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.
- **HX service account user—**A created Cisco HX Data Platform user. This user has read and modify permissions. The password is set during user creation.
- ***read-only*—**Other domain admins are read only users. 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.
Storage Controller VM with `hxcli` command line	Can perform most HX tasks.	Can perform most HX tasks.	Can perform most HX tasks.	Can only run non-interactive `hxcli` commands to view status. Cannot perform HX tasks. `vc-` prefix required for login. Example: `vc-hx_readonly`

HX Interface	admin	root	*hx_admin*	*hx_readonly*
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.	Can only run status level REST APIs. Cannot perform HX tasks.

- User Management Terms, on page 2
- Audit Logs for AAA Accounting, on page 3
- Creating RBAC Users for Cisco HX Data Platform, on page 3
- Assigning Users Privileges, on page 3

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.

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

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

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

Creating RBAC Users for Cisco HX Data Platform

CiscoHX Data Platform supports Role-Based Access Control (RBAC) for Authentication, Authorization, and Accounting (AAA) and the AAA implementation of the Open Authorization (OAuth) protocol. Cisco HX Data Platform interfaces use the Microsoft Active Direction integration for authentication and authorization domain.

Two roles are supported. Privileges associated with these roles cannot be modified.

- **Administrator—**The role allows users to modify the HX Storage Cluster. Most tasks that can be performed on a HX Storage Cluster require administrator privileges. Administrative users create other users and assign them roles.
- **Read Only—**The role allows users to monitor status and summary information. Read only users cannot perform any task that modifies the HX Storage Cluster.

RBAC created users have access to the HX Data Platform interfaces. This includes users assigned either administrator or read only permissions. The difference between the two is what the users are allowed to do.

- Cisco HX Connect
- Storage Controller VM command line for running `hxcli` commands
- Cisco HyperFlex Systems REST APIs

Assigning Users Privileges

Before you begin

Create the user.

Procedure

Step 1 Open Active Directory Users and Computers tool.

Step 2 Add user to **Administrators group** under the Builtin OU for Administrator privilege.

Step 3 Double click on **Administrators group** to add administrator privilege user or **Remote Desktop Users group** to add read only users.

Step 4 Navigate to the **Members** tab

Step 5 Click **Add** button

Step 6 Type the user in the search field and click **Check Names** button.

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