場合は、2 つの数字が必要です。

  要件を満たす例：

h#56Nu：6 文字。4 クラス。大文字で始まっていません。数字で終わっていません。

h5xj7Nu：7 文字。3 クラス。大文字で始まっていません。数字で終わっていません。

XhUwPcNu：8 文字。2 クラス。大文字で始まっていません。数字で終わっていません。

Xh#5*Nu：6 文字としてカウントされます。4 つの文字クラス。大文字で始まっています。数字で終わっていません。

h#5*Nu9：6 文字としてカウントされます。4 つの文字クラス。大文字で始まっていません。数字で終わっています。

- **連続文字数**：最大 2。たとえば、hhh###555 は許容されません。

  ただし、VSphere SSO ポリシーでこの値を設定することは可能です。

- **除外文字**：

  UCS Manager のパスワードには、エスケープ（\）文字を使用できません。

  ESX パスワードには、これらの文字を使用できません。

  - ユーザ名と同じものやユーザ名を逆にしたものは使用できません。
  - 辞書に載っている単語は使用できません。
  - パスワードには、エスケープ文字（\）、ドル記号（$）、疑問符（?）、等号（=）を使用できません。

- **辞書に載っている単語**：

  辞書に載っている単語は使用しないでください。

AAA 認証 REST API

Cisco HyperFlex は、ストレージクラスタのリソースにアクセスするための REST API を提供します。AAA 認証 REST API は、ユーザを認証し、入力されるログイン情報とアクセス トークンを交換するためのメカニズムを提供します。このアクセス トークンは他の REST API コールを呼び出すために使用できます。

認証 REST API (/auth) には、レート制限が適用されます。15 分のウィンドウでは、/auth は最大 5 回呼び出せます (正常に呼び出せた場合)。各ユーザは、取り消されていないトークンを最大 8 つ作成することができます。次に /auth を呼び出すと、新しいトークンの余地を設けるため、最も古い発行済みトークンが自動的に取り消されます。システムには、最大で 16 の取り消されていないトークンが存在できます。ブルートフォース攻撃を防ぐために、認証試行が 10 回連続で失敗した場合、ユーザアカウントは 120 秒間ロックされます。発行されたアクセス トークンは 18 日間 (1555200 秒) 有効です。

（注） HxConnect はログインのために /auth コールを使用します。この場合も同じ制限が適用されます。

HX Connect へのログイン

Cisco HyperFlex Connect は、HX ストレージのクラスタ モニタリング、およびレプリケーション、暗号化、データストア、および仮想マシンのタスクに対し、HTML5 ベースのアクセスを提供します。

セッションについて

HX Connectへの各ログインはセッションです。セッションは、HX Connect にログインした時からログアウトする時までの間のアクティビティの期間です。セッション中にブラウザのCookieを手動でオフにしないでください。それにより、セッションもドロップされるためです。ドロップした場合でも、セッションを閉じるためにブラウザを閉じないでください。そのセッションは、引き続きオープンなセッションとしてカウントされます。デフォルトのセッションの最大値は次のとおりです。

- ユーザごとに 8 の同時セッション
- HX ストレージ クラスタ全体での 16 の同時セッション。

始める前に

重要
- 読み取り専用ユーザの場合は、ヘルプに記載されているすべてのオプションが表示されないことがあります。HX Connect では、ほとんどのアクションの実行に管理者特権が必要です。
- vCenter 上の時間とコントローラ VM 上の時間が同期またはほぼ同期していることを確認します。vCenter の時間とクラスタの時間のずれが大きすぎると、AAA 認証は失敗します。

ステップ 1 HX ストレージ クラスタ管理 IP アドレスを探します。

個々の Storage Controller VM ではなく、管理 IP アドレスの完全修飾ドメイン名（FQDN）を使用します。

ステップ 2 ブラウザで、HX ストレージ クラスタ管理 IP アドレスを入力します。

ステップ 3 HXストレージクラスタのログインクレデンシャルを入力します。

- **RBAC ユーザ**：次のロールに基づくアクセス制御（RBAC）ログインを Cisco HyperFlex Connect サポートします。

- **管理者**：管理者ロールを持つユーザには、読み取りおよび変更操作の権限があります。これらのユーザは、HXストレージクラスタを変更できます。
- **読み取り専用**：読み取り専用ロールを持つユーザには、読み取り（表示）権限があります。HXストレージクラスタに変更を加えることはできません。

