



## ユーザの管理

- [Cisco HyperFlex ユーザー管理の概要 \(1 ページ\)](#)
- [Cisco HX データ プラットフォーム RBAC ユーザーの作成 \(4 ページ\)](#)
- [ユーザへの権限の割り当て \(4 ページ\)](#)

## Cisco HyperFlex ユーザー管理の概要

HX Data Platform 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 Data Platform に含まれている定義済みユーザー。パスワードは、HX Clusterの作成時に設定されます。同じパスワードが root に適用されます。このユーザは読み取りおよび変更のアクセス許可を持ちます。
- **root** : Cisco HX Data Platform に含まれている定義済みユーザー。パスワードは、HX Clusterの作成時に設定されます。同じパスワードが admin に適用されます。このユーザは読み取りおよび変更のアクセス許可を持ちます。
- **administrator** : 作成された Cisco HX Data Platform ユーザー。このユーザは vCenter を介して作成され、RBAC ロールの administrator が割り当てられます。このユーザは読み取りおよび変更のアクセス許可を持ちます。パスワードは、ユーザの作成時に設定されます。
- **read-only** : 作成された Cisco HX Data Platform ユーザー。このユーザは vCenter を介して作成され、RBAC ロールの read-only が割り当てられます。このユーザは読み取りアクセス許可のみを持ちます。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 Data Platform インストーラ	必須	任意	無効	無効

HX インターフェイス	admin	root	hx_admin	hx_readonly
HX Connect	ほとんどのHXタスクを実行できます。  ログインには Local/ の拡張子が必要です。例：  local/admin	無効	ほとんどのHXタスクを実行できます。  優先ユーザ。	モニタリング情報の参照のみが可能です。  HX タスクを実行できません。  優先ユーザ。
stcli コマンドラインを持つストレージコントローラ VM	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。	ログインには vc- の拡張子が必要です。例：  vc hx_admin	HX タスクを実行できません。  ログインには vc- の拡張子が必要です。例：  vc hx_readonly
vCenter を介した HX Data Platform Plug-in	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。  vCenter SSO ユーザ。	vCenter 情報のみ表示可能です。  HX Data Platform Plug-in を表示できません。  vCenter SSO ユーザ。
HX REST API	ほとんどのHXタスクを実行できます。  ログインには Local/ の拡張子が必要です。例：  local/admin	ほとんどのHXタスクを実行できます。  ログインには Local/ の拡張子が必要です。例：  local/root	ほとんどのHXタスクを実行できます。  ログインには vc- の拡張子が必要です。例：  vc hx_admin	ステータス レベル REST API のみ実行できます。  HX タスクを実行できません。  ログインには vc- の拡張子が必要です。例：  vc hx_readonly

## ユーザ管理用語

- **認証**：ログインクレデンシャルに関する用語。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、指名ユーザのユーザクレデンシャルを確認します。認証は、一般的にユーザクレデンシャルを確認して、セッションを認証されたユーザと関連付けます。

- **承認**：アクセス許可に関する用語。これらのプロセスは、ユーザ/クライアントアプリケーションが何らかのアクション（管理対象エンティティの作成、読み取り、更新、または削除、あるいはプログラムの実行など）を実行することをユーザの ID に基づいて許可します。承認により、認証済みユーザがサーバ上で実行できることが定義されます。
- **アカウンティング**：ユーザ操作の追跡に関する用語。これらのプロセスは、レコードをキープし、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の操作を追跡します。情報はログに保存されます。これらのログは、Cisco HX Connect または他の Cisco HX Data Platform 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**：個人には ID が付与されます。これは割り当てられたロールであり、付与された権限が伴っています。
- **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、リソースおよびリソースによって公開されている機能の間のリンクです。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ていますが、読み取り専用ロールは、そのデータストアが存在することを表示するだけです。
- **特権**：ID 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、いずれも、REST API を使用してクライアントアプリケーションに公開されているリソースです。
- **ロール**：権限範囲レベルを定義します。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 Data Platform 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 Connect を含む HX Data Platform 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。

- **stMgrAudit.log**：stcli アクティビティの監査記録を含みます。

以下は、サンプル エントリです。キーワード Audit に注目してください。

```
2017-03-27-22:10:02.528 [pool-1-thread-1] INFO Audit - 2017-03-27-03.10.02 127.0.0.1  
--> 127.0.0.1 POST /stmgr 200 : root 27ms
```

このファイルには、他の情報も含まれています。監査イベントを抽出するには、スクリプトを使用して単語 `Audit` を抽出します。

- **audit.log** : REST API 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@vsphere.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@vsphere.local 454ms
```

## Cisco HX データ プラットフォーム RBAC ユーザーの作成

Cisco HX Data Platform は、管理者および読み取り専用の 2 種類のユーザーをサポートしています。HX Data Platform の新しいユーザは、VMware vCenter インターフェイスを介して作成されます。

### 始める前に

ユーザを作成するには、管理者特権が必要です。

**ステップ 1** vCenter 管理者として vSphere Web Client にログインします。

**ステップ 2** [Navigator Home] から、[Administration] > [Users and Groups] > [Users] に進みます。

**ステップ 3** [Add] (+) アイコンをクリックして、ユーザを追加します。[New User] の情報を入力し、[OK] をクリックします。

新しいユーザのユーザ名およびパスワードを指定します。

パスワードには、エスケープ文字 (\) 、ドル記号 (\$) 、疑問符 (?) 、等号 (=) を使用しないでください。ユーザ名に使用できる特殊文字は、アンダースコア (\_) 、ダッシュ (-) 、ドット (.) のみです。ユーザ名およびパスワードの要件については [HX Data Platform の名前、パスワード、文字](#) を参照してください。

### 次のタスク

RBAC ロール グループにユーザを追加します。「[ユーザへの権限の割り当て \(4 ページ\)](#)」を参照してください。

## ユーザへの権限の割り当て

権限は、vCenter の RBAC ロールを通じてユーザに割り当てられます。権限を割り当てるには、管理者または読み取り専用グループにユーザを追加します。

### 始める前に

ユーザを作成します。

---

**ステップ 1** Cisco vSphere Web Client で、[**Navigator Home (ナビゲーション ホーム)**] > [**Administration (管理)**] > [**Global Permissions (グローバル権限)**] > [**Manage (管理)**] の順に選択します。

**ステップ 2** [Add] (+) アイコンをクリックして権限を割り当てます。

**ステップ 3** [Assigned Role] を選択します。

[Global Permission Root - Add Permission] ダイアログボックスで、[Assigned Role] ドロップダウンメニューから選択します。次のいずれかを選択します。

- 管理者
- Read only

**ステップ 4** [Users and Groups] 領域で、[Add] をクリックします。

**ステップ 5** [Select Users/Groups] ダイアログボックスで、*user\_name* を選択して [Add] をクリックします。

**ステップ 6** [Check names] ボタンをクリックしてユーザ名を確認します。

**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。

---

