Hewlett Packard Enterprise

HPE Private Cloud AI 1.5 Factory Integration Guide

Part Number: 20-PCAI-FIG
Published: September 2025
Edition: 1.0

HPE Private Cloud AI 1.5 Factory Integration Guide

Abstract

This document describes how to configure the components of the HPE Private Cloud AI engineered system at the Integration Center before it is shipped to the customer datacenter. It supports HPE Private Cloud AI version 1.5 with recipe version 202507.3 and applies to the Small, Medium, and Large configurations. This document is CONFIDENTIAL and is intended for HPE Integration Center (factory) engineers, cloud service providers, field solution engineers, and any personnel responsible for solution configuration and delivery.

Part Number: 20-PCAI-FIG
Published: September 2025
Edition: 1.0

Notices

Acknowledgments

Revision history

Edition	Date	Solution version	Recipe version	Configuration type	Summary
1.0	September 2025	1.5	202507.3	Small, Medium, and Large	• Initial release

Table of contents

Executive summary

HPE Private Cloud AI (AI), part of the NVIDIA AI Computing by HPE portfolio, is a turnkey, scalable, and AI-optimized private cloud designed to accelerate AI project deployment while ensuring data remains under enterprise control. The engineered system combines NVIDIA's accelerated computing, networking, and software with HPE's high-performance compute, storage and the HPE GreenLake cloud, along with HPE capabilities for data pipelines, orchestration, and Machine Learning Operations (MLOps). This integration enables enterprises of all sizes to gain a fast, flexible path for developing and deploying GenAI applications. Enterprises can leverage these capabilities to overcome barriers to AI adoption, ensuring faster time to value and seamless scalability to support future growth.

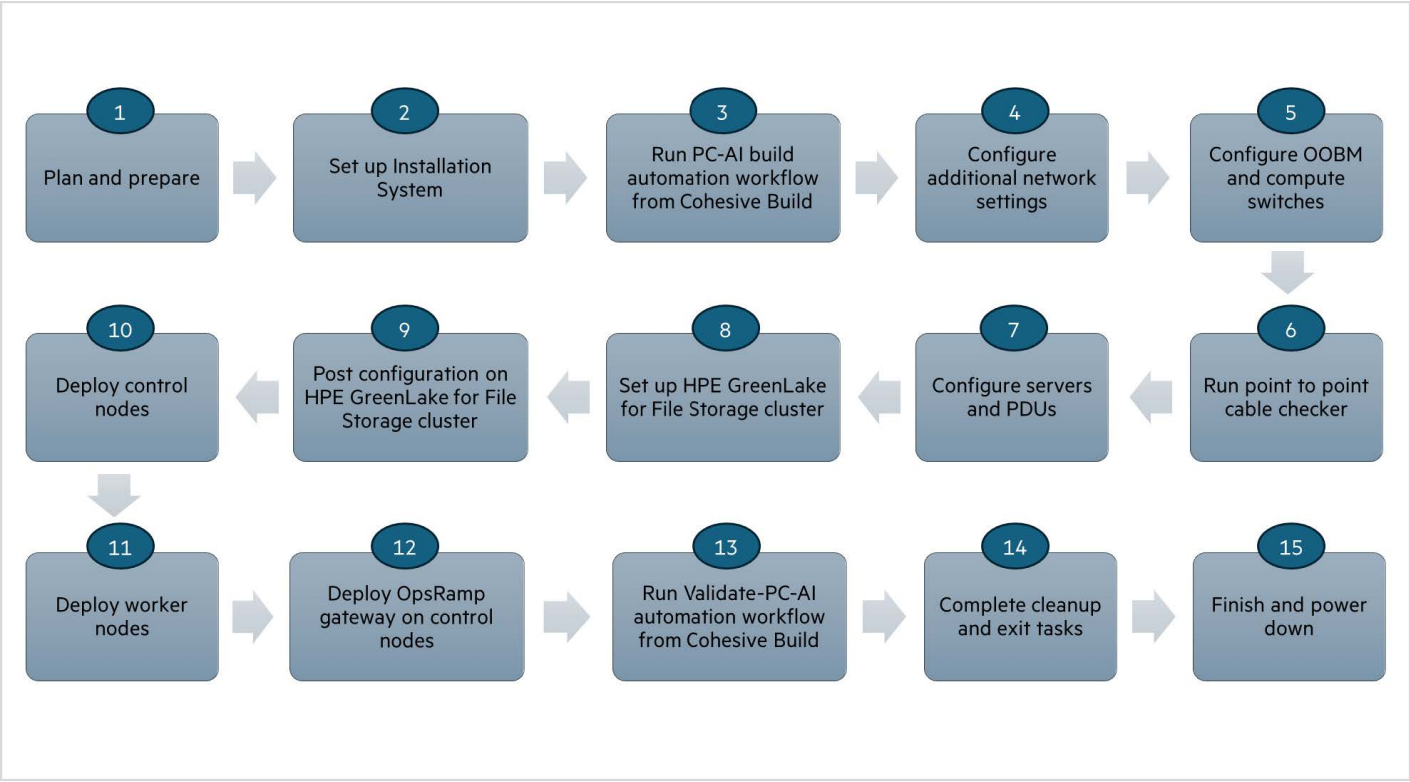
This document outlines the procedures for factory integration of the HPE Private Cloud AI engineered system.

Subtopics

Deployment workflow

This document describes the automation deployment along with manual procedures that must be performed for factory integration before the engineered system is shipped to the customer datacenter.

The following figure illustrates the steps used to deploy HPE Private Cloud AI engineered system at the Integration Center:



Terminology

Acronyms	Description
Integration Center (IC)	The Factory Express (FE) and Integration Center (IC) are terms interchangeably used for the manufacturing staging location where the engineered system is built before shipping to customers
CBOX	GL4FS Compute BOX, one CBOX has 2 IOMS (2 compute nodes or CNODE)
DBOX	GL4FS JBOF
Installation Phase 1	Indicates the Bootstrap and Easy Installer process
Installation Phase 2	Indicates the Text User Interface (TUI) factory integration setup
1x1 GL4FS cluster/array	1 CBOX and 1 DBOX

Plan and Prepare

Before starting with the build, it is essential to verify that the network cards are placed in the correct slots of the rack being used. The position of the network cards and MR controller is determined by the solution type:

- **Small and Medium configurations** - Two network cards and one MR controller must be placed in the following slots of the rack:

Network cards and MR controller	Slot
2p 200Gb card	PCIe Slot 2
MR416i p (P47777-B21)	PCIe Slot 3
2p 200Gb card	PCIe Slot 5

- **Large configuration** - Three network cards and one MR controller must be placed in the following slots of the rack:

Network cards and MR controller	Slot
MR416i p (P47781-B21)	OCP Slot 17
1p 400Gb card	PCIe Slot 2
1p 400Gb card	PCIe Slot 5
2p 200Gb card	PCIe Slot 6

Subtopics

Generating HPE Smart CID files

About this task

The HPE Smart CID portal generates the Smart CID JSON files that are used throughout the build and deployment process. During the Integration Center build, The HPE Smart CID portal generates Customer Intent Document (CID) JSON files required to build the HPE Private Cloud AI racks using Cohesive Build Airflow application.

For more information on using the HPE Smart CID portal, see **HPE Smart CID documentation** and download the user guide for the required solution.

When a solution is ordered, the HPE sales personnel, solution architects, and technical support personnel collect information from the customer to build the system according to customer-provided specifications. The specifications are stored in the customer intent document (CID), which is managed within the HPE Smart CID portal.

For building the HPE Private Cloud AI racks, perform the following steps:

Procedure

1. Fill all the required details as per the customer specifications on the HPE Smart CID portal and take care of the following while generating the JSON files:
   a. Use free or unused IP addresses and ranges that do not overlap within the solution.
   b. Do not change the default values available for the Kubernetes Pod Network and Kubernetes Service Network on the HPE Smart CID portal.
2. Download the following JSON files after they have been generated from the SCID portal:
   - **base-configuration.json** – Contains configuration details about solution networks
   - **infra-layout.json** – Contains configuration parameters for switches, servers, and storage hardware

Supporting documentation

The following documents provide supplemental information to this guide and aid in the configuration of the engineered system:

Document title	Purpose
HPE Private Cloud AI 1.5 Firmware and Software Compatibility Matrix	Provides the supported combination of software and firmware versions for all components based on the recipe version used in the deployment of the HPE Private Cloud AI engineered system.
HPE Private Cloud AI Infrastructure Factory Build Guide	Provides comprehensive instructions for the initialization of the HPE Aruba 6300M switches located in Rack1.
HPE Private Cloud AI Installation System Automation Guide	Provides configuration instructions for the HPE Private Cloud AI (engineered system) Installation System, which contains two infrastructure virtual machines (MirrorBox VM and Cohesive Build VM), to be used for complex integration.

See the HPE Private Cloud AI 1.5 Documentation List | Integration Center for supplemental information that complements this guide. This document contains additional resources and documentation crucial for the optimal configuration and deployment of the HPE Private Cloud AI engineered system.

Set up the installation system

Subtopics

Configure the installation system

See the HPE Private Cloud AI Installation System Automation Guide to completely configure an Installation System that will allow complex integration of the engineered system.

This document describes the steps to perform the following procedures:

- Deploy and configure VMware ESXi on Installation system

- Deploy MirrorBox Virtual Machine
- Deploy Cohesive Build Virtual Machine

Set up Cloud Modules Cohesive Build

This section describes the procedures to configure the Cloud Modules Cohesive Build and run the build workflow.

Subtopics

Accessing Cohesive Build UI

After the Cohesive Build virtual machine deployment is complete according to the procedure documented in the HPE Private Cloud AI Installation System Automation Guide, access the Cloud Modules Cohesive Build UI using the URL: **https://<Cohesive build_virtual machine_IP>:8443**.

Use the following user credentials to log in to the Cohesive Build VM:

- **Username:** airflow
- **Password:** Password!234

Importing automation bundle

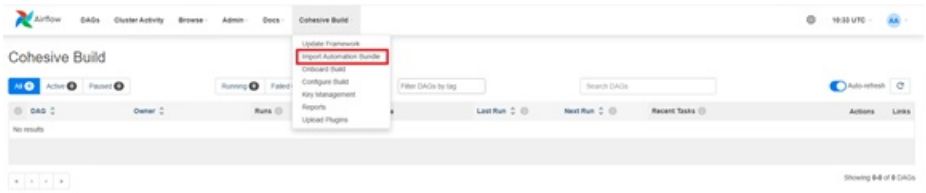
About this task

By default, whenever a new Cohesive Build VM is created, it does not include any baseline (recipe) automation bundles.

To import the required baseline automation bundle, perform the following steps:

Procedure

1. Navigate to the Cohesive Build menu and select Import Automation Bundle as shown in the following example:



2. On the Import Automation Bundle page, perform the following steps:
   a. Select PC-AI from the Solution Type drop-down list.
   b. Select MirrorBox from the Repository Type drop-down list.

NOTE

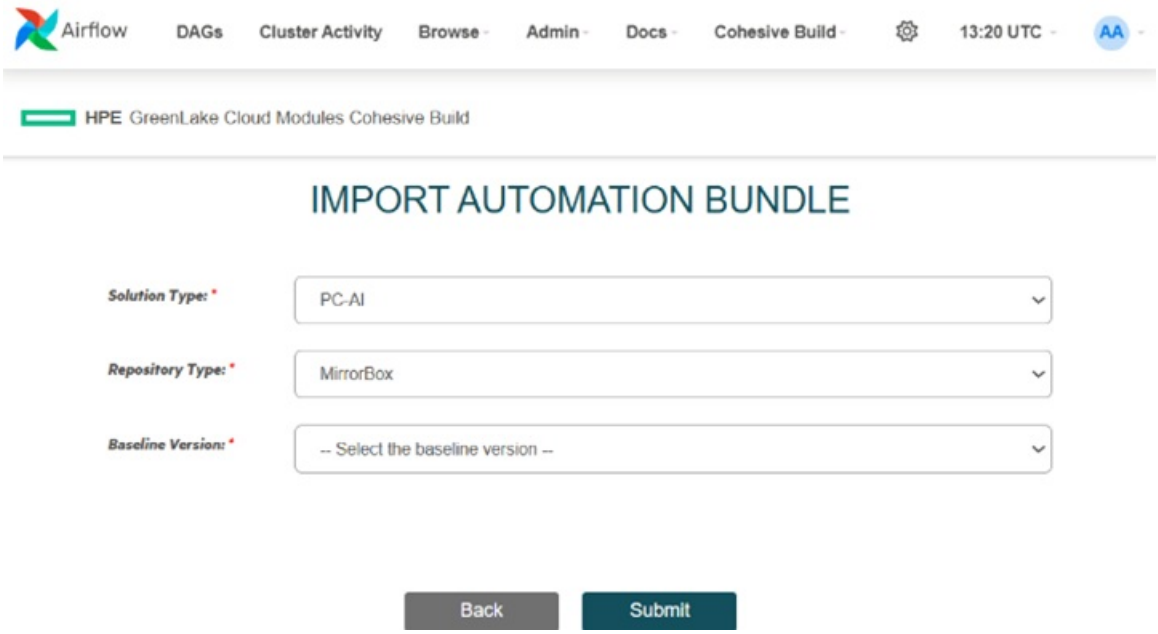
If the baseline versions are not rendered in the Baseline Version drop-down list when the MirrorBox option is selected, select Local from the Repository Type drop-down list to upload the baseline bundle.

c. Select the appropriate version from the Baseline Version drop-down list.

NOTE

If the baseline versions are not rendered in the Baseline Version drop-down list when the MirrorBox option is selected, copy the PC-AI automation bundle from the **/var/cached-images/PC-AI/<baseline_version>/cohesive-build/** directory on the MirrorBox to the Cohesive Build VM to upload the baseline bundle.

d. Click Submit.

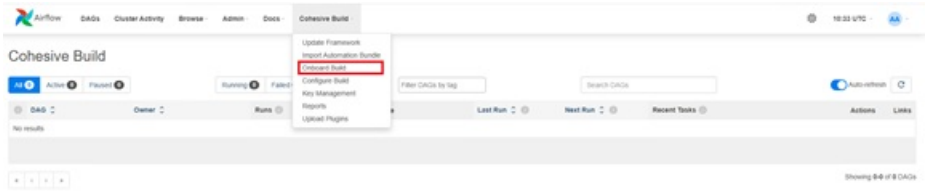


The baseline automation bundle is then imported into Cohesive Build and can be used to create the build workflow.

Onboarding build

Procedure

1. Navigate to the Cohesive Build menu and select Onboard Build.



2. On the Onboard Build page, perform the following steps:

   a. Enter the desired build name, for example, PC-AI, in the Build Name field.

b. Enter the description in the Description field.

c. Select the Build Validation option.

d. Select PC-AI from the Solution Type drop-down list.

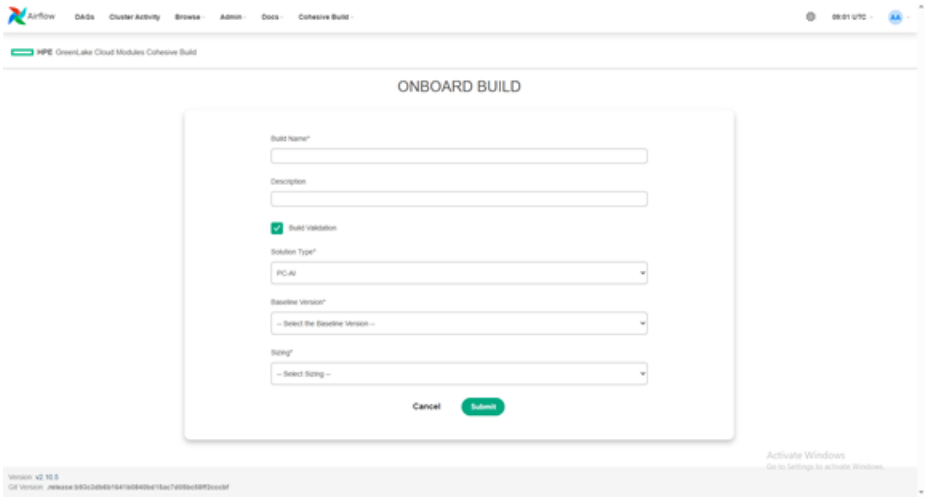
e. Select the imported baseline from the Baseline Version drop-down list.

f. Select Standard (S/M/L) from the Sizing drop-down list.

The following two values are available in the Sizing drop-down list, which signify the configuration type used for running the PC-AI workflow:

- Standard (S/M/L) - Used to configure the systems for small, medium, or large configurations
- Developer System - Used to configure the systems for Developer System configuration

g. Click Submit to onboard the build.



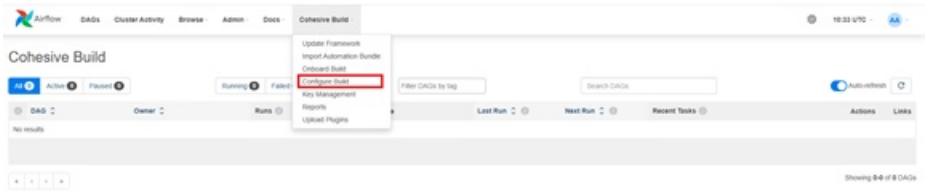
Results

The onboarded build is displayed on the DAGs page after a few seconds. Refresh the page to see the build DAG on the page.

Configuring build

Procedure

1. Navigate to the Cohesive Build menu and select Configure Build as shown in the following example:



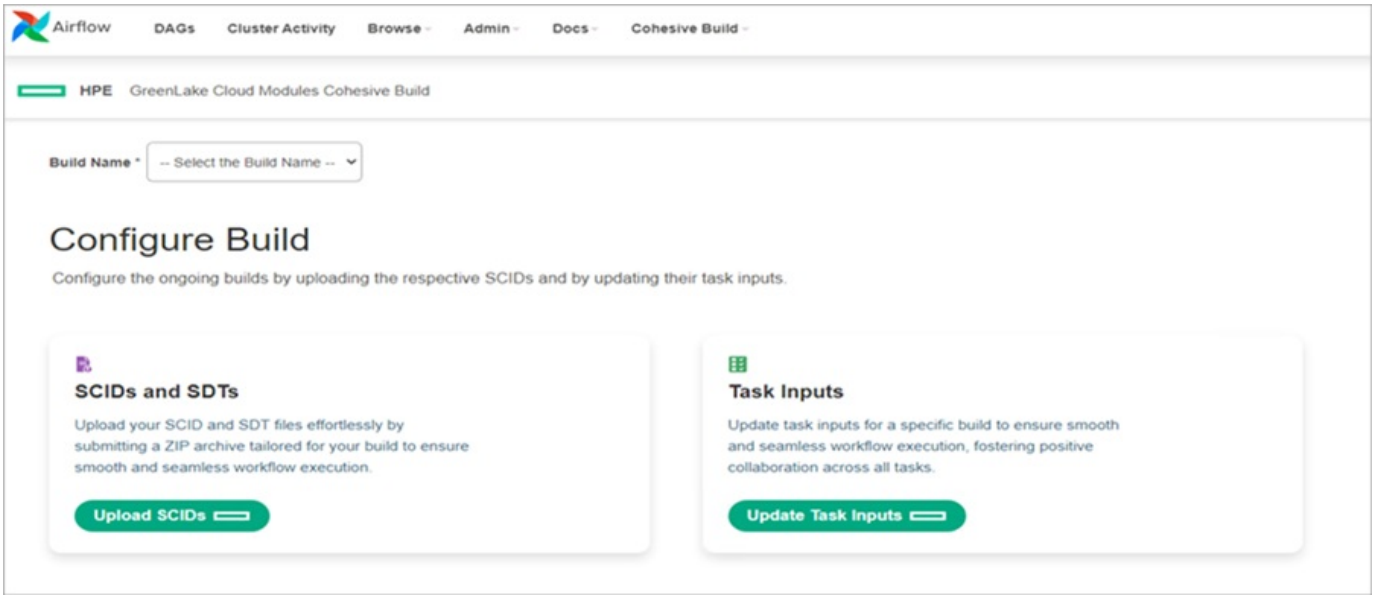
2. On the Configure Build page, upload the SCID files and update the task inputs as described in the consecutive sections.

Subtopics

Uploading SCID files

Procedure

1. On the Configure Build page, perform the following steps:
   a. Select the appropriate name of the build, created during Onboard Build, from the Build Name drop-down list.
   b. Click Upload SCIDs.

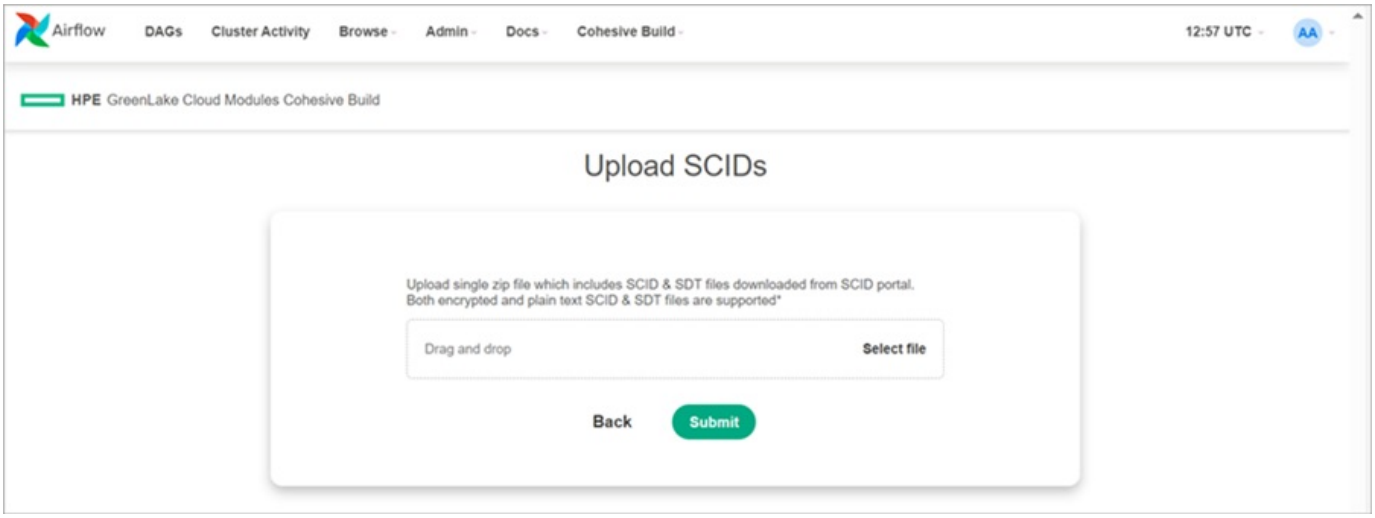


2. On the File Explorer of the Installation System, copy the SCID files (**base-configuration.json** and **infra-layout.json)** to a folder and create a zip file from it.

   Example:

   Copy the SCID files to the **PCAI_SCID** folder and create a **PCAI_SCID.zip** file from it.

3. On the Upload SCIDs page, perform the following steps:
   a. Click Select file, browse to the created zip file (for example, PCAI_SCID.zip), and click OK.
   b. Click Submit.

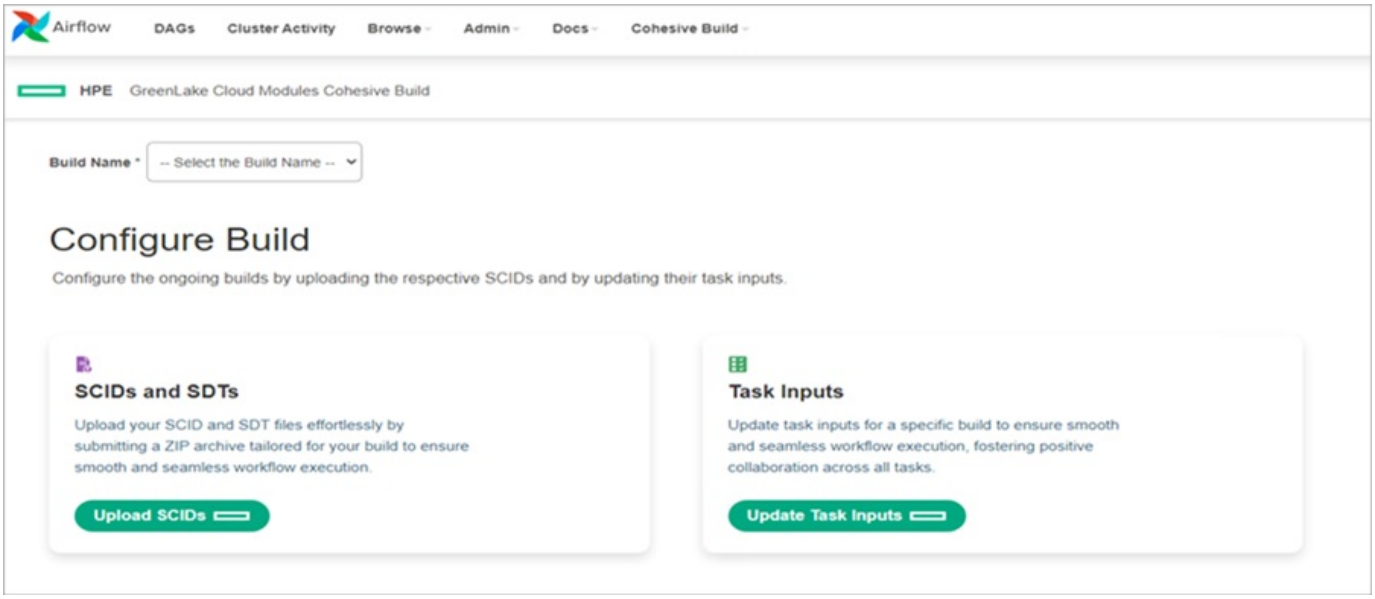


4. Click Back to go to the Configure Build page.

Updating task inputs

Procedure

1. On the Configure Build page, perform the following steps:
   a. Select the previously selected build name from the Build Name drop-down list.
   b. Click Update Task Inputs.



