HPE ProLiant for Microsoft Azure Stack Hub Solution Update Bundle Installation Guide

Part Number:
Z7550-97929
Published: July 2022
Edition: 1

HPE ProLiant for Microsoft Azure Stack Hub Solution Update Bundle Installation Guide

4.1.2

Abstract

Information and instructions for installing the Solution Update Bundle to the HPE ProLiant for Microsoft Azure Stack Hub solution.

Part Number: Z7550-97929
Published: July 2022
Edition: 1

© Copyright 2022 Hewlett Packard Enterprise Development LP

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Azure, Azure Stack, Azure Stack Hub, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

CISCO® is a registered trademark of Cisco Systems, Inc. in the U.S. or certain other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Table of contents

HPE solution update bundle overview (4.1.2) 5
Installation instructions 7
Update process 7
Verifying system health 7
Checking Azure Stack Hub admin portal accessibility from the HLH 11
Step 1: Schedule a maintenance window (if applicable) 12
Step 2: Download and extract the update bundle 13
Step 3: Update Azure Stack Hub software (if appropriate) 14
Step 4: Execute Start-UpdateBundle.cmd 14
Update Bundle Compliance Precheck 19
Recovering from installer failures 21
Step 5: Update HPE OneView user role to infrastructure administrator (if appropriate) 23
Step 6: Install OEM package 25
Step 7: HLH OS updates 27
Migrating the HLH OS from Microsoft Windows 2016 to Microsoft Windows 2019 29
Migration Process Overview 29
Migrating from Microsoft Windows 2016 to Microsoft Windows 2019 30
Migration process 31
Running Start-UpdateBundle.cmd 32
SkipOemPackageUpload parameter 36
Mounting the iso file 37
Manually mounting ISO on iLO Virtual Media of the HLH 38
Reboot the HLH 41
Installing Windows 2019 42
Importing AzureStack Hub certificates into the HLH 46
Creating an additional backup of HLH files 47
Manually restoring files after installing Windows 2019 48
Clearing stale/errored custom SPPs from the HPE OneView appliance 48
Known issues 50
OEM installation may fail during "Firmware Update" stage 50
Start-UpdateBundle.cmd occasionally fails in rerun scenarios 53
Start-postOSUpgrade.ps1 occasionally fails in rerun scenarios 53
The restored user account is disabled during postOSUpgrade 54
Start-UpdateBundle.cmd fails to initiate Start-UpdateBundle.ps1 after CDS 54

Software version of "Identifiers for Intel Xeon Scalable Processors (First and Second Generation) for Windows" doesn't match expected versions on HLH from TestHPENodes report 55
Enhancements and fixed issues 55
Additional resources and helpful links 56
Support and other resources 56
Accessing Hewlett Packard Enterprise Support 56
Accessing updates 57
Remote support 58
Customer self repair 59
Warranty information 59
Regulatory information 59
Documentation feedback 60

HPE solution update bundle overview (4.1.2)

Introduction

This document outlines the contents and specific installation procedures for an HPE solution update bundle.

HPE solution update bundles are released for HPE ProLiant for Microsoft Azure Stack Hub to coincide with Microsoft-provided Azure Stack Hub updates as discussed at **https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-updates**.

Each released HPE solution update bundle provides a single bundle of updates, for the HPE portion of the solution, that are installed using the Hardware Lifecycle Host (HLH). HPE solution update bundles typically include one or more of the following:

- Firmware and driver updates for the Azure Stack Hub nodes delivered by either the custom Service Pack for ProLiant or the Microsoft Azure Stack Hub OEM update bundles
- Firmware and driver updates for the HLH management node
- New HPE solution management tools and fixes
- New solution supported third-party tools in the `C:\hpe\third-party` folder
- HPE OneView Updates
- Security fixes
- Windows 2019 OS (for migrations only)

The primary method for installing the update bundle is to download and install the bundle onto the HLH. For details on the general process for downloading and installing the HPE solution update bundle, see the “HPE solution update bundle” section of the **HPE ProLiant for Microsoft Azure Stack Hub User Guide**.



IMPORTANT:

OEM extension bundle installation may involve automated **node maintenance actions such as draining and resuming nodes** similar to what Microsoft describes as "Full" update packages at **https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-updates#plan-for-updates**. Hewlett Packard Enterprise recommends following the Microsoft guidance for scheduling a maintenance window to account for the potential impact to tenant workloads resulting from those actions.

Applicability

The 4.1.2 Update Bundle is applicable for Microsoft Azure Stack Hub solutions with HLH version 3.23.0.13, 4.0.0.53, 4.0.1.1, and 4.1.0.18.

Dependencies and expected update duration

The following table contains an overview of the timeline for installing this HPE solution update bundle, as well as details on any dependencies that must be considered before installing the bundle. This information is provided to help estimate the overall effort and duration involved in the update process for scheduling purposes.

Table 1: HPE solution update bundle overview table

HPE solution update bundle version	**4.1.2**
Co-ordinate Azure Stack Hub update details (if any)	To find supported Azure Stack Hub versions, see the Installation Instructions tab in the HPE Support Portal. **NOTE:** To check the current Azure Stack Hub stamp version, refer to the version displayed on the "Update" tile in the dashboard of the admin portal.
Azure Stack Hub tenant workloads and portal downtime expected	Tenant workloads are potentially impacted.
Estimated duration to install HPE solution update bundle	**Expected automated step duration** (using `StartUpdateBundle.cmd`): • ~ 4 hours on the HLH **Expected automated step duration** (using `StartUpdateBundle.cmd` for migration): • ~ 1.5 hours for operations before Windows 2019 OS install • ~ 2 hours for OS install • ~ 6-7 hours for operations after Windows 2019 OS install **Expected OEM Bundle and SPP installation on nodes (using OEM orchestration)**: • ~ 5 hours for 4-node systems

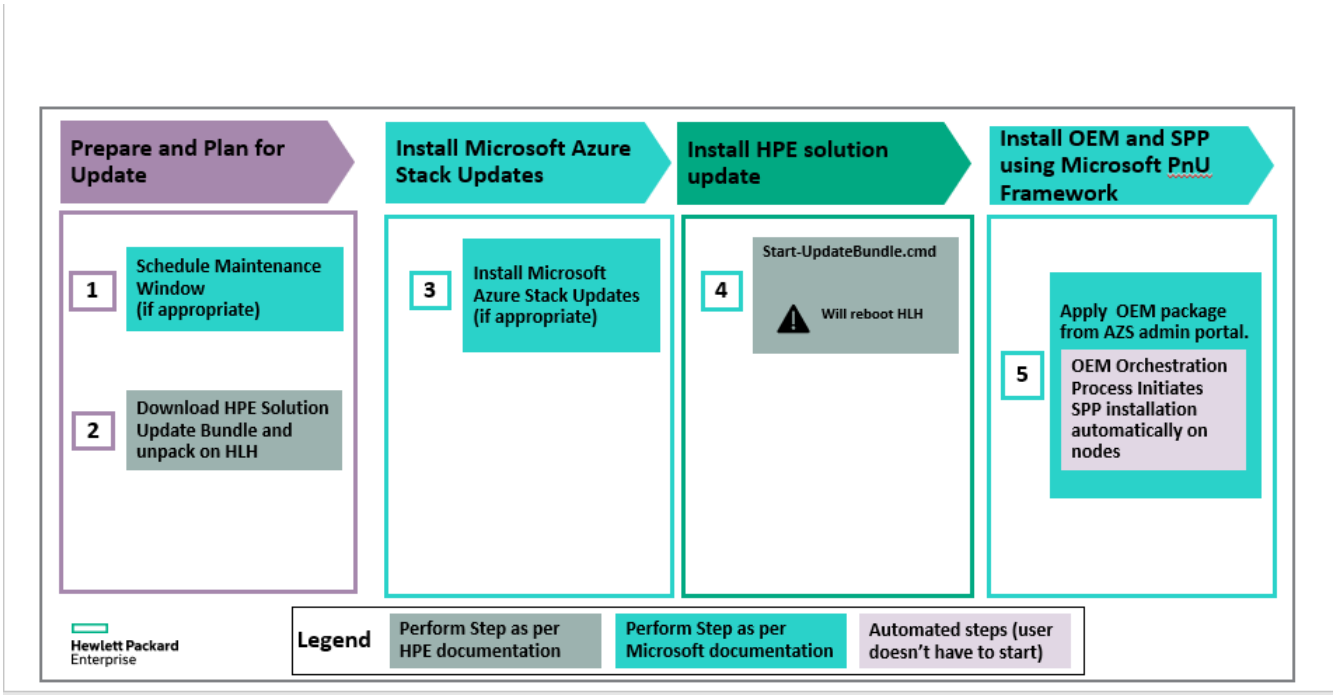
Installation instructions

Update process

Please read these instructions in their entirety before starting the update.

The overall solution update process for this update bundle is outlined in Figure 1.

Figure 1: Planning and installing combined updates from Microsoft and HPE for HPE ProLiant for Microsoft Azure Stack Hub



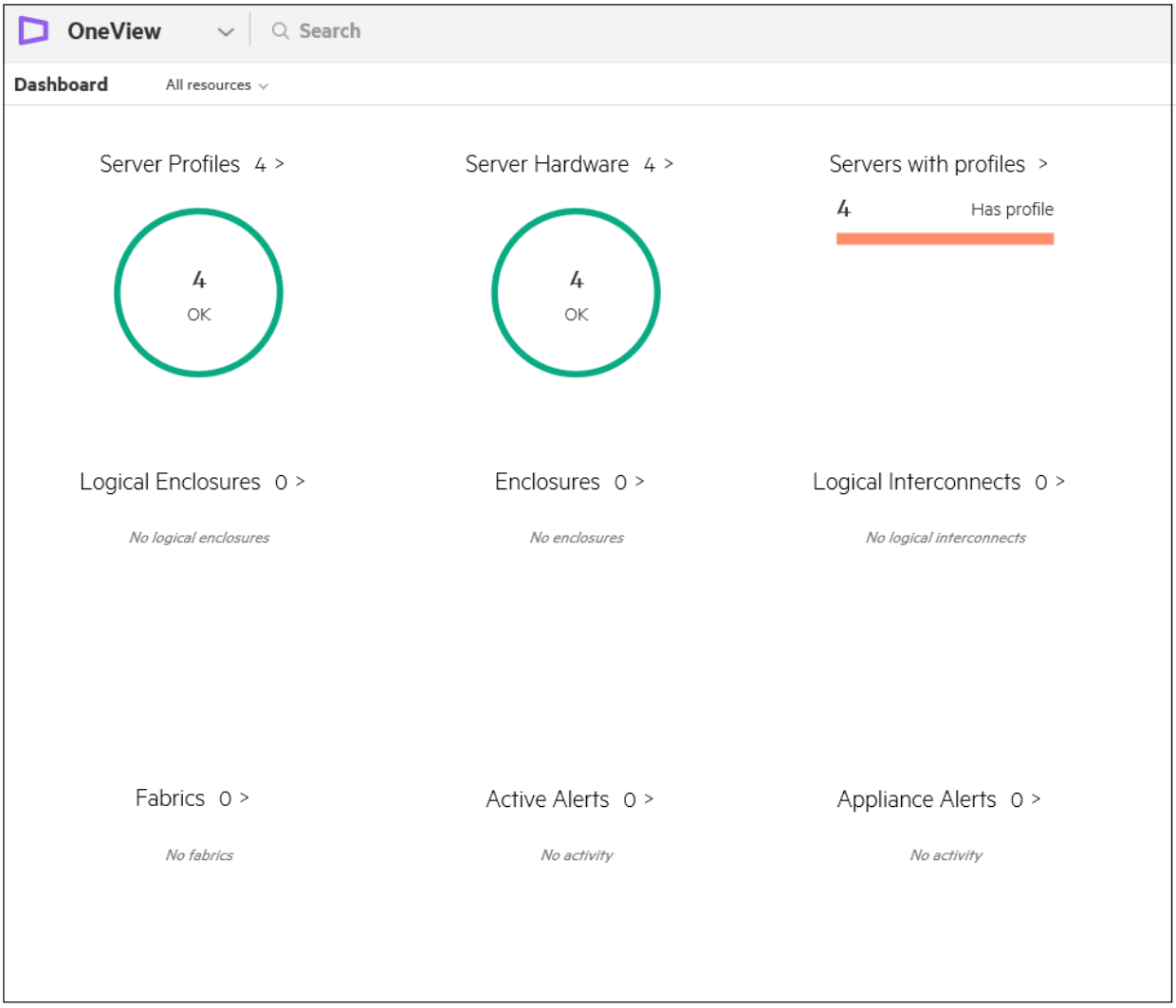
Verifying system health

Before attempting to update the HPE ProLiant for Microsoft Azure Stack Hub solution, verify the health of the system.

Procedure

1. Verify the health of the system from HPE OneView.
   a. Log in to HPE OneView.
   b. From the dropdown next to the HPE OneView icon at the top of the window, click **Dashboard**.
   c. Verify that the primary circles for **Server Profiles** and **Server Hardware** are green and there are no critical **Active Alerts**.

> **NOTE:**
> Because the HLH is not managed by HPE OneView, **Servers with profiles** will indicate one server without a profile.



d. If there are any alerts, click the **Active Alerts** on the Dashboard to find information about the alerts.

   You can also click **Activity** in the dropdown menu next to the **OneView** icon at the top of the window.

e. On the Activity page, filter alerts by **Status** as "Critical" and **State** as "Active" and "Locked".



f. If there are any active or locked alerts, they must be resolved prior to performing the update. Click on each alert to see the recommended action, and work with HPE support to resolve the alert.

> **WARNING:**
>
> Recommended actions for resolving alerts in HPE OneView may in some cases recommend steps, such as re-applying a profile or repairing hardware, that require a server to be shut down. Because Azure Stack Hub only supports one node being down, only one node should be repaired at a time.

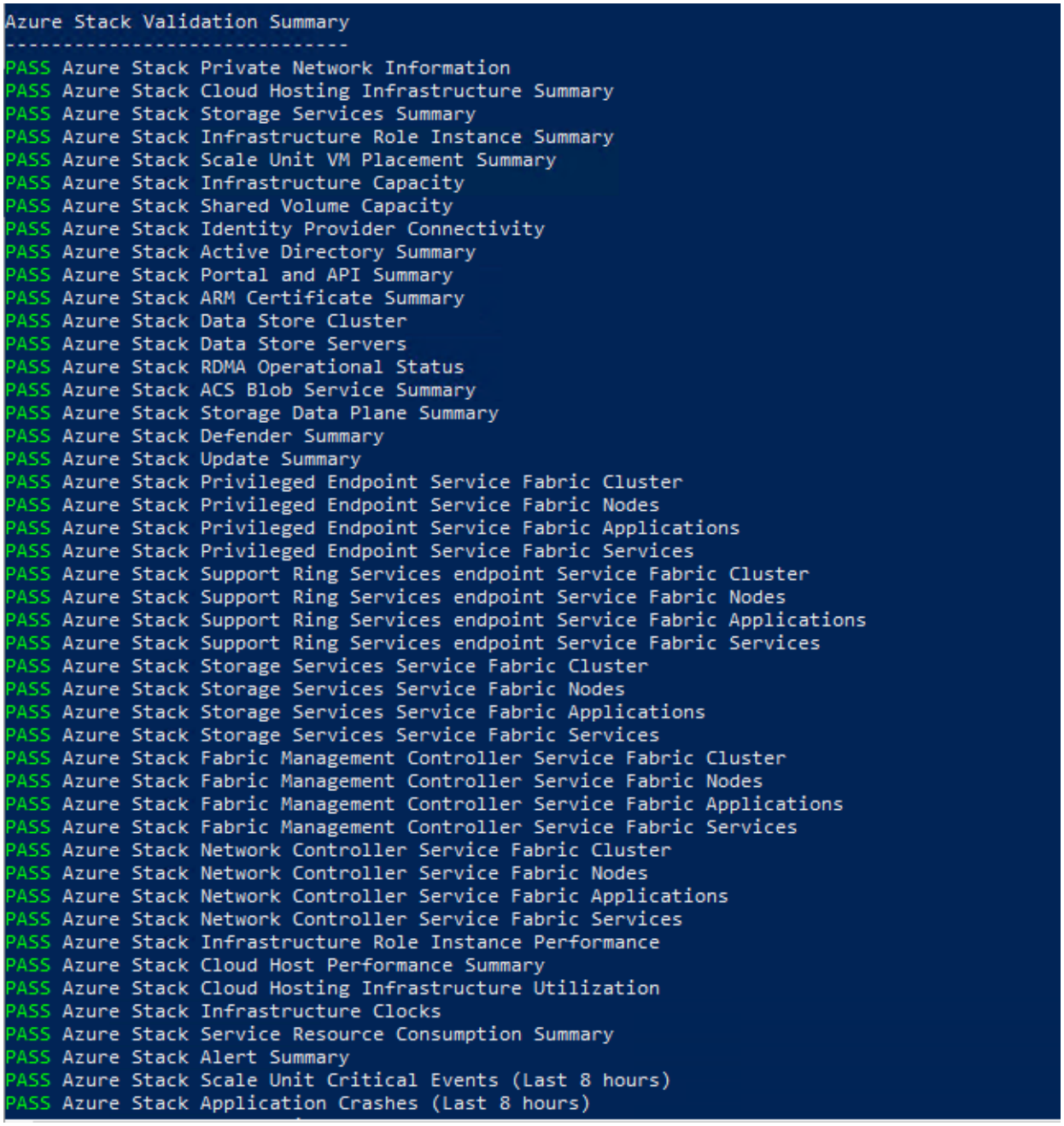
   See **https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-replace-node** for details on node repair actions and contact HPE support for assistance.

