



ユーザーの管理

- [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ー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 Data Platform 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。このユーザーには読み取り権限と変更権限が付与されます。
- **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 Data Platform 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。このユーザーには読み取り権限と変更権限が付与されます。
- **administrator** : 作成された Cisco HX Data Platform ユーザー。このユーザーは vCenter で作成され、RBAC ロール administrator がこれに割り当てられます。このユーザー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、ユーザー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。このユーザーは vCenter で作成され、RBAC ロール read-only がこれに割り当てられます。このユーザーには読み取り権限だけが付与されます。パスワードは、ユーザー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	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 の hxcli コマンドライン	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。	ログインする際は、local/プレフィックスが必要です。例： vc-hx_admin	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
vCenter を介した HX Data Platform プラグイン	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 ユーザです。	VCenter 情報のみを表示できます。 HX Data Platform プラグインを表示できません。 vCenter SSO ユーザです。
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	無効	無効

ユーザー管理の用語

- **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。

- **stMgrAudit.log**：stcli アクティビティの監査記録を含みます。
サンプル エントリ。キーワード Audit に注意してください。

```
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、その他の情報も含まれます。監査イベントに絞り込むには、スクリプトを使用して単語 `Audit` をフィルタリングします。

- **audit.log** : REST API アクティビティの監査レコードが格納されます。

サンプル エントリ。ユーザ名 `administrator@vsphere.local` に注意してください。

```
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 は、管理者および読み取り専用の 2 種類のユーザーを HX データ プラットフォーム サポートしています。VMware vCenter インターフェイスを介して HX Data Platform の新しいユーザが作成されます。

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 vSphere Web クライアントに vCenter 管理者としてログインします。

ステップ 2 [ナビゲーション ホーム (Navigator Home)] から、[管理 (Administration)] > [ユーザとグループ (Users and Groups)] > [ユーザ (Users)]。

ステップ 3 [追加 (Add)] (+) アイコンをクリックして、ユーザを追加します。[ユーザの新規作成 (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。ユーザ名とパスワードの要件に関する情報は、[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

vCenter で、RBAC を介してユーザーに特権が割り当てられます。特権を割り当てるには、ユーザを管理者グループまたは読み取り専用グループに追加します。

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 [追加 (Add)] (+) アイコンをクリックし、ロールを割り当てます。

ステップ 3 [ロールの割り当て (Assigned Role)] を選択します。

[グローバル権限ルート - 権限の追加 (Global Permission Root - Add Permission)] ダイアログボックスで、[ロールの割り当て (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
- 読み取り専用 (Read only)

ステップ 4 [ユーザとグループ (Users and Groups)] 領域で、[追加 (Add)] をクリックします。

ステップ 5 [ユーザ/グループの選択 (Select Users/Groups)] ダイアログボックスで、*user_name* を選択し、[追加 (Add)] をクリックします。

ステップ 6 [名前の確認 (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。

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。