2. On the Update Task Inputs page, in the P2P Cable Checker tab, perform the following steps:
   a. Select top or bottom from the PDUPowerFeed drop-down list.

> **NOTE**
>
> The values specified in the PDUPowerFeed drop-down list signify the position of PDUs on the rack.

   b. Select the appropriate value from the Mode drop-down list.

      The following two values are available in the Mode drop-down list, which signify the mode used for running the cabling validation checks:

      factory

      This mode is recommended when configuring the PC-AI build for the first time.

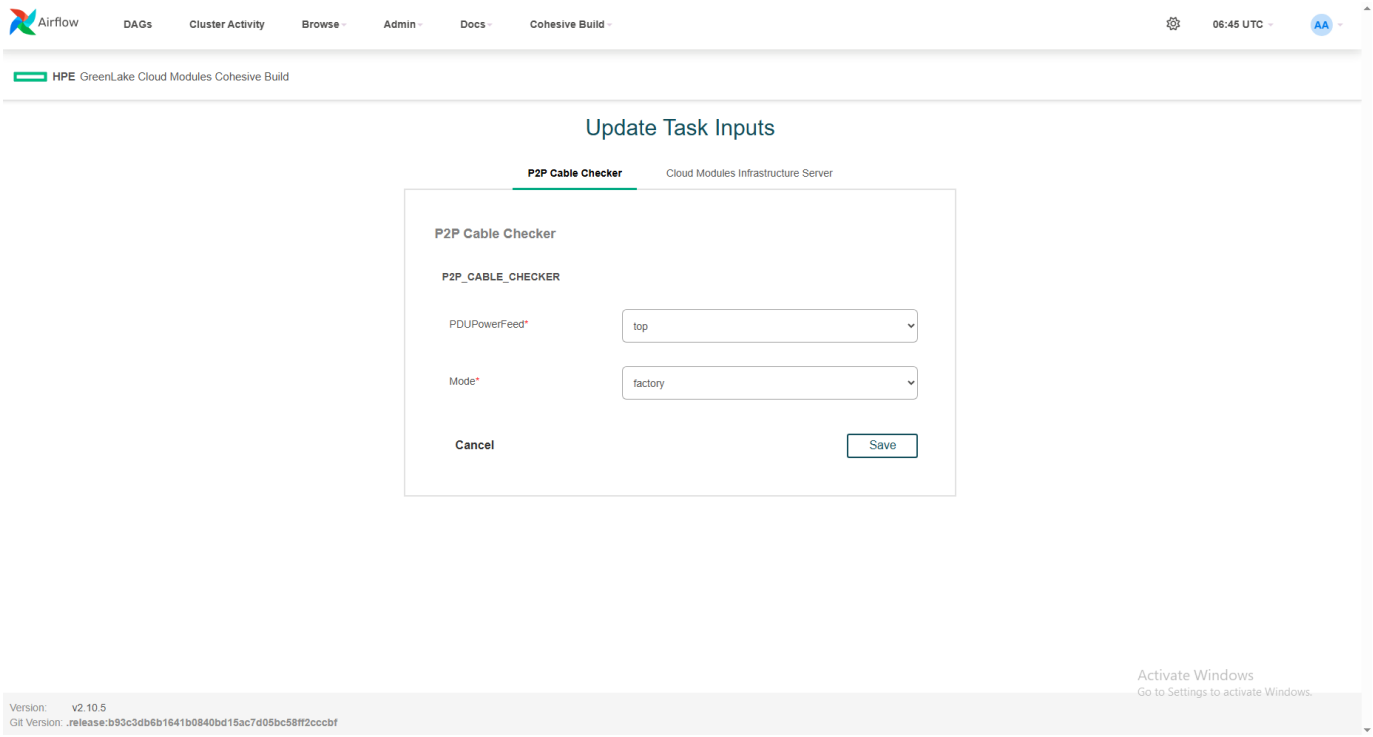
      All servers are power-cycled, regardless of their current power state. Full cabling and data validation is performed, and the servers are restored to their original power state after validation.

      normal

      Use this mode to run the cabling validation checks on a configured Private Cloud AI engineered system.

      During validation, the powered on servers are not power-cycled while only powered off servers are power-cycled. After the validation is complete, all servers are restored to their original power state and data validation is skipped for the powered on servers.

   c. Click Save.

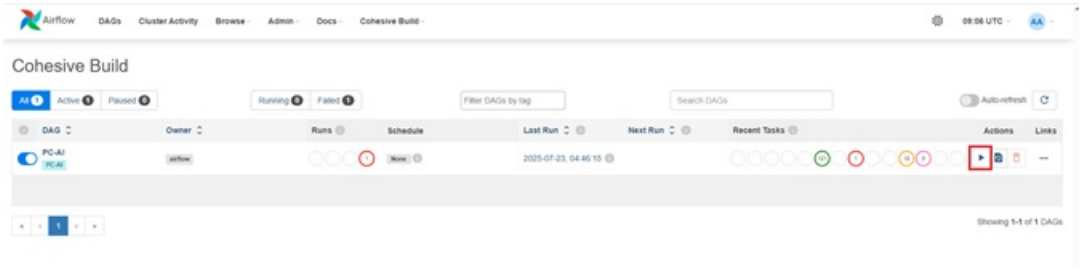


3. Skip the Cloud Modules Infrastructure Server tab and proceed to the next section.

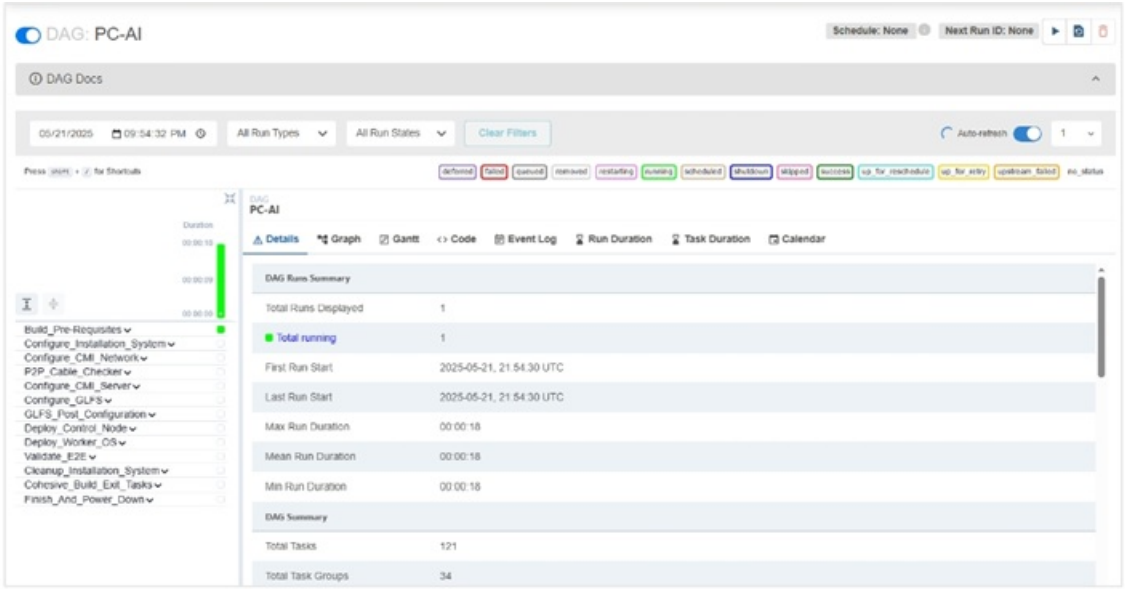
Running the build workflow

Procedure

1. On the DAGs page, click the Play icon under Actions to trigger the DAG as shown in the following figure:



2. On the DAG page, click the appropriate build name to view the build workflow in the grid layout.



Validate installation system configuration

This section outlines the tasks to validate the installation system configuration at the Integration Center.

> **NOTE**
> Verify that each manual task is completed according to the HPE Private Cloud AI Installation System Automation Guide and mark the status as Success in the workflow.

The following tasks in the Build_Pre-Requisites task group must be completed to ensure that all the prerequisites are met before starting the automated tasks:

Workflow tasks in Build_Pre-Requisites task group

Task Group	Task Name	Task Type	Remarks
Build_Pre-Requisites	Manual-Generate_Smart_CID	Manual	
	Manual-Validate_Installation_System_Connections	Manual	
	Manual-Verify_Local_Repo_Sync_Images	Manual	
	Manual-Upload_Recipe_JSON	Manual	

Configure additional network settings

This section maps to the Configure_Installation_System task group, which configures additional network settings of the Cohesive Build Virtual Machine.

- Before proceeding, ensure that the following IP addresses are not currently assigned to any other devices in the network to avoid potential IP conflicts:
  - Cohesive Build VM IP address
  - Management Network Gateway
  - Management Network DNS Server IP address

- Management Network NTP Server IP address

- If a previously used IP address is assigned to any device in the network, it can lead to network instability and service disruptions. To prevent these conflicts, perform the following steps:
  - Validate the availability of the IP addresses required in the network.
  - Update the SCID files with the IP addresses that are confirmed to be unused and available.
  - Verify that the selected IP addresses align with the defined network range.

The workflow progresses through the following sequence of tasks:

Workflow tasks in Configure_Installation_System task group

Task Group	Task Name	Task Type	Remarks
Configure_Installation_System	Preconfiguration_Setup	Automated	
	Configure_Solution_Management_Network	Automated	
	Disable_Firewall	Automated	
	Configure_NTP	Automated	
	Configure_DNS	Automated	
	Configure_NAT	Automated	

Configure Infrastructure

Prerequisites

- The following prerequisite must be met before running any automation for Cloud Modules Infrastructure (CMI) service:
  - Ensure that the HPE Aruba 6300M switches are initialized successfully in Rack 1.

    For information on initializing every HPE Aruba 6300M switch infrastructure located in Rack 1, including HPE Aruba and NVIDIA switches, associated with the engineered system, see the HPE Private Cloud AI Infrastructure Factory Build Guide.

    IMPORTANT

    The HPE Aruba 8325 switches for HPE GreenLake for File Storage, NVIDIA switches, and the single HPE Aruba 6300M switch in Rack 2, which are part of the large configuration in the HPE Private Cloud AI engineered system, are automatically configured through the Cloud Modules Infrastructure automation.

- The following prerequisites must be met to run the Cloud Modules Infrastructure Server automation for HPE Private Cloud AI:
  - The Cohesive Build Virtual Machine must be configured to have access to the Management Network; which is required to access the iLO IPv6 addresses for all the worker nodes and control nodes in the engineered system.
  - All servers must have an iLO Advanced License installed.

    NOTE

    The iLO Advanced Trial Licenses can be downloaded from **My HPE Software Center**.

About this task

This section describes the infrastructure procedures to configure the OOBM and compute switches.

The workflow progresses through the following sequence of task groups:

Procedure

1. Configure_CMI_Network task group - Configures the HPE Aruba and NVIDIA switches and network configuration.
2. P2P_Cable_Checker task group - Checks that all the cables are connected according to the customer-specific cabling guidance for the engineered system, also known as the point-to-point cabling guide.
3. Configure_CMI_Server task group - Configures BIOS and iLO security settings including PDU configuration.

Subtopics

Configure Cloud Modules Infrastructure Network

This section maps to the Configure_CMI_Network task group.

The workflow progresses through the following sequence of tasks:

Workflow tasks in Configure_CMI_Network task group

Task Group	Task Name	Task Type	Remarks
Prerequisites	Install_Python_Modules	Automated	
	Manual-Initialize_Rack1_OOBM_Switches	Manual	To perform this task, see the Initialize switches section.
Aruba_Configuration	Upgrade_Rack1_OOBM_Switch_Firmware	Automated	
	Generate_Rack_Data_JSON_File	Automated	The files can be found in the respective build DAG directory under the **/opt/airflow/scripts/builds/** directory.
	Generate_OOBM_CFG_File	Automated	
	Enable_Rack1_OOBM_Ports_For_Switches	Automated	
	Initialize_Remaining_Aruba_Switches	Automated	
	Upgrade_Firmware_On_Remaining_Switches	Automated	
	Increase_MAC_Timeout	Automated	
	Configure_OOBM_Switch_Hostname_DNS_NTP	Automated	
	Configure_Switch_Hostnames	Automated	
	Disable_Bluetooth_On_Switches	Automated	
	Disable_Spanning-Tree_On_OOBM_Switches	Automated	
	Delete_Default_NTP_Config_On_Switches	Automated	
	Configure_OOBM_Rack1_Static_Route	Automated	
	Configure_OOBM_VLANs	Automated	
	Configure_OOBM_Ports_Description	Automated	
	Configure_OOBM_Ports	Automated	
	Secure_OOBM_Unused_Ports	Automated	
	Save_Config_On_OOBM_Switches	Automated	
Compute_Configuration	Configure_Switch_Password	Automated	
	Upgrade_Switch_Firmware	Automated	
	Clean_Up_Switch_Firmware_Images	Automated	
	Reconfigure_Switch_Password	Automated	
	Initialize_Nvidia_Compute_Switches	Automated	
	Generate_Compute_Config_Files	Automated	
	Apply_Switch_Config_Files	Automated	

Subtopics

Initializing switches

This section maps to the Manual-Initialize_Rack1_OOBM_Switches task under the Prerequisites task group.

- **Description:** This manual task is used to initialize the HPE Aruba 6300M switch located in Rack 1 only, while all the other switches are initialized through the automated tasks in the workflow.
- **Manual task:** For information on initializing the HPE Aruba 6300M located in Rack 1, see the HPE Private Cloud AI Infrastructure Factory Build Guide.

Point to point cable checker

The primary function of the P2P_CABLE_CHECKER task is to report missing and misconnected connections. This task ensures that all the cables are connected according to the customer-specific cabling guidance for the solution, also known as the point-to-point cabling guide, and helps you to find the cable errors before the build starts.

The workflow goes through the following sequence of tasks:

Workflow tasks in P2P_Cable_Checker task group

Task Group	Task Name	Task Type	Remarks
P2P_Cable_Checker	Install_Python_Modules_P2P_Cable_Checker	Automated	
	P2P_CABLE_CHECKER	Automated	Before running this task, complete the prerequisites mentioned in the Run the point to point cable checker section.

Subtopics

Running the point to point cable checker task

Prerequisites

The following prerequisites must be completed before running this task:

- HPE GreenLake for File Storage switches must be configured as VSX pair. To configure them as VSX pair, perform the following steps on both the switches:

  1. Connect to one of the HPE GreenLake for File Storage switch through a serial port (for example, switch-005).
  2. Bring up all the ports on the switch using the following commands:

     ```
     config t
     int 1/1/1-1/1/4,1/1/31-1/1/32
     no shut
     no routing
     mac-address-table age-time 1800
     exit
     ```

  3. Configure the switch in VSX pair using the following commands:

     ```
     config t
     interface lag 256
      description ISL
      no shutdown
      no routing
      vlan trunk native 1
      vlan trunk allowed all
      lacp mode active
     interface 1/1/31
      description VSX - DO NOT MODIFY
      no shutdown
      mtu 9198
      lag 256
     interface 1/1/32
      description VSX - DO NOT MODIFY
     ```

```
 no shutdown
 mtu 9198
 lag 256
 vsx
inter-switch-link lag 256
 role primary
 keepalive peer
<switch-06IP>
 source
<switch-05IP>

 vsx-sync vsx-global
```

4. Repeat the previous steps on the second switch.

NOTE

Ensure that the source and peer IP addresses for the second switch are set using the `keepalive peer` **`<source-ip>`** **`<peer-ip>`** command.

For example, if the second switch is switch-006, run the following command:

```
keepalive peer
<switch-05IP>
 source
<switch-06IP>
```

- Initial password reset must be performed on PDUs and ensure that the firmware is updated to 2.0.0.R or later.
- REST API access must be enabled in PDUs. If not, perform the following steps to enable REST API access in PDU:

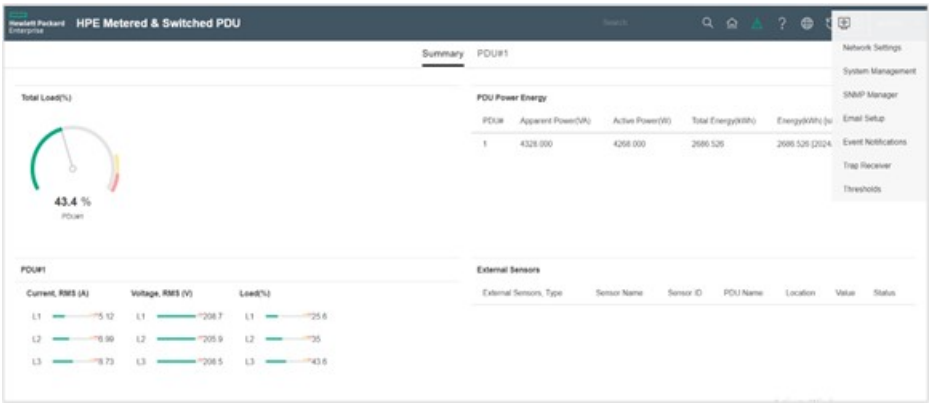
1. Log in to the HPE Metered & Switched PDU web interface using the appropriate IP address and user credentials.

NOTE

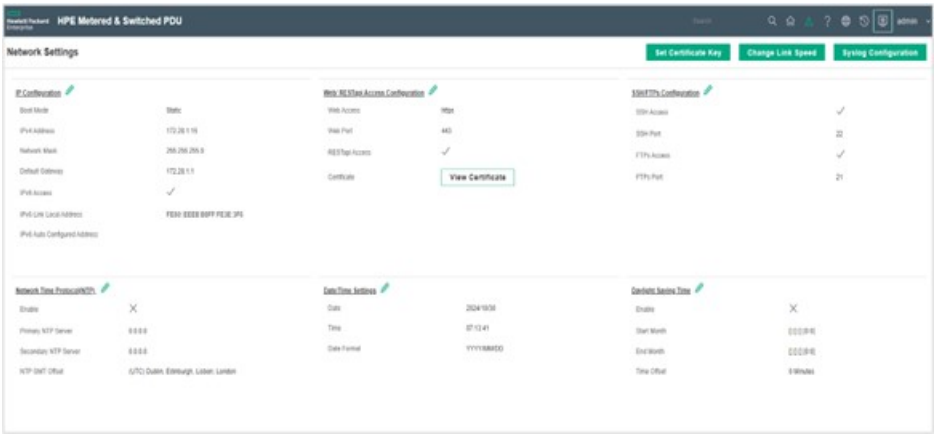
You can find the IP address and user credentials for PDUs in the **base-configuration.json** and **infra-layout.json** SCID files.

- In the **base-configuration.json** file, find the `"ipAddress"` field for the `"componentId": "pdu-001"` and the `"componentId": "pdu-002"` under `"infrastructure" > "racks" > "pdus" > "networkConnections"` to retrieve the IP addresses for both the PDUs.
- In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for the `"target": "PDU"` under `"racks" > "pdus" > "accessCredentials"` to retrieve the user credentials for both the PDUs.

2. Click Network Settings.



3. Verify that the REST API access is enabled. If not, enable it.



4. Repeat the steps for all PDUs.

About this task

This section maps to the P2P_CABLE_CHECKER task under the P2P_Cable_Checker task group.

The P2P_CABLE_CHECKER task is automatically triggered as part of the PC-AI build DAG workflow.

> **NOTE**
> This task takes more than 15 minutes to complete. Wait until this task is complete before proceeding.

Output scenarios:

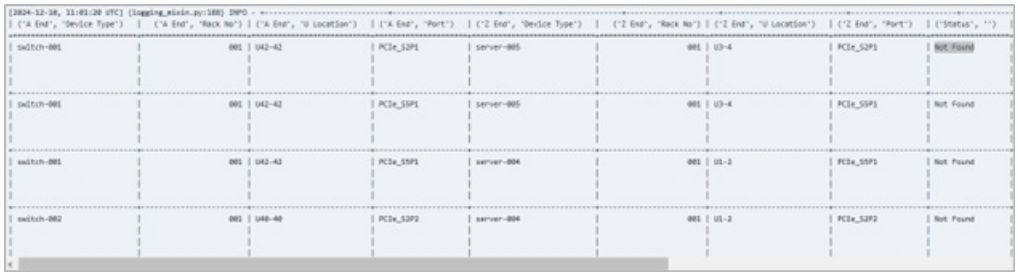
- **Success scenario:** No error statements are displayed on the Cohesive Build UI and the table shows the status for all the connections.
- **Failed scenarios:** The task output displays a specific error that needs to be resolved to complete validation.

  If you encounter any of the following errors, you can resolve them with their corresponding resolution:

  - **InterfaceError:** If you encounter a `"processInterfaces: not found"` error, it means the interface ens33 netmask is not matching with the SCID file.
  - **401 Unauthorized:** If you encounter a `"401 unauthorized"` error, it means that the credentials for the devices are incorrect. To resolve this issue, verify and update the device credentials as needed from the **infra-layout.json** SCID file.
  - **SSH Timeout Error:** If you encounter this error, you can manually set `NO_PROXY` to `*` on the Cohesive Build VM to proceed and revert to the original value after the task is complete. The proxy issues can cause this issue.
  - **Switch Port Error:** If you encounter an `"endpoint cnode-006-rack-001:U16B2-17:S2P1 is not connected to any enabled switch port"` error while running the point-to-point cable checker in the normal mode, validate the cables manually to proceed further.

  Example: This output displays all the connections that are found, missing, and misconnected. The "A End" and "Z End" columns represent

the two ends of a connection.



Configure Cloud Modules Infrastructure Server

This section maps to the Configure_CMI_Server task group.

The workflow goes through the following sequence of tasks:

Workflow tasks in Configure_CMI_Server task group

Task Group	Task Name	Task Type	Remarks
Prerequisites	Install_Python_Modules	Automated	
Server_Configuration	ILO_Cabling_Validation	Automated	
	Power_On_Servers	Automated	
	Server_ILO_Prerequisites_Validation	Automated	
	Enable_Ethernet_Link_Mode	Automated	
	Stamp_Module_ID	Automated	
	Stamp_Instance_Type	Automated	
	BIOS_Configuration	Automated	
	Create_iLO_User	Automated	
	Configure_iLO_Network	Automated	
	Reset_iLO	Automated	
	Restart_Servers	Automated	
	Validate_Server_Configuration	Automated	
	Power_Off_Servers	Automated	
	Configure_Auto_Power_On_Settings	Automated	
PDU_Configuration	PDU_Cabling_Validation	Automated	
	Admin_Password_Configuration	Automated	
	REST_API_Enablement	Automated	
	IPv4_Address_Configuration	Automated	
	Admin_Password_Validation	Automated	
	Download_PDU_Firmware	Automated	
	Upgrade_PDU_Firmware	Automated	
	Cleanup_PDU_Firmware	Automated	

Set up HPE GreenLake for File Storage

Installing and setting up the HPE GreenLake for File Storage is divided into two phases. Phase 1 is performed at the Integration Center. This section covers phase 1, install and setup of HPE GreenLake for File Storage at the Integration Center.

NOTE

This process takes approximately 1 hour and 25 minutes to complete. Wait until this process is complete before proceeding.

The workflow goes through the following sequence of tasks:

Workflow tasks in Configure_GLFS task group

Task Group	Task Name	Task Type	Remarks
Configure_GLFS	Manual-Install_GLFS	Manual	To perform this task, see Install HPE GreenLake for File Storage section.
	Manual-Enable_Dark_Mode	Manual	To perform this task, see Disable HPE GreenLake Cloud Services section.
	Manual-Update_Vtool_Setting	Manual	To perform this task, see Update Vtool settings section.
	Manual-Create_Setup_Status_JSON	Manual	To perform this task, see Update setup_status.json file section.