2. Test the Azure Stack Hub stamp health from the privileged endpoint (PEP) session.

   a. Access the PEP at **https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-privileged-endpoint#access-the-privileged-endpoint**.

   b. Execute the `Test-AzureStack` command.

   c. Verify that the Azure Stack Validation summary has all green "PASS" indicators.



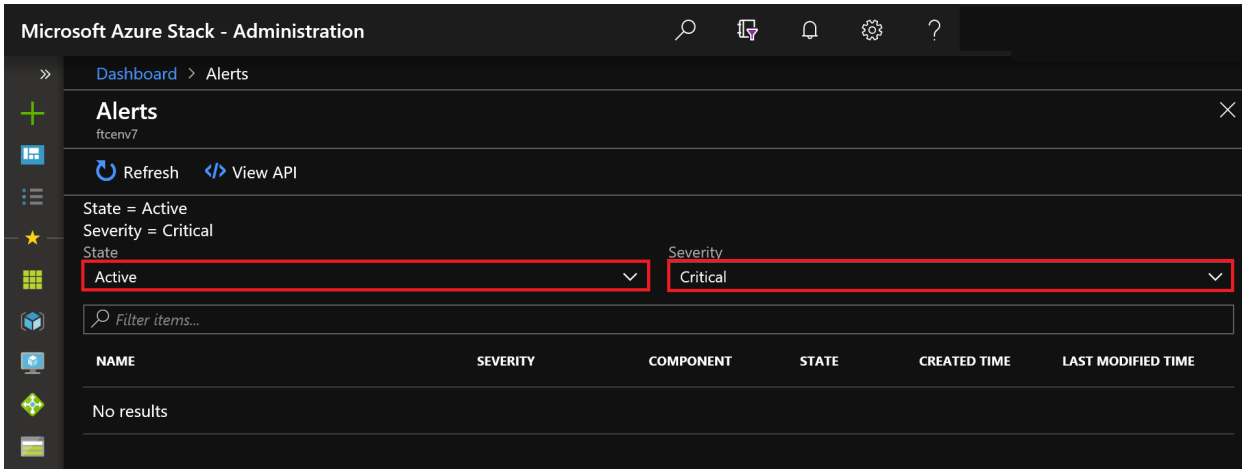
d. If there are any test failures, address each issue appropriately before continuing.

3. Check the Azure Stack stamp health from the Admin portal.

   a. Log in to the AZS Admin portal.

   b. On the Dashboard, click **Alerts**.

   c. Filter the alerts with **State** as "Active" and **Severity** as "Critical".



IMPORTANT:

If there are any Critical or Active alerts on the system, address each issue appropriately before continuing.

Checking Azure Stack Hub admin portal accessibility from the HLH

Since the update bundle workflow uploads the OEM package to Azure Stack Hub, the Azure Stack Hub admin portal must be accessible from the HLH. Before starting the installation of the update bundle, HPE recommends using the Internet Explorer browser to ensure that the Azure Stack Hub admin portal UI is accessible from the HLH. Use the procedure below to access the Azure Stack Hub admin portal from the HLH.

Procedure

To access the Azure Stack Hub admin portal from the HLH:

1. Make sure that a correct DNS server has been set.

   The server has DNS configurations with relevant delegations and rules that forward to the appropriate upstream DNS server that resolves the Azure Stack Hub admin portal URL.

2. Import Azure Stack Hub certificates into the HLH.

   See Importing Azure Stack Hub certificates into the HLH.

3. Add the following URLs to the IE browser trusted sites list on the HLH.

   - https//*.<*ExternalDomainFQDN* from `ConfigurationData.json`>

- https://*.microsoft.com
- https://login.live.com
- https://logincdn.msauth.net

Also, add all trusted URLs that display while trying to access the Azure Stack Hub admin portal from HLH.

Because the IE enhanced security configuration will probably be enabled on the HLH, this will display Azure Stack Hub admin portal UI properly.

In the case of ADFS mode of deployment, add following URLs to the HLH trusted sites.

- https://*.<*CustomDomainName*>
- about:blob

4. Enable JavaScript in Internet Explorer.
5. Disable security settings when connecting through Remote Desktop.

   For more information, see the Microsoft documentation: **https://docs.microsoft.com/en-us/azure-stack/user/azure-stack-connect-azure-stack?view=azs-2102**

Step 1: Schedule a maintenance window (if applicable)

In some cases, HPE solution update bundles will only impact the HLH node and thus, not impact tenant workloads directly. Review the details in the Table 1: HPE solution update bundle overview table for the given HPE solution update bundle to determine if any impact to tenant workloads is expected. If the Table 1: HPE solution update bundle overview table indicates that tenant workload impact is expected or associated Azure Stack Hub software updates are also planned, Hewlett Packard Enterprise recommends notifying users and scheduling a planned maintenance window for the update. See Step 3: Update Azure Stack Hub software (if appropriate) for guidance on installing Azure Stack Hub software updates.

IMPORTANT:

Before starting the update process, Hewlett Packard Enterprise recommends recording the BitLocker recovery key as a precaution. The key can be found using this command at an elevated CMD or PowerShell prompt:

```
manage-bde -protectors -get c:
```

Record the numerical password ID and password value for future reference.

Step 2: Download and extract the update bundle

Prerequisites

Download the HPE solution update bundle from **My HPE Software Center**. Be sure to select the correct bundle as listed in Table 1: HPE solution update bundle overview table. To extract the files for updating the HPE components of the solution, perform the following steps:

Procedure

1. Transfer the update bundle zip file to the Hardware Lifecycle Host (HLH).

   For connected environments, simply download the bundle using Internet Explorer on the HLH. For disconnected environments, the transfer can be accomplished by one of the following:

   - Mount an SMBv3 file share containing the file.

     a. Download the bundle to a host computer that is network accessible to the HLH.

     b. Create a file share on the host computer that is accessible from the HLH.

     > **NOTE:**
     >
     > HLH firewall rules may block access. You may need to revise the firewall rules to grant access or temporarily disable the HLH firewall for transfer purposes only.

   - Insert a USB storage device into the HLH and transfer the file.

2. Extract all files from the update bundle zip file on the HLH.

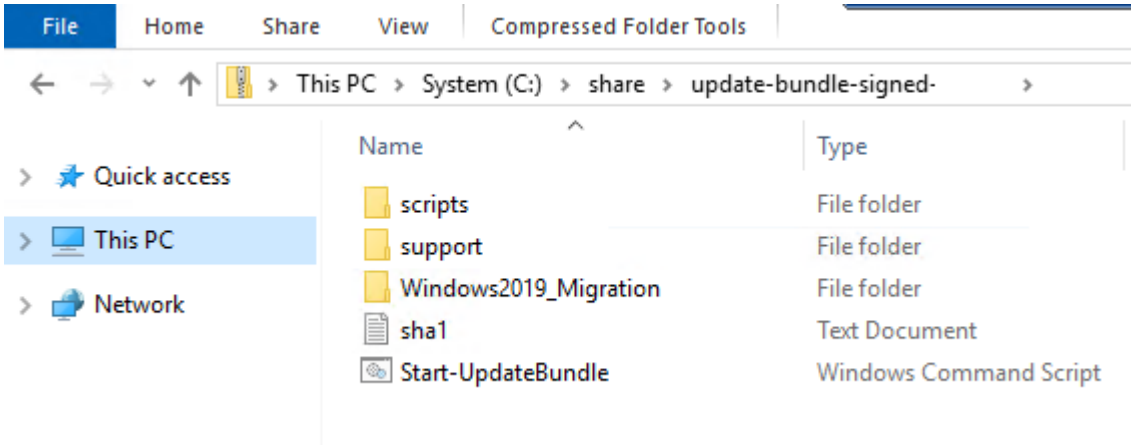
   a. Open File Explorer to the location of the zip file.

   b. Right-click the zip file and select **Extract all...**.

   c. In the extract dialog box, enter any convenient, new path and click **Extract**.

   Example: `C:\Users\Administrator\Desktop\update-bundle-4.1.2.x`

   Extraction will begin and a progress box will display. The following screenshot shows the folder structure after extraction.



Step 3: Update Azure Stack Hub software (if appropriate)

Hewlett Packard Enterprise recommends having a combined maintenance plan for updating the Microsoft Azure Stack Hub software and for installing HPE Solution update bundles. Review the Azure Stack Hub release notes and the to determine if it is appropriate to also update the Azure Stack Hub software. If no Azure Stack Hub software update is needed, proceed to Step 4: Execute Start-UpdateBundle.cmd.

Step 4: Execute Start-UpdateBundle.cmd

The `Start-UpdateBundle.cmd` script initiates the update bundle installation process. On executing `Start-UpdateBundle.cmd`, the update bundle installation continues with a PowerShell credentials window to enter OneView and Azure Stack Hub admin portal login credentials. This launches update bundle installation wizard.

Before running `Start-UpdateBundle.cmd`, close all third-party applications.

WARNING:

`Start-UpdateBundle.cmd` disables the Device Guard and reboots the HLH. Be sure that you have saved any work before executing `Start-UpdateBundle.cmd`.

NOTE:

To ensure ability to monitor the server as it reboots, Hewlett Packard Enterprise recommends using the HLH iLO Remote Console or a crash cart connected to the HLH to perform the following steps.

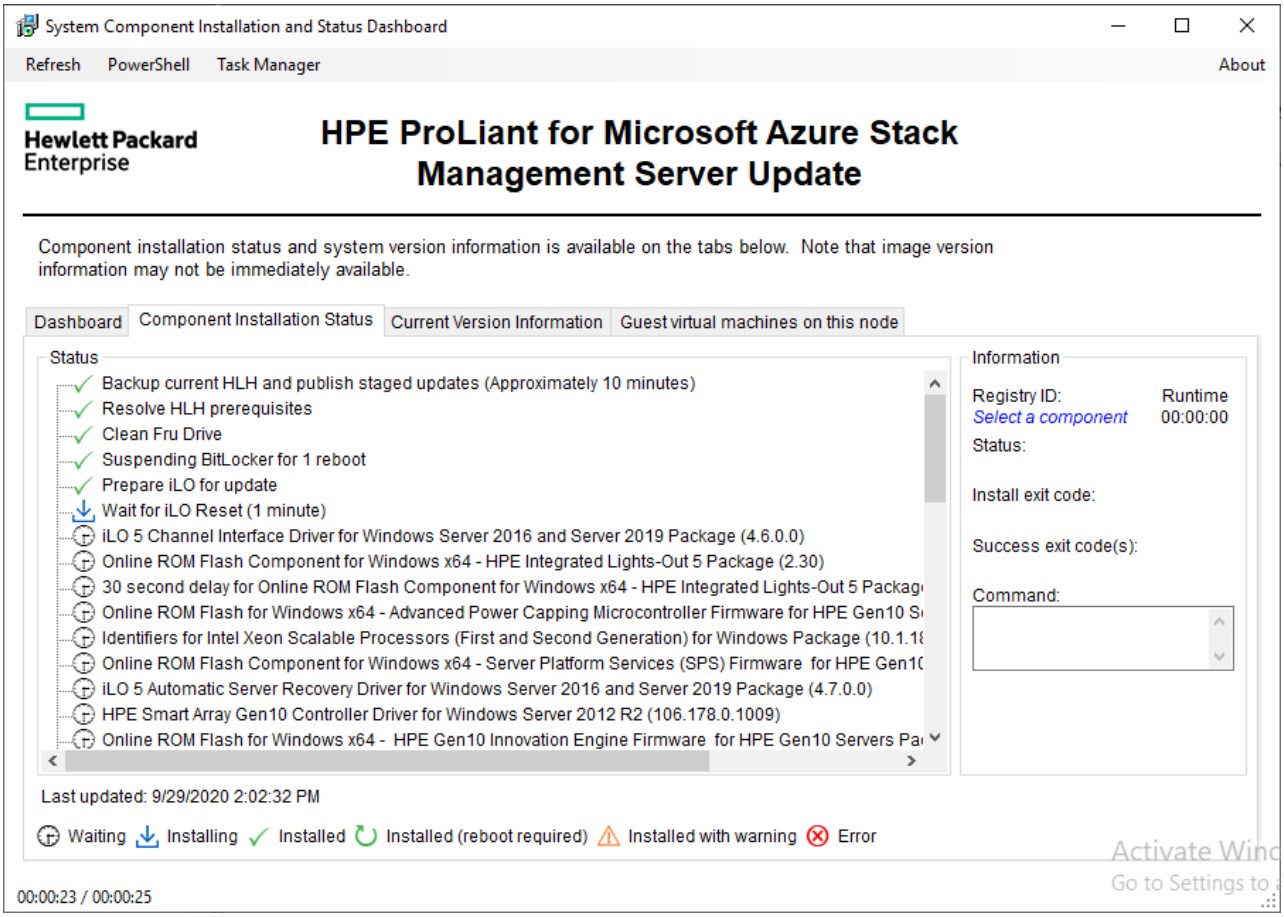
Procedure

1. Navigate to the extracted folder and double-click the `Start-UpdateBundle.cmd` file.
2. In the **User Account Control** pop-up window, select **Yes** to continue the update bundle installation.
3. Enter your HPE OneView credentials when prompted.
4. Enter the login credentials in the webpage credentials pop-up window for the Azure Stack Hub admin portal.

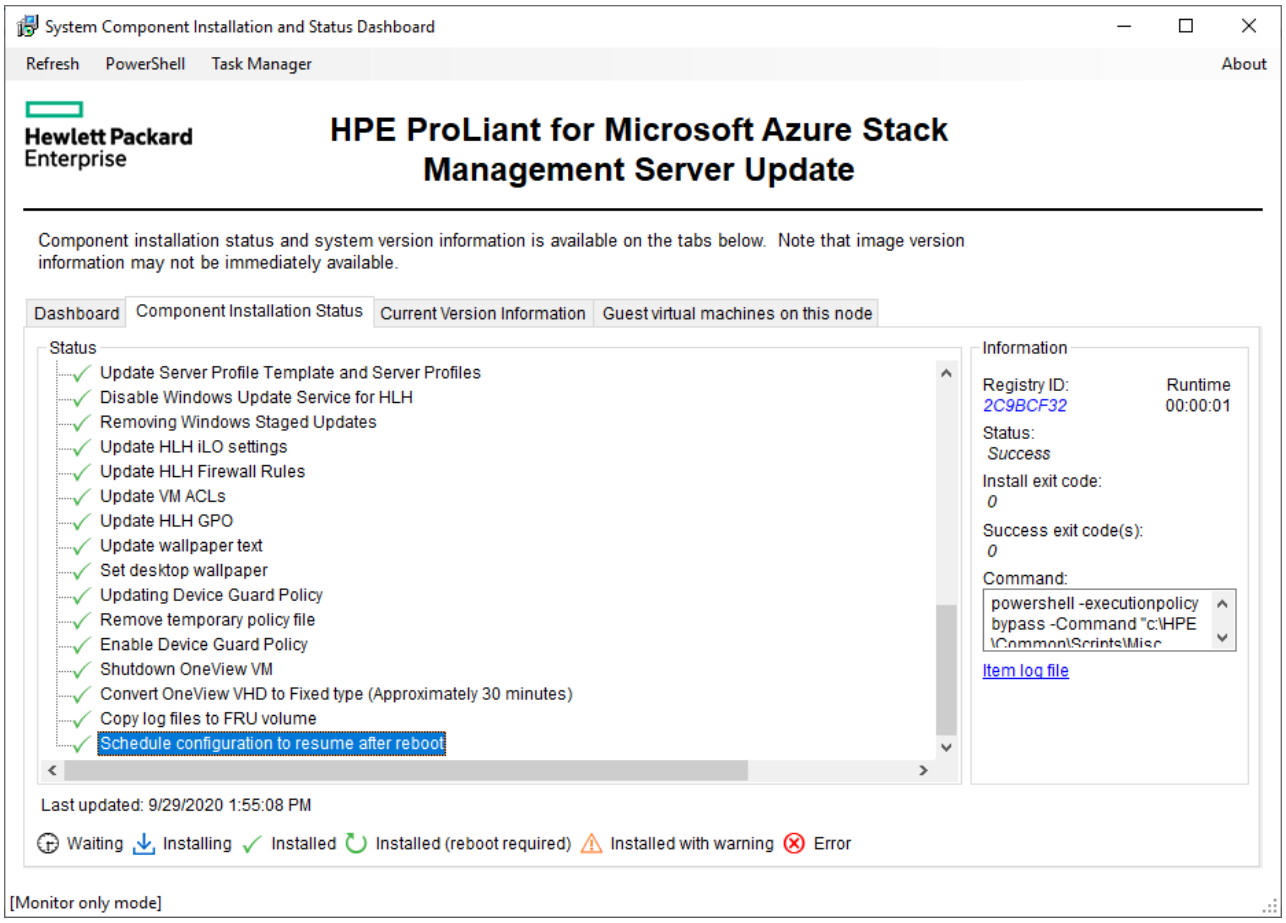
   After validating the provided HPE OneView and Azure Stack Hub admin portal login credentials, the script launches the update bundle installer window.
5. The progress of the update bundle installation can be monitored using the update bundle installer Dashboard.

   Each step executed by the installer will have a status icon. To map the icon with the status, use the legend at the bottom of the window. You can also check the log that is generated from each script by clicking the item log link on the right side of the window. When the status of the last step or action has a green checkmark, the script is complete.

   The following example illustrates an update of a Gen10 HLH that is still in progress.


