ユーザーの管理

Cisco HyperFlex ユーザー管理の概要

HXデータプラットフォームでアクションを実行したり、コンテンツを表示できるユーザのタイプには次のものがあります。

- **admin**：Cisco HX データ プラットフォーム に含まれている定義済みユーザー。パスワードは HX クラスタの作成時に設定されます。同じパスワードが `root` にも適用されます。このユーザには読み取り権限と変更権限が付与されます。
- **root**：Cisco HX データ プラットフォーム に含まれている定義済みユーザー。パスワードは HX クラスタの作成時に設定されます。同じパスワードが `admin` にも適用されます。このユーザには読み取り権限と変更権限が付与されます。
- **HX サービス アカウント ユーザ**: 作成されたCisco HX データ プラットフォーム ユーザです。このユーザには読み取り権限と変更権限が付与されます。パスワードは、ユーザの作成時に設定されます。
- **読み取り専用**: 他のドメイン管理者は読み取り専用ユーザです。このユーザには読み取り権限だけが付与されます。パスワードは、ユーザの作成時に設定されます。

HX インターフェイス	admin	root	*hx_admin*	*hx_readonly*
HX データ プラットフォーム インストーラ	必須	オプション	無効	無効

HX インターフェイス	admin	root	*hx_admin*	*hx_readonly*
HX 接続	ほとんどの HX タスクを実行できます。 ログインする際は、`local/` プレフィックスが必要です。例： `local/admin`	無効	ほとんどの HX タスクを実行できます。 優先されるユーザです。	モニタリング情報のみを表示できます。 HX のタスクを実行することはできません。 優先されるユーザです。
ストレージ コントローラ VM`hxcli`コマンドラインを使用する場合	ほとんどの HX タスクを実行できます。	ほとんどの HX タスクを実行できます。	ほとんどの HX タスクを実行できます。	ステータスの表示は、非インタラクティブな `hxcli` コマンドだけが実行できます。 HX のタスクを実行することはできません。 ログインする際は、`local/` プレフィックスが必要です。例： `vc-hx_readonly`
HX REST API	ほとんどの HX タスクを実行できます。 ログインする際は、`local/` プレフィックスが必要です。例： `local/admin`	ほとんどの HX タスクを実行できます。 ログインする際は、`local/` プレフィックスが必要です。例： `local/root`	ほとんどの HX タスクを実行できます。	ステータス レベルの RST API のみを実行できます。 HX のタスクを実行することはできません。

ユーザ管理の用語

- **認証**：ログイン クレデンシャルに関する処理。これらのプロセスは、通常、ユーザ名とパスワードに基づいて、指定されたユーザのユーザ クレデンシャルを確認します。一般に、認証によってユーザ クレデンシャルを確認し、認証されたユーザにセッションを関連付けます。

- **承認**：アクセス権限に関する処理。これらのプロセスでは、ユーザのアイデンティティに基づき、ユーザ/クライアントアプリケーションに対して、管理対象エンティティの作成、読み取り、更新、削除、あるいはプログラムの実行などのアクションを許可します。承認により、認証済みユーザがサーバ上で何を実行できるかが定義されます。
- **アカウンティング**：ユーザ アクションの追跡に関する処理。これらのプロセスでは、レコードを保持し、ログインセッションおよびコマンドの実行を含むユーザ操作を追跡します。情報はログに保存されます。これらのログは、Cisco HX 接続 または他の Cisco HX データ プラットフォーム インターフェイスを通じて生成することができるサポート バンドルに含まれます。
- **アイデンティティ（ID）**：ユーザ個人にアイデンティティが与えられ、特定の権限を持つロールがそれに割り当てられます。
- **権限**：リソースを使用するためにロールに与えられる設定。これは、ロールと、リソースおよびリソースによって公開される機能との間のリンクです。たとえば、データストアはリソースであり、変更ロールにはデータストアをマウントする権限が付与されますが、読み取り専用ロールでは単にそのデータストアの存在を表示できるだけです。
- **特権**：アイデンティティとアプリケーションの間のリンク。アプリケーションとの特定のインタラクションのコンテキストで使用されます。例：仮想マシンの電源をオンにする、データストアを作成する、データストアの名前を変更する。
- **リソース**：Cisco HX プラットフォーム全体であり、その機能および管理制御は、GET、POST、PUT、DELETE、HEAD などの HTTP 動詞を使用して HTTP 経由で公開されています。データストア、ディスク、コントローラ ノード、クラスタ属性はすべて、REST API を使ってクライアント アプリケーションに公開されるリソースです。
- **ロール**：権限レベルを定義します。各アプリケーション機能は、1 つまたは複数のロールによって実行される可能性があります。例：管理者、仮想マシン管理者、リソース プール管理者。ロールは特定の ID に割り当てられます。