これらのユーザーは vCenter を介して作成されます。vCenter ユーザー名の形式は `<name>@domain.local` で、ユーザー プリンシパル名（UPN）形式で指定されています。例：`administrator@vsphere.local`。ユーザー名に「ad:」などのプレフィックスを追加しないでください。

- **HX 事前定義ユーザ**： HX データ プラットフォーム事前定義ユーザ `admin` または `root` を使用してログインするには、`local/` プレフィックスを入力します。例：`local/root` または `local/admin`。

  `local/` ログインで実行したアクションは、ローカル クラスタにのみ影響します。

  vCenter は HX Connect でセッションを認識します。このため vCenter で発生するシステム メッセージは `local/root` ではなくセッションのユーザを示す可能性があります。たとえば、アラームで、`Acknowledged By might list com.springpath.sysmgmt.domain-c7` と表示されます。

目のアイコンをクリックすると、パスワード フィールドのテキストが表示または非表示となります。このアイコンは、他のフィールド要素によって見えにくくなる場合があります。それでも、目のアイコンの領域をクリックすると、切り替え機能は動作します。

次のタスク

- HX Connect に表示されたコンテンツを更新するには、更新（円形）アイコンをクリックします。これによってページが更新されない場合は、キャッシュをクリアして、ブラウザをリロードします。
- HX Connect をログアウトして、適切にセッションを閉じるには、**[ユーザ（User）]** メニュー（右上）> **[ログアウト（Logout）]** を選択します。

コントローラ VM（stcli）コマンド ラインへのログイン

すべての `stcli` コマンドは、HX クラスタ情報を読み取るコマンドと HX クラスタを変更するコマンドに分かれています。

- 変更のコマンド：管理者レベルのアクセス許可が必要です。例：

  ```
  stcli cluster create
  ```

  ```
  stcli datastore create
  ```

- 読み取りのコマンド：管理者レベルのアクセス許可または読み取り専用レベルのアクセス許可で許可されます。例：

  ```
  stcli <cmd> -help
  ```

  ```
  stcli cluster info
  ```

```
stcli datastore info
```

HX Data Platform の stcli コマンドを実行するには、HX Data Platform ストレージ コントローラ VM コマンド ラインにログインします。

重要 コマンド文字列にパスワードを含めないでください。コマンドは、プレーンテキストとしてログに頻繁に渡されます。コマンドからパスワードの入力を求められるまで待ちます。これは、ログイン コマンドだけでなく stcli コマンドにも当てはまります。

ストレージ コントローラ VM の HX Data Platform コマンドライン インターフェイスには、次の方法でログインできます。

- コマンド ターミナルから
- HX Connect Web CLI ページから

  HX Connect では直接コマンドのみサポートされます。

  - 直接コマンド：1 回のパスで完了し、コマンドラインを介した応答を必要としないコマンド。直接コマンドの例：`stcli cluster info`
  - 間接コマンド：コマンドラインを介したライブ応答を必要とするマルチレイヤのコマンド。対話型コマンドの例：`stcli cluster reregister`

ステップ 1 コントローラ VM の DNS 名を探します。

1. **[VM]** > **[概要（Summary）]** > **[DNS 名（DNS Name）]** を選択します。
2. vSphere Web クライアント **[ホーム（Home）]** > **[VVM とテンプレート（VMs and Templates）]** > **[vCenter サーバ（vCenter server）]** > **データセンター** > **[ESX エージェント（ESX Agents）]** > **[VM]** から。
3. コントローラ VM のストレージ クラスタ リストにクリック スルーします。