System Component Installation and Status Dashboard
Refresh
PowerShell
Task Manager
About
Hewlett Packard Enterprise
HPE ProLiant for Microsoft Azure Stack Management Server Update
Component installation status and system version information is available on the tabs below. Note that image version information may not be immediately available.
Dashboard
Component Installation Status
Current Version Information
Guest virtual machines on this node
Status
Backup current HLH and publish staged updates (Approximately 10 minutes)
Resolve HLH prerequisites
Clean Fru Drive
Suspending BitLocker for 1 reboot
Prepare iLO for update
Wait for iLO Reset (1 minute)
iLO 5 Channel Interface Driver for Windows Server 2016 and Server 2019 Package (4.6.0.0)
Online ROM Flash Component for Windows x64 - HPE Integrated Lights-Out 5 Package (2.30)
30 second delay for Online ROM Flash Component for Windows x64 - HPE Integrated Lights-Out 5 Packag
Online ROM Flash for Windows x64 - Advanced Power Capping Microcontroller Firmware for HPE Gen10 S
Identifiers for Intel Xeon Scalable Processors (First and Second Generation) for Windows Package (10.1.18
Online ROM Flash Component for Windows x64 - Server Platform Services (SPS) Firmware for HPE Gen10
iLO 5 Automatic Server Recovery Driver for Windows Server 2016 and Server 2019 Package (4.7.0.0)
HPE Smart Array Gen10 Controller Driver for Windows Server 2012 R2 (106.178.0.1009)
Online ROM Flash for Windows x64 - HPE Gen10 Innovation Engine Firmware for HPE Gen10 Servers Pa
Information
Registry ID:
Runtime
Select a component
00:00:00
Status:
Install exit code:
Success exit code(s):
Command:
Last updated: 9/29/2020 2:02:32 PM
Waiting
Installing
Installed
Installed (reboot required)
Installed with warning
Error
Activate Windows
Go to Settings to
00:00:23 / 00:00:25

The following example illustrates a completed Gen10 HLH update.



NOTE:

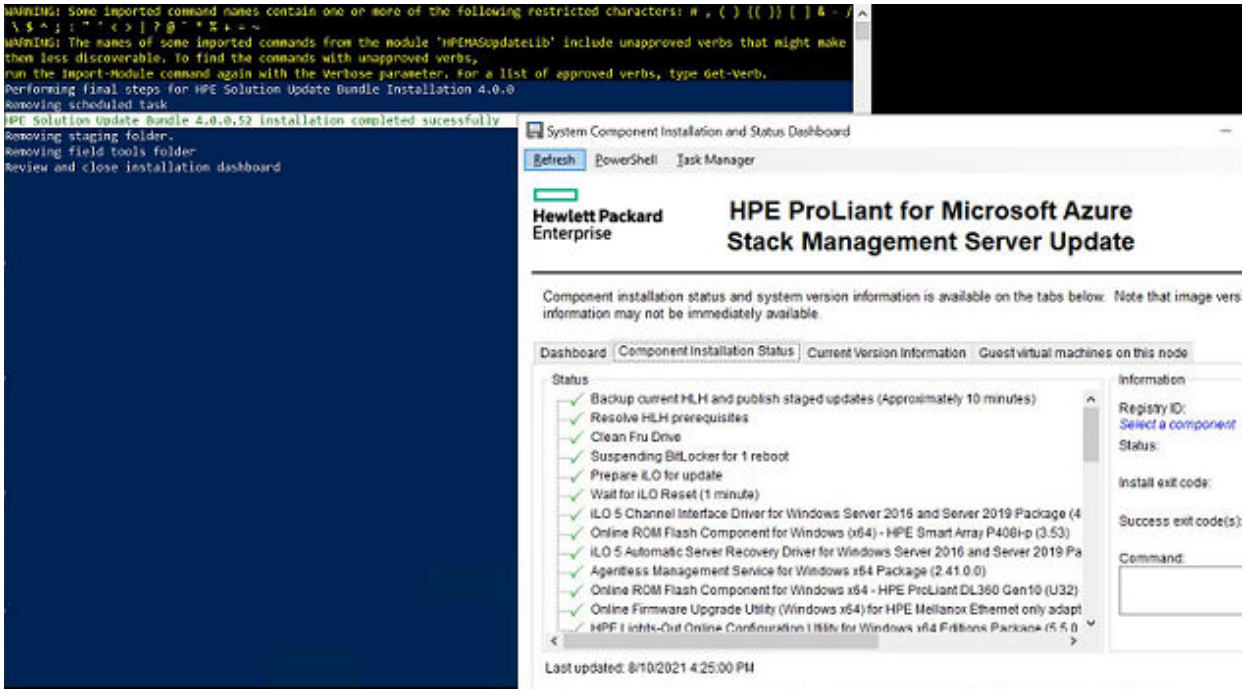
You can view the log output for individual steps by selecting a step in the installer window and clicking the item log file link on the right side of the window. Alternatively, all log files can be browsed at `C:\hpe\logs\`.

6. For changes to take effect, the update bundle installation gracefully shuts down HPE OneView and reboots the HLH.

7. Confirm that the update bundle was installed successfully.

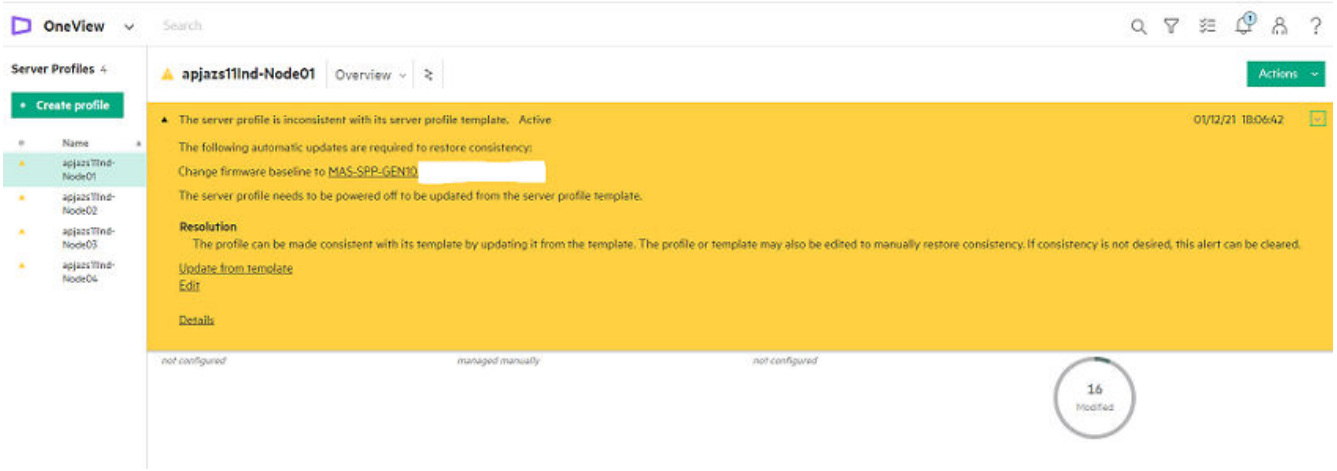
   a. Log in to the HLH after the reboot.

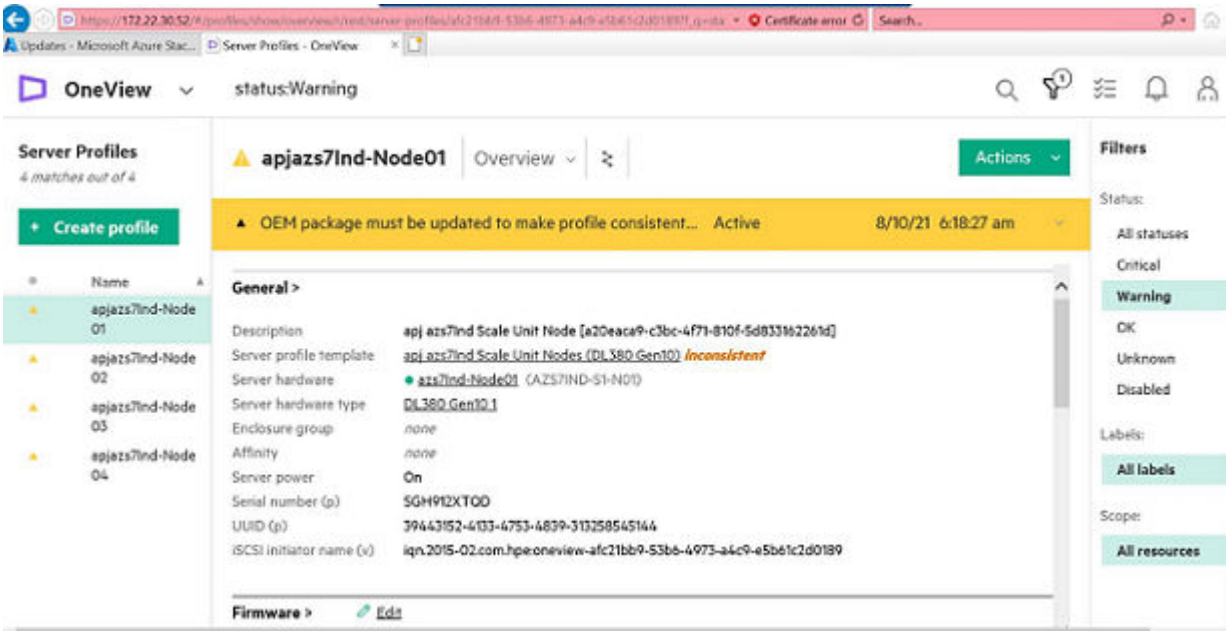
   b. A message indicating a successful installation should display in a PowerShell window and the installer will be opened. Review the installation steps and close the installer.



c. Press **Enter** to exit the PowerShell session.

As part of the update bundle installation, a new SPP included in the update bundle is uploaded into HPE OneView, and the server profile template associated with Azure Stack Hub nodes will be updated to use the new SPP. When logging into HPE OneView, you will see the following warnings:





IMPORTANT:

Do NOT attempt to resolve the inconsistent profile warning to make the MAS Hub node server profiles consistent with the server profile template. The inconsistency will be resolved automatically as part of the OEM package installation using the new firmware orchestration feature built into the OEM package.

Update Bundle Compliance Precheck

The update bundle installation procedure will automatically execute the compliance check as a part of update bundle precheck before installation.

The update bundle/migration process will not proceed if Windows is not activated on the HLH.

As a part of the compliance check, the below components will be verified and if they are not compliant, the update bundle installation will abort with an associated error message.

- Installed version of HLH and Microsoft Azure Stack hub is not supported.
- 30Gb of required free space is not available on the C: drive and V: drive.
- BIOS settings on the HLH and Microsoft Azure Stack Hub servers are not compliant as per HPE standards.
- iLO settings on the HLH and Microsoft Azure Stack Hub servers are not compliant as per HPE standards.

- The environment is a fresh deployment and `Complete-DeploymentService` is not run.

> **NOTE:**
> A known issue exists while restating Start-UpdateBundle.cmd after CDS.
> See Start-UpdateBundle.cmd fails to initiate Start-UpdateBundle.ps1 after CDS.

If there are discrepancies in the compliance check process, it prompts the user for confirmation to proceed with or abort the update bundle installation.

HPE recommends resolving the discrepancies and re-running `Start-UpdateBundle.cmd`. Contact HPE support for assistance.

Changing the BIOS settings:

1. List the non-compliant bios settings and it's expected values from the PowerShell output or from `V:\component-status\UpdateBundle-Precheck-4.1.2.XX\PreUpdateBundle-validationError.html`

   .

2. Suspend BitLocker

   a. Open PowerShell as an Administrator.

   b. Execute the `Suspend-BitLocker -MountPoint C: -RebootCount 1` command.

3. Reboot HLH.

For more information on changing the required BIOS settings, see "BIOS/Platform Configuration (RBSU)" in the "**UEFI System Utilities User Guide for HPE ProLiant Gen9 Servers**.

Example:

If Start-UpdateBundle.cmd fails with an error message, such as:

“`10.31.29.2 HLH.bios.AsrStatus Node value differs (Expected: '"Enabled"' / Current: '"Disabled"')`“

This means that the ASR (Automatic Server Recovery) setting on the HLH is expected to be in “Enabled” state. However, it is disabled. To fix this issue, use the following procedure:

1. Suspend Bit locker.
2. Reboot HLH.
3. From the System Utilities screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Availability** > **ASR Status**, and press **Enter** (See the **UEFI System Utilities User Guide for HPE ProLiant Gen9 Servers** for other settings).

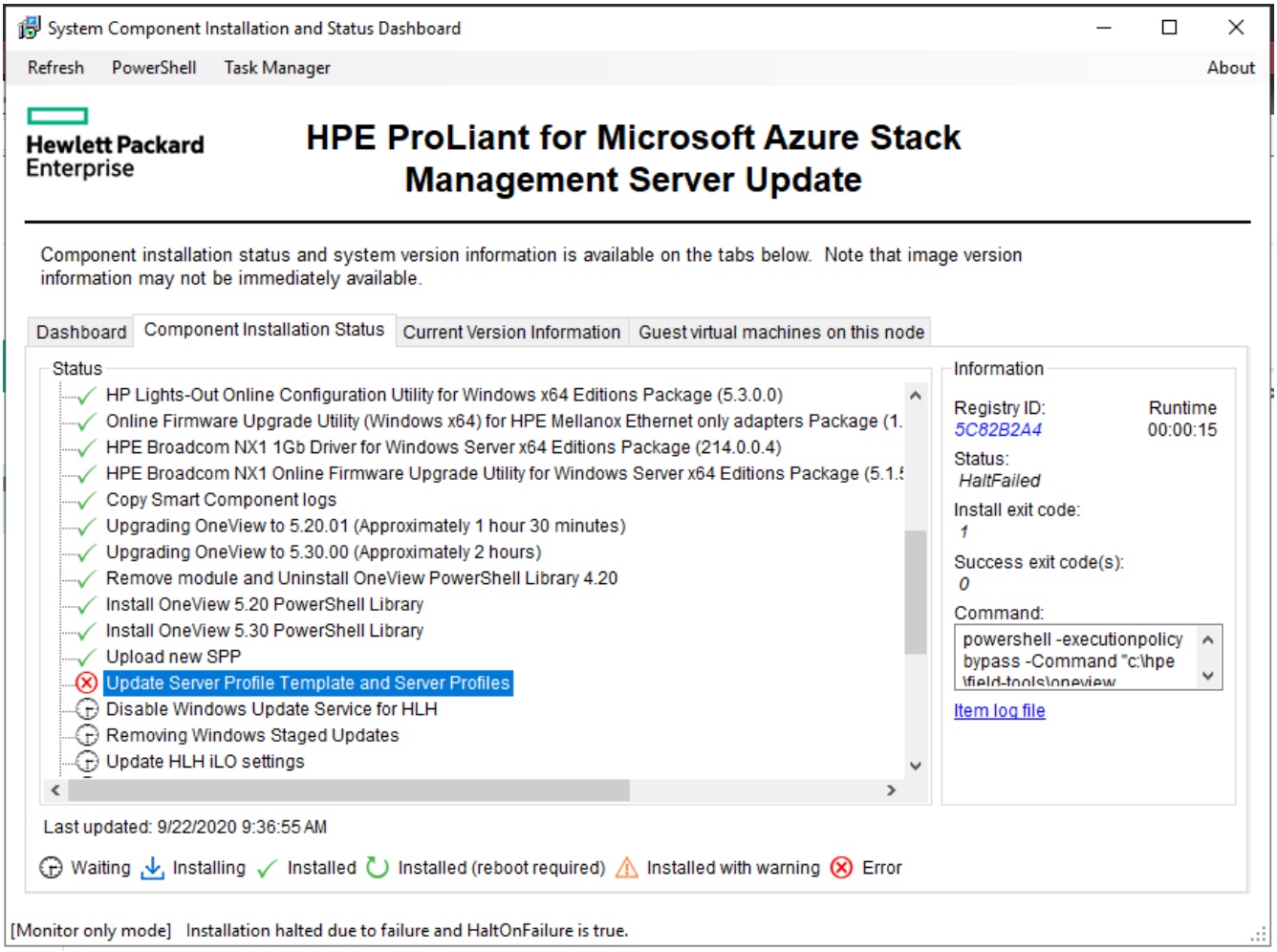
4. Select the ‘Enabled’ setting and press **Enter**. Then, press **F10** to reboot HLH.

> **NOTE:**
>
> Do NOT attempt to resolve the inconsistent profile warning to make the MAS Hub node server profiles consistent with the server profile template. The inconsistency will be resolved automatically as part of the OEM package installation using the new firmware orchestration feature built into the OEM package

After HLH reboot, go to the Update bundle extracted folder and double-click on the Start-UpdateBundle.cmd file to resume the installation.

Recovering from installer failures

If there is a step failure after the installer dashboard has started, `Start-UpdateBundle.ps1` will reopen the installer in Monitor only mode. This will allow the user to see what steps passed or failed and quickly review the log by selecting the step that failed and clicking the **Item log file** link.



Procedure

1. Attempt to determine the cause of the update step failure using the exit code or log output.
2. Close the Installer dashboard window to allow update bundle installer script execution to complete.
3. On the `Start-UpdateBundle.ps1` PowerShell window, press **Enter** to exit the update bundle installation process.
4. Once the original issue has been resolved, you can rerun `Start-UpdateBundle.ps1` to start the patch process from the step where it last failed.
5. After successful completion of the last action, close the dashboard by clicking the **X** in the upper right corner of the dashboard.

Step 5: Update HPE OneView user role to infrastructure administrator (if appropriate)

Hewlett Packard Enterprise recommends using a separate HPE OneView "Infrastructure administrator" user role specifically to perform OEM package firmware update operations. As part of the 4.1 update bundle installation workflow, make sure that at least one infrastructure administrator user role exists.



