Lockdown Mode

Overview

This section provides an introduction to Lockdown mode, which is used to increase the security of an ESXi host by limiting the access allowed to the host. When this mode is enabled, the ESXi host can only be accessed through the vCenter server or the Direct Console User Interface (DCUI). Enabling Lockdown mode affects which users are authorized to access host services.

Note When enabling lockdown mode, you must add the hxuser account to each ESXi host exception user list.

Note Once Lockdown mode is enabled, and if root or administrator@vsphere.local or any other use is not part of the Exception user list, SSH to that ESX is not allowed. Similarly, if the host has been removed from the vCenter for some reason, adding the host back to vCenter is not allowed.

Table 1: Lockdown Mode Behavior

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions.	vCenter(vpxuser) Exception includes users, based on permissions.	vCenter(vpxuser) Exception includes users, based on permissions. vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host.	vCenter (vpxuser) Exception includes users, based on permissions. vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception includes users, based on permissions. vCloud Director (vslauser, if available)

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the DCUI. Access advanced option.	Users defined in the DCUI access advanced option. Exception includes users with administrator privileges on the host.	DCUI service is stopped.
ESXi Shell (if enabled)	Users with administrator privileges on the host.	Users defined in the DCUI access advanced option. Exception includes users with administrator privileges on the host.	Users defined in the DCUI access advanced option. Exception includes users with administrator privileges on the host.
SSH (if enabled)	Users with administrator privileges on the host.	Users defined in the DCUI access advanced option. Exception includes users with administrator privileges on the host.	Users defined in the DCUI access advanced option. Exception includes users with administrator privileges on the host.

- Enable or Disable Lockdown Mode, on page 2
- Troubleshoot Lockdown Mode, on page 3

Enable or Disable Lockdown Mode

This section describes how to enable or disable Lockdown mode either from the DCUI or from the vSphere web client.

Note Once Lockdown mode is enabled, and if root or administrator@vsphere.local or any other use is not part of the Exception user list, SSH to that ESX is not allowed. Similarly, if the host has been removed from the vCenter for some reason, adding the host back to vCenter is not allowed.

Enable or Disable Lockdown Mode from the DCUI:

Step 1 Log directly in to the ESXi host.

Step 2 Open the Direct Console User Interface (DCUI) on the host.

Step 3 Press **F2** for Initial Setup.

Step 4 Press **Enter** to toggle the Configure Lockdown Mode setting.

Step 5 Browse to the host in the vSphere Web Client inventory.

Enable or Disable Lockdown Mode from the vSphere Web Client:

Step 1 Browse to the host in the vSphere Web Client inventory.

Step 2 Click the **Manage** tab and click Settings.

Step 3 Under System, select **Security Profile**.

Step 4 In the Lockdown Mode panel, click **Edit**.

Step 5 Click **Exception Users** and select +Add user to add hxuser (all lowercase).

Step 6 Click **Lockdown Mode** and select one of the Lockdown mode options.

Troubleshoot Lockdown Mode

If you receive an error dialog box and/or the software upgrade fails in Lockdown mode, proceed with the following resolution options based on either of the following scenarios:

- At least one host is in Lockdown mode.
- The host is in Lockdown mode while the upgrade is in progress.

When at least one host is in Lockdown mode:

1. Check the host Lockdown mode in pre-upgrade validation.
2. Detect the situation, throw an error, and terminate the cluster upgrade.
3. Disable Lockdown mode and try the upgrade again.

When the host is in Lockdown mode while the upgrade in progress:

Step 1 Check the host Lockdown mode before host upgrade.

Step 2 Detect the situation and error out and failed the upgrade.

Step 3 Disable Lockdown mode and try the upgrade again.

Add Hosts to vCenter in Deploy Phase Error

Validation for Lockdown during HX installation is a check for ESXi host's SSH accessibility with the 'root' user. Adding the root user in the exception list is bypassing the deploy validation check for Lockdown mode. In this case, when hosts are being added to the vCenter in the deploy phase, it fails and therefore the HX installation also fails.

If adding hosts to vCenter in the deploy phase fails, and you receive the error message **Failed to add hosts to vCenter**:

Check for the Lockdown mode status, disable it, and remove the ‘root’ user from exception.