Subtopics

Install HPE GreenLake for File Storage

Prerequisites

- VAST ISO installation must be completed on both CNodes and DNodes at FoxConn Czech Republic factory site before arriving at the Integration Center. Verify that the firmware versions loaded in CNodes and DNodes match the supported Private Cloud AI recipe.
- The iLO must be accessible on CNodes to run the **configure_network.py** script.
- All the management port RJ45 cables must be connected to the private switch.

About this task

This section maps to the Manual-Install_GLFS task under the Configure_GLFS task group.

- **Description:** This manual task is used to install the HPE GreenLake for File Storage cluster.
- **Manual task:** To install HPE GreenLake for File Storage system in a private network, perform the following steps:

Procedure

1. Configure the switch.
2. Configure the network. - 10 mins
3. Bootstrap the star bundle. - 20 mins
4. Discover the existing nodes. - 10 mins

5. Perform Eazy install. - 40 mins
6. Create s3enable file. - 2 mins
7. Enable S3.
8. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Subtopics

Configuring the switch

About this task

To configure the HPE GreenLake for File Storage switch using the `switch_conf.py` script, perform the following steps:

Procedure

1. Download the **Alto GLFS Install Guide.zip** file from the MirrorBox shared drive.

   NOTE

   All the required files are available in the **/var/cached-images/PC-AI/<baseline_version>/software/GLFS/3.2.0** directory on the MirrorBox. The **<baseline_version>** directory indicates the current baseline version mentioned in the **infra-layout.json** SCID file. For example, if the baseline version is PCAI202507.3, the files are stored in the **/var/cached-images/PC-AI/PCAI202507.3_0/software/GLFS/3.2.0** directory.

2. Extract the downloaded **Alto GLFS Install Guide.zip** file and navigate to the **Aruba Switch Configuration Files** directory where you can find the switch configuration script (`switch_config.py`) for HPE Aruba 8325 switches.
3. Run the `switch_conf.py` script using the following syntax and parameters to generate the configuration files for Switch-A and Switch-B:

   Syntax:

   ```
   python3 switch_config.py aruba --mgmt-ips --mgmt-subnet --mgmt-gateway --ntp --
   node-ports --isl-ports --cluster-name --hostname --mtu
   ```

   Parameters: For information on obtaining the parameter values from the **base-configuration.json** SCID file, see the Parameter list for switch_config.py script.

   Example:

   ```
   $ python3 switch_config.py aruba --mgmt-ips 172.28.1.82,172.28.1.83 --
   mgmt-subnet 24 --mgmt-gateway 172.28.1.1 --ntp 172.28.1.200 --node-
   ports 1-10 --isl-ports 31,32 --cluster-name PCAI --hostname ArubaHost -
   -mtu 9198
   ```

4. Retrieve the IP address and user credentials for Switch-A and Switch-B from the **base-configuration.json** and **infra-layout.json** SCID files.

- In the **base-configuration.json** file, find the `"ipAddress"` field for `"role": "GLFS"` and `"purpose": "Network Switch Management"` under `"infrastructure" > "racks" > "storageArrays" > "networkSwitches" > "networkConnections"` to retrieve the IP addresses for Switch-A and Switch-B.
- In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for `"type": "HPE Alletra Storage MP 32-port 100GbE Switch Bundle"` under `"racks" > "storageArrays" > "networkSwitches" > "accessCredentials"` to retrieve the user credentials for Switch-A and Switch-B.

5. Connect to the HPE Alletra Storage MP Switch-A using the assigned IP address and perform the following steps:
   a. Log in to the switch using **admin** credentials.
   b. Enable the QoS pool configuration using the following commands:

```
configure terminal
qos pool 1 lossless size factory-default percent headroom factory-default kbytes
priorities 0
write mem
```

   c. Restart the switch.

```
boot system
```

   d. After the switch is restarted, log in to the switch using **admin** credentials.
6. Run the following command and paste the content of the Switch-A configuration file generated by the `switch_config.py` script:

```
configure terminal
```

7. Repeat the steps 5a to 5d to connect to the HPE Alletra Storage MP Switch-B using the assigned IP address.
8. Run the following command and paste the content of the Switch-B configuration file generated by the `switch_config.py` script:

```
configure terminal
```

Configuring the network

Procedure

1. Retrieve the IP address and user credentials for CNodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for `"role": "Compute"` and `"$comment": "Cbox iLO"` under `"infrastructure" > "racks" > "storageArrays" > "enclosures" > "nodes" > "networkConnections"` to retrieve the IP addresses for CNodes.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for `"type": "S1F26A"` and `"target": "ILO_FACTORY_DEFAULT"` under `"racks" > "storageArrays" > "enclosures" > "nodes" > "accessCredentials"` to retrieve the iLO credentials for CNodes.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for `"type": "S1F26A"` and `"target": "OS"` under `"racks" > "storageArrays" > "enclosures" > "nodes" > "accessCredentials"` to retrieve the vastdata credentials for CNodes.
2. Configure the network using iLO .
3. Disable the northbound connections on c-node1 .

> **NOTE**
>
> This process takes approximately 10 minutes to complete. Wait until this process is complete before proceeding.

Subtopics

Configuring the network using iLO

Procedure

1. Connect to one of the CNodes using the following steps:
   a. Enter **https://<iLO IPv4 or IPv6 address>** from the browser.
   b. Log in to the iLO web interface using appropriate credentials.
2. On the iLO homepage, open HTML5 and log in to the CNode with username as **vastdata** and password as **vastdata** to access the virtual console.
3. Run the `configure_network.py` script using the following command with parameters based on your network configuration:

   This script is used to assign a temporary management IP address to the CNode you are connected to, thus, allowing it to function as the management node:

   > **NOTE**
   >
   > If this script requires a reboot, reboot the CNode and rerun the script.

   Syntax:

   ```
   sudo python3 /usr/bin/configure_network.py 1 --mgmt-vip --ext-ip --ext-gateway --ext-dns --ext-netmask --ntp --hostname --data-netmask --auto-ports-ext-iface outband --retain-ipv6 --skip-sshd --auto-ports eth
   ```

   Parameters: For information on obtaining the parameter values from the **base-configuration.json** SCID file, see the Parameter list for configure_network.py script.

   Example:

   ```
   $ sudo python3 /usr/bin/configure_network.py 1 --mgmt-vip 172.28.1.81 --ext-ip 172.28.1.82 --ext-gateway 172.28.1.1 --ext-dns 10.10.22.30 --ext-netmask 255.255.255.0 --ntp 10.10.22.30 --hostname CNode1 --data-netmask 255.255.192.0 --auto-ports-ext-iface outband --retain-ipv6 --skip-sshd --auto-ports eth
   ```

If the output of this script displays the error `"FW parameters have changed. please reboot and rerun!"`, perform the following steps:

1. Reboot the CNode using the following command:

   ```
   sudo shutdown -r now
   ```

2. Rerun the `configure_network.py` script with the same parameters.

> **NOTE**
>
> If this command is run using the IPv6 link-local address, the session hangs but the script runs properly.

Disabling the northbound connections on c-node1

About this task

The northbound cables are plugged in to c-nodes so the cable checker will pass. The northbound ports must be disabled on c-node1.

Procedure

1. Open an SSH session using VMS IP address and log in to the management port for C-Node1 with username as `vastdata` and password as `vastdata`.
2. Disable the northbound connections on c-node1 using the following commands:

```
sudo ip link set dev ens2f0 down
sudo ip link set dev ens2f1 down
```

Bootstrapping the star bundle

About this task

> **NOTE**
>
> The star package version provided in this section is an example. Use the version provided as the beta build.

To bootstrap the star bundle, perform the following steps:

Procedure

1. Download the star package (**file-service-3.2.0-154.star**) from the MirrorBox shared drive.

   > **NOTE**
   >
   > All the required files are available in the **/var/cached-images/PC-AI/<baseline_version>/software/GLFS/3.2.0** directory on the MirrorBox. The `<baseline_version>` directory indicates the current baseline version mentioned in the **infra-layout.json** SCID file. For example, if the baseline version is PCAI202507.3, the files are stored in the **/var/cached-images/PC-AI/PCAI202507.3_0/software/GLFS/3.2.0** directory.

2. Copy the star package containing the bootstrap files to the `/vast/bundles` directory.

```
scp
<star package>
 /vast/bundles
```

3. Change the current directory to the `/vast/bundles` directory.

```
cd /vast/bundles
```

4. Extract the star package.

```
tar -xvf
<star file>
```

5. Extract the tar package from the extracted star directory.

```
tar -xvf
<tar file>
```

6. Copy the `bootstrap.sh` script to the current directory.

```
cp ./
<directory>
/
<bootstrap script>
 .
```

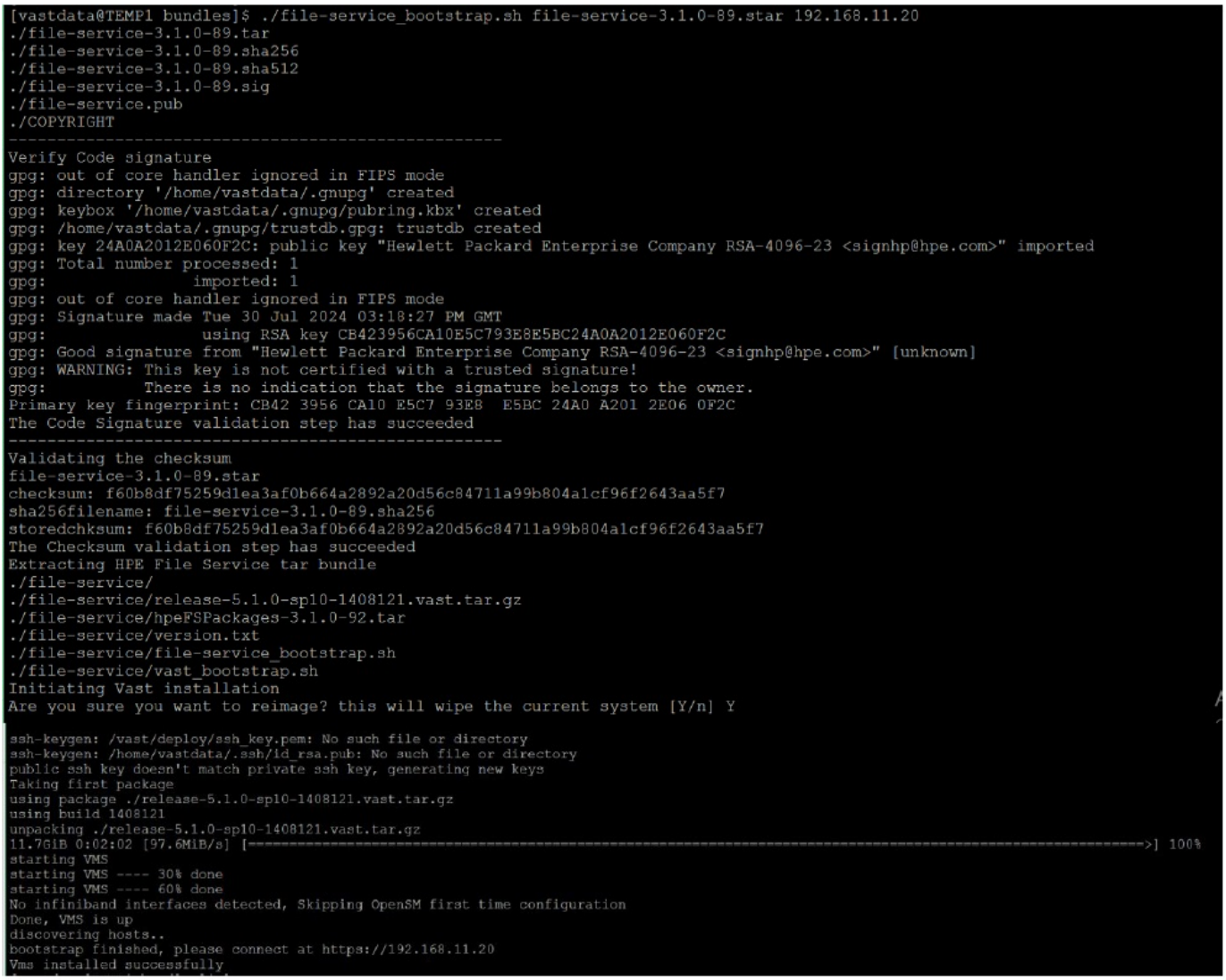
7. Bootstrap the star package using the `bootstrap.sh` script.

```
./file-service_bootstrap.sh
<star package>

<vms-ip>
```

Press Y and Enter when the bootstrap script prompts `"Are you sure you want to reimage? this will wipe the current system [Y/n]"`.

Example:

```
$ scp file-service-3.1.0-104.star /vast/bundles
$ scp file-service_bootstrap.sh /vast/bundles
$ cd /vast/bundles
$ tar -xvf file-service-3.1.0-104.star
$ tar -xvf file-service-3.1.0-104.tar
$ cp ./file-service/file-service_bootstrap.sh .
$ ./file-service_bootstrap.sh file-service-3.1.0-104.star 172.28.1.81

"Are you sure you want to reimage? this will wipe the current system
[Y/n]"
```



> **NOTE**
>
> This process takes approximately 20 minutes to complete. Wait until this process is complete before proceeding.

Discovering the existing nodes

Prerequisites

The NorthBound interfaces, ens2f0 and ens2f1, must be shut down on the VMS CNode before the discovery of the nodes for VAST. To bring down the interfaces, run the following commands as the **vastdata** user:

```
sudo ifdown ens2f0
sudo ifdown ens2f1
```

About this task

To discover the existing nodes, perform the following steps:

Procedure

1. Log in to the HPE GreenLake for File Storage UI using the VMS IP address and password as **123456**.

> **NOTE**
>
> You can find the VMP IP address as specified in the Parameter list for configure_network.py script.

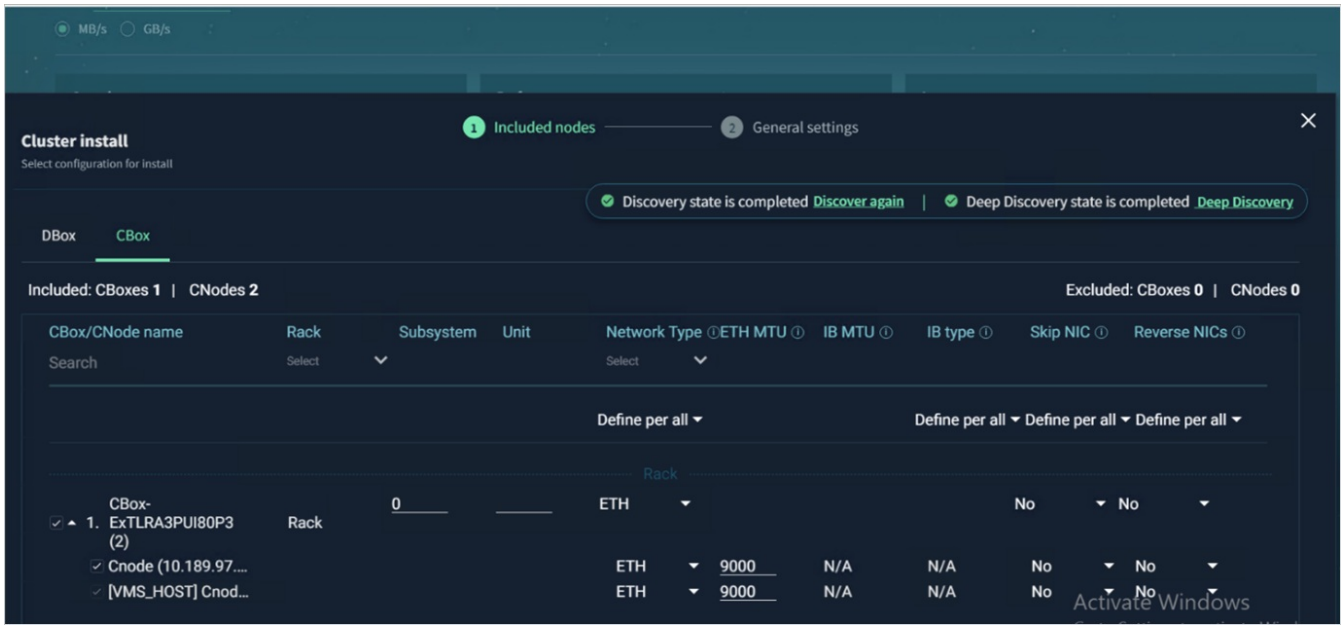
The discovery state of the CNodes and DNodes is displayed. Depending on your storage system or cluster size, it may take some time for all the nodes to display the status.

2. On the Included nodes page, perform the following steps:

   a. Select the CBox tab to display the list of CNodes that are discovered and provide the appropriate rack unit number.

   > **NOTE**
   >
   > You can find the rack unit number mentioned as the "U" locations in the point-to-point cabling guide. The "U" locations indicate the height positions of the components measured from the bottom of the rack.

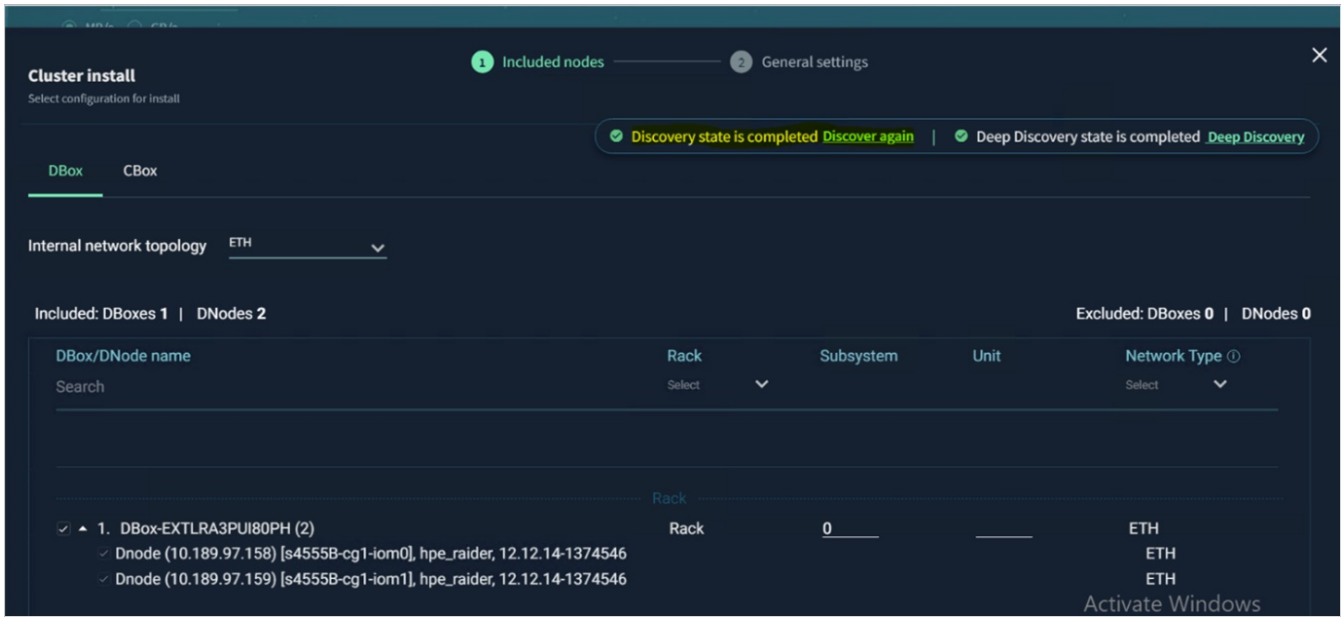
   The following example displays the discovery state of CNodes on the system:



   b. Select the DBox tab to display the list of DNodes that are discovered and provide the appropriate rack unit number.

   > **NOTE**
   >
   > You can find the rack unit number mentioned as the "U" locations in the point-to-point cabling guide. The "U" locations indicate the height positions of the components measured from the bottom of the rack.

   The following example displays the discovery state of DNodes on the system:



If the CNodes and DNodes are powered on before the switches are configured and the Cluster install page in the Management UI does not list the nodes, perform the following steps and retry the discovery:

a. Connect to CNode or DNode using the Technician port or iLO.

b. Run the `config_ipv6.py` script on all the CNodes and DNodes.

```
sudo python3 /usr/bin/config_ipv6.py
```

If you encounter any other issues, see HPE GreenLake for File Storage: Installing and configuring the field-integrated system (service edition).

3. After all the C-Nodes and D-Nodes are discovered, power on the NorthBound interfaces, ens2f0 and ens2f1, on the VMS CNode using the following commands as the **`vastdata`** user:

```
sudo ifup ens2f0
sudo ifup ens2f1
```

> **NOTE**
>
> This process takes approximately 10 minutes to complete. Wait until this process is complete before proceeding.

Performing Eazy install

Procedure

1. Retrieve the relevant IP addresses for the HPE GreenLake for File Storage switches.

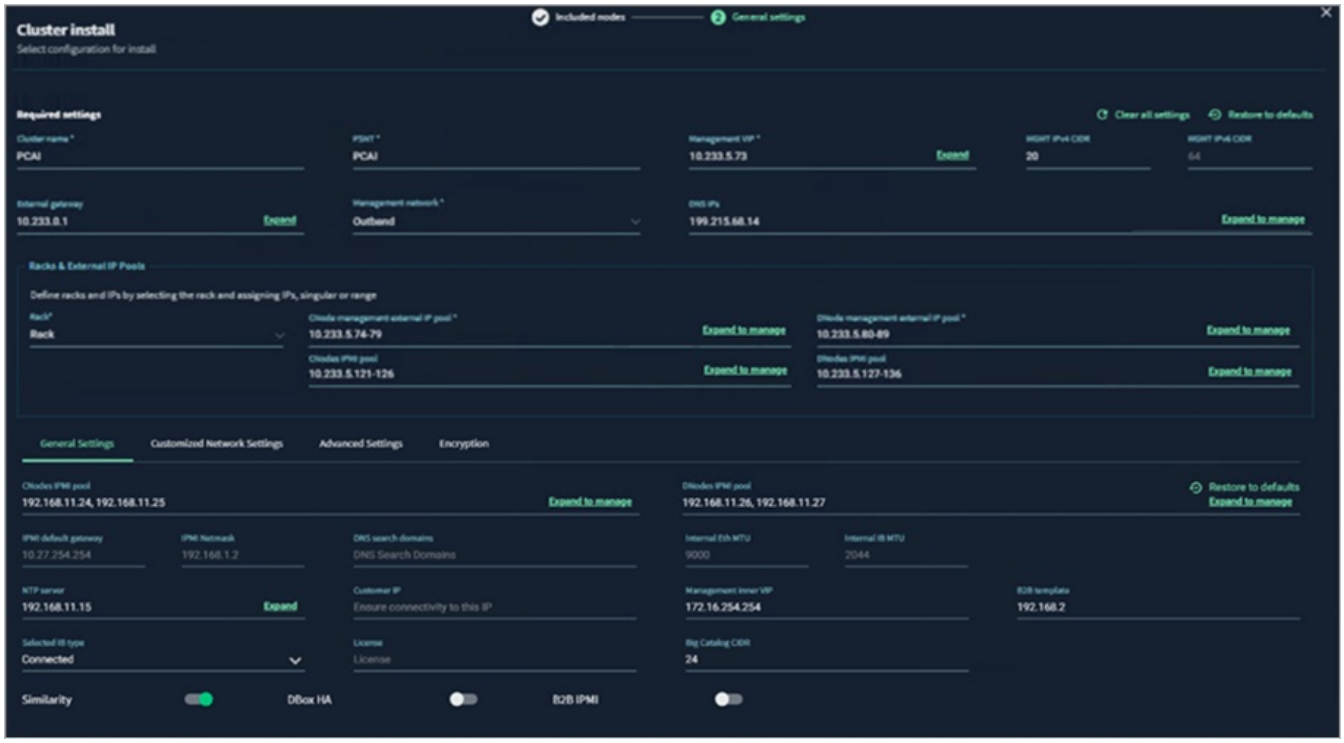
   In the **`base-configuration.json`** SCID file, find all the IP addresses where **`"name": "Management Network"`** under **`"networks"`**.