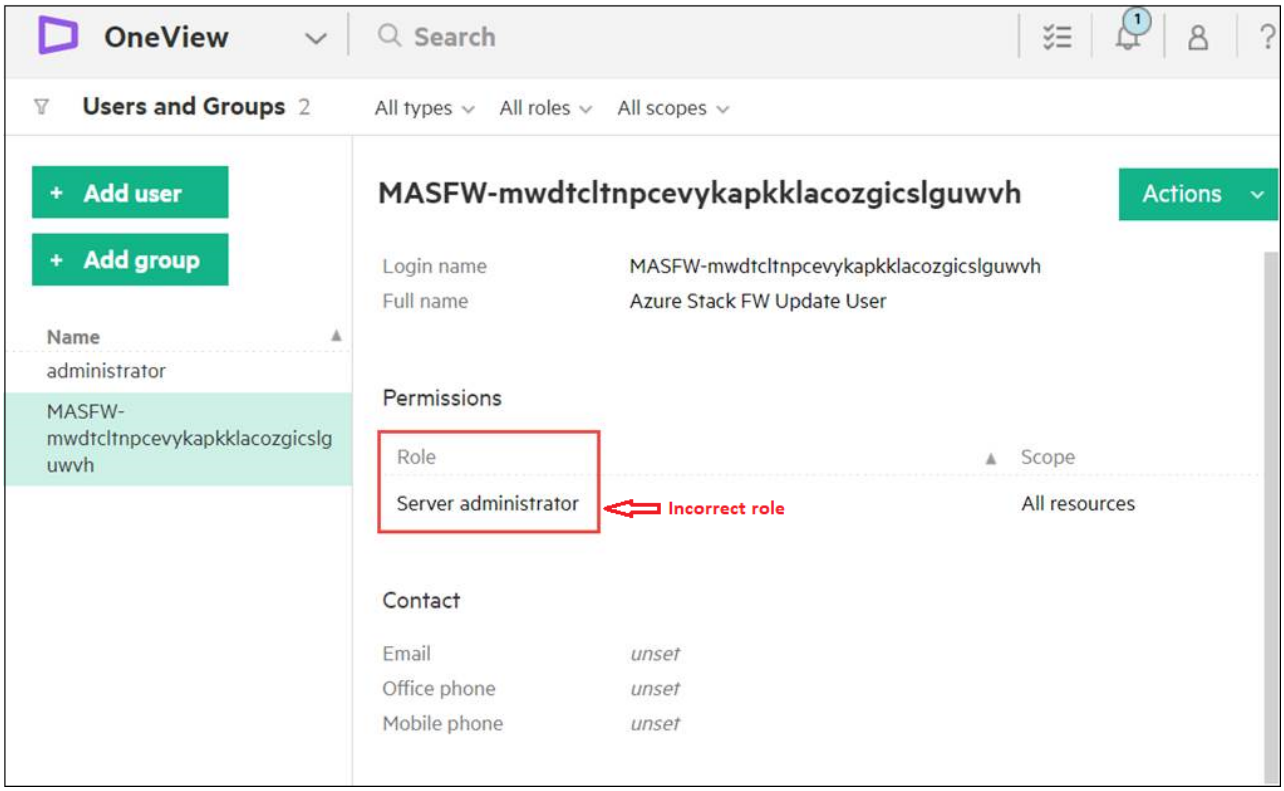
NOTE:

If your solution was deployed after July 2019, this account will have a login name with the format "MASFW-*<random characters>*". However, if the account was created manually by following a prior release of HPE ProLiant for Microsoft Azure Stack Hub Solution Update Bundle Installation Guide, it may have a different login name format.

Procedure

Verify that you have a user, other than an administrator, with appropriate permissions to perform OEM package firmware update operations.

1. Log in to HPE OneView.
2. From the drop-down next to the HPE OneView icon at the top of the window, select **Users and Groups**.
3. If there is a user other than the administrator that has been created to perform OEM package updates, verify that the user role is **not** set to "Server administrator".

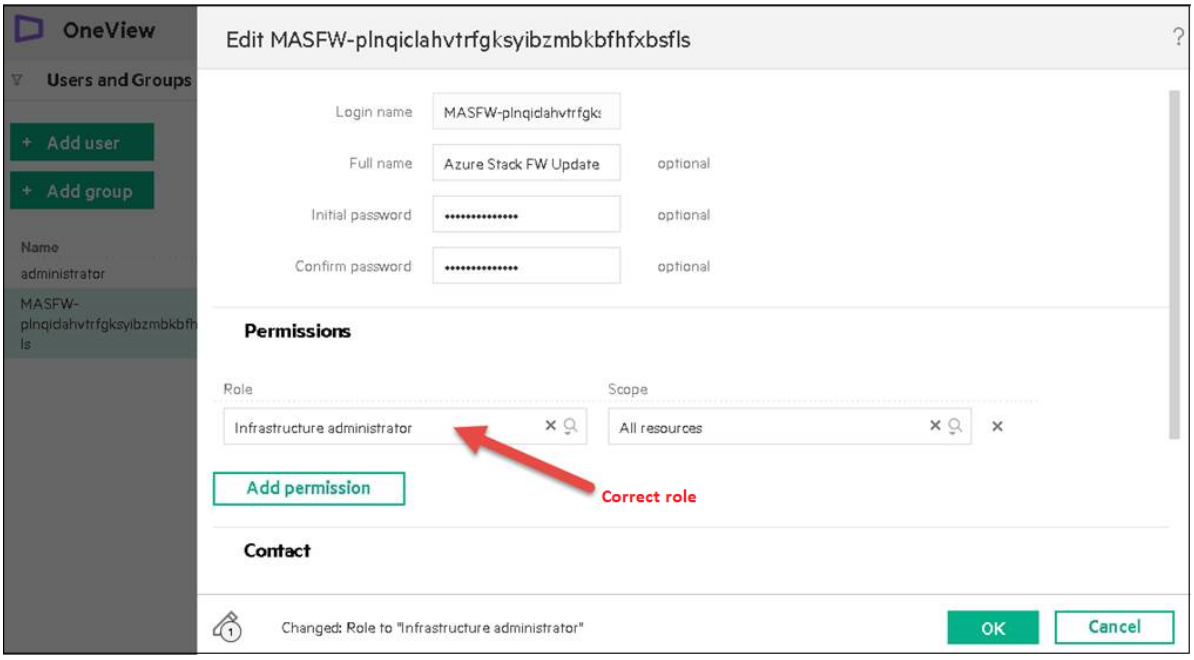


4. Based on the observed permissions role, perform **one** of the following actions:

   - If the role is "Infrastructure administrator", bypass the remaining steps in this procedure and skip directly to Step 6: Install OEM package.
   - If the role is **not** "Infrastructure administrator", then change the role to "Infrastructure administrator".

     a. Under the **Actions** menu, select **Edit**.

     b. From the Edit screen, specify the "Infrastructure administrator" role and click **OK**.



5. After the user role is updated, go to Step 6: Install OEM package.

Step 6: Install OEM package

After logging in to the Azure Stack Hub admin portal, select **Install Now** on the updates page to install the new OEM bundle.

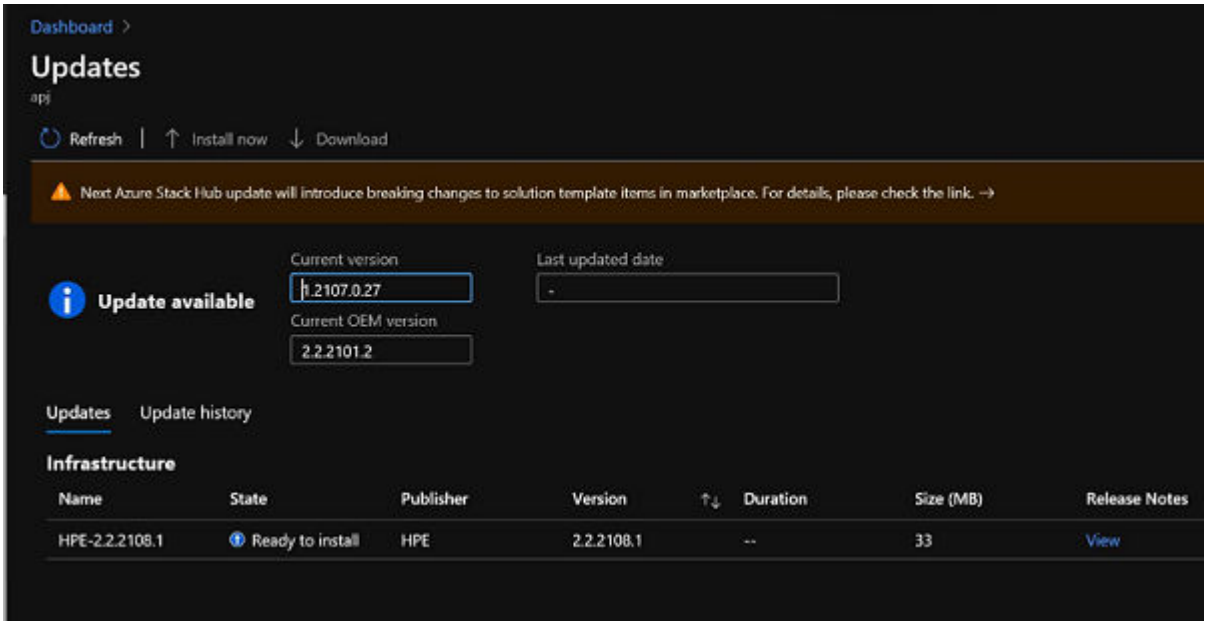
Along with the HPE OEM package installation, the latest SPP is automatically applied on the MAS nodes through the new OEM orchestration feature.

Prerequisites

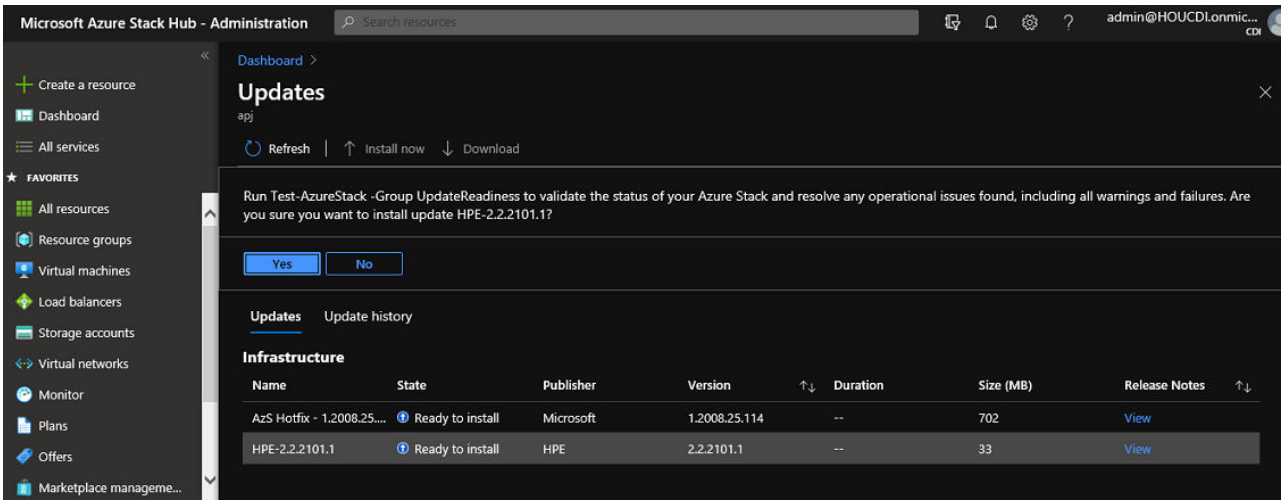
Verify that no errors exist on the Azure Stack Hub admin portal and Test-Azure Stack Hub command output. Additionally, before updating the OEM package from the Azure Stack Hub admin portal, check for critical alerts in HPE OneView.

Procedure

1. Log in to the admin portal.
2. Select **Dashboard**, and then click the **Update** tile.
3. Verify that the required OEM bundle version is reported in the admin portal.



4. Select the OEM package and click **Install now**.

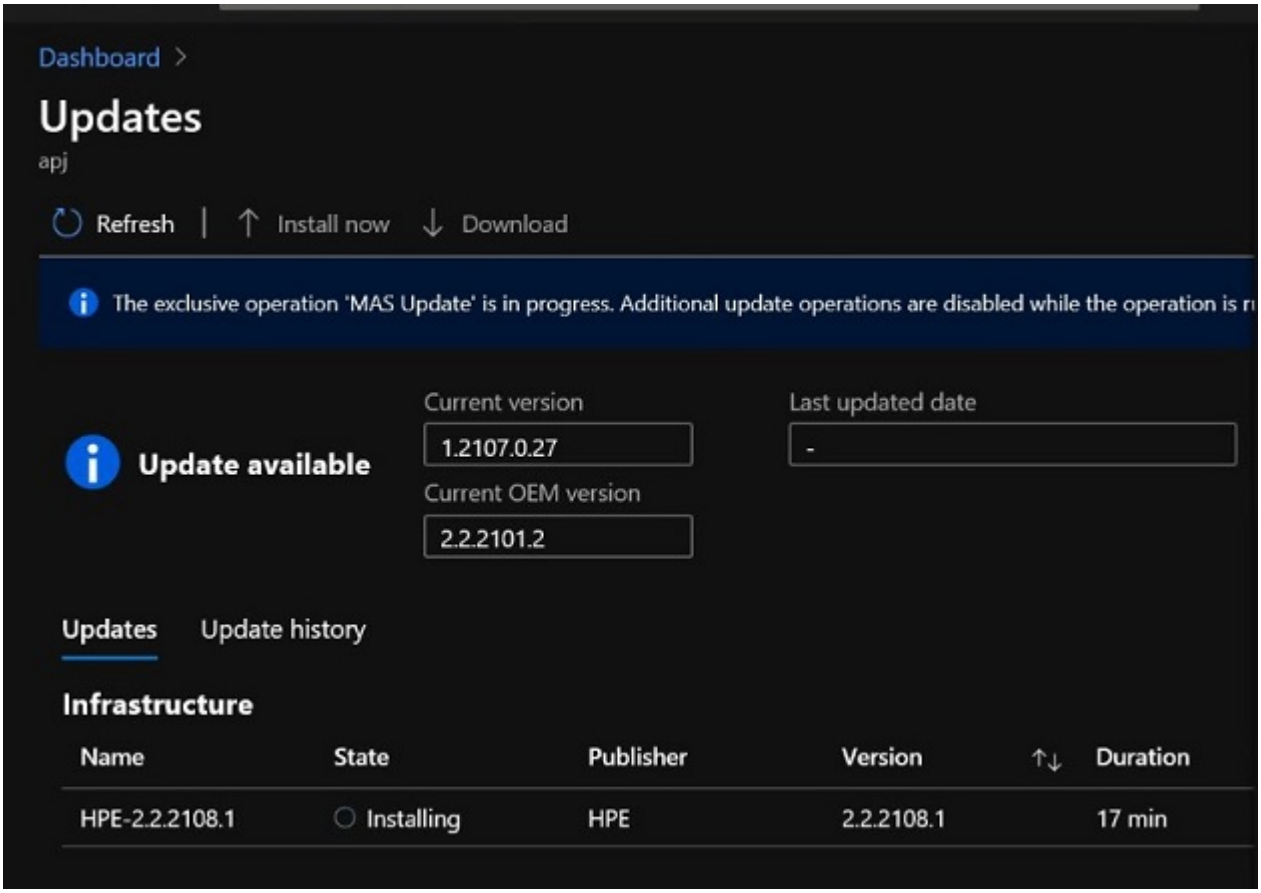


The message, "Run Test-AzureStack -Group UpdateReadiness...", displays on the admin portal.

5. From a privileged endpoint, execute "Test-AzureStack -Group UpdateReadiness" identified in the previous step.

6. Verify that the system remains healthy and that there are no errors or active alerts on Test-AzureStack -Group UpdateReadiness command output and on HPE OneView (see Verifying system health). Then, click **Yes** on the Updates page.

   This starts the OEM package installation and SPP application on MAS Hub nodes as controlled by the OEM orchestration feature.



7. When the OEM upgrade is complete, check the status of the OEM upgrade job.
8. Log into HPE OneView and verify that there are no warning messages, such as "server profile is inconsistent with its server profile template", and that the server profile indicates a green status.

   To install the OEM package and apply the server profiles on MAS Hub nodes, OEM orchestration will take approximately 6 hours for a 4-node environment due to the live update of physical nodes. Since there are several factors that can influence the runtime, do not be concerned if the update takes considerably longer.

> **NOTE:**
>
> In case of a failure while executing the update bundle installation, Hewlett Packard Enterprise recommends contacting the HPE support team for help.

Step 7: HLH OS updates

After installing the HPE Solution Update Bundle, Hewlett Packard Enterprise recommends applying the latest Windows updates to the HLH OS.

Procedure

1. Check the windows version by running the `winver` command from powershell.
2. Click the following **link** and select the windows version from the left side.
3. Scroll down on the left side to select the latest available update.

   As of writing of this document below are the latest link for updates:

   - **https://support.microsoft.com/en-us/help/5004244** (version 1809)

   > **NOTE:**
   >
   > Microsoft releases monthly cumulative updates for security and non-security updates. Installing the most recent update ensures that you also get any previous updates that you might have missed, including any important security fixes.

4. Select the latest monthly update.

   Example: July 13, 2021 (OS Build 17763.2061)

5. Follow the steps in **How to get this update** to download the update and transfer to the HLH.

   > **NOTE:**
   >
   > If the cumulative update requires a servicing stack update (SSU) before installation, the relevant information is also available in the **How to get this update** section.