ステップ 2 ブラウザから、DNS 名と /cli パスを入力します。

a) パスを入力します。

例

```
# cs002-stctlvm-a.eng.storvisor.com/cli
```

想定されるユーザ名：admin、パスワード： HX クラスタ作成時に定義。

b) プロンプトが表示されたら、パスワードを入力します。

ステップ 3 コマンド ライン ターミナルから ssh を使用します。

（注） ssh ログイン文字列にパスワードを含めないでください。ログインは、プレーン テキストとしてログに渡されます。

a) ssh コマンド文字列を入力します。

b) 証明書の警告が表示される場合があります。yes と入力して警告を無視して続行します。

```
------------------------------------------------------------
                  !!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
------------------------------------------------------------
HyperFlex StorageController 2.5(1a)# exit
logout
Connection to 10.198.3.22 closed.]$ssh root@10.198.3.24
The authenticity of host '10.198.3.24 (10.198.3.24)' can't be established.
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)?
```

c) プロンプトが表示されたら、パスワードを入力します。

```
# ssh admin@10.198.3.22
 HyperFlex StorageController 2.5(1a)
admin@10.198.3.22's password:
```

ステップ 4 [HX Connect] から：[HX Connect] にログインし、**[Web CLI]** を選択します。

（注） HX Connect Web CLI からは非対話型のコマンドのみを実行できます。

ストレージ コントローラのパスワードの変更

インストール後に HyperFlex ストレージ コントローラのパスワードをリセットするには、次の手順を実行します。

ステップ 1 ストレージ コントローラ VM にログインします。

ステップ 2 Cisco HyperFlex ストレージ コントローラ パスワードを変更します。

```
# stcli security password set
```

このコマンドによって、ストレージ クラスタ内のすべてのコントローラ VM に変更が適用されます。

（注） 新しいコンピューティング ノードを追加し、**stcli security password set** コマンドを使用してクラスタ パスワードをリセットしようとすると、コンバージド ノードは更新されますが、コンピューティング ノードはデフォルト パスワードのままになることがあります。コンピューティング ノードのパスワードを変更するには、次の手順を使用します。

ステップ 3 新しいパスワードを入力します。

ステップ 4 **Enter** を押します。

Cisco HX Data Platform インストーラへのログイン

次に、HX Data Platform ソフトウェアをインストールします。

（注） Cisco HX Data Platform インストーラを起動する前に、ストレージ クラスタに含める予定の vCenter クラスタにあるすべての ESXi サーバがメンテナンス モードであることを確認します。

ステップ 1 ブラウザで、HX データ プラットフォーム インストーラがインストールされた VM の URL を入力します。

このアドレスは、前のセクション**「HX Data Platform インストーラの展開」**で入手しています。たとえば、*http://10.64.4.254* です。

ステップ 2 次のクレデンシャルを入力します。

- **[ユーザ名（Username）]**：*root*
- **パスワード**（デフォルト）：Cisco123

注目 システムに同梱されているデフォルトのパスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

EULA を読みます。[利用規約に同意します（I accept the terms and conditions）] をクリックします。

右下隅に記載された製品バージョンが正しいことを確認します。**[ログイン（Login）]** をクリックします。

ステップ 3 [HX Data Platform Installer Workflow] ページには、さらに移動するための 2 つのオプションがあります。

- **[クラスタの作成]** ドロップダウン リスト：標準のクラスタ、ストレッチ クラスタ、または Hyper-V クラスタを展開できます。
- **クラスタ展開**：データを提供して、既存の標準的なストレージ クラスタにコンバージド ノードやコンピューティング ノードを追加できます。

SSH を使用した SCVM の root/admin パスワードのリセット

このトピックでは、HX 4.5(1a) および 4.5(2a) で SCVM の root/admin パスワードをリセットするためのプロセスを開始する方法について説明します。これは、システムへのルート アクセスを制限する HX 4.5 で導入されたセキュア シェル機能を使用する新しい要件によるものです。このプロセスを完了するには、Cisco TAC に連絡して協力する必要があることに注意してくだ

さい。開始する前に、製品のパスワードをリセットする手順へのアクセスを制御する、軽減策を講じるとよいでしょう。

始める前に

製品パスワードのリセット手順へのアクセスを制御するため、軽減策が講じられています。

ステップ 1 任意の ESXi ホストに root として SSH で接続します。

ステップ 2 次のコマンドを使用して、ストレージ コントローラー データ ネットワーク経由で証明書を使用して、この ESXi ホストに存在する SCVM に SSH で接続します。「Y」を入力して承認します。