2. Navigate to the HPE GreenLake for File Storage On-Prem Management UI.

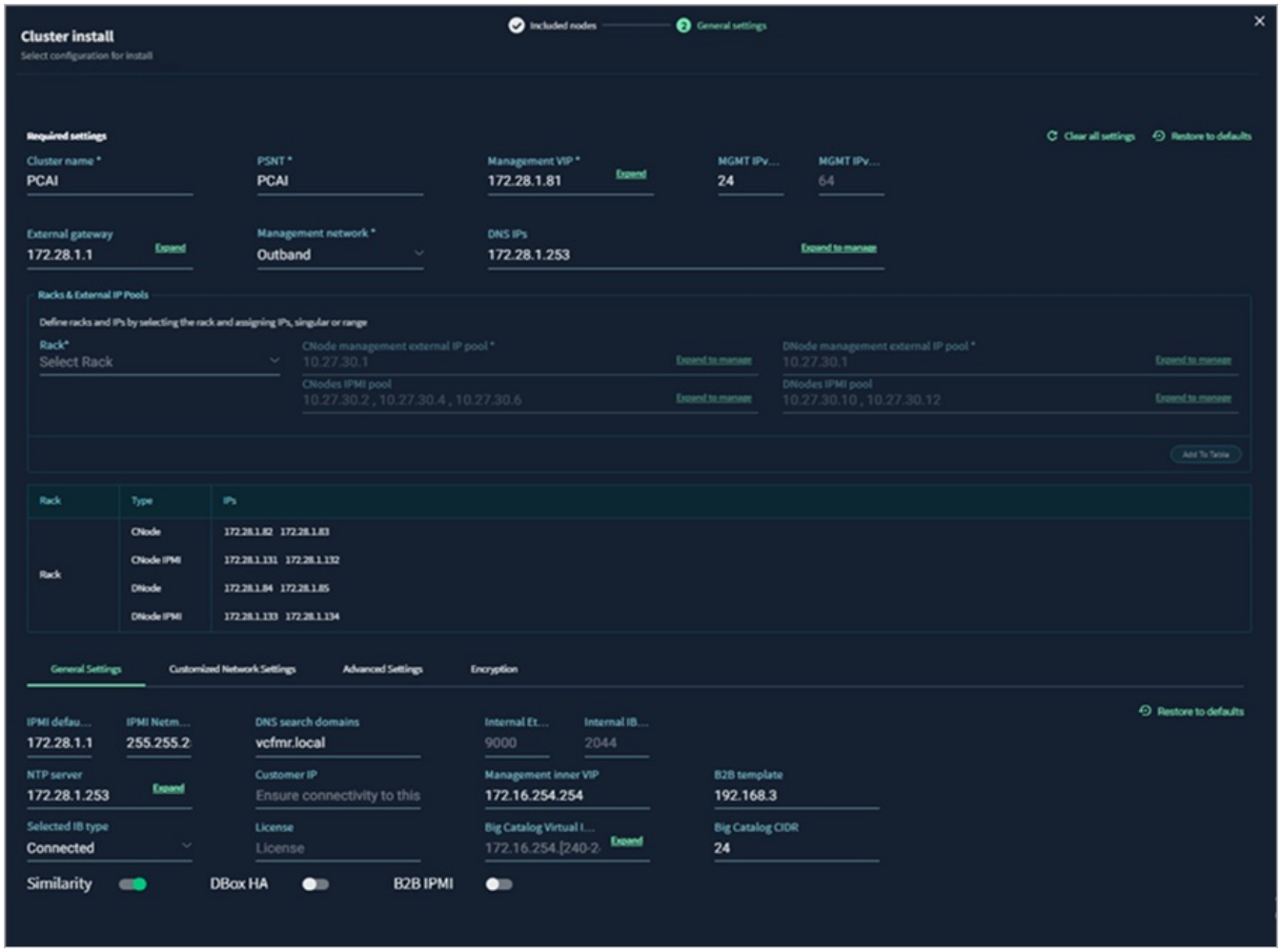
3. On the Cluster install page, perform the following steps:

   a. Continue to the General Settings page.

b. On the General Settings page, in the Racks & External IP Pools section, enter the relevant IP addresses for CNodes and DNodes and click Add to Table.



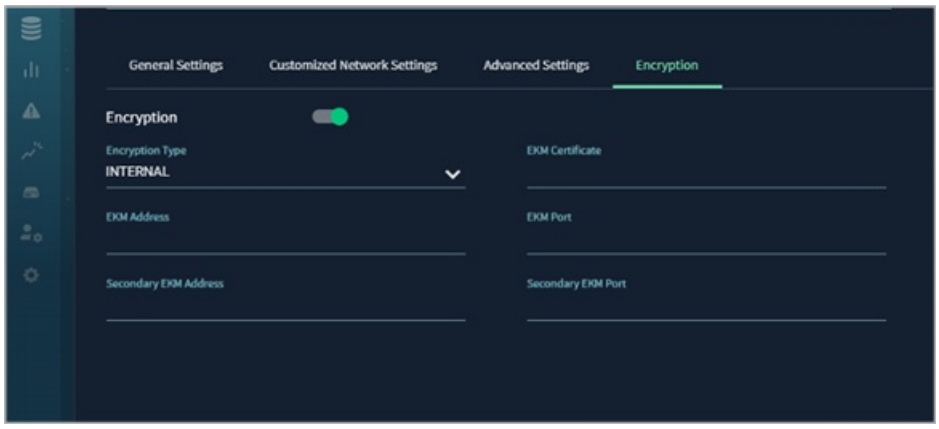
c. On the General Settings tab, enter the relevant IP addresses for DNS and NTP and perform Easy Install.



d. Leave the default values as is in the Advanced Settings tab.

e. On the Customized Network Settings tab, change the value from 100 to 101 in the Start Index DNode field.

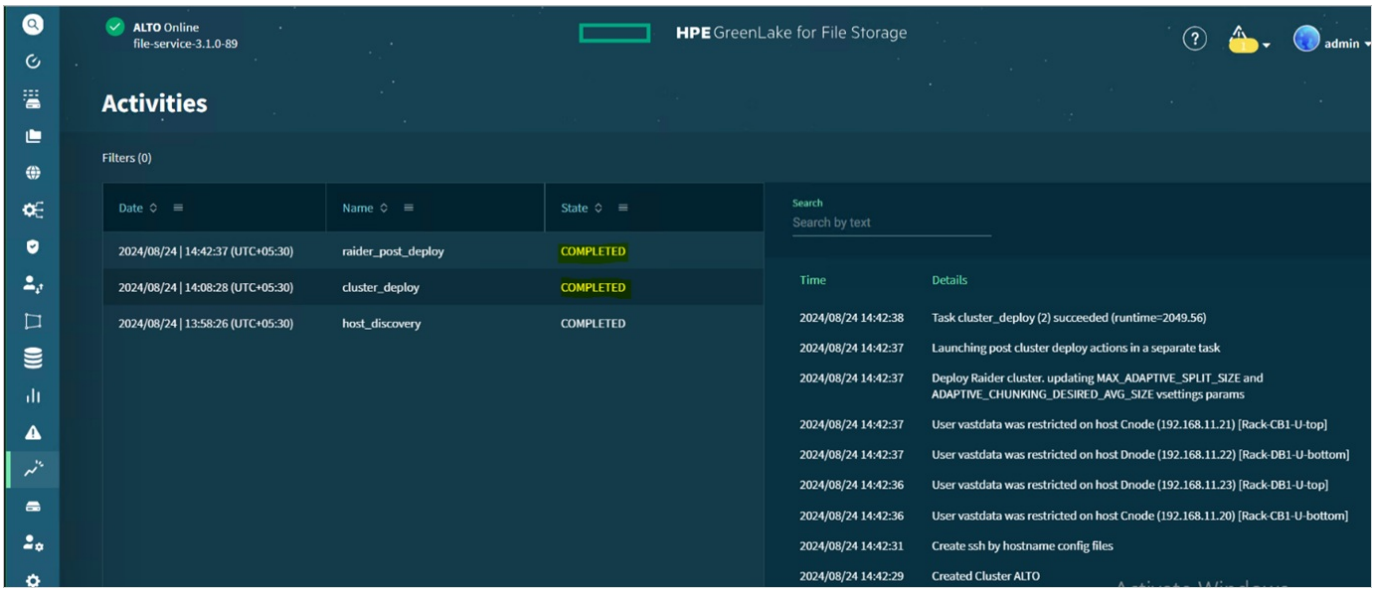
f. On the Encryption tab, select INTERNAL from the Encryption Type drop-down list.



4. Click Activities from the left pane to check the installation progress.

> **NOTE**
>
> When the nodes reboot, the screen may show errors such as `Error: Unknown Error` or `Can't r each VMS` at the top-left corner. This is expected behavior.

5. Verify that the raider_post_deploy and cluster_deploy tasks are in the COMPLETED state.



> **NOTE**
>
> The installation takes approximately 40 minutes to complete. Wait until the installation is complete before proceeding.

Creating s3enable file

About this task

This section describes the procedure to create the **s3enable** file.

> **NOTE**
> The **s3enable** file is required to enable S3 automatically during TUI factory integration at the customer site.

Procedure

1. Open an SSH session using VMS IP address and log in to the VMS node with username as **root** and password as **rootvastdata**.

   > **NOTE**
   > You can find the VMP IP address as specified in the Parameter list for configure_network.py script.

2. Create **s3enable** file (**/etc/hpe/s3enable**) on the CNodes.

   ```
   sudo -u vastdata clush -g cnodes 'sudo touch /etc/hpe/s3enable'
   ```

3. Verify the **s3enable** file created on all the nodes.

   ```
   sudo -u vastdata clush -g cnodes ls -lrth /etc/hpe/s3enable
   ```

   The following output is displayed:

   ```
   172.16.128.1: -rw-r--r--. 1 root root 0 Aug 24 09:22 /etc/hpe/s3enable
   172.16.128.2: -rw-r--r--. 1 root root 0 Aug 24 09:22 /etc/hpe/s3enable
   ```

   > **NOTE**
   > This process takes approximately two minutes to complete. Wait until this process is complete before proceeding.

Enabling S3

About this task

This section describes the procedure to enable S3.

> **NOTE**
> Skip this section if the **s3enable** file is already created as mentioned in the previous section.

Procedure

1. Open an SSH session using VMS IP address and log in to the VMS node with username as **root** and password as **rootvastdata**.

   > **NOTE**
   > You can find the VMP IP address as specified in the Parameter list for configure_network.py script.

2. Retrieve the cluster ID using the following command:

   ```
   curl --location 'https://
   <vms_admin>
   :
   <vms_password>
   ```

```
@
<vms_ip>
/api/clusters/?fields=id' --header 'Content-Type: application/json' --insecure
```

Example:

```
curl --location 'https://admin:******@10.189.98.77/api/clusters/?
fields=id' --header 'Content-Type: application/json' --insecure
```

3. Add the retrieved cluster ID in the URL and enable S3 using the following command:

```
curl --location --request PATCH 'https://
<vms_admin>
:
<vms_password>
@
<vms_ip>
/api/clusters/
<id>
/' --header
'Content-Type: application/json' --insecure --data '{
"enable_s3": true
}'
```

Example:

```
curl --location --request PATCH
'https://admin:******@10.189.98.77/api/clusters/1/' --header 'Content-
Type:
application/json' --insecure --data '{
"enable_s3": true
}'
```

> **NOTE**
>
> This process takes approximately two minutes to complete. Wait until this process is complete before proceeding.

Disable HPE GreenLake Cloud Services

About this task

This section maps to the Manual-Enable_Dark_Mode task under the Configure_GLFS task group.

- **Description:** This manual task is used to enable dark mode in the HPE GreenLake for File Storage cluster.
- **Manual task:** To disable HPE GreenLake Cloud Services, perform the following steps:

> **NOTE**
>
> The dark site file will be deleted after TUI Day 0 at the customer site to enable activation to HPE GreenLake.

Procedure

1. Open an SSH session using VMS IP address and log in to the VMS node with username as **root** and password as **rootvastdata**.

> **NOTE**
>
> You can find the VMP IP address as specified in the Parameter list for configure_network.py script.

2. Create a dark site file on the CNodes.

```
sudo -u vastdata clush -g cnodes 'sudo touch /opt/hpe/dark_site_exception_ccd'
```

3. Verify the dark site file is created on all the cnodes.

```
sudo -u vastdata clush -g cnodes 'ls -lrth /opt/hpe/dark_site_exception_ccd'
```

   The following output is displayed:

```
172.16.128.2: -rw-r--r--. 1 root root 0 Aug 24 09:23
/opt/hpe/dark_site_exception_ccd
172.16.128.1: -rw-r--r--. 1 root root 0 Aug 24 09:24
/opt/hpe/dark_site_exception_ccd
```

> **NOTE**
>
> This process takes approximately two minutes to complete. Wait until this process is complete before proceeding.

4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Update Vtool settings

About this task

This section maps to the Manual-Update_Vtool_Setting task under the Configure_GLFS task group.

- **Description:** This manual task is used to update the Vtool settings on all the CNodes.
- **Manual task:** To update Vtool settings, perform the following steps:

Procedure

1. Open an SSH session using VMS IP address and log in to the VMS node with username as `root` and password as `rootvastdata`.

> **NOTE**
>
> You can find the VMP IP address as specified in the Parameter list for configure_network.py script.

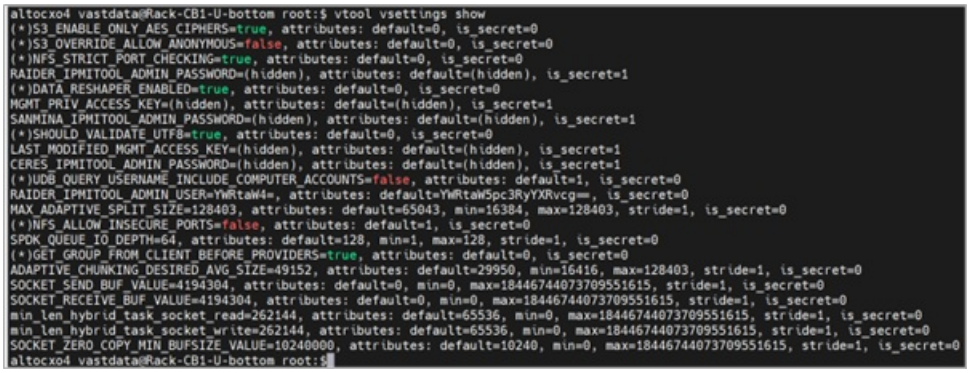
2. Update the Vtool settings using the following commands:

```
vtool vsettings set min_len_hybrid_task_socket_read=262144
vtool vsettings set min_len_hybrid_task_socket_write=262144
vtool vsettings set SOCKET_ZERO_COPY_MIN_BUFSIZE_VALUE=10240000
```

3. Verify that the Vtool settings are updated on all the CNodes.

```
vtool vsettings show
```

   Example:



4. Disable the collapse option on any CNode to resolve the HPE GreenLake for File Storage data inconsistency observed in a workload running VM Essentials manager.

   a. On any CNode, check if the collapse option is enabled.

   ```
   vtool vsettings show LAUNCH_BITMAP_INPLACE_ENTRIES_COLLAPSE
   ```

   b. Disable the collapse option if it is enabled.

   ```
   vtool vsettings set LAUNCH_BITMAP_INPLACE_ENTRIES_COLLAPSE=false
   ```

   c. Verify that the collapse option is disabled.

   ```
   vtool vsettings show LAUNCH_BITMAP_INPLACE_ENTRIES_COLLAPSE
   ```

5. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Update setup_status.json file

About this task

This section maps to the Manual-Create_Setup_Status_JSON task under the Configure_GLFS task group.

- **Description:** This manual task is used to update the **`setup_status.json`** file to enable VAST UI without TUI.
- **Manual task:** To update the **`setup_status.json`** file and enable VAST UI without TUI, perform the following steps:

Procedure

1. Open an SSH session using VMS node IP address and log in to the VMS node (for example, master CNode) with username as **`root`** and password as **`rootvastdata`**.

   > **NOTE**
   >
   > You can find the VMS IP address as specified in the Parameter list for configure_network.py script.

2. Create a **`fileservice`** directory to update the **`setup_status.json`** file.

   ```
   sudo -u hpeadmin mkdir -p /opt/sharedFolder/hpe/fileservice
   ```

3. Edit the **`setup_status.json`** file and update the following details:

   ```
   echo '{
    "overall_status": "configured",
    "pre_setup": "configured",
    "pre_setupTool": "configured",
    "dns_settings": "",
    "ntp_settings": "",
   ```

```
 "proxy_settings": "configured",
 "support_settings": "configured",
 "add_switches": "configured",
 "change_password": "configured",
 "hpeadmin": "configured",
 "hpecliadmin": "configured",
 "hpelogs": "configured",
 "ipmiAdmin": "configured",
 "vastAdmin": "configured",
 "vastSupport": "configured",
 "post_setup": "configured",
 "mandatory_features": "configured"
}' > /opt/sharedFolder/hpe/fileservice/setup_status.json
```

Example:

4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Complete post configuration on HPE GreenLake for File Storage system

This section outlines the procedures for mounting shared partition, copying OVA files, and unmounting the shared partition on the HPE GreenLake for File Storage system.

The workflow goes through the following sequence of tasks:

Workflow tasks in GLFS_Post_Configuration task group

Task Group	Task Name	Task Type	Remarks
Prerequisite	Create_Softlink_For_Images	Automated	This task creates soft links from the Cohesive Build VM to the shared location on MirrorBox. If this automated task fails, perform the optional manual procedure as mentioned in the Create soft links for images section.
	Install_Python_Modules	Automated	
	Enable_Trash_Folder_Access	Automated	
Copy_Files_onGLFS	Create_GLFSPartition	Automated	
	Copy_Files	Automated	Complete the prerequisites before running this automated task and verify the virtual IP pool, view policies, views, user, and user group created for the cluster as mentioned in the Verify the HPE GreenLake for File Storage configuration section.

Subtopics

Prepare HPE GreenLake for File Storage system

This section describes the manual tasks to be performed for preparing the HPE GreenLake for File Storage system to copy OVA files.

Subtopics

Creating soft links for images

About this task

This section describes the manual procedure to validate all the required files on the MirrorBox shared drive and verify MD5 checksum before copying OVA files on the HPE GreenLake for File Storage system.

NOTE

Perform this manual procedure only if the Create_SoftLinks_for_Images automated task under the Prerequisite task group fails.

To create soft links to the images on the MirrorBox and verify the checksum on the MD5 files, perform the following steps:

Procedure

1. Verify that the following files are present on the MirrorBox shared drive:

NOTE

All the required files are available in the **/var/cached-images/PC-AI/<baseline_version>/software/Staging** directory on the MirrorBox. The **<baseline_version>** directory indicates the current baseline version mentioned in the **infra-layout.json** SCID file. For example, if the baseline version is PCAI202507.3, the files are stored in the **/var/cached-images/PC-AI/PCAI202507.3_0/software/Staging** directory.

Small (S)/Medium (M)/Large (L) configuration type	MirrorBox path
HPE-AI-Essentials-EzFab-rockylinux-8.10-1.9.0-ec79ab7-67.x86_64.qcow2	../PC-AI/<baseline_version>/software/Staging/AIE
HPE-AI-Essentials-EzFab-rockylinux-8.10-1.9.0-ec79ab7-67.x86_64.md5	
rockylinux-8.10-1.9.0-ec79ab7-67.x86_64.qcow2	../PC-AI/<baseline_version>/software/Staging/ROCKY_Linux
rockylinux-8.10-1.9.0-ec79ab7-67.x86_64.md5	
DF_7.9_ubuntu18_8July.qcow2	../PC-AI/<baseline_version>/software/Staging/EDF
DF_7.9_ubuntu18_8July.md5	
cloud-init-cp-1.iso	../PC-AI/<baseline_version>/software/Staging/Cloud_Init
cloud-init-cp-1.md5	
cloud-init-cp-2.iso	
cloud-init-cp-2.md5	
cloud-init-cp-3.iso	
cloud-init-cp-3.md5	
cloud-init-ezfab.iso	
cloud-init-ezfab.md5	

2. Create a soft link to the nginx path for all the images mentioned in previous table.

```
ln -sf /mnt/mirrorbox-images/PC-AI/
<baseline_version>
/software/Staging/
<directory-name>
/
<filename>
 /usr/share/nginx/html/
```

Example:

```
ln -sf /mnt/mirrorbox-images/PC-AI/PCAI202507.3_0/software/Staging/ROCKY_Linux/rockylinux-8.10-1.9.0-ec79ab7-67.x86_64.qcow2 /usr/share/nginx/html/
```

3. Verify the MD5 checksum for all the files.

NOTE

Ensure that all the MD5 files are downloaded for validation. If not downloaded, the Copy_Files task will fail.

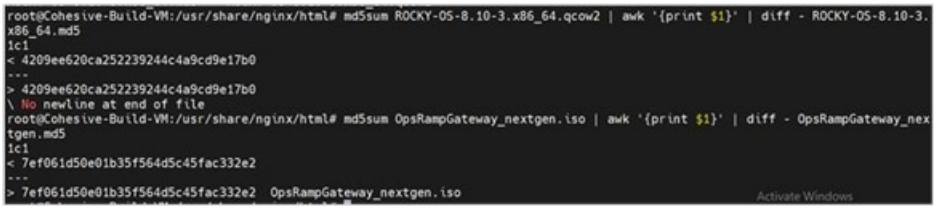
a. Navigate to the **nginx** directory where all the ISO and MD5 files are downloaded.

```
cd /usr/share/nginx/html/
```

b. Verify the MD5 checksum.

```
md5sum
<filename>
 | awk '{print $1}' | diff -
<checksum_file>
```

> **NOTE**
>
> Ensure that the md5 hash matches.



c. Repeat the previous step for each MD5 file.

4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Copy files on HPE GreenLake for File Storage

This section outlines the prerequisites for running the tasks under the Copy_Files_onGLFS task group and the checklist to verify the HPE GreenLake for File Storage configuration. These tasks are responsible for mounting shared partition, copying OVA files, and unmounting the shared partition on the HPE GreenLake for File Storage system.

Subtopics

Checklist: Verifying the HPE GreenLake for File Storage configuration

Prerequisites

The following prerequisites must be completed before running the Copy_Files task under the Copy_Files_onGLFS task group:

- Ensure that the HPE GreenLake for File Storage installation is completed before starting the Copy_Files task.
- Ensure that the VMS node credentials (username and password) are updated on the Update Task Inputs page. For more information, see the Update task inputs section.

About this task

The Copy_Files task is automatically triggered as part of the PC-AI build DAG workflow.

After all the tasks under the Copy_Files_onGLFS task group are complete, verify that the virtual IP pool, view policies, views, user, and user group are created properly in the HPE GreenLake for File Storage cluster at the Integration Center.

> **NOTE**
>
> Do not delete the virtual IP pool, view policies, and views created at the Integration Center. These configurations will be reused at the customer site.

Procedure

- [ ] Verify the virtual IP pool name and the assigned IP addresses.
  - [ ] Virtual IP pool name is **pcai**.
  - [ ] **Start IP** and **End IP** range is assigned as per the values in the SCID file.
- [ ] Verify the names of the two view policies and make sure both the view policies are associated with the **pcai** virtual IP pool.
  - [ ] View policy is created as **nfspolicy** to access NFS from the ESX Server.
  - [ ] View policy is created as **s3policy** to access S3 from the HPE AI Essentials software.
- [ ] Verify the user and group names.
  - [ ] Name of the created user is **s3user**.
  - [ ] Name of the created group is **s3group** and the user is added to this group.
- [ ] Verify the names of the three views and make sure they are mapped correctly.
  - [ ] View created as **/esxshare** is mapped to **nfspolicy** and OVAs are copied to this view.
  - [ ] View created as **/aiessentials** is mapped to **nfspolicy**.
  - [ ] View created as **/s3access** is mapped to **s3policy**, **s3user**, and **s3group**.

Deploy control nodes

This section describes the procedures to prepare and deploy SPP, operating system, and Data Services Controller VM on the control nodes.

> **NOTE**
> This section is applicable only for control nodes, which start from server-001 in the SCID file. Skip this entire section for the worker nodes.

The workflow goes through the following sequence of tasks:

Workflow tasks in Deploy_Control_Node task group

Task Group	Task Name	Task Type	Remarks
Prerequisite	Create_SoftLinks_for_Images	Automated	This task creates soft links from the Cohesive Build VM to the shared location on MirrorBox. If this automated task fails, perform the optional manual procedure as mentioned in the Create soft links for imagesCreating soft links for images section.
	Start_Nginx_Server	Automated	
	Install_Python_Modules	Automated	
Update_SPP	Build_SPP_Image	Automated	
	Power_On_Servers	Automated	
	Update_SPP	Automated	
	Reboot_Servers	Automated	
	Validate_SPP_Update	Automated	
Deploy_VME	Manual-Cleanup_ControlNode_Disks	Manual	To perform this task, see Clean up the control node disks section.
	Create_Boot_Volume	Automated	If this automated task fails, perform the optional manual procedure as mentioned in the Create boot volume section.
	Caution-Update-Grub_Entry_During_Deploy_VME	Manual	During VM Essentials deployment, update the GRUB entry as mentioned in the Update GRUB entry during VM Essentials deployment section.
	Deploy_VME	Automated	
	Manual-Assign_OS_IP	Manual	To perform this task, see Assign IP addresses after VM Essentials deployment section.
	Validate_VME	Automated	
Load_DSC_VM	Load_DSC_VM	Automated	
	Validate_DSC_VM	Automated	
Cleanup	Stop_Nginx_Service	Automated	
	Delete_Images_And_Checksum	Automated	

Subtopics

Prepare control node

This section describes the manual tasks to be performed for preparing the control node to deploy the operating system.

Subtopics

Creating soft links for images

About this task

This section describes the manual procedure to validate all the required files on the MirrorBox shared drive and verify MD5 checksum before deploying the operating system on the control nodes.