6. Open a PowerShell window as administrator.
7. Enable and start the Windows Update Service.

   a. `Set-Service -Name wuauserv -StartupType Manual`

   b. `Start-Service -Name wuauserv`

8. Install the Windows update that is downloaded/transferred to HLH by following the Microsoft update instructions.
9. After the update completes, stop and disable the Windows Update Service.

   a. `Stop-Service -Name "wuauserv"`

b. `Set-Service -Name "wuauserv" -StartupType Disabled`

Migrating the HLH OS from Microsoft Windows 2016 to Microsoft Windows 2019

Migration Process Overview

Planning

As a part of migration process, few files are backed up by default in the FRU drive (V:). Therefore, it is important to keep at least 30GB free in the FRU Drive (V:).

The Windows 2019 Operating System image (ISO) is part of the update bundle package. This needs to be copied to a network share that is accessible from the HLH iLO. The ISO can be manually mounted to the iLO before starting Start-UpdateBundle.cmd, or automatically mounted as a part of the workflow. For automatic mounting, the network share must be accessible via HTTP, and the HTTP location must be provided when prompted.

The migration code backs up both C:\CDW and C:\CDW.FINAL into V: . Verify that the latest CDW configuration is within these folders. Also, be sure to keep the certificates needed to access admin portal in one of these folders as a backup.



NOTE:

The backup process will not fail if certificates are not placed in these folders, however, an error will occur if either of these folders are unavailable.

See the known issues and take appropriate actions, if applicable, before starting migration process.

New Terms

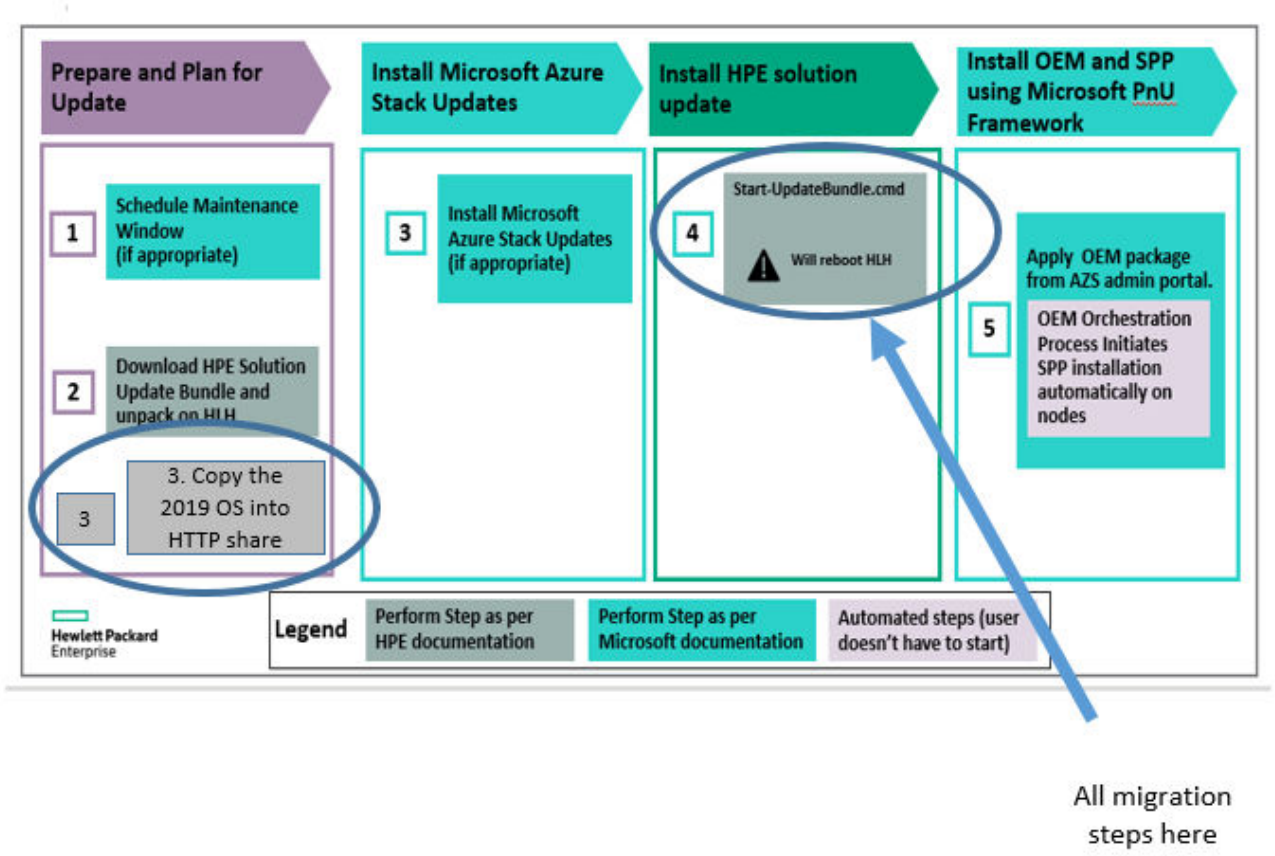
See below for a list of new terms and their meaning as used in this section of the guide.

- preOSUpgrade - procedures completed before OS installation
- HLH OS install - Installs Windows Server 2019 OS
- postOSUpgrade - procedures completed after OS installation

Overall process

This procedure is is applicable for environments where the HLH uses Microsoft Windows 2016 OS with a 3.23 version of HPE Azure Stack Hub.

The following image provides a summary of the update process. Circled items show where the migration flow diverges from the standard update bundle installation.



Migrating from Microsoft Windows 2016 to Microsoft Windows 2019

Prerequisites

- Verify the health of the system.
- Verify that the AzureStack admin portal is accessible from the HLH.
- Copy the Windows 2019 ISO to a network accessible to the HLH iLO to verify checksum is matched.
- (optional) Manually mount the network share to the HLH iLO.

Procedure

1. Schedule a maintenance window (if applicable).
2. Download and extract the update bundle zip file.
3. Update the Azure Stack Hub software (if applicable).

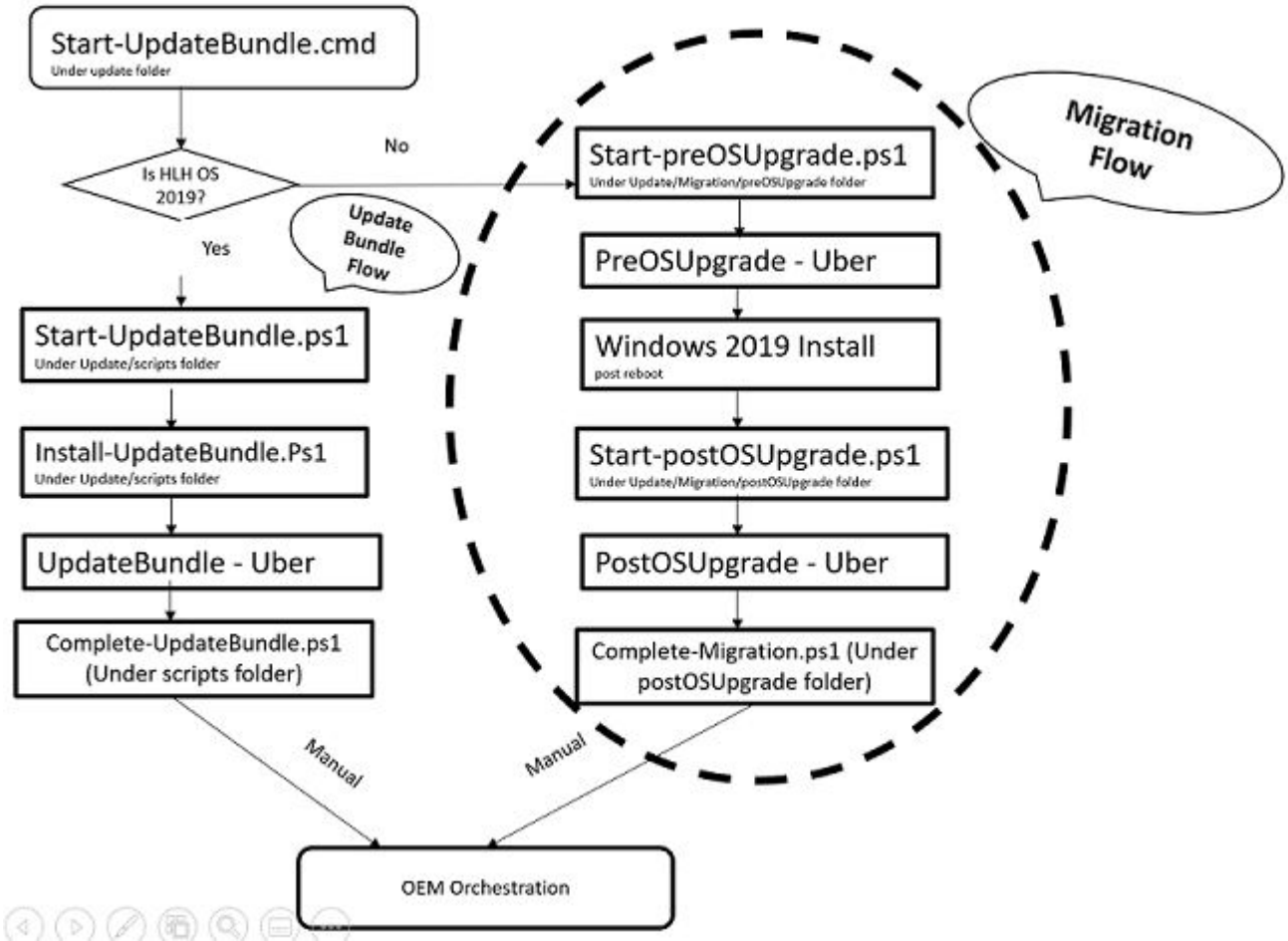
4. Execute the `start-updatebundle.cmd` script.

   The `Start-UpdateBundle.cmd` initiates the `Start-UpdateBundle.ps1` script.

5. Complete the steps in the Migration process.

Migration process

The following image shows the migration flow process from `Start-UpdateBundle.cmd`.



The `Start-UpdateBundle.cmd` script initiates the `Start-UpdateBundle.ps1`, which begins running the required steps before installing the new OS. This script does the following:

- Verifies that 30GB on the FRU Drive (V:) is available.
- Completes the compliance precheck.

Running Start-UpdateBundle.cmd

The `Start-UpdateBundle.cmd` script initiates the OS migration installation process. Upon executing `Start-UpdateBundle.cmd`, the installation launches the migration installation wizard. Before proceeding with the installation, the installation wizard will display a prompt to enter HPE iLO, HPE OneView and Azure Stack Hub admin portal login credentials.

Procedure

1. Navigate to the extracted folder and double-click the Start-UpdateBundle.cmd file.

   The Migration Installation window displays.

2. When prompted, enter your HPE iLO and HPE OneView credentials.

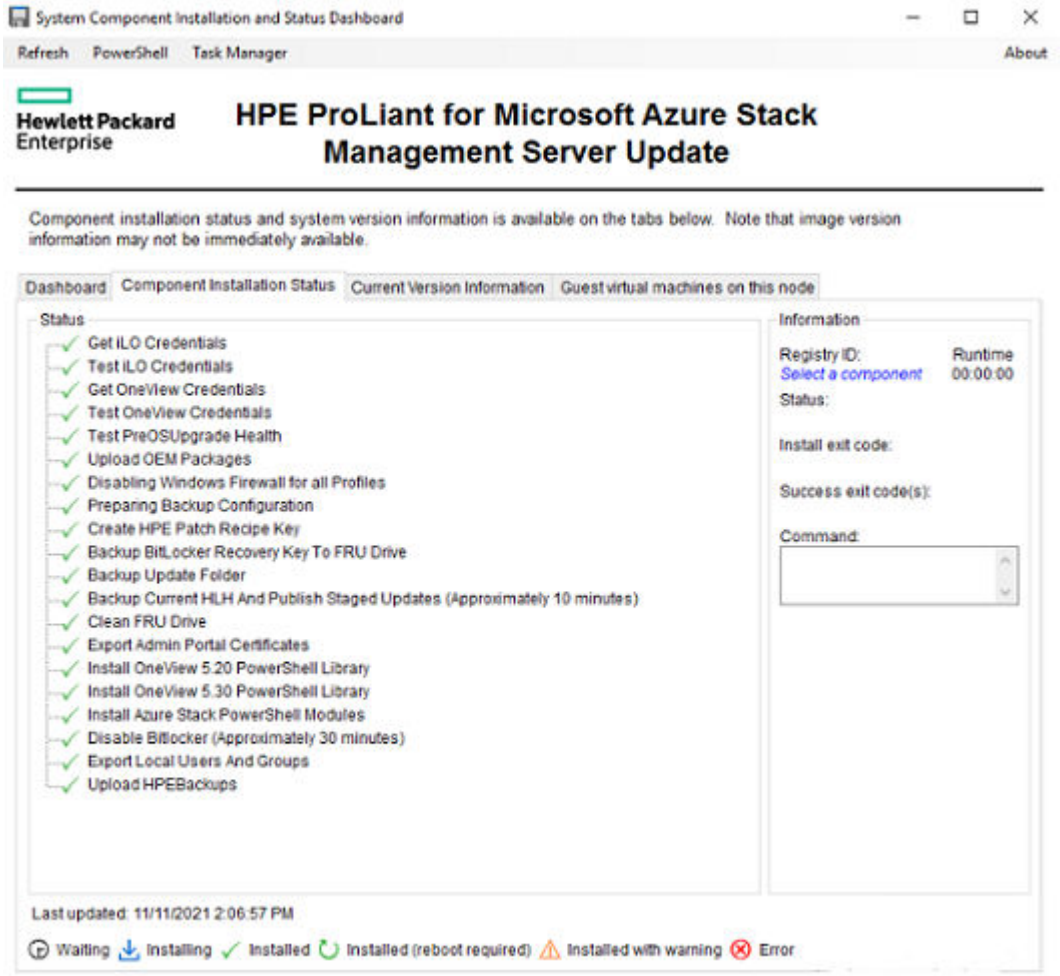
3. When prompted, enter the credentials for the Azure Stack Hub admin portal.

   After validating the credentials entered, the migration process will continue. You can monitor the progress of the update bundle installation using the Update Bundle Installer Dashboard.

   Each step executed by the installer will have a status icon. To map the icon with the status, use the legend at the bottom of the window. You can also check the log generated from each script by clicking the item log link on the right side of the window. When the status of the last step or action has a green checkmark, the script is complete.

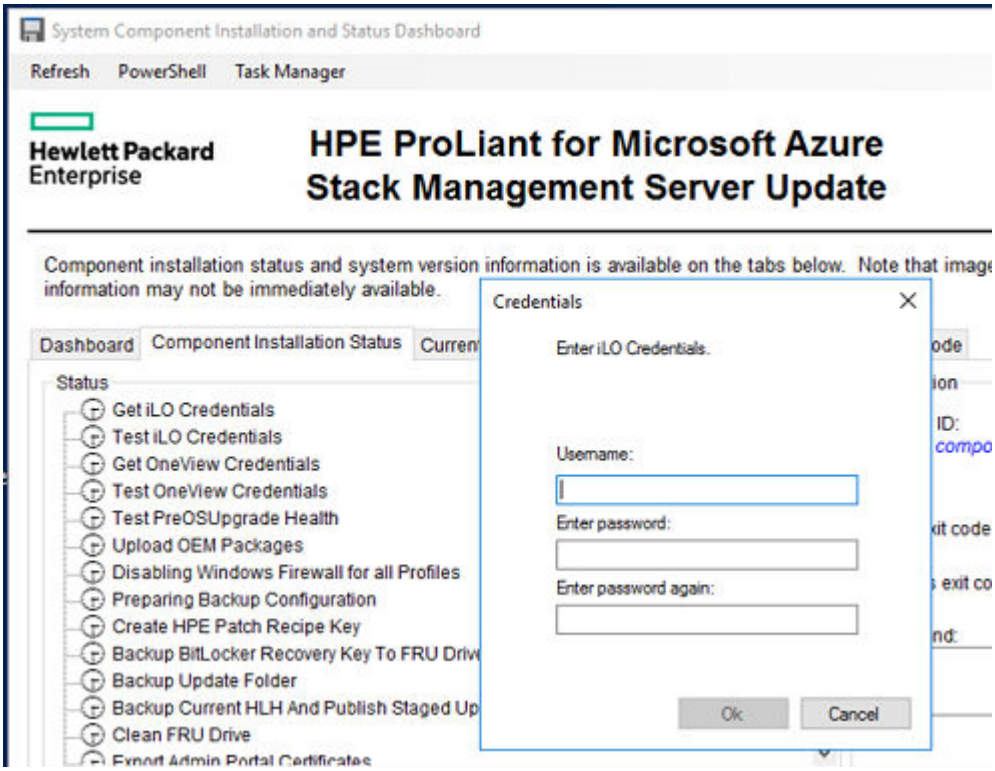
Procedure

The following example illustrates a migration procedure in progress.