例：

```
[root@hx-03-esxi-01:/opt/cisco/support]
ssh root@`/opt/cisco/support/getstctlvmip.sh "Storage Controller Data Network"` -i
/etc/ssh/ssh_host_rsa_key

HyperFlex StorageController 4.5(1a)------------------------------------------------------------
!!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.------------------------------------------------------------


HyperFlex StorageController 4.5(1a)
Last login: Mon Mar 2217:10:192021from192.168.150.67
WARNING: By accepting this support session, you give your consent and hereby authorize Cisco
to have privileged access to the supported Cisco device for the purpose of providing technical
support.
At the conclusion of this session you must exit root shell fromall the open ssh sessions of all the

controller vms of the cluster and invalidate the consent token in order to terminate Cisco’s access

and close the privileged access portal. You are hereby advised that failure to do so may create a
vulnerability in your product.
Accept(Y/n): y
```

ステップ 3 1 を入力して、ルート シェル アクセスのチャレンジを生成します。root シェル アクセスの時間の長さ（分単位）を設定します（たとえば、4320 分に設定します）。

例：

```
Consent token is needed to access root shell !!
1. Generate Challenge For root Shell Access
2. Accept Response
3. Exit
Enter CLI Option:1
Enter time period in minutes for root shell access(max4320 mins):4320
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
**************************************BEGIN TOKEN*****************************************
**************************************END TOKEN*******************************************
```

ステップ 4 TAC に連絡してプロセスを完了してください。これには、応答キーを生成して入力し、同意トークンをクラスタ内の他のコントローラ VM に同期することが含まれます。

SCVM のルート パスワードの復元

ルート パスワードを復元するために実行する唯一のオプションは、Linux シングル ユーザー モードを使用することです。Cisco TAC に連絡してこのプロセスを完了してください。

HX4.5(2c) の管理者パスワードの回復

このトピックでは、HX 4.5(2c) で SCVM の管理者パスワードをリセットする方法について説明します。

手順の概要

1. SSH を使用して ESXi ホストにログインします。
2. **host_rsa_key** を使用して、ESXi から、パスワードを回復する必要があるストレージ コントローラ VM に SSH で接続します。
3. `stcli security password set` コマンドを使用して、パスワードをリセットします。

手順の詳細

ステップ 1 SSH を使用して ESXi ホストにログインします。

ステップ 2 **host_rsa_key** を使用して、ESXi から、パスワードを回復する必要があるストレージ コントローラ VM に SSH で接続します。

```
root@ucs-120:~] ssh admin@`/opt/cisco/support/getstctlvmip.sh "Storage Controller Data Network"` -i
 /etc/ssh/ssh_host_rsa_key
HyperFlex StorageController 4.5(2c)
-------------------------------------------------------------
!!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
-------------------------------------------------------------

 HyperFlex StorageController 4.5(2c)
Last login: Tue Mar 8 08:26:41 2022 from 10.104.144.24
This is a Restricted shell.
Type '?' or 'help' to get the list of allowed commands.
admin:~$
```

ステップ 3 `stcli security password set` コマンドを使用して、パスワードをリセットします。

```
admin:~$ stcli security password set

Enter new password for user admin:
Re-enter new password for user admin:
```

SCVM の管理パスワードの復元

HX 4.5(2c) 以降、および HX 5.0(2x) では、RSA キーを使用して ESXi ホストから SSH を使用し、**recover-password** コマンドを実行することにより、ストレージコントローラ VM（SCVM）ルート パスワードを回復できます。 このプロセスを完了するには、TAC に連絡する必要があります。

始める前に

同意トークン ワークフローをサポートするには、TAC にお問い合わせください。

ステップ 1 SSH を使用して ESXi ホストにログインします。

ステップ 2 **host_rsa_key** コマンドを使用して、ESXi から、パスワードを回復する必要があるストレージコントローラ VM に SSH で接続します。

例

```
ssh admin@`/opt/cisco/support/getstctlvmip.sh` -i /etc/ssh/ssh_host_rsa_key
The authenticity of host '10.21.1.104 (10.21.1.104)' can't be established.
ECDSA key fingerprint is SHA256:OkA9czzcL7I5fYbfLNtSI+D+Ng5dYp15qk/9C1cQzzk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.21.1.104' (ECDSA) to the list of known hosts.
 HyperFlex StorageController 4.5(2c)
hostfile_replace_entries: link /.ssh/known_hosts to /.ssh/known_hosts.old: Function not implemented
update_known_hosts: hostfile_replace_entries failed for /.ssh/known_hosts: Function not implemented
This is a Restricted shell.
Type '?' or 'help' to get the list of allowed commands.
```

