Managing Users

Managing Cisco HyperFlex Users Overview

The user types allowed to perform actions on or view content in the HX Data Platform, include:

- **admin**—A predefined user included with Cisco HX Data Platform. The password is set during HX Cluster creation. Same password is applied to `root`. This user has read and modify permissions.
- **root**—A predefined user included with Cisco HX Data Platform. The password is set during HX Cluster creation. Same password is applied to `admin`. This user has read and modify permissions.
- ***administrator***—A created Cisco HX Data Platform user. This user is created through vCenter and assigned the RBAC role, `administrator`. This user has read and modify permissions. The password is set during user creation.
- ***read-only***—A created Cisco HX Data Platform user. This user is created through vCenter and assigned the RBAC role, `read-only`. This user only has read permissions. The password is set during user creation.

HX Interface	admin	root	*hx_admin*	*hx_readonly*
HX Data Platform Installer	Required	Optional	Not valid	Not valid
HX Connect	Can perform most HX tasks. `local/` prefix required for login. Example: `local/admin`	Not valid	Can perform most HX tasks. A preferred user.	Can only view monitoring information. Cannot perform HX tasks. A preferred user.

HX Interface	admin	root	*hx_admin*	*hx_readonly*
Storage Controller VM with `stcli` command line	Can perform most HX tasks.	Can perform most HX tasks.	Can perform most HX tasks. `vc-` prefix required for login. Example: `vc-hx_admin`	Can only run non-interactive `stcli` commands to view status. Cannot perform HX tasks. `vc-` prefix required for login. Example: `vc-hx_readonly`
HX Data Platform Plug-in through vCenter	Can perform most HX tasks.	Can perform most HX tasks.	Can perform most HX tasks. A vCenter SSO user.	Can only view vCenter information. Cannot view HX Data Platform Plug-in. A vCenter SSO user.
HX REST API	Can perform most HX tasks. `local/` prefix required for login. Example: `local/admin`	Can perform most HX tasks. `local/` prefix required for login. Example: `local/root`	Can perform most HX tasks. `vc-` prefix required for login. Example: `vc-hx_admin`	Can only run status level REST APIs. Cannot perform HX tasks. `vc-` prefix required for login. Example: `vc-hx_readonly`

User Management Terms

- **Authentication—**For login credentials. These processes verify user credentials for a named user, usually based on a username and password. Authentication generally verifies user credentials and associates a session with the authenticated user.
- **Authorization—**For access permissions. These processes allow a user/client application to perform some action, such as create, read, update, or delete a managed entity or execute a program, based on the user's identity. Authorization defines what an authenticated user is allowed to do on the server.
- **Accounting—**For tracking user actions. These processes perform record-keeping and track user activities including login sessions and command executions. The information is stored in logs. These logs are included in the support bundle that can be generated through Cisco HX Connect or other Cisco HX Data Platform interface.
- **Identity—**Individuals are provisioned with identities that are assigned roles with granted permissions.
- **Permission—**Settings given to roles to use the Resource. It is the link between roles, resource and the function exposed by the resource. For example, Datastore is a resource and a modifying role is granted permission to mount the datastore, while a read only role can only view that the datastore exists.

- **Privilege—**The link between Identity and the application. It is used in the context of specific interaction with the application. Examples: Power On a Virtual Machine, Create a Datastore, or Rename a datastore.
- **Resource—**The entire Cisco HX Platform, whose functionality and management controls are exposed over HTTP using GET, POST, PUT, DELETE, HEAD and other HTTP verbs. Datastores, Disks, Controller Nodes, Cluster Attributes, are all resources that are exposed to client applications using REST API.
- **Role—**Defines an authority level. An application function may be performed by one or more roles. Examples: Administrator, Virtual Machine Administrator, or Resource Pool Administrator. Role is assigned to a given Identity.

Audit Logs for AAA Accounting

To support AAA accounting, Cisco HX Data Platform implements audit logs of user activity. These logs are included in the generated support bundle.

See the *Cisco HyperFlex Systems Troubleshooting Guide* for information on generating the support bundles through HX Data Platform interfaces, including Cisco HX Connect.

- **stMgrAudit.log—**Contains audit recoreds of `stcli` activity.

  Sample entry. Note the keyword, `Audit`.

  ```
  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
  ```

  This file contains other information as well. To filter for audit events, use a script to filter for the word, `Audit`.

- **audit.log—**Contains audit records for REST API activity.

  Sample entry. Note the user name, `administrator@vsphere.local`

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

Creating Cisco HX Data Platform RBAC Users

Cisco HX Data Platform supports two users: Administrator and Read Only. New users are created for the HX Data Platform through the VMware vCenter interface.

Before you begin

Creating users requires Administrator privileges.

Step 1 Login to vSphere Web Client as a vCenter administrator.

Step 2 From **Navigator Home**, **Administration** > **Users and Groups** > **Users**.

Step 3 Click **Add** (+) icon to add a user. Then complete the **New User** information and click **OK**.

Specify a user name and password for the new user.

For passwords, do not use escape character (\), dollar sign ($), question mark (?), equal sign (=). In user names, the only special characters allowed are underscore (_), dash (-), dot (.). See HX Data Platform Names, Passwords, and Characters for user name and password requirements.

What to do next

Add the user to an RBAC role group. See Assigning Users Privileges, on page 4.

Assigning Users Privileges

Privileges are assigned to users through the RBAC roles in vCenter. To assign privileges, add users to either the Administrator or Read-only group.

Before you begin

Create the user.

Step 1 From the Cisco vSphere Web Client, select **Navigator Home** > **Administration** > **Global Permissions** > **Manage**.

Step 2 Click **Add** (+) icon to assign roles.

Step 3 Select an **Assigned Role**.

In the **Global Permission Root - Add Permission** dialog box, select from the **Assigned Role** drop down menu. Choose one:

- **Administrator**
- **Read only**

Step 4 In the **Users and Groups** area, click **Add**.

Step 5 In the **Select Users/Groups** dialog box, select the *user_name* and click **Add**.

Step 6 Click **Check names** button, to verify the user name.

Step 7 Then click **OK** to close out of each dialog box.