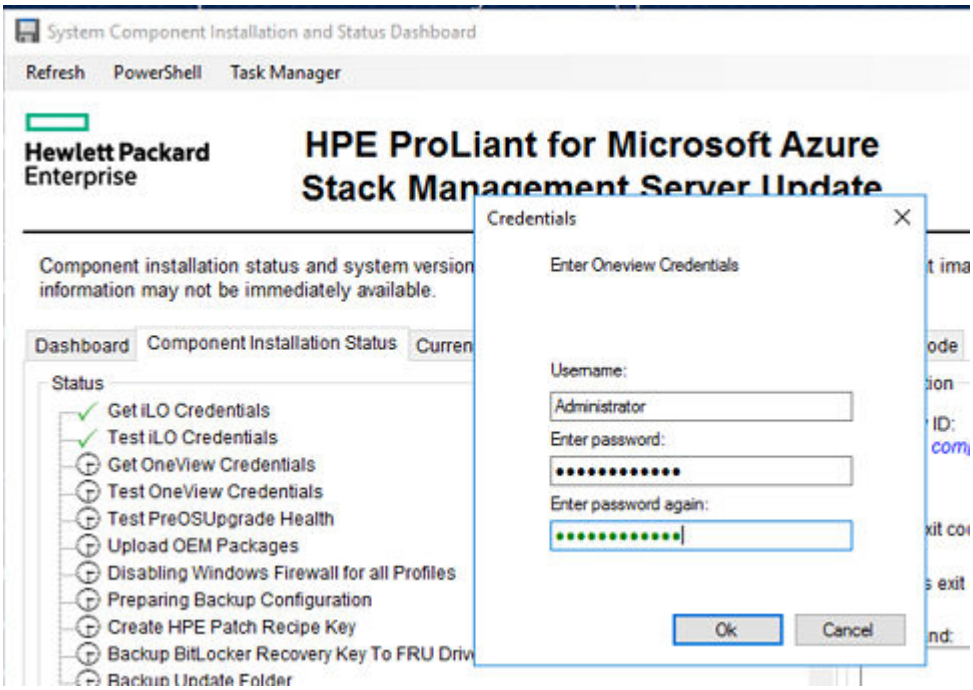


[Monitor only mode]

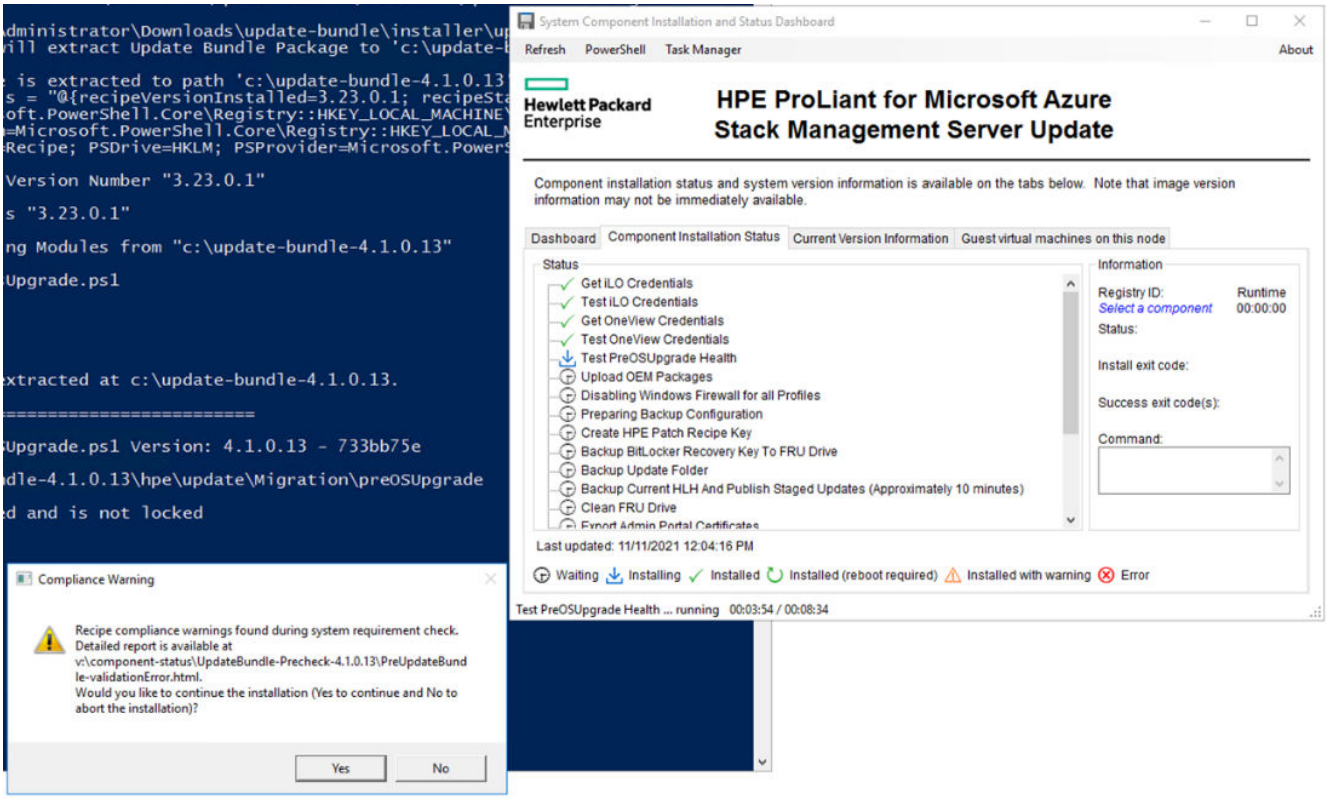
When the Installer wizard launches, the prompt displays to enter HPE iLO credentials.



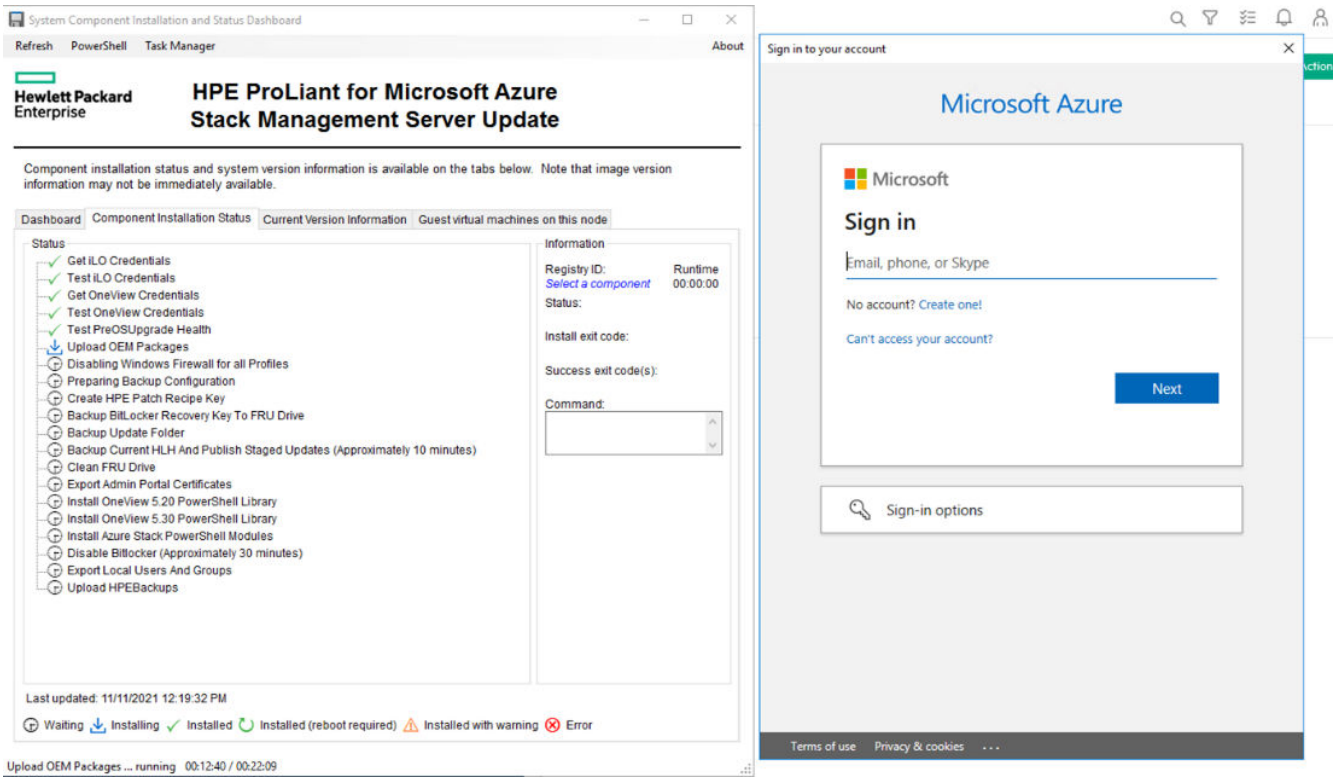
The prompt for HPE OneView credentials displays.



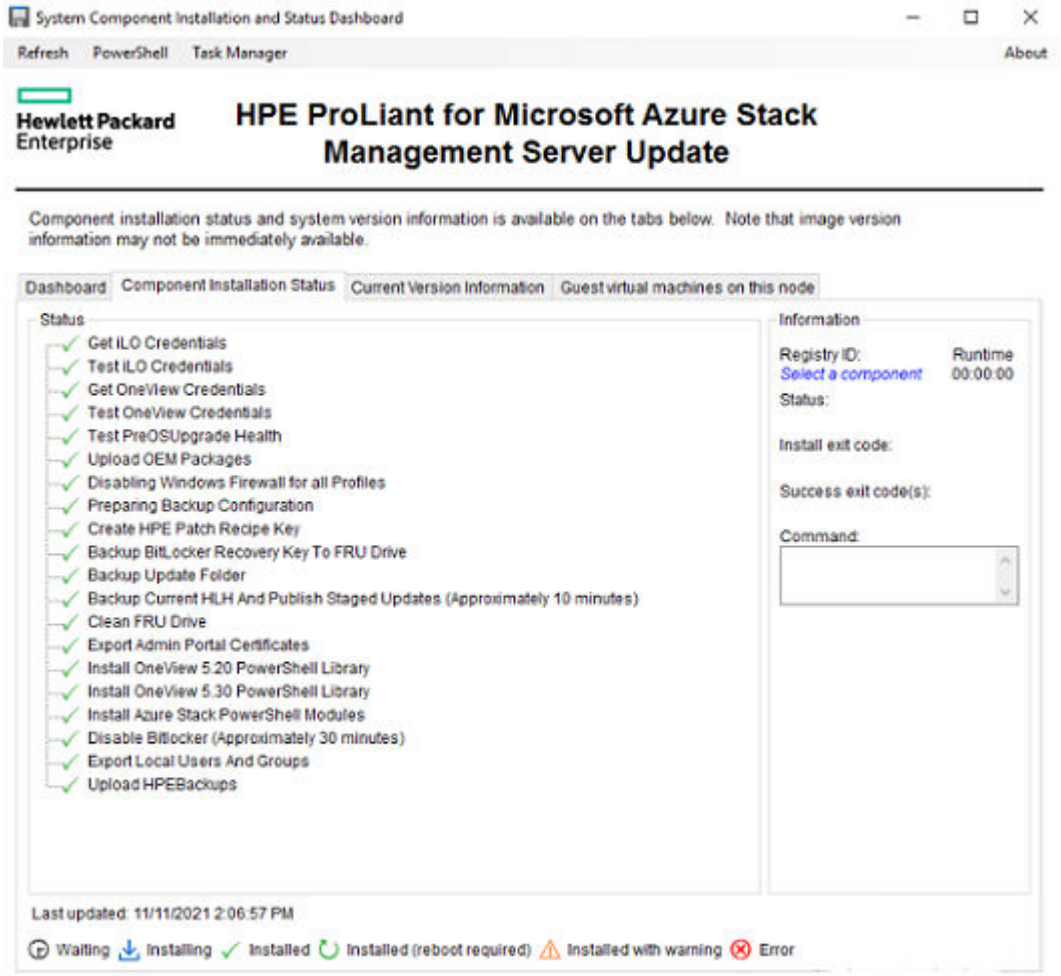
In case of compliance errors or the installation stops, the user has the option to continue or abort the installation if alerts display.



The prompt displays to enter Microsoft Azure Stack credentials.



The following image shows a successful completion of the installation steps in the migration process.



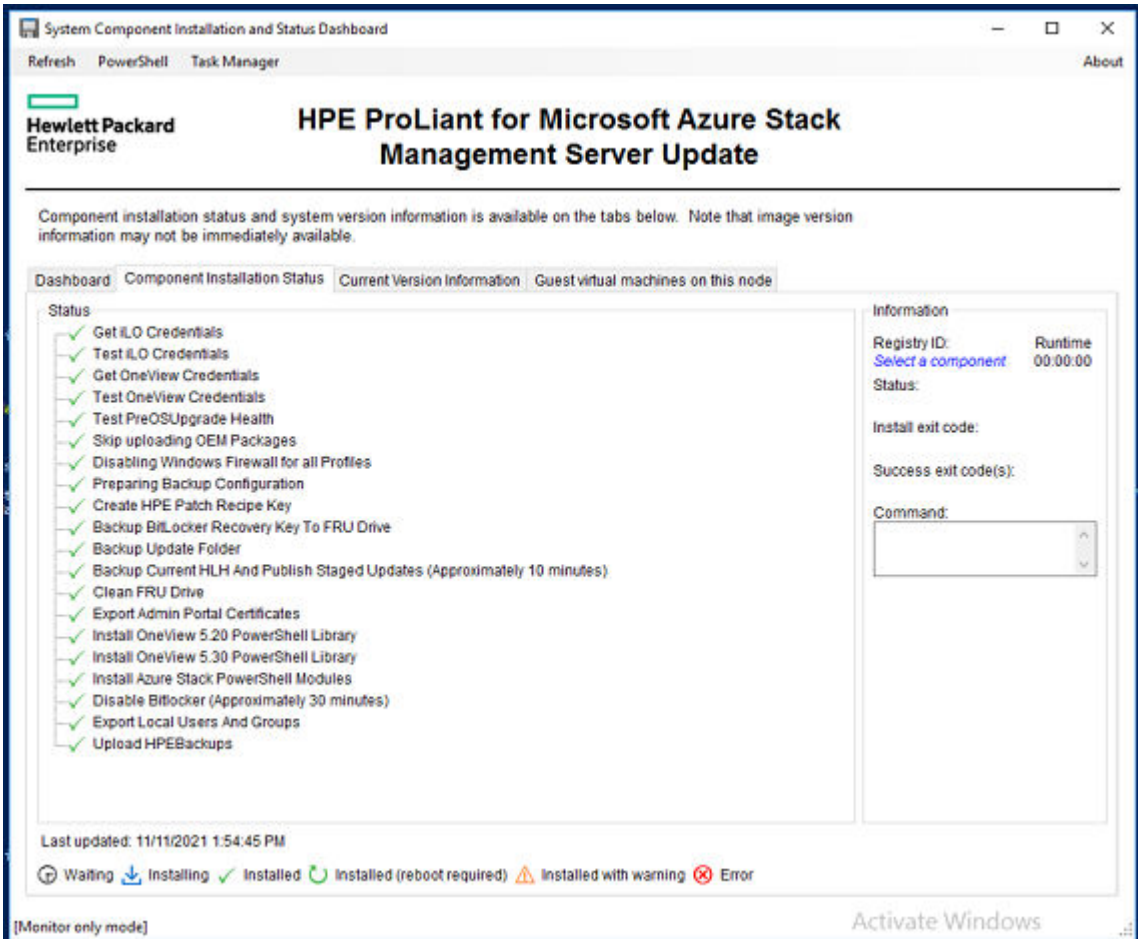
[Monitor only mode]

SkipOemPackageUpload parameter

The migration process contains a step to upload the HPE Azure Stack OEM Bundle to the admin portal. If the OEM bundle upload to the admin portal is intended to be done manually, use SkipOemPackageUpload along with Start-UpdateBundle.ps1 to skip the step in the migration flow. See **Prepare an Azure Stack Hub update package** for steps to import and install OEM updates.

1. Open a new Power Shell window in administrator mode.
2. Navigate to the extracted update bundle folder and change the directory to "scripts".
3. Run the following command: `.\Start-UpdateBundle.ps1 - SkipOemPackageUpload -Migration`

The following is an example of a successful migration.

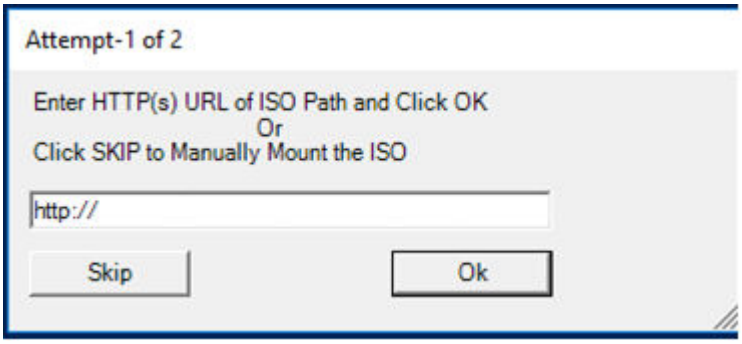


Mounting the iso file

Procedure

1. In the user prompt, enter the URL of the Windows 2019 OS image file, `hpemas-hlh-signed-4.1.2.XX.iso`, to mount on the iLO virtual media for OS installation.

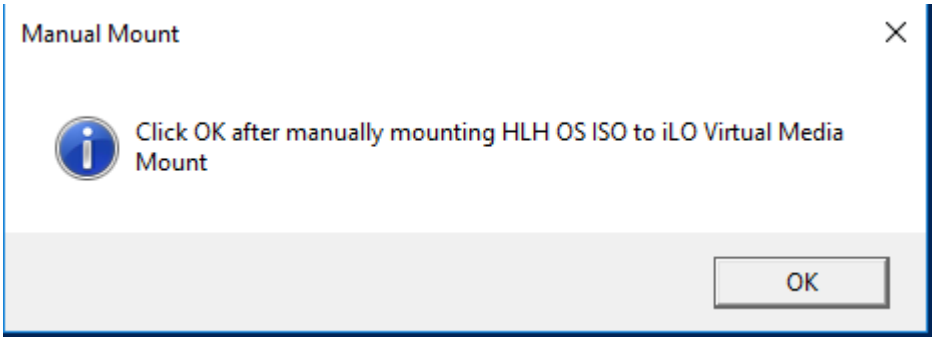
> **NOTE:**
>
> Before beginning the OS installation, be sure to backup any important files. For more information, see Additional secondary backup of HLH files. This is optional, as the migration tool backs up all files to V: and uses them to restore.