（注） ESXi 7.0 を実行している場合、通常のログインは機能しません。次のコマンドを実行する必要があります。

```
ssh -o PubkeyAcceptedKeyTypes=+ssh-rsa admin@`/opt/cisco/support/getstctlvmip.sh` -i
/etc/ssh/ssh_host_rsa_key
```

ステップ 3 `recover-password` コマンドを実行します。同意トークンを要求するプロンプトが表示されます。

（注） 同意トークンの提供については、TAC にお問い合わせください。

a) オプション 1 を入力してチャレンジを生成します。
b) 同意トークンをコピーします。
c) オプション 2 を入力して応答を受け入れます。
d) 同意トークンを入力します。
e) 管理者のための新しいパスワードを入力します。
f) 管理者のための新しいパスワードを再入力します。

例

```
admin:~$ recover-password
Consent token is needed to reset password. Do you want to continue?(y/[n]):
y
------------------------------------
```

```
1.  Generate Challenge
2.  Accept Response
3.  Exit
-----------------------------------
Enter Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
**************************************BEGIN TOKEN*****************************************
2g9HLgAAAQEBAAQAAAABAgAEAAAAAQMACL7HPAX+PhhABAAQo9ijSGjCx+Kj+Nk1YrwKlQUABAAAAGQGAAlIeXBl
cmZsZXgHAAxIeXBlcmZsZXhfQ1QIAAlIWVBFUkZMRVgJACBhNzAxY2VhMGZlOGVjMDQ2NDllMGZhODVhODIyYTY2NA==
**************************************END TOKEN*******************************************
-----------------------------------
1.  Generate Challenge
2.  Accept Response
3.  Exit
-----------------------------------
Enter Option:
2
Starting background timer of 30 mins
Please input the response when you are ready:
Gu4aPQAAAQEBAAQAAAABAgAEAAAAAQMBYnlQdnRGY1NiNkhtOUlyanlDQVJic0ZXYnp3MVpzdm1pcVh3ZzJLSlZZSVl
yeXBydU9oejVQWkVXdlcvWWdFci8NCnBrVFVpS1d0dVRlczZ6TkdITXl0T3dNaFhaT2lrM3pKL1M5cDJqR0xxcGFOY1
Ruc05SVFNybCtQeGwvK1Z1b1gNCjBHYVVxcExXdUhtUUc0UG9ZU2FBL0lwelRFYzlaRmFNeUFmYUdkOThMSmliZnl2UF
c2d0tNY1FCM3lPWmRjU1ENCklGeWZJTVpKL1RWd1lOaERZT001dXQveHZxUU1HN1hTbjdXb2R4Wng2NVNqVktWK2lId
FMyZzdxZUIzc3R2TEgNCld1VWNYS3lWdFdOaXRiaHBvWUIwT1J0N2l3dHlrSkcyWldWbnk4KzZIUUNJbW9xdnFoSU91S
kk4aElsWWNNaUENCnlEbEpkQ0wwcHVObSswNVVyTWM0M1E9PQ==
Response Signature Verified successfully !
Response processed successfully.
Consent token workflow is successful, allowing password reset.
Enter the new password for admin:
Re-enter the new password for admin:
Changing password for admin...
Password changed successfully for user admin.
```

recover-password コマンドを使用してパスワードを変更すると、パスワードはすべてのノードで同期されなくなります。すべてのノードでパスワードを再度変更および同期するには、**stcli security password set** を使用する必要があります。

ステップ 4 すべてのノードでパスワードを同期するには、任意のノードから **stcli security password set** コマンドを実行し、新しいパスワードを入力します。

例

```
admin:~$ stcli security password set
Enter new password for user admin:
Re-enter new password for user admin:
admin:~$
```

HX Data Platform REST API へのアクセス

Cisco HyperFlex HX シリーズ システムは、完全内包型の仮想サーバ プラットフォームを通じて、コンピューティング、ストレージ、ネットワークの 3 つのレイヤと強力な Cisco HX Data Platform ソフトウェア ツールを結合し、シングル ポイント接続による簡素化された管理を実現します。Cisco HyperFlex System は、単一の UCS 管理ドメインに HX ノードを追加することに