> **NOTE**
> Perform this manual procedure only if the Create_SoftLinks_for_Images automated task under the Prerequisite task group fails.

To create soft links to the images on the MirrorBox and verify the checksum on the MD5 files, perform the following steps:

Procedure

1. Verify the following files are present on the MirrorBox shared drive:

   > **NOTE**
   > All the required files are available in the **/var/cached-images/PC-AI/<baseline_version>/software/Control_Node** directory on the MirrorBox. The **<baseline_version>** directory indicates the current baseline version mentioned in the **infra-layout.json** SCID file. For example, if the baseline version is PCAI202507.3, the files are stored in the **/var/cached-images/PC-AI/PCAI202507.3_0/software/Control_Node** directory.

Small (S)/Medium (M)/Large (L) configuration type	MirrorBox path
HPE-VME-HostOS-8905-1.0.0.31-release.iso	**../PC-AI/<baseline_version>/software/Control_Node/Ubuntu-OS**
HPE-VME-HostOS-8905-1.0.0.31-release.md5	
bp-PrivateCloud-spp-2025.05.00.00.zip	**../PC-AI/<baseline_version>/software/Control_Node/SPP_ISO**
bp-PrivateCloud-spp-2025.05.00.00.md5	
HPE-MVM-Data-Services-Connector-9591-103.0.1.0-release.qcow2	**../PC-AI/<baseline_version>/software/Control_Node/DSC_VM**
HPE-MVM-Data-Services-Connector-9591-103.0.1.0-release.qcow2.sha256sum (kickstart file to install DSC VM)	
hpe-virt-mvm-kickstart-16Jun2025.md5	
hpe-virt-mvm-kickstart-16Jun2025.zip	

2. Create soft link to the nginx path for all the images mentioned in the previous table.

```
ln -sf /mnt/mirrorbox-images/PC-AI/
<baseline_version>
/software/Control_Node/
<directory-name>
/
<filename>
 /usr/share/nginx/html/
```

Example:

```
ln -sf /mnt/mirrorbox-images/PC-
AI/PCAI202507.3_0/software/Control_Node/Ubuntu-OS/HPE-VME-HostOS-8905-
1.0.0.31-release.iso /usr/share/nginx/html/
```

3. Verify the MD5 checksum for all the files.

   a. Navigate to the **nginx** directory where all the ISO and MD5 files are downloaded.

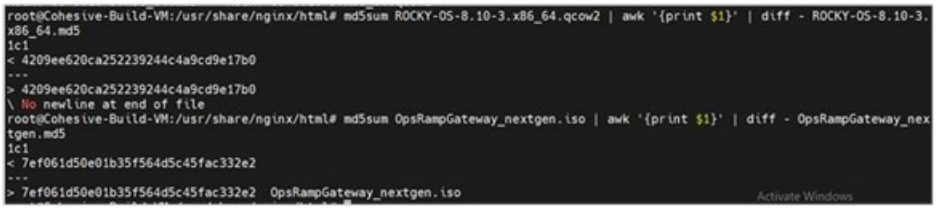
   ```
   cd /usr/share/nginx/html/
   ```

   b. Verify the MD5 checksum.

   ```
   md5sum
   <filename>
    | awk '{print $1}' | diff -
   <checksum_file>
   ```

   > **NOTE**
   >
   > Ensure that the md5 hash matches.

   Example:

   c. Repeat the previous step for each MD5 file.

4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Deploy VM Essentials

This section describes the tasks to be performed for deploying the VM Essentials Ubuntu operating system on the control node.

Subtopics

Cleaning up the control node disks

About this task

This section maps to the Manual-Cleanup_ControlNode_Disks task under the Deploy_VME task group.

- **Description:** This manual task is used to clear the disk partitions from Intelligent Provisioning and the RAID configuration from the BIOS settings and verify the volume used for storage on the control node.
- **Manual task:** To clean up the control node disks, perform the following steps:

Procedure

1. Retrieve the IP address and user credentials for the control nodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for the first three servers starting from `"componentId": "serv`

er-001" to "componentId": "server-003" where "purpose": "iLO Management" under "infrastructure" > "racks" > "servers" > "networkConnections" to retrieve the IP address for each control node.

- In the **infra-layout.json** file, find the "userName" and "password" fields for the first three servers where "type": "DL325" and "target": "ILO" under "racks" > "servers" > "accessCredentials" to retrieve the iLO user credentials for each control node.

2. Clean up the disk partitions from Intelligent Provisioning .
3. Clear RAID configuration.
4. Verify storage information.
5. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

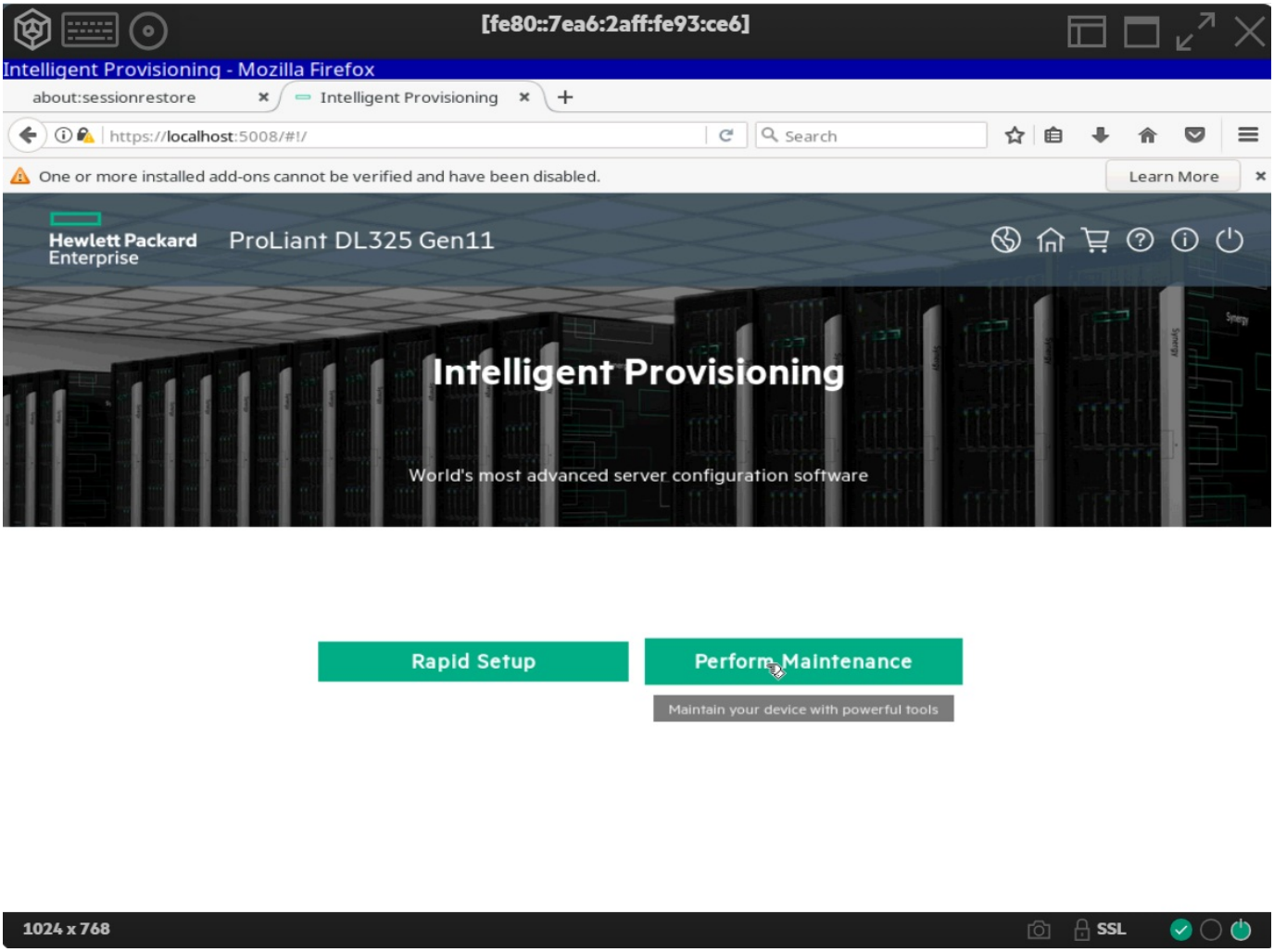
Subtopics

Cleaning up the disk partitions from Intelligent Provisioning

Procedure

1. Log in to the iLO user interface on the control node using the IP address and credentials retrieved in the previous step.
2. Reset or reboot the control node.
3. During server POST, press F10 to log in to Intelligent Provisioning.

   Wait until the Intelligent Provisioning homepage opens.
4. Click Perform Maintenance.

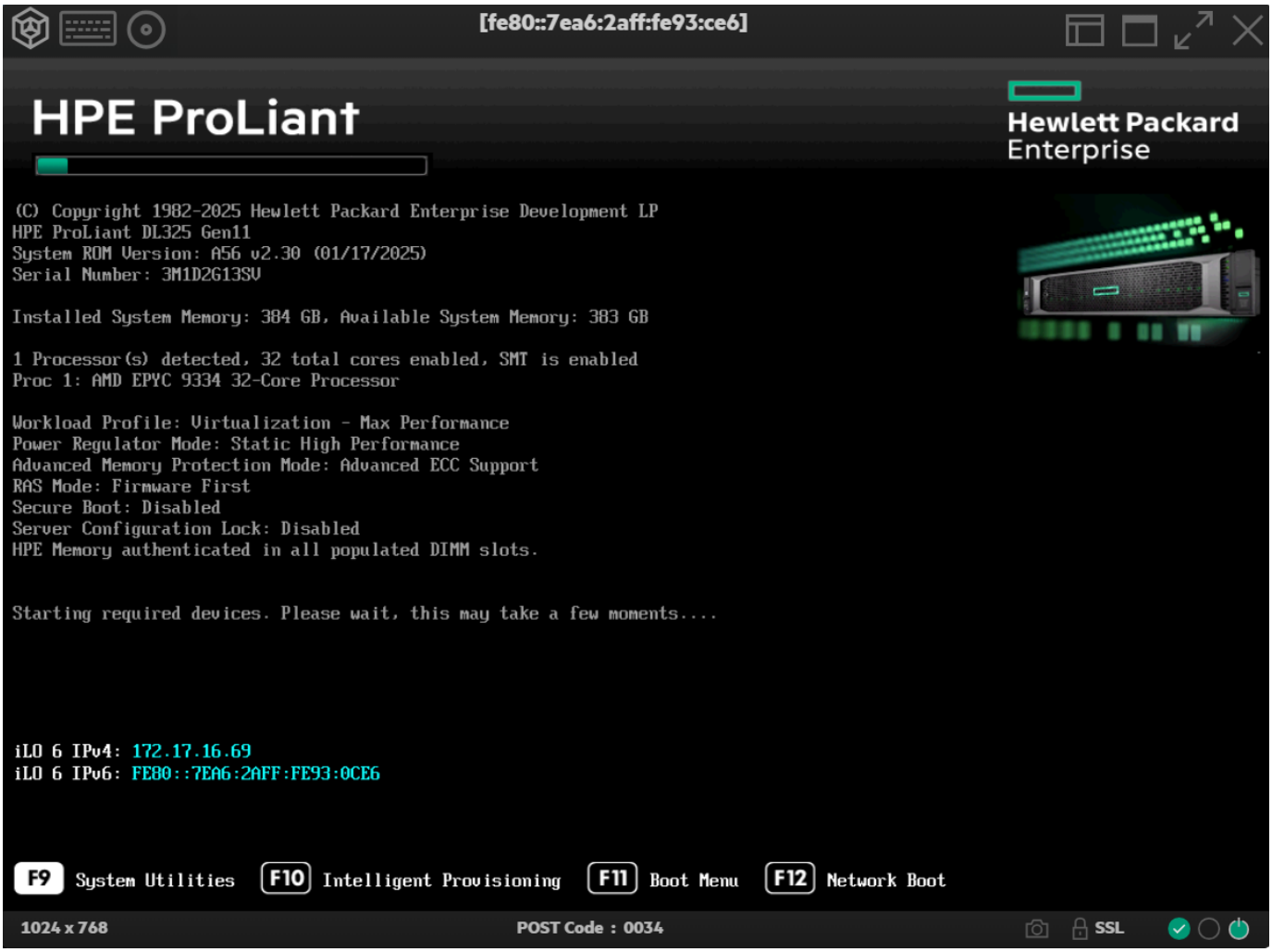


5. On the Perform Maintenance page, select System Erase and Reset.
6. Select all HDD and SDD and click Submit.
7. Launch the Job and wait for the task to complete.
8. Click Reboot.

Clearing RAID configuration

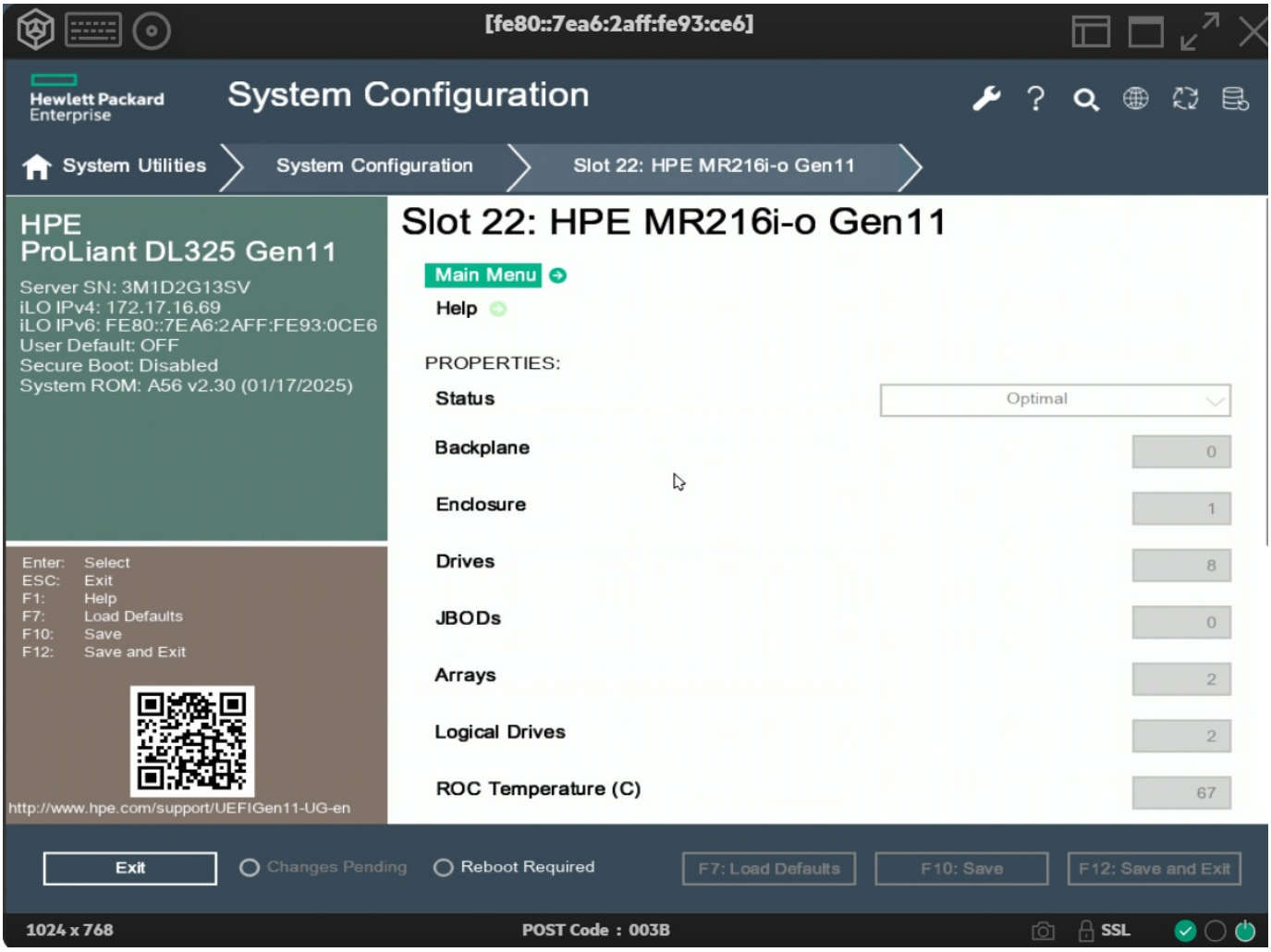
Procedure

1. Reboot the server and press F9 to open the System Utilities screen.

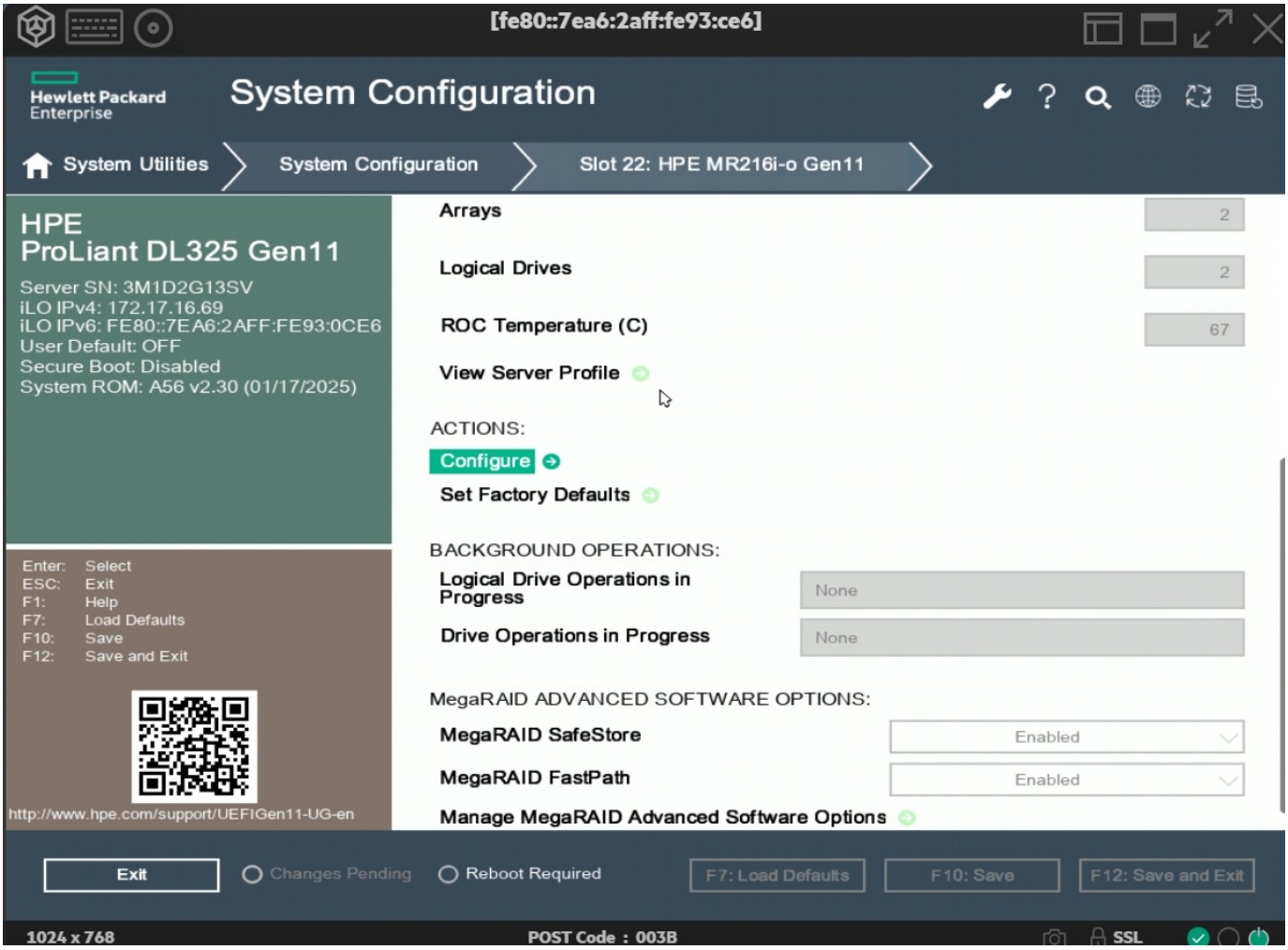


2. Click System Configuration.
3. Select HPE MR 216i-o controller.

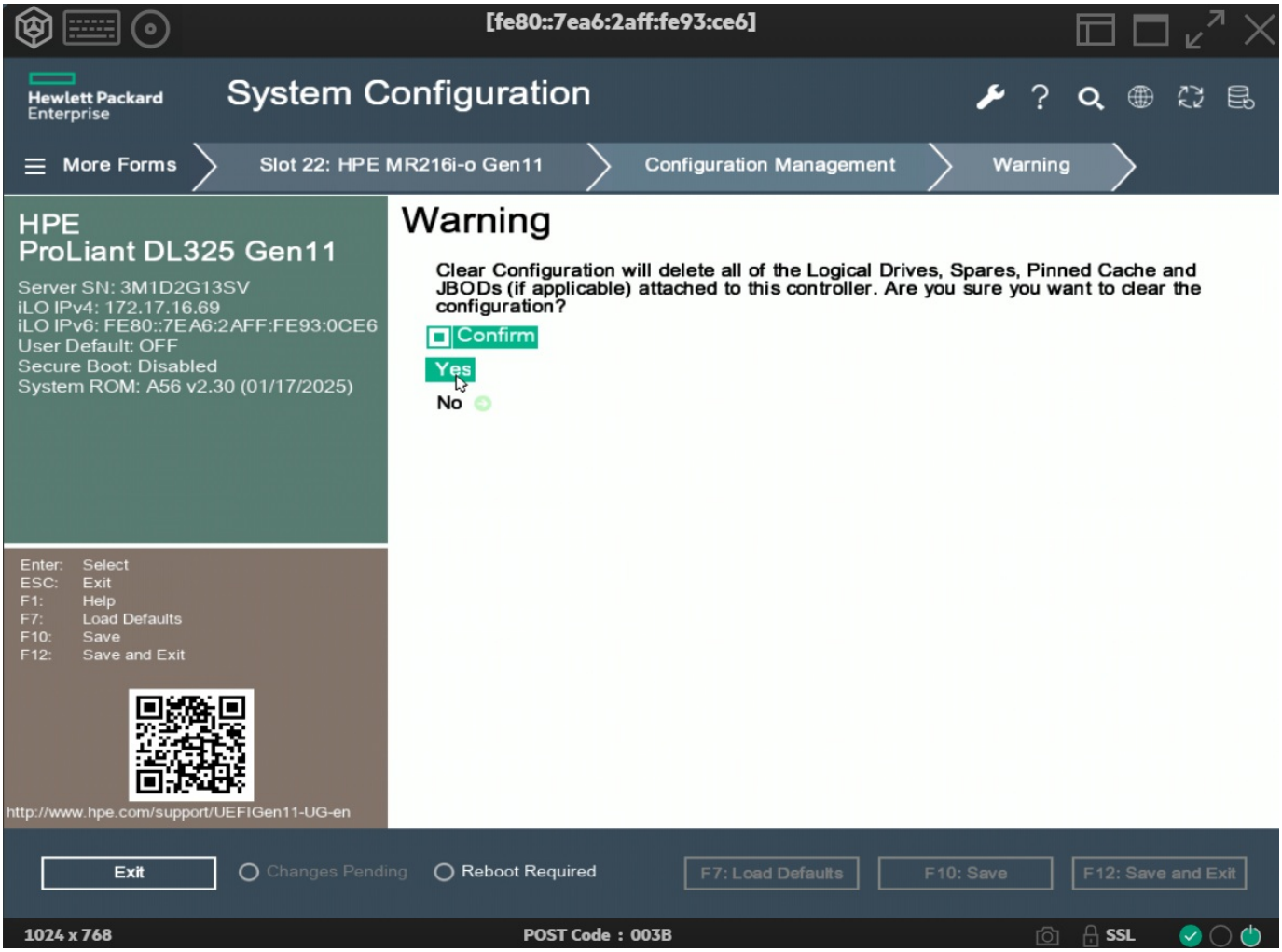
   The HPE MR 216i-o controller page appears.