To manually mount the ISO, click **Skip**.

The `hpemas-hlh-signed-4.1.2.XX.iso` file is located in the solution update bundle package extracted path under the **Windows2019_Migration** folder.

If Skip is selected or two unsuccessful attempts have been made, the prompt to manually mount the ISO displays.

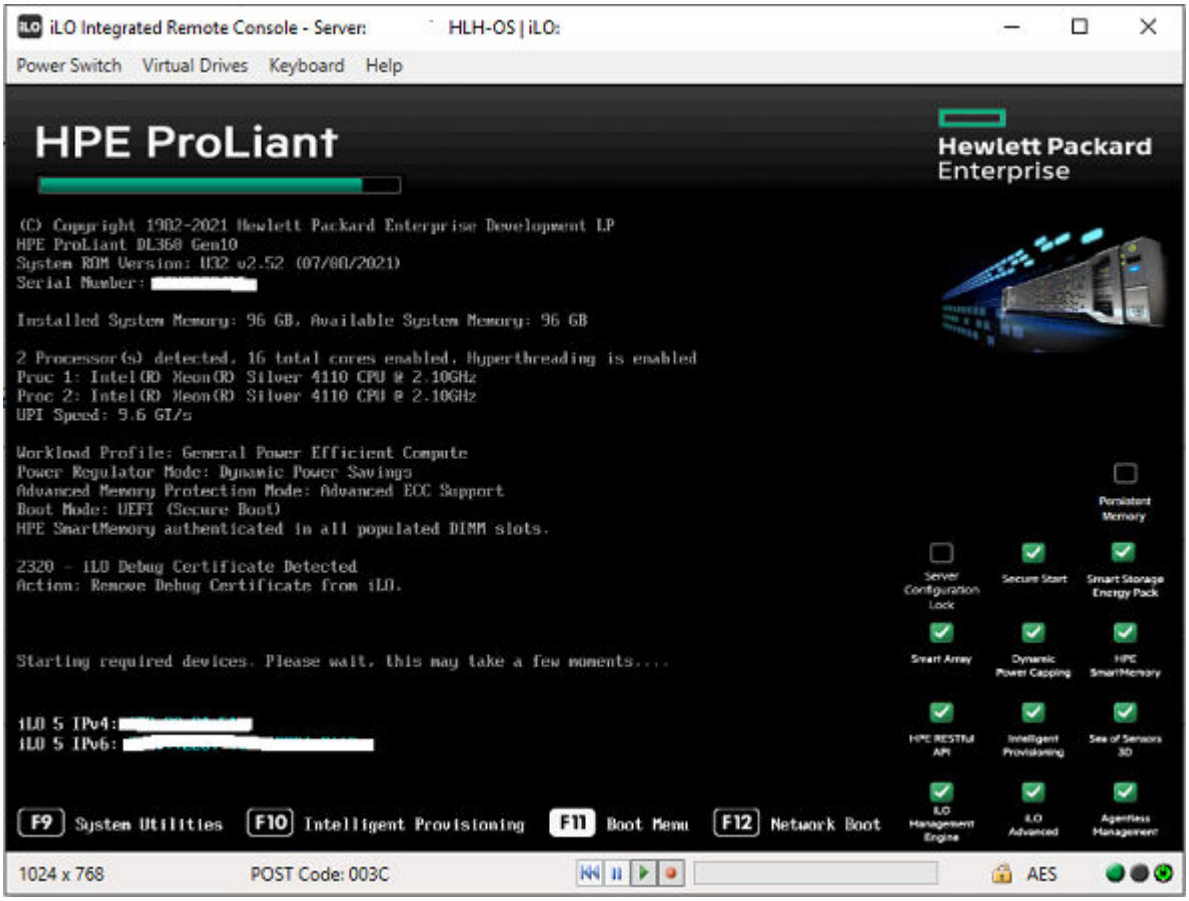


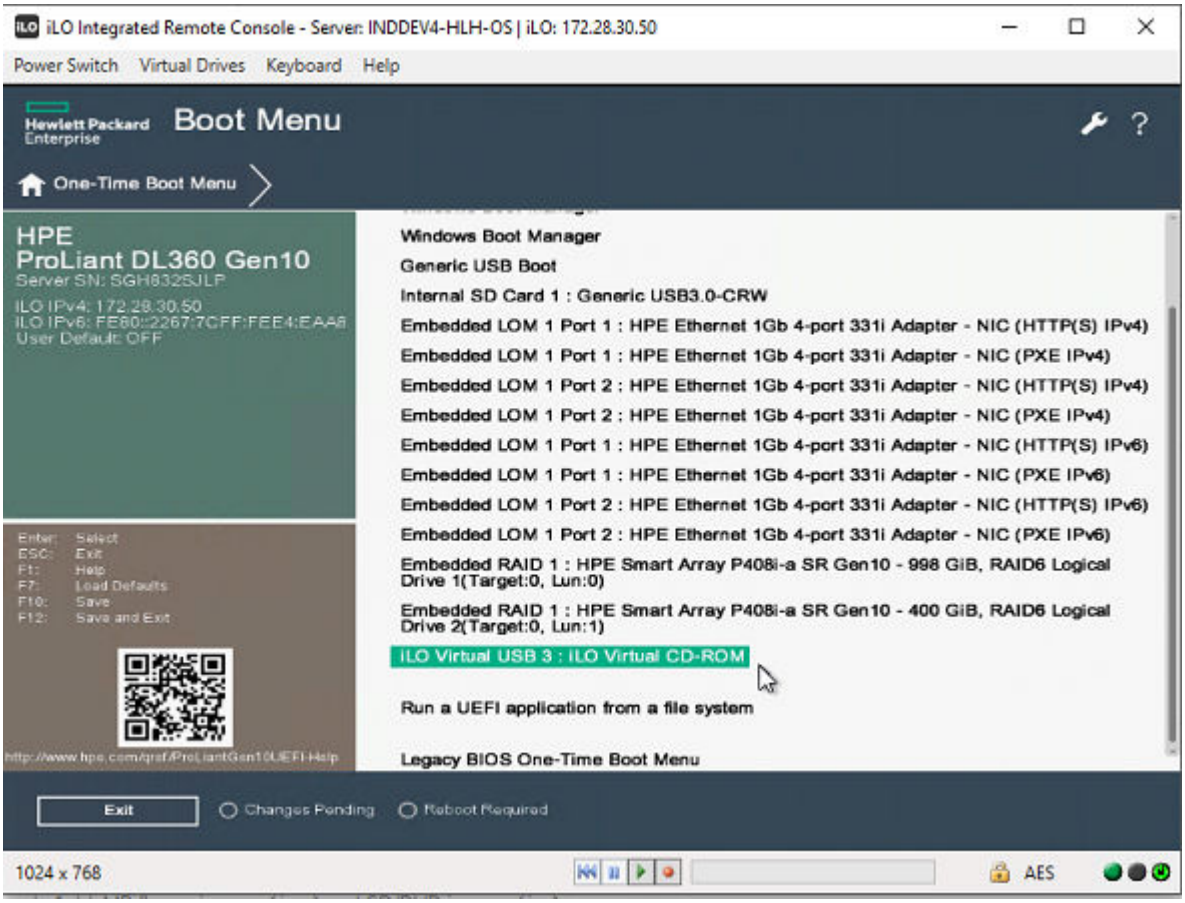
2. Click **OK** after manually mounting the Windows 2019 OS image. To complete this process, see Manually mounting the ISO on Virtual Media of the HLH.

Manually mounting ISO on iLO Virtual Media of the HLH

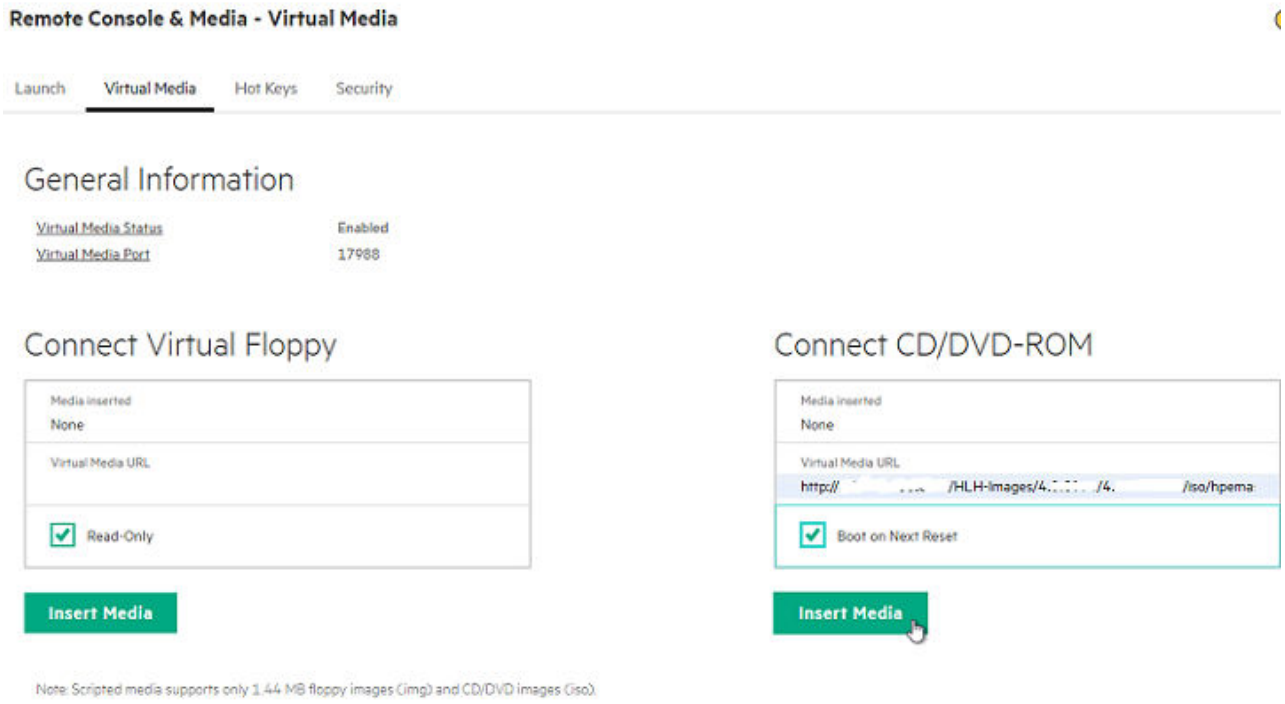
Procedure

1. If using HPE Remote iLO Console Software to mount the virtual media, manually enter F11 – Boot Menu after rebooting the HLH, during POST, and select the “iLO Virtual USB 3: iLO Virtual CD-ROM” option to boot into the ISO image.


iLO Integrated Remote Console - Server: HLH-OS | iLO:
Power Switch Virtual Drives Keyboard Help
HPE ProLiant
Hewlett Packard Enterprise
(C) Copyright 1982-2021 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v2.52 (07/08/2021)
Serial Number:
Installed System Memory: 96 GB, Available System Memory: 96 GB
2 Processor(s) detected, 16 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
Proc 2: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
UPI Speed: 9.6 GT/s
Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI (Secure Boot)
HPE SmartMemory authenticated in all populated DIMM slots.
2320 - iLO Debug Certificate Detected
Action: Remove Debug Certificate from iLO.
Starting required devices. Please wait, this may take a few moments....
iLO 5 IPv4:
iLO 5 IPv6:
Persistent Memory
Server Configuration Lock
Secure Start
Smart Storage Energy Pack
Smart Array
Dynamic Power Capping
HPE SmartMemory
HPE RESTful API
Intelligent Provisioning
Sea of Sensors 3D
iLO Management Engine
iLO Advanced
Agentless Management
F9 System Utilities
F10 Intelligent Provisioning
F11 Boot Menu
F12 Network Boot
1024 x 768
POST Code: 003C
AES



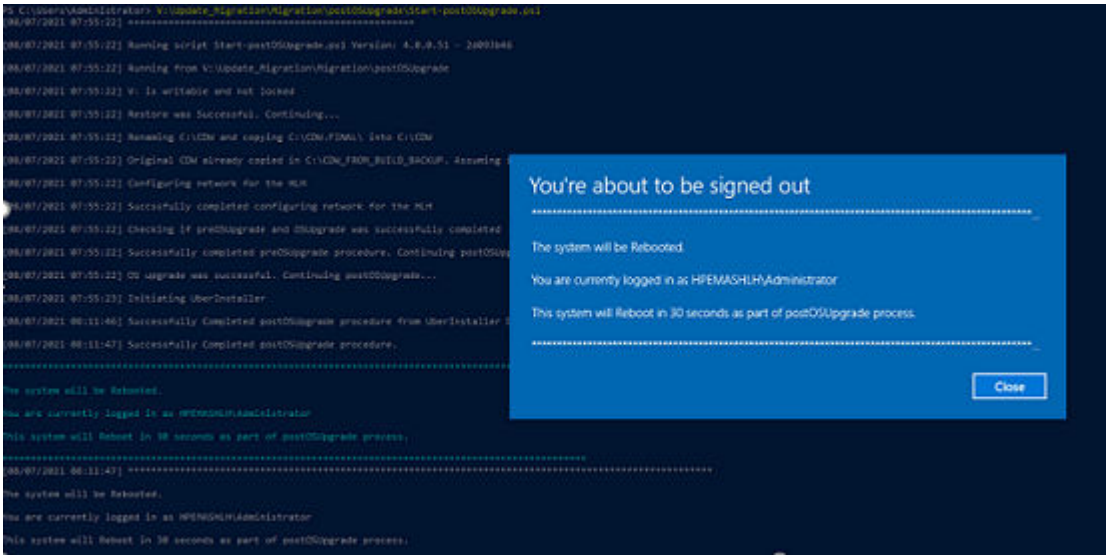
2. If using the HPE iLO webpage to mount the HTTP URL or Virtual media, enter the Virtual Media URL and select **Boot on Next Reboot**. Then, click **Insert Media** as shows in screenshot below.



3. After manually mounting the file, click **OK** to continue and complete pending items, such as updating registry, export registry, backup log file. Then, reboot the machine to begin the OS installation.

Reboot the HLH

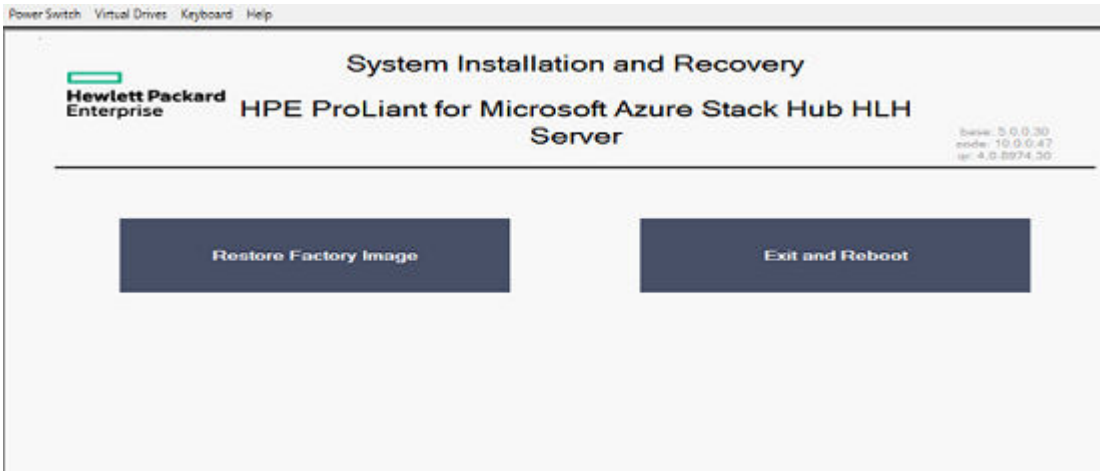
Upon successful completion of preOSUpgrade, the HLH will automatically reboot if virtual media was mounted through the script.