AAA アカウンティングの監査ログ

AAA アカウンティングをサポートするため、Cisco HX データ プラットフォーム ではユーザ アクティビティの監査ログを実装しています。これらのログは、生成されたサポート バンドルに含まれます。

Cisco HX データ プラットフォーム を含む HX 接続 インターフェイスを介したサポート バンドルの生成については、『*Cisco HyperFlex システム トラブルシューティング ガイド*』を参照してください。

- **audit.log**：REST API および hxcli のアクティビティの監査レコードが含まれます。

  以下は、サンプル エントリです。ユーザ名、`administrator@yourdomain.local` に注目してください。

  ```
  2017-03-29-01:47:28.779 - 127.0.0.1 -> 127.0.0.1 - GET /rest/clusters 200;
  administrator@yourdomain.local 454ms
  ```

Cisco HX Data Platform の RBAC ユーザの作成

シスコ HX データ プラットフォーム は、認証、許可、アカウンティング (AAA)、および Open Authorization (OAuth) プロトコルの AAA 実装に対して、ロールベースのアクセス コントロール (RBAC) をサポートしています。Cisco HX データ プラットフォーム インターフェイスは、認証および認可ドメインに Microsoft Active DIrectory の統合を使用します。

2 つのロールがサポートされています。これらのロールに関連付けられている権限は変更できません。

- **[管理者 (Administrator)]** ロールは、ユーザが HX ストレージ クラスタ を変更できるようにします。HX ストレージ クラスタ で実行できるタスクのほとんどは、 管理者権限が必要です。管理ユーザは他のユーザを作成し、それらのロールを割り当てます。
- **[読み取り専用 (Read Only)]** ロールは、ユーザがステータスとサマリー情報をモニタできるようにします。読み取り専用ユーザは、HX ストレージクラスタを変更するタスクを実行できません 。

RBAC で作成されたユーザは、HX データ プラットフォーム のインターフェイスにアクセスできます。これには、管理者権限または読み取り専用権限を割り当てられたユーザが含まれます。この 2 つの違いは、ユーザが何を実行できるかということです。

- Cisco HX 接続
- `hxcli`コマンドを実行するための ストレージ コントローラ VM コマンドライン
- Cisco HyperFlex System REST API

ユーザへの権限の割り当て

始める前に

ユーザを作成します。

ステップ 1 Active Directory のユーザとコンピュータ ツールを開きます。

ステップ 2 管理者権限を与えるため、Builtin OU の下の**管理者グループ**にユーザを追加します。

ステップ 3 **[管理者 (Administrators)]** グループをダブルクリックして、管理者権限ユーザを追加するか、または**[リモート デスクトップユーザ (Remote Desktop Users)]** グループに読み取り専用ユーザを追加します。

ステップ 4 **[メンバー (Members)]** タブに移動します。

ステップ 5 **[追加 (Add)]** ボタンをクリックします。

ステップ 6 [検索 (search)] フィールドにユーザを入力し、**[名前の確認 (Check Names)]** ボタンをクリックします。

ステップ 7 **[OK]** をクリックして各ダイアログボックスを閉じます。