よってスケールアウトするように設計されたモジュラ システムです。ハイパーコンバージド システムはユーザのワークロード ニーズに基づいて統一されたリソースのプールを提供します。

HTTP 動詞を使用した Cisco HyperFlex System RESTful API は、HTTP 呼び出しを実行するように構成できる他のサードパーティ製の管理および監視ツールと統合されています。また、オンデマンド ステートレス プロトコルを介した HyperFlex システムの認証、レプリケーション、暗号化、監視、および管理を可能にします。この API を使用すれば、外部アプリケーションを HyperFlex の管理プレーンと直接インターフェイスさせることができます。

これらのリソースには URI（Uniform Resource Identifier）を介してアクセスし、これらのリソースに対する操作は POST（作成）、GET（読み取り）、PUT（更新）、DELETE（削除）などの HTTP 動詞を使用して実行します。

REST API は、Python、JAVA、SCALA、Javascript などのさまざまな言語でクライアント ライブラリを生成することも可能な Swagger を使用して記述されます。このように生成したライブラリを使用して、HyperFlex リソースを使用するためのプログラムとスクリプトを作成できます。

HyperFlex は、組み込み REST API アクセス ツールである REST エクスプローラも備えています。このツールは、リアルタイムで HyperFlex リソースにアクセスし、応答を監視するために使用します。REST エクスプローラは、コマンドラインから実行可能な CURL コマンドも生成します。

ステップ 1 ブラウザを開いて、https://developer.cisco.com/docs/ucs-dev-center-hyperflex/ DevNet アドレスにアクセスします。

ステップ 2 [Login] をクリックし、必要に応じてクレデンシャルを入力します。

セキュア管理シェル

Cisco HX リリース 4.5（1a）以降では、アクセスを制限することで次のことが可能になります。

- SSH を介したリモート **root** アクセスを介したクラスタ外部からのコントローラ VM は無効になります。
- 管理者ユーザのシェルアクセスは制限されており、使用できるコマンドは制限されています。管理シェルで許可されているコマンドを確認するには、**priv** と **help** または **?** コマンドを実行します。
- アクセスは、ローカル **root** の同意トークン プロセスを介してのみ使用できます。
- トラブルシューティングのためにコントローラの root シェルにログインするには、Cisco TAC が必要です。

注意事項と制約事項

- クラスタ外からコントローラVMへのSSH経由のリモートルートアクセスは無効になります。クラスタの一部のノードのみが、データネットワークを介して他のノードへのルートとしてSSH接続できます。
- 同意トークンの生成中または生成前にESXノードをメンテナンスモード（MM）にすると、そのSCVMでトークンを使用できなくなり、ノードがMMになりSCVMがオンラインに戻った後に同期ユーティリティを起動する必要があります。
- HX リリース 4.0(x) 以前のクラスタにルート対応ユーザが存在する場合は、HX リリース 4.5(1a) へのアップグレードを開始する前に削除します。ルート対応ユーザーが削除されない場合、アップグレードは続行されません。

同意トークンに関する情報

同意トークンは、管理者と Cisco Technical Assistance Centre（Cisco TAC）の相互の同意により、システム シェルにアクセスする組織のシステム ネットワーク管理者を認証するために使用されるセキュリティ機能です。

一部のデバッグシナリオでは、Cisco TAC エンジニアが特定のデバッグ情報を収集したり、実稼働システムでライブデバッグを実行する必要がある場合があります。このような場合、Cisco TACエンジニアは、デバイスのシステムシェルにアクセスするようユーザー（ネットワーク管理者）に依頼します。同意トークンは、システムシェルへの特権アクセス、制限アクセス、およびセキュアアクセスを提供する、ロック、ロック解除、および再ロックのメカニズムです。

セキュアシェル限定アクセスの場合、ネットワーク管理者とCisco TACが明示的な同意を提供する必要があります。Admin としてログインすると、admin として診断コマンドを実行するか、または TAC 支援を要求して **root** シェルを要求することができます。**root** シェル アクセスは、HyperFlex データ プラットフォーム内の問題のトラブルシューティングと修正のみを目的としています。

TAC が必要なトラブルシューティングを完了したら、同意トークンを無効にして root アクセスを無効にすることを推奨します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。