4. Scroll down and click Configure.



5. Click Clear configuration.
6. Select Confirm and click Yes.



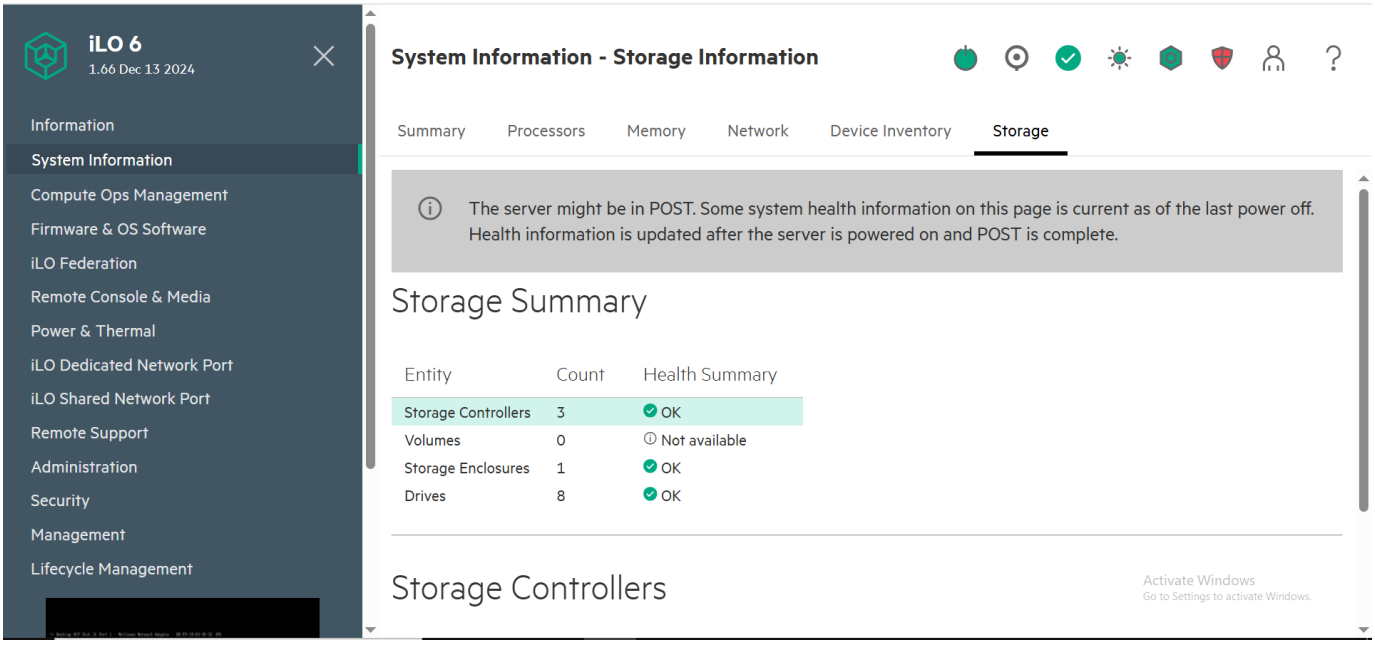
Verifying storage volume

About this task

To verify that the drives are cleared, perform the following steps:

Procedure

1. On the iLO web interface, navigate to System Information.
2. On the System Information – Storage Information page, select the Storage tab.
3. On the Storage Summary page, verify that the number of volumes is 0.



Creating boot volume

About this task

This section describes the manual procedure to create RAID 1 logical drive on the control node.

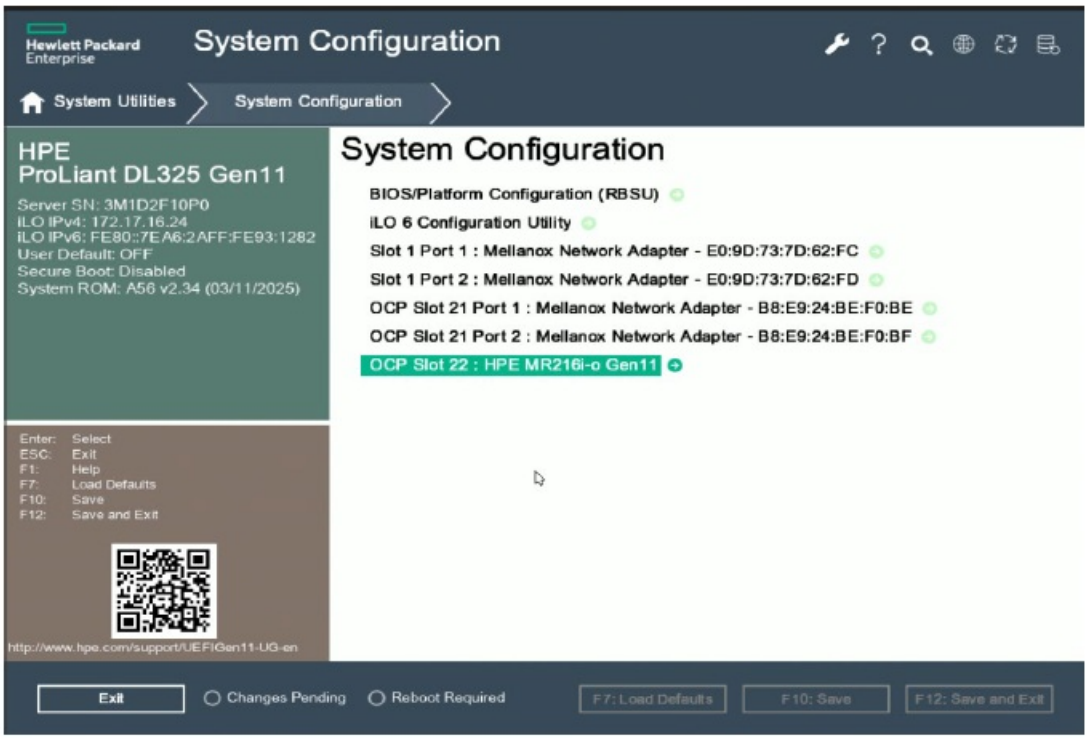
> **NOTE**
>
> Perform this manual procedure only if the Create_Boot_Volume automated task under the Deploy_VME task group fails.

To create the RAID 1 logical drive on the control node, perform the following steps:

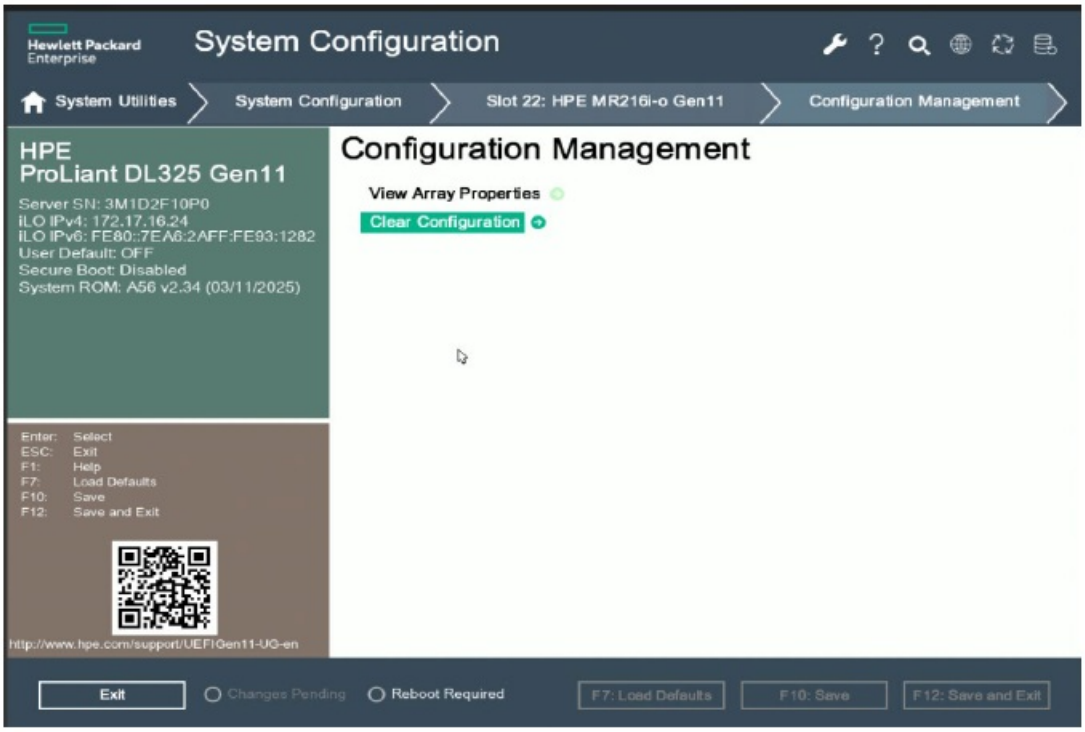
Procedure

1. Log in to the iLO UI on the control node.
2. Restart or power on the control node.

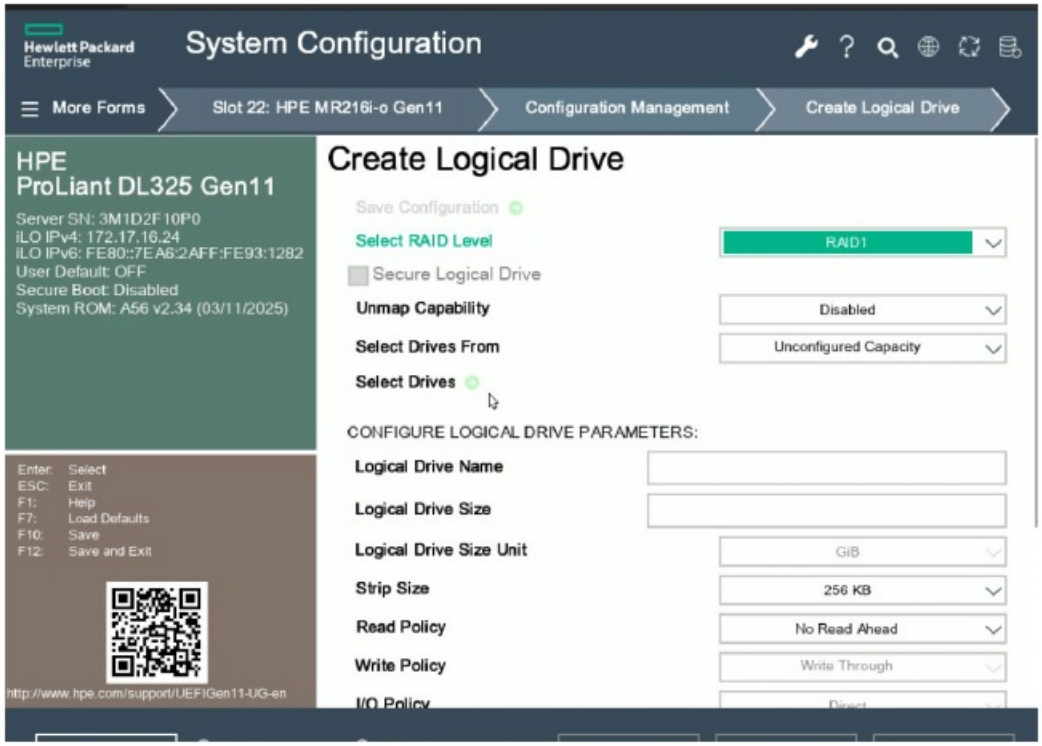
   The server restarts, and the POST screen appears.
3. On the POST screen of the server, press F9 to open System Utilities in server BIOS.
4. Navigate to System Configuration and select the appropriate MR controller.



5. On the MR controller screen, click Configure.
6. On the Configuration Management screen, click Clear Configuration if any exists already.



7. Click Confirm, and then click OK.
8. On the Configuration Management screen, click Create Logical Drive.
9. On the Create Logical Drive screen, perform the following steps:
   a. Select RAID1 from the RAID Level drop-down list.



b. Click Select Drives.

c. On the Select Drives screen, select two SAS disks, select Apply and then click OK.

> **NOTE**
>
> Do not select NVMe disks.

d. Click Save Configuration.

10. Press F12 to save and exit.

11. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Updating GRUB entry during VM Essentials deployment

About this task

This section maps to the Caution-Update-Grub_Entry_During_Deploy_VME task under the Deploy_VME task group.

- **Description:** This manual task is used to add an entry on the GRUB screen to make sure that the operating system is installed on the correct volume on the control node.
- **Manual task:** To add an entry on the GRUB screen during VM Essentials deployment, perform the following steps:

> **NOTE**
>
> This task acts as a caution for you to intervene during the system boot to modify the GRUB entry, as the GRUB menu times out after a few seconds.

Procedure

1. Monitor the VM Essentials deployment process from the iLO HTML5 console on the control nodes.

   When the Deploy_VME automated task is triggered, the operating system will begin booting.

2. Keep the HTML5 console open for all the control nodes.

   The Install Ubuntu OS screen appears briefly for a few seconds.

3. Press e immediately to enter the GRUB modification screen.

4. On the GRUB screen, add the following entry to make sure the operating system is installed on the correct volume:

   > **IMPORTANT**
   >
   > Do not skip this step as it may cause the operating system to install on an incorrect volume.

   ```
   rd.kiwi.oem.installdevice=/dev/sda
   ```

5. After modifying the GRUB entry, press F10 within a threshold of 5 minutes to proceed with the boot process.

   > **NOTE**
   >
   > If you do not press F10 in time, the operating system will not load, and the Deploy_VME task will be incorrectly marked as Success in the workflow.

6. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Assigning IP addresses after VM Essentials deployment

About this task

This section maps to the Manual-Assign_OS_IP task under the Deploy_VME task group.

- **Description:** This manual task is used to configure the static IP address on the management interface of the Ubuntu operating system after the VM Essentials is deployed as per the recipe version.
- **Manual task:** To configure the static IP address on the management interface of the Ubuntu operating system, perform the following

steps:

Procedure

1. Retrieve the IP address and user credentials for the control nodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for the first three servers starting from `"componentId": "server-001"` to `"componentId": "server-003"` where `"purpose": "iLO Management"` under `"infrastructure" > "racks" > "servers" > "networkConnections"` to retrieve the IP address for each control node.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for the first three servers where `"type": "DL325"` and `"target": "ILO"` under `"racks" > "servers" > "accessCredentials"` to retrieve the iLO user credentials for each control node.
2. Log in to the control node HTML5 console using the ILO IP address and credentials retrieved in the previous step.
3. Assign the appropriate IP address on the control node:
   a. Edit the **default-net.yaml** file using the following command:

      ```
      sudo vim /etc/netplan/default-net.yaml
      ```

   b. Add the management interface to the **/etc/netplan/default-net.yaml** file in the provided format:

      ```
      mgmt:
       dhcp4: false
       accept-ra: false
       addresses:
         -
      <IP address/CIDR>

       routes:
       - to: default
         via:
      <Gateway>

       nameservers:
         addresses:
           -
      <DNS>

       interfaces:
       - bond0
       link-local:
       - ipv4
       - ipv6
       openvswitch: {}
      ```

      Example:

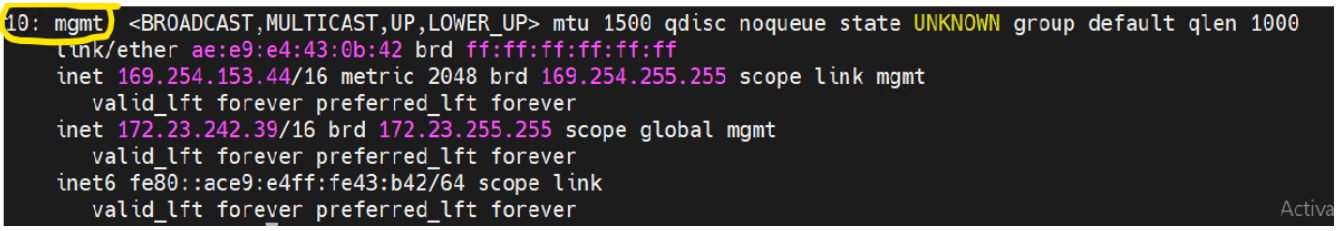
      ```
      mgmt:
       dhcp4: false
       accept-ra: false
       addresses:
         - 172.17.16.97/24
       routes:
       - to: default
         via: 172.17.16.1
       nameservers:
         addresses:
           - 172.17.16.4
      ```

```
interfaces:
- bond0
link-local:
- ipv4
- ipv6
openvswitch: {}
```

c. Apply the network settings with the following command:

```
sudo netplan apply
```

d. Validate the assigned IP is pinging and able to connect to the control nodes using SSH.



4. Repeat the previous steps for all the control nodes.
5. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Deploy worker nodes

This section describes the procedures to prepare the worker nodes for deploying the operating system.

> **NOTE**
> This section is applicable only for worker nodes, which starts from server-004 in the SCID file. Skip this entire section for the control nodes.

The workflow goes through the following sequence of tasks:

Workflow tasks in Deploy_Worker_OS task group

Task Group	Task Name	Task Type	Remarks
Prerequisite	Create_SoftLinks_for_Images	Automated	This task creates soft links from the Cohesive Build VM to the shared location on MirrorBox. If this automated task fails, perform the optional manual procedure as mentioned in the Create soft links for images section.
	Install_Python_Modules	Automated	
	Start_Nginx	Automated	
	Manual_PowerOn_Server	Manual	To perform this task, see Power on worker nodes section.
Adhoc_Validation_And_Updates	Pre-Build_Validation	Automated	
	Manual_Adhoc_update	Manual	This task is required only if there are ad hoc updates. Since there are no ad hoc tasks for this version, mark the status of this task as Success to continue to the next task in the workflow.
Deploy_RHEL_OS	Configure_Raid1	Automated	If this automated task fails, verify that RAID 1 is created as mentioned in the Verify RAID 1 section.
	Build_RHEL_OS	Automated	
	Install_RHEL_OS	Automated	
	Configure_Network	Automated	
	Configure_dns_ntp_proxy	Automated	
	Validate_RHEL_Installation	Automated	
	GPU_Firmware_Upgrade	Automated	
Deploy_SPP	Install_SPP	Automated	
	Validate_SPP_Installation	Automated	
Cleanup	Stop_Nginx	Automated	
	Delete_ISO	Automated	This task is optional. By default, this task is skipped. It can be run by clearing the task in Airflow UI.

Subtopics

Prepare worker nodes

This section describes the manual tasks to be performed for preparing the worker nodes to deploy the operating system.

Subtopics

Creating soft links for images

About this task

This section describes the manual procedure to validate all the required files on the MirrorBox shared drive and verify MD5 checksum before deploying the operating system on the worker nodes.

> **NOTE**
> Perform this manual procedure only if the Create_SoftLinks_for_Images automated task under the Prerequisite task group fails.

To create soft links to the images on the MirrorBox and verify the checksum on the MD5 files, perform the following steps:

Procedure

1. Verify the following files are present on the MirrorBox shared drive:

   > **NOTE**
   > All the required files are available in the **/var/cached-images/PC-AI/<baseline_version>/software/Worker_Node/** directory on the MirrorBox. The **<baseline_version>** directory indicates the current baseline version mentioned in the **infra-layout.json** SCID file. For example, if the baseline version is PCAI202507.3, the files are stored in the **/var/cached-images/PC-AI/PCAI202507.3_0/software/Worker_Node/** directory.

Small (S)/Medium (M)/Large (L) configuration type	MirrorBox path
PCAI-GenAI-RHEL810-20250715-369-release.ISO	**../PC-AI/<baseline_version>/software/Worker_Node/RHEL_OS**
PCAI-GenAI-RHEL810-20250715-369-release.md5	
P84266_001_gen11spp-2025.05.00.00-Gen11SPP2025050000.2025_0604.20.iso	**../PC-AI/<baseline_version>/software/Worker_Node/SPP_Upgrade**
P84266_001_gen11spp-2025.05.00.00-Gen11SPP2025050000.2025_0604.20.md5	
NVIDIA_L40S_GPU_VBIOS-95.02.66.00.15-1-0.x86_64.rpm	**../PC-AI/<baseline_version>/software/Worker_Node/GPU_Firmware**
NVIDIA_L40S_GPU_VBIOS-95.02.66.00.15-1-0.x86_64.md5	
NVIDIA_H100_NVL_94GB_PCIe_GPU-96.00.AF.00.02-CEC-00.02.0185.0000.zip	
NVIDIA_H100_NVL_94GB_PCIe_GPU-96.00.AF.00.02-CEC-00.02.0185.0000.md5	

2. Create soft link to the nginx path for all the images mentioned in the previous table.

```
ln -sf /mnt/mirrorbox-images/PC-AI/
<baseline_version>
/software/Worker_Node/
<directory-name>
/
<filename>
 /usr/share/nginx/html/
```

Example:

```
ln -sf /mnt/mirrorbox-images/PC-
AI/PCAI202507.3_0/software/Worker_Node/RHEL_OS/PCAI-GenAI-RHEL810-
20250715-369-release.ISO /usr/share/nginx/html/
```

3. Verify the MD5 checksum for all the files.

   a. Navigate to the **nginx** directory where all the ISO and MD5 files are downloaded.

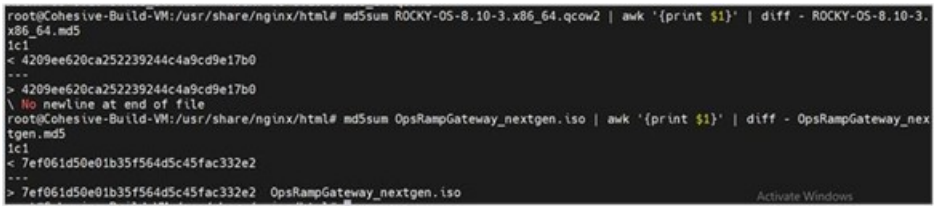
   ```
   cd /usr/share/nginx/html/
   ```

   b. Verify the MD5 checksum.

   ```
   md5sum
   <filename>
   | awk '{print $1}' | diff -
   <checksum_file>
   ```

   > **NOTE**
   > Ensure that the md5 hash matches.

   Example:

   c. Repeat the previous step for each MD5 file.

4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Powering on worker nodes

About this task

This section describes the procedure to power on the worker nodes and maps to the Manual_PowerOn_Server task under the Prerequisite task group.

> **NOTE**
> Perform this manual procedure only if the servers are powered off.

Procedure

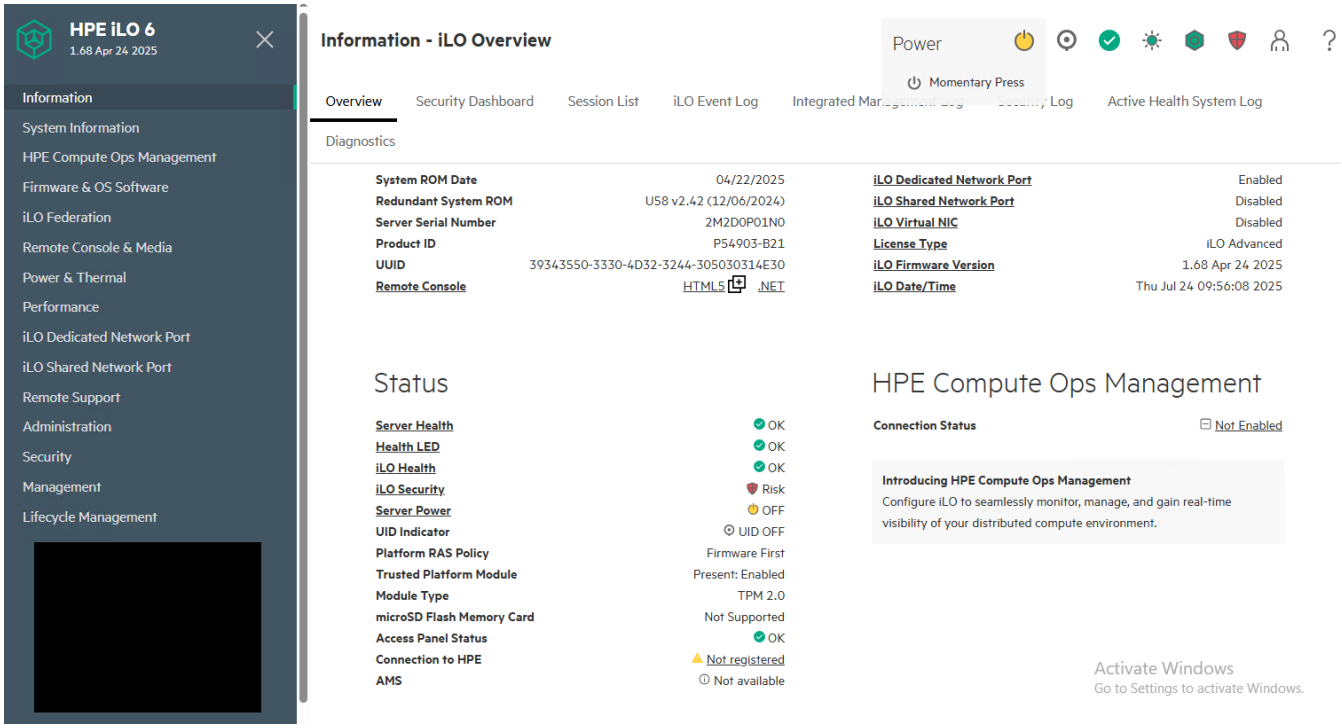
1. Retrieve the IP address and iLO user credentials for the worker nodes from the **base-configuration.json** and **infra-layout.json** SCID files.

   - In the **base-configuration.json** file, find the `"ipAddress"` field for all the servers starting from `"componentId": "server-004"` to the last `"componentId"` where `"purpose": "iLO Management"` under `"infrastructure" > "racks" > "servers" > "networkConnections"` to retrieve the iLO IP address for each worker node.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for all the servers starting from `"componentId": "server-004"` where `"type": "DL380a"` and `"target": "ILO"` under `"racks" > "servers" > "accessCredentials"` to retrieve the iLO user credentials for each worker node.

2. Power on the server.

   a. Log in to the iLO user interface from the browser using the IP address and credentials retrieved in the previous step.

b. Click the Power icon from the toolbar on the top of the page and select Momentary Press to power on the server.



c. Repeat the previous steps for all worker nodes.

3. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Deploy Red Hat Enterprise Linux (RHEL) operating system

This section describes the manual tasks to be performed for deploying the Red Hat Enterprise Linux (RHEL) operating system on the worker nodes.

Subtopics

Verifying RAID 1

Verifying RAID 1

About this task

This section describes the manual procedure to verify that RAID 1 is created.

> **NOTE**
> Perform this manual procedure only if the Configure_RAID1 automated task under the Deploy_RHEL_OS task group fails.

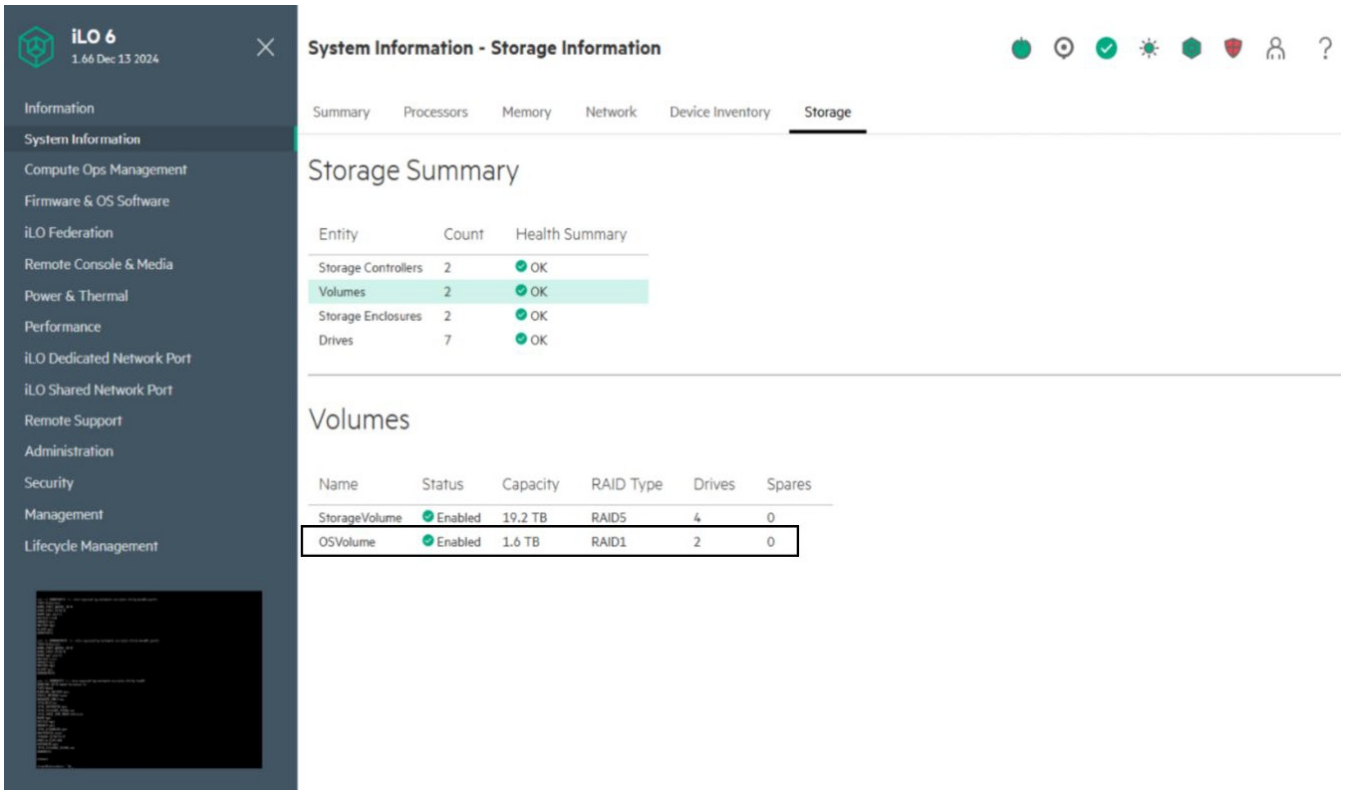
Procedure

1. Retrieve the IP address and iLO user credentials for the worker nodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for all the servers starting from `"componentId": "server-00`

4" to the last "componentId" where "purpose": "iLO Management" under "infrastructure" > "racks" > "servers" > "networkConnections" to retrieve the iLO IP address for each worker node.

- In the **infra-layout.json** file, find the "userName" and "password" fields for all the servers starting from "componentId": "server-004" where "type": "DL380a" and "target": "ILO" under "racks" > "servers" > "accessCredentials" to retrieve the iLO user credentials for each worker node.

2. Verify that RAID 1 is created.
   a. Log in to the iLO user interface on the worker node using the IP address and credentials retrieved in the previous step.
   b. Navigate to the System Information from the left pane.
   c. On the System Information – Storage Information page, select the Storage tab.
   d. On the Storage tab, click Volumes.
   e. In the Volumes section, if a volume shows Name as OSVolume and RAID Type as RAID1, the RAID 1 is successfully created.



3. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Deploy OpsRamp gateway on control nodes

This section describes the procedures for deploying the OpsRamp gateway on the control nodes.

The workflow goes through the following sequence of tasks:

Workflow tasks in Deploy_OpsRamp_Gateway task group

Task Group	Task Name	Task Type	Remarks
Prerequisite	Install_Python_Modules	Automated	
	Copy_Images_To_Control_Node	Automated	
	Prerequisite_Validation	Automated	
Deploy_OpsRamp_GatewayVM	Install_OpsRamp_Gateway	Automated	
	Set_HostName_and_Proxy	Automated	
	Validate_OpsRamp_Gateway	Automated	
Configure_OpsRamp_Gateway	Install_K3S_On_Gateway	Automated	
	Validate_K3S_On_Gateway	Automated	
Configure_SNMP	Configure_Nvidia_Switches	Automated	
	Configure_OOBM_Switches	Automated	
	Configure_Storage_Switches	Automated	
	Configure_PDUs	Automated	
Validate_SNMP	Validate_OOBM_Switches	Automated	
	Validate_Storage_Switches	Automated	
	Validate_Nvidia_Switches	Automated	
Create_iLO_Service_Accounts	Control_and_Worker_Nodes	Automated	
Registration_Prerequisite	Generate_Registration_Input_Definition	Automated	
Pre-Shutdown_GatewayVM	Remove_Storage_Pool	Automated	
	Validate_Storage_Pool	Automated	
	Detach_Mounts	Automated	

Pre-shutdown validation

This section outlines the tasks perform solution validation, clean up the installation system, and perform exit tasks before finishing the component deployment.

Subtopics

Complete end-to-end validation

This section maps to the Validate_E2E task group that performs the health, configuration, and recipe validation of the engineered system.

The workflow goes through the following sequence of tasks:

Workflow tasks in Validate_E2E task group

Task Group	Task Name	Task Type	Remarks
Validate_E2E	Validate_E2E	Automated	Before running this task, complete the prerequisites mentioned in the Run the end-to-end validation task section.

Subtopics

Running the end-to-end validation task

Prerequisites

The following prerequisites must be completed before running the Validate_E2E task:

- Ensure that the **baseline.json** file is available in the **/opt/airflow/scripts/builds/<build_name>/artifacts/uploads** directory.
- REST API access must be enabled on the PDUs.

About this task

This section maps to the Validate_E2E task under the Validate_E2E task group.

Procedure

The Validate_E2E task is automatically triggered as part of the PC-AI build DAG workflow.

Downloading Config checker report

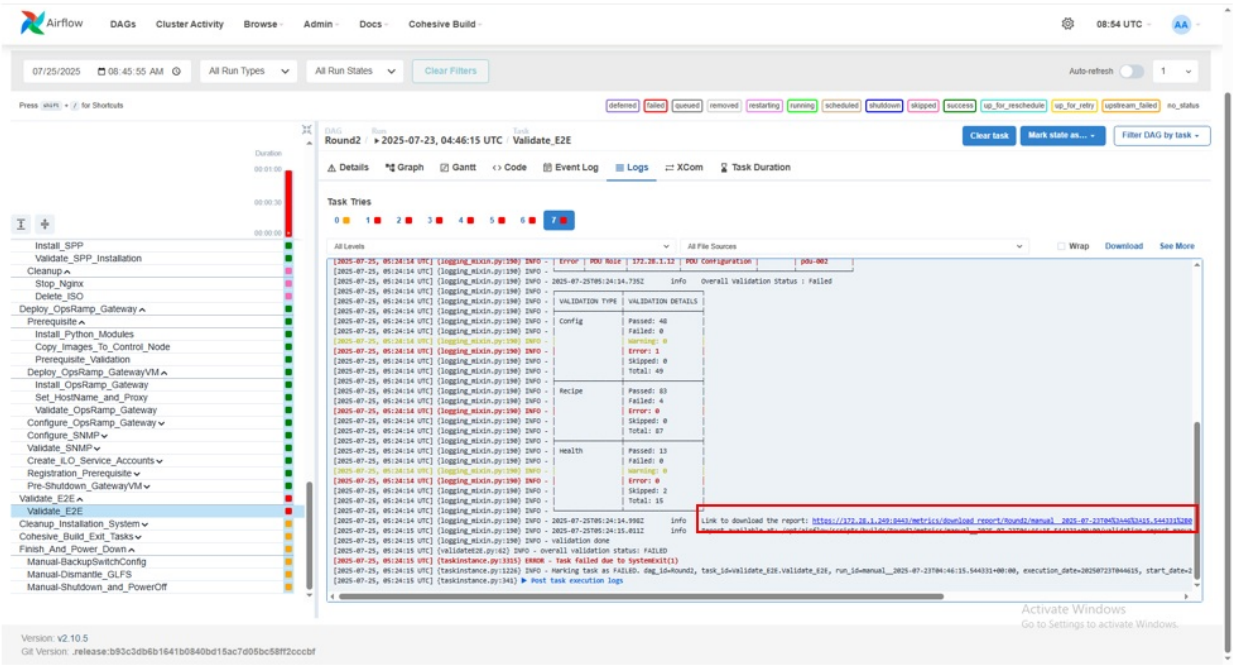
About this task

This section outlines the procedure to download the log report of the Validate_E2E task to get a complete list of validations.

You can download the Config checker report using one of the two ways:

Procedure

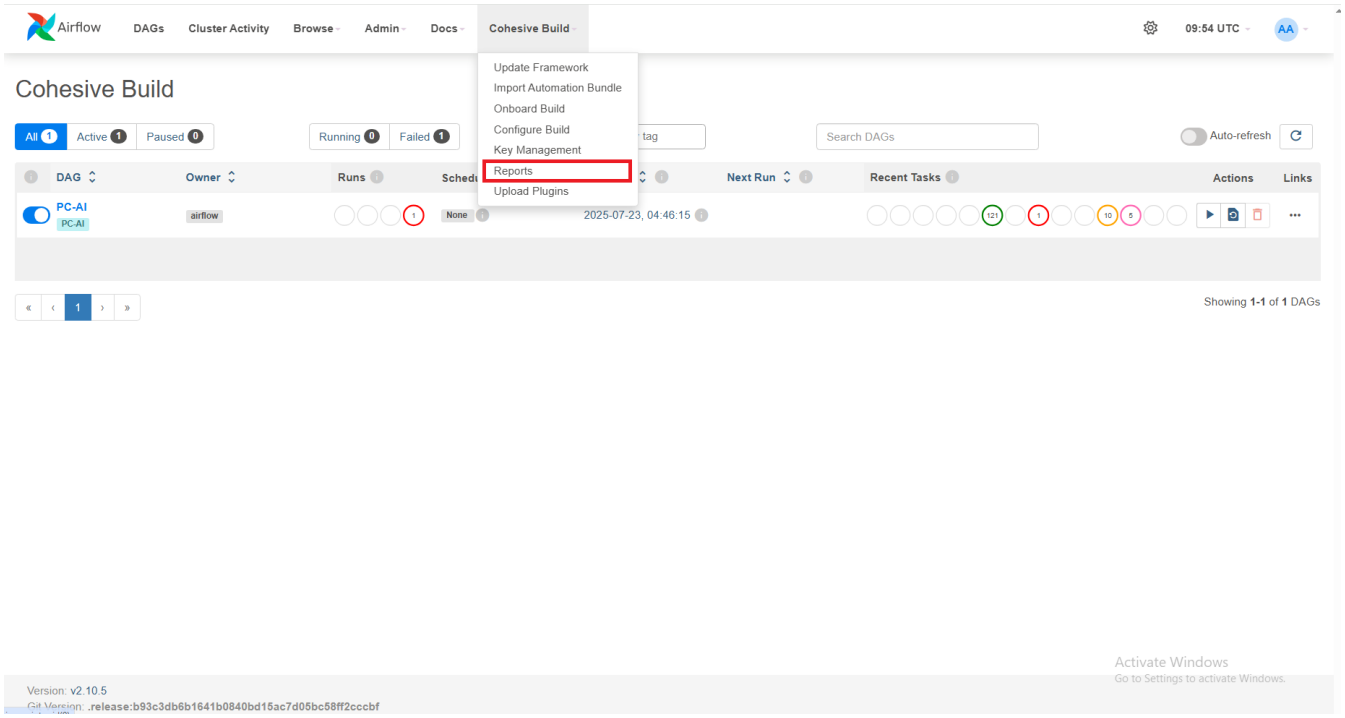
1. Download the report from the DAG page.
   a. On the DAG page, navigate to the logs screen of the Validate_E2E task.
   b. Click the link to download the report from the right pane at the bottom.



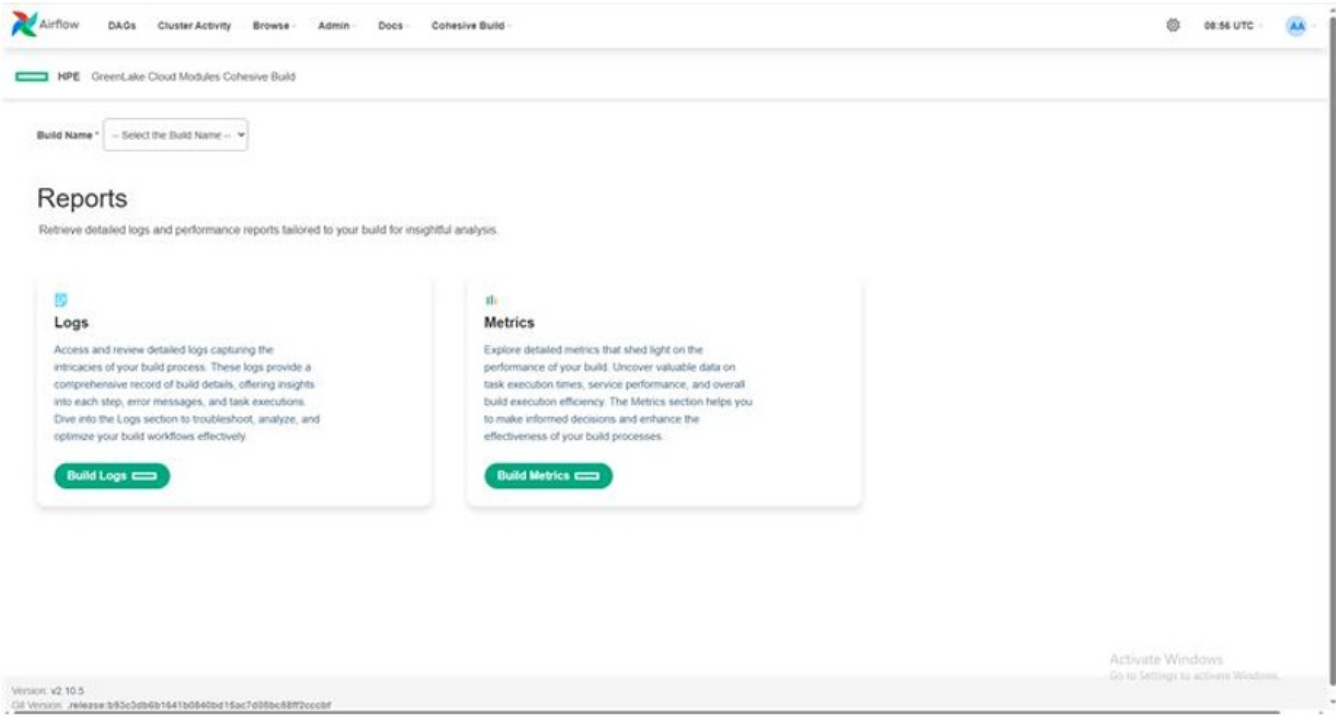
The Excel files with a complete list of validations is downloaded to your system.

2. Download the report from the Reports page.

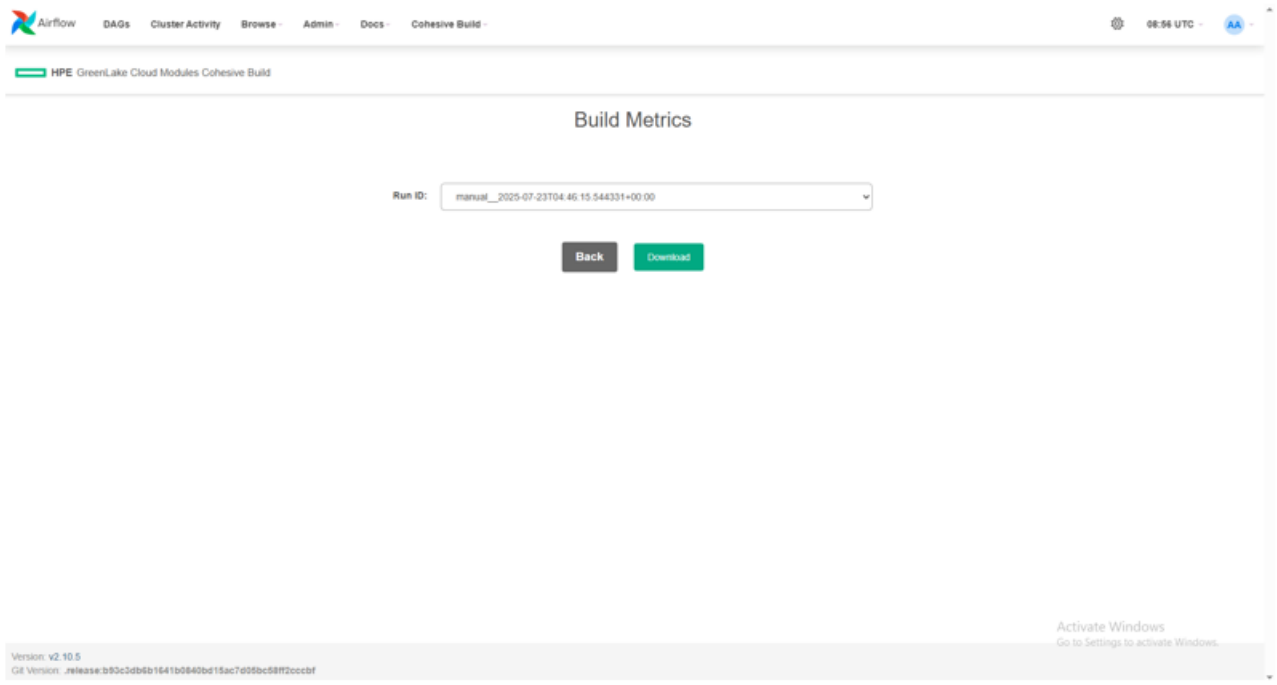
   a. Navigate to the Cohesive Build menu and select Reports.



   b. On the Reports page, click Build Metrics.



c. On the Build Metrics page, click Download.



The zip file is downloaded to your system. It contains Excel files with a complete list of validations and build metrics.

If the Excel file report shows an error status for any PDU, especially in the Config Report, perform the following steps for manual validation:

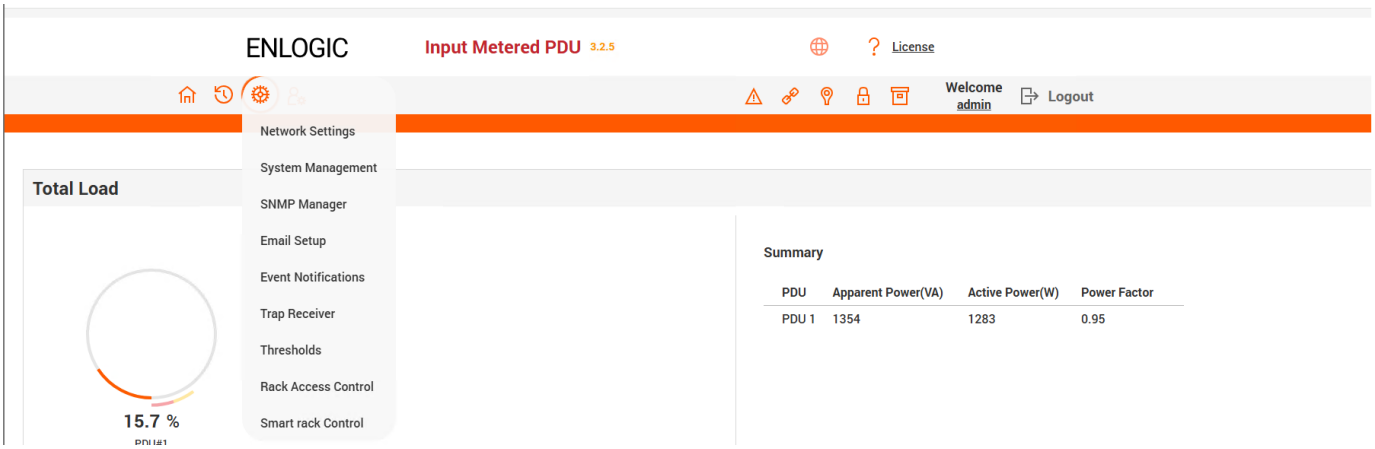
1. Log in to the PDU UI using PDU IP address from the **base-configuration.json** SCID file.

NOTE

You can find the IP address and user credentials for PDUs in the **base-configuration.json** and **infra-layout.json** SCID files.

- In the **base-configuration.json** file, find the `"ipAddress"` field for the `"componentId": "pdu-001"` and the `"componentId": "pdu-002"` under `"infrastructure" > "racks" > "pdus" > "networkConnections"` to retrieve the IP addresses for both the PDUs.
- In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for the `"target": "PDU"` under `"racks" > "pdus" > "accessCredentials"` to retrieve the user credentials for both the PDUs.

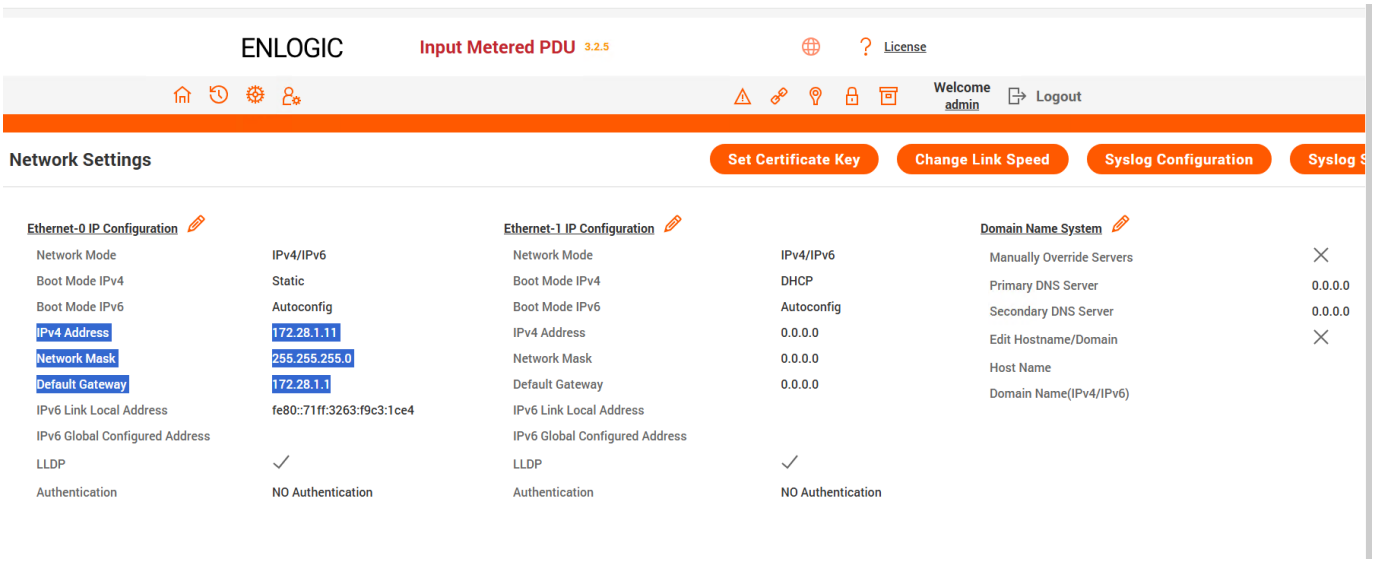
2. Navigate to Settings > Network Settings.



3. On the Network Settings page, verify that the IPV4 address, network mask and, default gateway are set as per the **base-configuration.json** file.

   In the **base-configuration.json** file, find the following IP addresses:

   - In the **base-configuration.json** file, find the `"ipAddress"` field under `"infrastructure" > "racks" > "pdus" > "networkConnections"` to retrieve the IPv4 address for the PDU.
   - In the **base-configuration.json** file, find the `"networkMask"` field under `"networks"` where `"name": "Management Network"` to retrieve the network mask for the PDU.
   - In the **base-configuration.json** file, find the `"gatewayIpAddress"` field under `"networks"` where `"name": "Management Network"` to retrieve the default gateway address for the PDU.



Clean up installation system

The workflow goes through the following sequence of tasks:

Workflow tasks in Cleanup_Installation_System task group

Task Group	Task Name	Task Type	Remarks
Cleanup_Installation_System	Manual-PreCleanup_Confirmation	Manual	Requests confirmation from the user before cleaning up the Solution instance-specific configuration on the Installation System. Ensure that the built Solution instance is working properly and backup any information as needed and confirm.
	Cleanup_NAT	Automated	
	Cleanup_DNS	Automated	
	Cleanup_NTP	Automated	
	Cleanup_Firewall	Automated	
	Cleanup_Solution_Management_Network	Automated	

Complete exit tasks on PC-AI build workflow

The following tasks in the Cohesive_Build_Exit_Tasks task group are automatically triggered as part of the PC-AI build DAG workflow:

Workflow tasks in Cohesive_Build_Exit_Tasks task group

Task Group	Task Name	Task Type	Remarks
Backup_Build_Data	Generate_Metrics_And_Collect_Run_Logs	Automated	

Finish and power down

This chapter describes the sequential steps to finish the component deployment and power down the components at the Integration Center.

Workflow tasks in Finish_And_Power_Down task group

Task Group	Task Name	Task Type	Remarks
Finish_And_Power_Down	Manual-BackupSwitchConfig	Manual	To perform this task, see the Backup switch configuration section
	Manual-Dismantle_GLFS	Manual	To perform this task, see the Dismantle HPE GreenLake for File Storage cluster section.
	Manual-Shutdown_and_PowerOff	Manual	To perform this task, see the Power down all components section.

Subtopics

Backup switch configuration

About this task

This section maps to the Manual-BackupSwitchConfig task under the Finish_And_Power_Down task group.

- **Description:** This manual task is used to save the switch configurations on all switch infrastructure before powering off the rack.
- **Manual task:** To save the switch configuration based on the switch type, perform the following steps:

> **NOTE**
> These backups are crucial for disaster recovery, troubleshooting, and system restoration.

Procedure

1. Backup HPE Aruba switch configuration.
2. Backup NVIDIA switch configuration.
3. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Subtopics

Backup HPE Aruba switch configuration

About this task

To save the startup configuration files, perform the following steps on the HPE Aruba 6300M OOBM switches:

Procedure

1. Retrieve the IP address and user credentials for HPE Aruba 6300M switches from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for `"role": "OOBM"` under `"infrastructure" > "racks" > "networkSwitches" > "networkConnections"` to retrieve the IP addresses for the HPE Aruba 6300M switches.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for `"type": "HPE Aruba 6300M"` under `"racks" > "networkSwitches" > "accessCredentials"` to retrieve the user credentials for the HPE Aruba 6300M switches.
2. Connect to one of the switches using the following steps:
   a. Enter **https://<switch management IP>** from the browser.
   b. Click OK on the pre-login banner and log in to the AOS-CX switch web UI using admin credentials.
3. Navigate to System > Config Mgmt from the left pane.
4. On the Config Mgmt page, under Checkpoints, select the startup-config entry from the Name column and click DOWNLOAD.
5. Log out from the switch.
6. Repeat the steps for all HPE Aruba switches.

Backup NVIDIA switch configuration

About this task

To save the startup configuration files, perform the following steps on the NVIDIA Cumulus switches:

Procedure

1. Retrieve the IP address and user credentials for both the NVIDIA switches from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for the `"role": "Compute"` and `"purpose": "Network Switch Management"` under `"infrastructure" > "racks" > "networkSwitches" > "networkConnections"` to retrieve the IP addresses for NVIDIA switches.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for the `"type": "HPE NVIDIA Switch SN4700M"` under `"racks" > "networkSwitches" > "accessCredentials"` to retrieve the user credentials for NVIDIA switches.
2. Open an SSH session and log in to the NVIDIA switch (SN4600cM or SN4700M) using switch IP address and cumulus credentials.
3. Save the current configuration to the **/etc/nvue.d/startup.yaml** file.

   ```
   nv config save
   ```
4. Create a copy of the **/etc/nvue.d/startup.yaml** file.

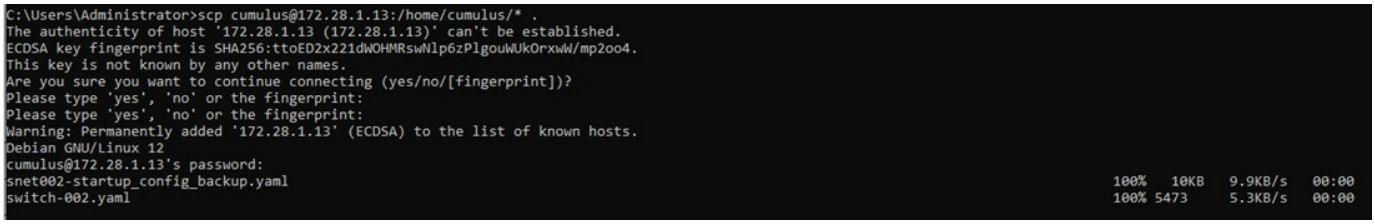
   ```
   sudo cp /etc/nvue.d/startup.yaml
   <switchname>
   _startup_config_backup.yaml
   ```
5. Change the permission on the file for SCP session.

   ```
   sudo chmod 644
   <switchname>
   _startup_config_backup.yaml
   ```

6. Navigate to the local directory where the files will be stored.
7. Initiate a SCP session to transfer the switch backup file from the switch to the local host.

   This process involves establishing a secure connection to the switch and downloading the backup file directly to the local host.

   ```
   scp cumulus@
   <switch mgmt IP>
   :/home/cumulus/* .
   ```

8. Repeat the steps for all NVIDIA switches.

Dismantle HPE GreenLake for File Storage cluster

Prerequisites

- Identify the CNode on which the cluster VMS is running.
- Identify the IP address of the CNode running the VMS using the following command:

  ```
  clush -g cnodes docker ps |grep vms
  ```

About this task

This section maps to the Manual-Dismantle_GLFS task under the Finish_And_Power_Down task group.

- **Description:** This manual task is used to dismantle the HPE GreenLake for File Storage cluster before shipping out the entire rack.
- **Manual Task:** To deactivate the HPE GreenLake for File Storage cluster, perform the following steps:

Procedure

1. Delete the tuiconfig and fileservice directories .
2. Deactivate the cluster . - 5 mins
3. Disable the leader. - 5 mins
4. Shut down the nodes . - 12 mins
5. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

   NOTE

   Ensure that you power down immediately to avoid logs filling up so plan accordingly.

Subtopics

Deleting the tuiconfig and fileservice directories

Procedure

1. Open an SSH session using VMS node IP address and log in to the VMS node (for example, master CNode) with username as `root` and password as `rootvastdata`.

   > **NOTE**
   >
   > You can find the VMP IP address in the Parameter list for configure_network.py script.

2. Verify the tuiconfig directory is present under the /vast/hpe directory.

   ```
   ls -lrth /vast/hpe/tuiconfig
   ```

3. Delete the tuiconfig directory.

   ```
   rm -rf /vast/hpe/tuiconfig
   ```

4. Delete the fileservice directory before shutting down the cluster.

   ```
   rm -rf /opt/sharedFolder/hpe/fileservice
   ```

Deactivating the cluster

About this task

To deactivate the cluster, perform one the following steps:

Procedure

1. Deactivate the existing cluster from CLI using the following command:

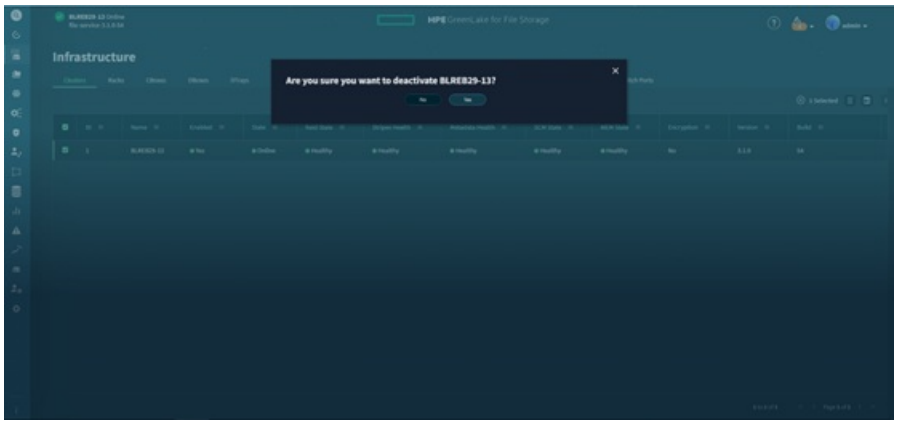
   ```
   cluster deactivate
   ```

2. Deactivate the cluster using the HPE GreenLake for File Storage UI

   a. On the HPE GreenLake for File Storage UI, navigate to Infrastructure > Cluster.

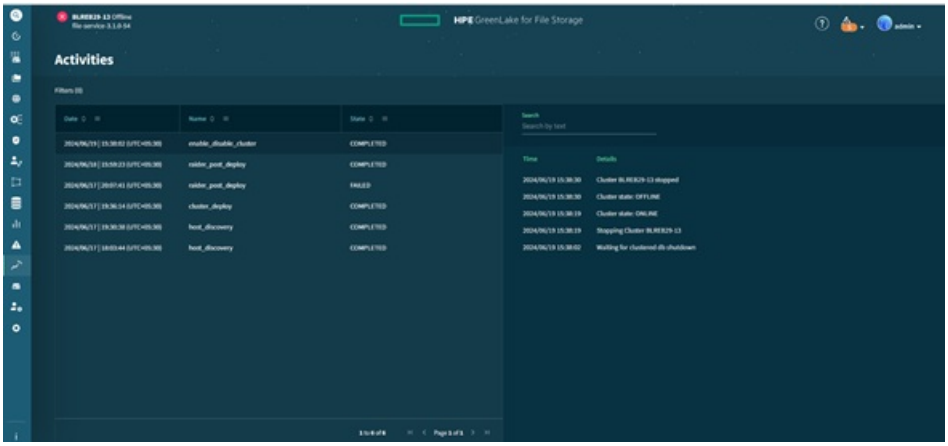
   b. Select Deactivate/Pause for the cluster you want to deactivate.

   c. Click Yes to confirm the deactivation.

   Wait for the entire cluster to deactivate on its own.

The Activities page is displayed with the status of the deactivated cluster.



> **NOTE**
>
> This process takes approximately 5 minutes to complete. Wait until this process is complete before proceeding

Disabling the leader

About this task

To disable the leader, perform the following steps:

Procedure

1. Log in to a CNode from the Linux shell as the `root` user.

   > **NOTE**
   >
   > Contact HPE Support to obtain the root password.

2. After logging in to a CNode as root, set the current user as the `vastdata` user using the following command before running any other command:

   ```
   su vastdata
   ```

3. Set the cluster control into maintenance mode to avoid any attempts for the leader to access the DNodes.
4. Disable leader election on all CNodes using the following command:

   ```
   clush -g cnodes 'touch /vast/data/DONT_RUN_LEADER'
   ```

5. Verify that the file is set on all CNodes.

   ```
   clush -g cnodes 'ls /vast/data/DONT_RUN_LEADER'
   ```

6. Verify the leader election before ending it.

   ```
   find-leader
   ```

7. End the leader process using the following command:

   ```
   vtool suicide
   ```

8. Verify that no new leader process is running using the following command:

```
find-leader
```

> **NOTE**
>
> This process takes approximately 5 minutes to complete. Wait until this process is complete before proceeding.

Example

```
BLREB29-13 root@Rack-CB1-U-bottom ~:$ su vastdata
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ clush -g cnodes 'touch
/vast/data/DONT_RUN_LEADER'
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ clush -g cnodes 'ls
/vast/data/DONT_RUN_LEADER'
172.16.128.2: /vast/data/DONT_RUN_LEADER
172.16.128.1: /vast/data/DONT_RUN_LEADER
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ find-leader
172.16.128.1
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ vtool suicide
<vapi.vmsg.rpc_client.Future object at 0x7f2cb3a976a0>
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ find-leader
```

Shutting down the nodes

Procedure

1. Retrieve the IP address and user credentials for CNodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the "ipAddress" field for "role": "Compute" and "$comment": "Cbox OS" under "infrastructure" > "racks" > "storageArrays" > "enclosures" > "nodes" > "networkConnections" to retrieve the CNode IP addresses.
   - In the **infra-layout.json** file, find the "userName" and "password" fields for "type": "S1F26A" and "target": "OS" under "racks" > "storageArrays" > "enclosures" > "nodes" > "accessCredentials" to retrieve the root credentials.
2. Log in to any CNode.

> **NOTE**
>
> Use the clush command to shut down the system at the Linux level. Hewlett Packard Enterprise recommends stopping the CNodes first followed by DNodes, after a few minutes later. This process avoids immediate shutdown and clush command failure.

3. Shut down all the nodes.
   a. Verify that the cluster is healthy, and all nodes are reachable.

```
clush -a hostname
```

> **NOTE**
>
> If the terminal is not healthy and causes shut down failure, Hewlett Packard Enterprise recommends logging out and logging in to the nodes.

Example:

```
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ clush -a hostname
172.16.128.2: Rack-CB1-U-top
172.16.128.1: Rack-CB1-U-bottom
172.16.128.101: Rack-DB1-U-top
172.16.128.100: Rack-DB1-U-bottom
```

b. Stop CNodes within the specified time.

```
clush -g cnodes 'sudo /usr/sbin/shutdown -h
<no. of minutes>
'
```

Example: Stop CNodes in two minutes using the following command:

```
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ clush -g cnodes 'sudo
/usr/sbin/shutdown -h +2'
172.16.128.1: Shutdown scheduled for Wed 2024-06-19 10:16:46 UTC, use
'shutdown -c' to cancel.
172.16.128.2: Shutdown scheduled for Wed 2024-06-19 10:18:00 UTC, use
'shutdown -c' to cancel.
```

c. Stop DNodes within the specified time.

```
clush -g dnodes 'sudo /usr/sbin/shutdown -h
<no. of minutes>
'
```

Example: Stop DNodes in five minutes using the following command:

```
BLREB29-13 vastdata@Rack-CB1-U-bottom ~:$ clush -g dnodes 'sudo
/usr/sbin/shutdown -h +5'
172.16.128.100: Shutdown scheduled for Wed 2024-06-19 10:16:46 UTC, use
'shutdown -c' to cancel.
172.16.128.101: Shutdown scheduled for Wed 2024-06-19 10:18:00 UTC, use
'shutdown -c' to cancel.
```

4. Ping the nodes over the management network to check if the nodes are offline.
5. After the cluster is deactivated, unplug the power manually in the following sequence:

> **NOTE**
>
> DBoxes continue to consume power even after the operating system is shut down.

a. Power down CNodes.

b. Power down DNodes.

c. Power down Switch A and Switch B.

> **NOTE**
>
> This process takes approximately 12 minutes to complete. Wait until this process is complete before proceeding.

Power down all components

About this task

This section maps to the Manual-Shutdown_and_PowerOff task under the Finish_And_Power_Down task group.

- **Description:** This manual task is used to shut down all the components before the engineered system is shipped to the customer datacenter.
- **Manual task:** To power down all the components, perform the following steps:

Procedure

1. Shut down HPE ProLiant DL380a Gen11 worker nodes.
2. Shut down HPE ProLiant DL325 Gen11 control nodes.
3. Shut down HPE Aruba and NVIDIA switches.
4. After completing these steps, mark the status of this task as Success to continue to the next task in the workflow.

Subtopics

Shutting down HPE ProLiant DL380a Gen11 worker nodes

About this task

> **NOTE**
> Powering down any of these components shuts down the engineered system.

To shut down the HPE ProLiant DL380a Gen11 worker nodes using iLO, perform the following steps:

Procedure

1. Retrieve the IP address and iLO user credentials for the worker nodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for all the servers starting from `"componentId": "server-004"` to the last `"componentId"` where `"purpose": "iLO Management"` under `"infrastructure" > "racks" > "servers" > "networkConnections"` to retrieve the iLO IP address for each worker node.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for all the servers starting from `"componentId": "server-004"` where `"type": "DL380a"` and `"target": "ILO"` under `"racks" > "servers" > "accessCredentials"` to retrieve the iLO user credentials for each worker node.
2. Connect to one of the worker nodes using the following steps:
   a. Enter **https://<iLO host name or IP address>** from the browser of the server that needs to be shut down.
   b. Log into the iLO web interface using Administrator credentials.
3. Click the Power icon from the toolbar on the top of the page and select Momentary Press.

   The worker node powers down.

4. Repeat the previous steps for all HPE ProLiant DL380a Gen11 servers.

Shutting down HPE ProLiant DL325 Gen11 control nodes

About this task

To shut down the HPE ProLiant DL325 Gen11 control nodes using iLO, perform the following steps:

Procedure

1. Retrieve the IP address and user credentials for the control nodes from the **base-configuration.json** and **infra-layout.json** SCID files.
   - In the **base-configuration.json** file, find the `"ipAddress"` field for the first three servers starting from `"componentId": "server-001"` to `"componentId": "server-003"` where `"purpose": "iLO Management"` under `"infrastructure" > "racks" > "servers" > "networkConnections"` to retrieve the IP address for each control node.
   - In the **infra-layout.json** file, find the `"userName"` and `"password"` fields for the first three servers where `"type": "DL325"` and `"target": "ILO"` under `"racks" > "servers" > "accessCredentials"` to retrieve the iLO user credentials for each control node.
2. Connect to one of the control nodes using the following steps:
   a. Enter **https://<iLO host name or IP address>** from the browser of the server that needs to be shut down.
   b. Log into the iLO web interface using Administrator credentials.
3. Click the Power icon from the toolbar on the top of the page and select Momentary Press.

   The control node powers down.
4. Repeat the previous steps for all HPE ProLiant DL325 Gen11 servers.

Shutting down HPE Aruba and NVIDIA switches

Procedure

Flip the breaker on the PDUs to shut down the HPE Aruba 6300M and NVIDIA switches (SN4600M or SN4700N).

Appendix A: Python scripts for configuring HPE GreenLake for File Storage

Subtopics

`switch_conf.py` script

Syntax

```
python3 switch_config.py aruba --mgmt-ips --mgmt-subnet --mgmt-gateway --ntp --
node-ports --isl-ports --
```

```
cluster-name --hostname --mtu
```

Description

This script can be run on any Linux client where Python 3 is installed to generate the configuration files for Switch-A and Switch-B that can be applied to the HPE GreenLake for File Storage switches.

Parameters

The following table specifies the locations of the field values from the **base-configuration.json** SCID file, which are required as the parameter values in the switch_config.py script command:

Parameter	Description	Values from the **base-configuration.json** SCID file
<mgmt-ips>	Management IP addresses	• Find the "ipAddress" field for the "role": "GLFS" and "purpose": "Network Switch Management" under "infrastructure" > "racks" > "storageArrays" > "networkSwitches" > "networkConnections" to retrieve the Switch-A and Switch-B IP addresses. • Add both the IP addresses as the value for the --mgmt-ips parameter, separated by comma.
<mgmt-subnet>	Management subnet mask	Enter the value as 24.
<mgmt-gateway>	Management Gateway IP	Find the "gatewayIpAddress" field for the "name": "Management Network" under "networks" to retrieve the value of the management gateway IP address.
<ntp>	NTP Server	Find the "ntpIpAddress" field for the "name": "Management Network" under "networks" > "specificAttributes" to retrieve the value of the NTP IP address.
<node-ports>	Port numbers in the node	Enter the value as 1-10.
<isl-ports>	ISL ports	Enter the value as 31,32.
<cluster-name>	Cluster name	Find the "clusterName" field under "infrastructure" > "racks" > "storageArrays" to retrieve the name of the cluster.
<hostname>	Hostname	Find the value of the "hostName" field for the "role": "GLFS" and "purpose": "Network Switch Management" under "infrastructure" > "racks" > "storageArrays" > "networkSwitches" to retrieve the Switch-A and Switch-B hostnames.
<mtu>	MTU version	Enter the value as 9198 for HPE Aruba.

Example input

```
$ python3 switch_config.py aruba --mgmt-ips 172.28.1.82,172.28.1.83 --
mgmt-subnet 24 --mgmt-gateway 172.28.1.1
--ntp 172.28.1.200 --node-ports 1-10 --isl-ports 31,32 --cluster-name
PCAI --hostname ArubaHost --mtu 9198
```

configure_network.py script

Syntax

```
sudo python3 /usr/bin/configure_network.py 1 --mgmt-vip --ext-ip --ext-gateway --ext-
dns --ext-netmask --
ntp --hostname --data-netmask --auto-ports-ext-iface outband --retain-ipv6 --skip-
sshd --auto-ports eth
```

Description

This script is used to assign a temporary management IP address to the CNode you are connected to, thus, allowing it to function as the management node on the HPE GreenLake for File Storage switches.

Parameters

The following table specifies the locations of the field values from the **base-configuration.json** SCID file, which are required as the parameter values in the configure_network.py script command:

Parameter	Description	Values from the **base-configuration.json** SCID file
<mgmt-vip>	VMS IP	Find the "ipAddress" field for the "$comment": " SW MGMT" under "infrastructure" > "racks" > "storageArrays" > "networkConnections" to retrieve the VMS IP address.
<ext-ip>	Node Management IP	Find the "ipAddress" field for "role": "Compute" and "$comment": "Cbox OS" under "infrastructure" > "racks" > "storageArrays" > "enclosures" > "nodes" > "networkConnections" to retrieve the CNode IP addresses.
<ext-gateway>	External Gateway IP	Find the "hpeIntegrationCenter" tree and retrieve the value of the "installationSystemIp" field.
<ext-dns>	External DNS IP	Find the "dnsIpAddress" field for "name": "Management Network" under "networks" > "specificAttributes" to retrieve the DNS IP address.
<ext-netmask>	External Netmask	Find the "networkMask" field for "name": "Management Network" under "networks" to retrieve the network mask.
<ntp>	NTP Server	Find the "ntpIpAddress" field for "name": "Management Network" under "networks" > "specificAttributes" to retrieve the NTP IP address.
<hostname>	Hostname	Enter the value as cnode1. The hostname is a temporary name, which is overwritten by EasyInstall.
<data-netmask>	Data network netmask	Use the fixed netmask of 255.255.192.0.

Example input

```
$ sudo python3 /usr/bin/configure_network.py 1 --mgmt-vip 172.28.1.81 -
-ext-ip 172.28.1.82 --ext-gateway
172.28.1.1 --ext-dns 10.10.22.30 --ext-netmask 255.255.255.0 --ntp
10.10.22.30 --hostname CNode1 --datanetmask
255.255.192.0 --auto-ports-ext-iface outband --retain-ipv6 --skip-sshd
--auto-ports eth
```

Websites

HPE Private Cloud AI websites

Log in to the Hewlett Packard Enterprise Support Center as an HPE Employee to access the internal documents.

HPE Private Cloud AI Documentation | Product Search

https://www.hpe.com/support/Private-Cloud-AI-Docs

HPE Private Cloud AI Documentation List

https://www.hpe.com/support/Private-Cloud-AI-Doc-List

HPE Private Cloud AI customer documentation

HPE Private Cloud AI Administration Guide

https://www.hpe.com/support/PCAIAdminGuide

HPE Private Cloud AI Release Notes

https://www.hpe.com/support/PCAIReleaseNotes

HPE AI Essentials Software Documentation

https://www.hpe.com/support/AIEDocs

HPE Private Cloud AI QuickSpecs

https://www.hpe.com/support/PCAIQuickSpecs

Storage websites

NVIDIA Network Hardware Compatibility List (HCL)

https://www.nvidia.com/en-us/networking/ethernet-switching/hardware-compatibility-list/

HPE Smart CID portal

https://smartcid.itcs.hpe.com/xFrameworkCIDRestAPI/index-new.html

Subtopics

Documentation feedback

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.