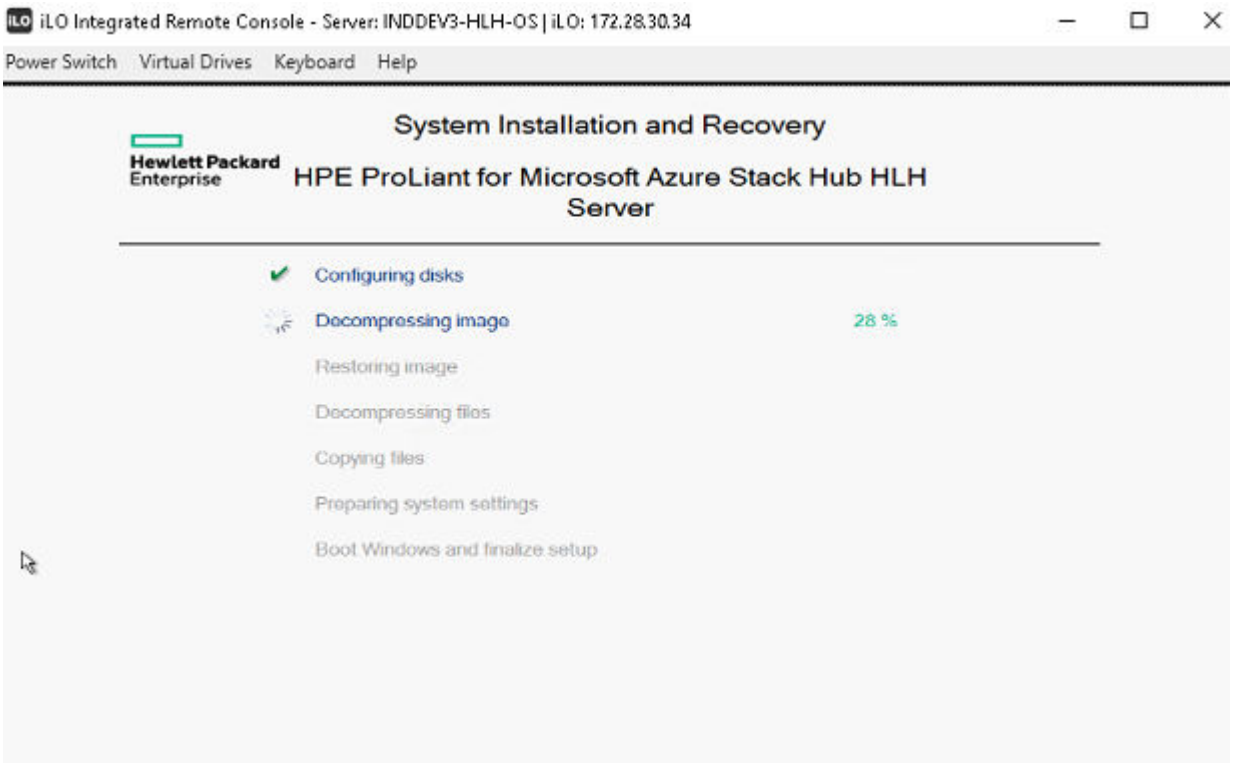


Installing Windows 2019

Procedure

1. Install Windows 2019.

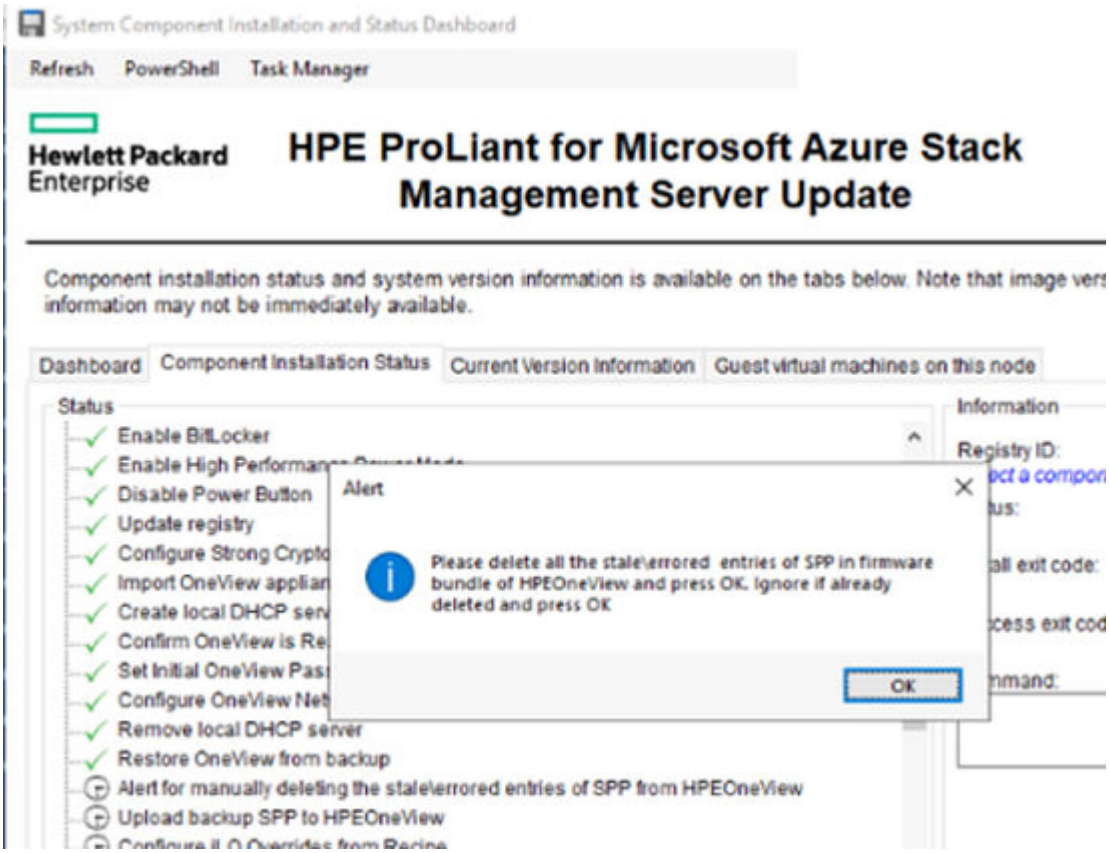




After the Windows 2019 installation is complete, the following actions happen:

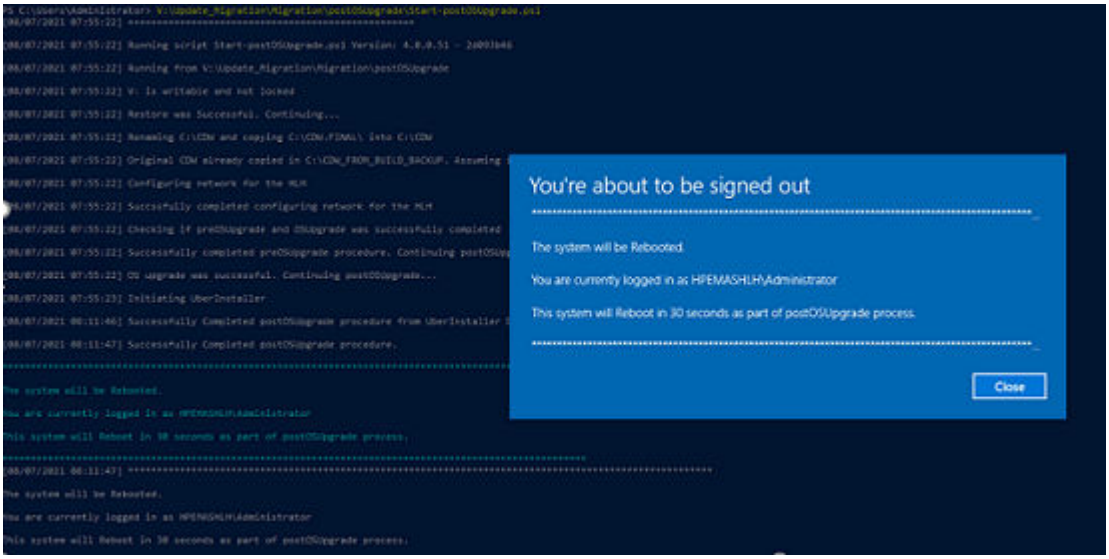
- The OS reboots.
- The `setupcomplete.ps1` script is automatically invoked in the HLH.
- The `Start-postOSUpgrade.ps1` script begins the steps required to configure the HLH.

2. When prompted, enter the HPE OneView and HPE iLO credentials.
3. When prompted, Clear Stale/Errored SPP from the HPE OneView appliance. See "Clearing Stale/Errored Custom SPP from HPE OneView Appliance".

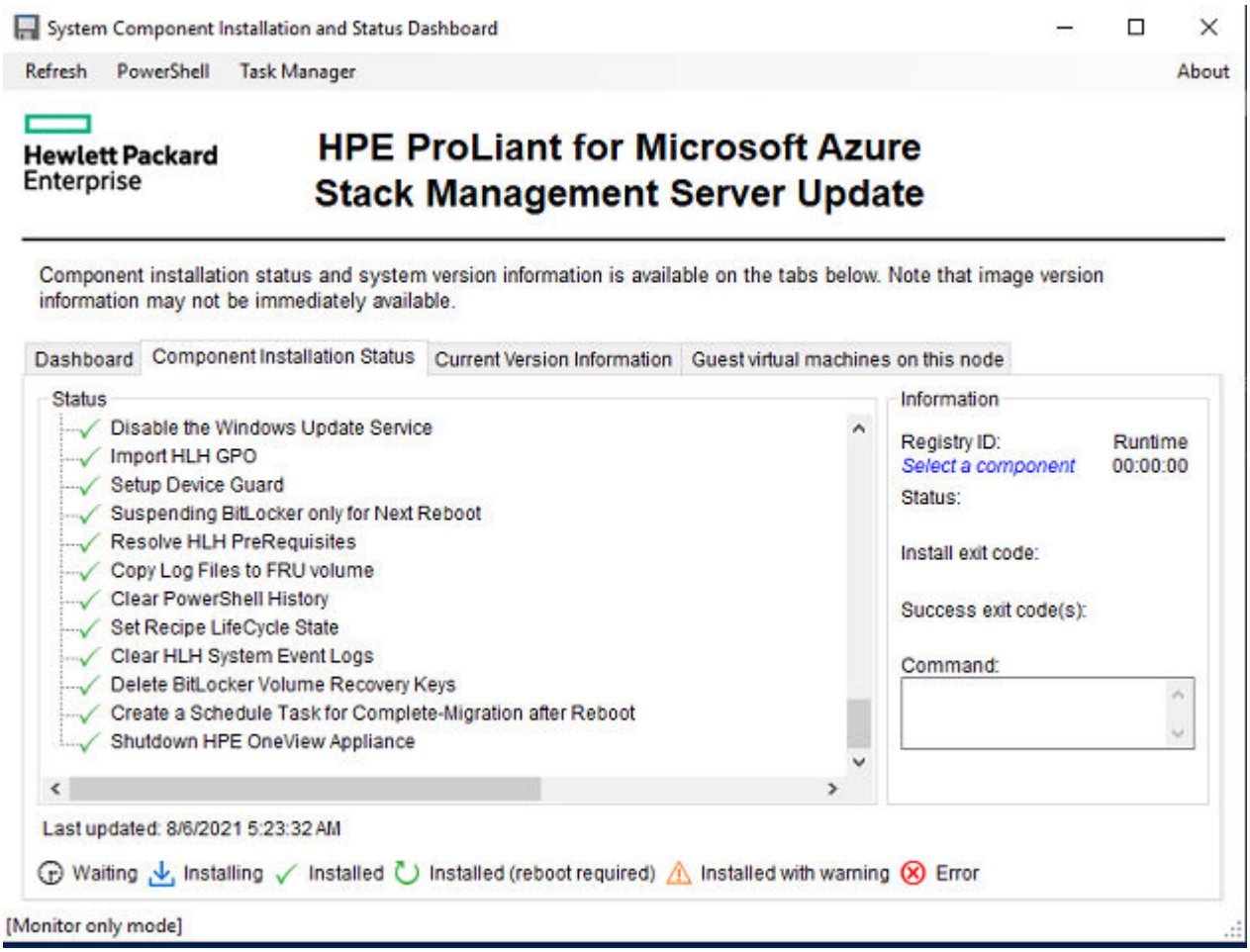


After all steps are complete, the `Start-postOSUpgrade.ps1` script reboots the HLH.

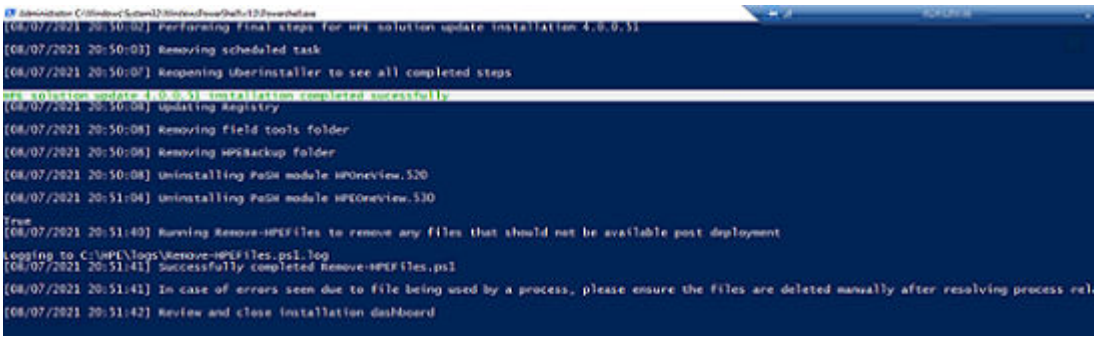
The following image shows the PowerShell window when postOSUpgrade is complete (system reboot phase).



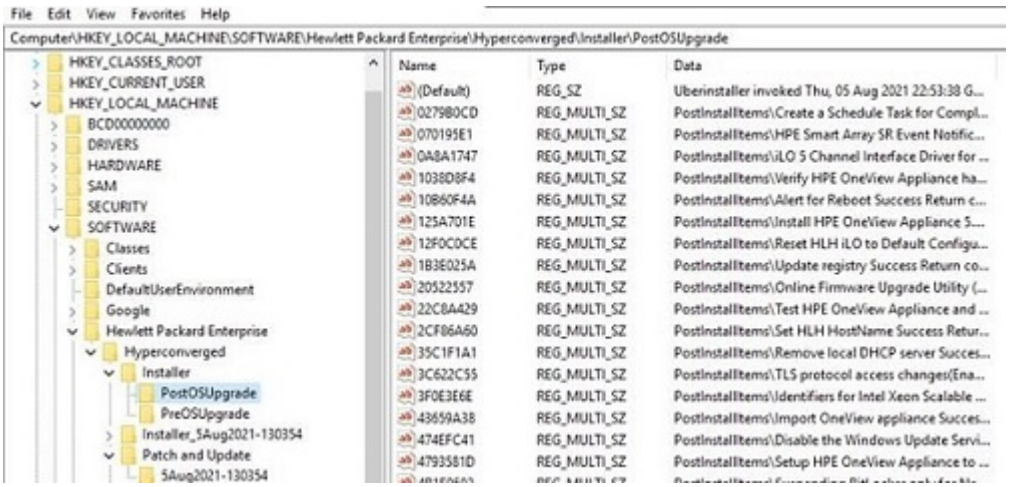
The following image shows the UberInstaller window when PostOSUpgrade is complete.

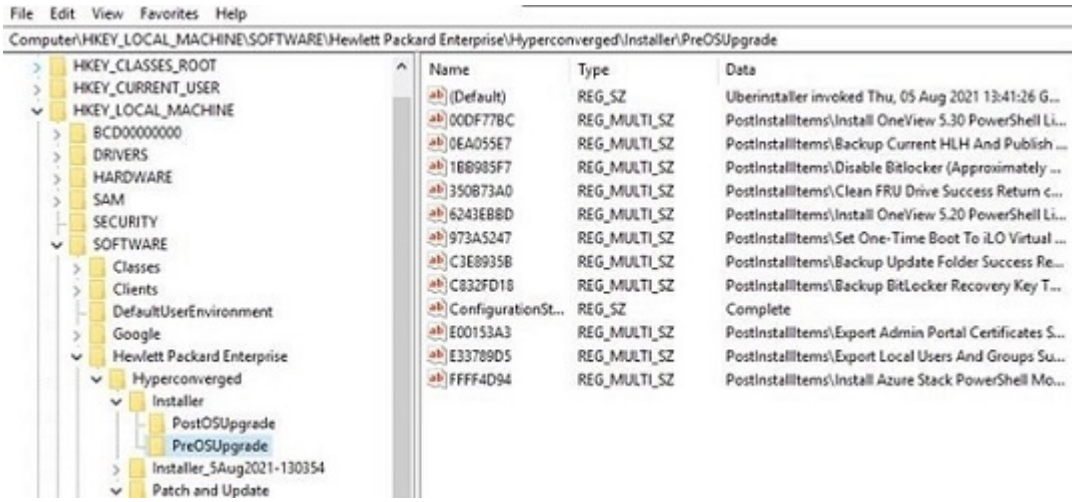


The system will reboot when the PostOSUpgrade steps are complete. After the reboot, the Complete-Migration.ps1 script is called. The following image shows the PowerShell window with Complete-Migration.ps1.



The following images shows the registry after Complete-Migration.ps1, which contains the preOSpgrade and postOSUpgrade folders.





4. (If applicable) Update the HPE OneView user role to infrastructure administrator.
5. Install the OEM package.
6. Complete the HLH OS updates.

Importing AzureStack Hub certificates into the HLH

Procedure

1. On the HLH, navigate to the Azure Stack **Certificates** folder.

   This folder contains the certificates that have been used to deploy the AzureStack AAD or ADFS solution on your environment.

2. Locate and click the ssl.pfx certificate in the Admin Portal folder.
3. On the Welcome to the Certificate Import Wizard screen, select the **Local Machine** radio button and click **Next**.
4. Click **Yes** on the User Account Control screen.
5. On the File to import, enter the file name with the path and click **Next**.
6. On the **Private key protection** screen, enter the password that was used to generate the certificates and click **Next**.
7. Click **Next** on the **Certificate Store** screen.
8. Click **Finish** on the **Completing the Certificate Import Wizard** screen.
9. When the "Import was successful" message displays, click **OK**.

Creating an additional backup of HLH files

This procedure is optional for customers who want to create an additional backup of HLH files prior to beginning the OS migration.

The steps must be performed before executing `Start-UpdateBundle.cmd`.

Procedure

1. Map a network share to a drive letter. For instance, W:.
2. On the network share, create a folder called "W:\HPEBackup".
3. On the network share, create another folder called "W:\Update_Migration".
4. Copy C:\update-bundle-4.1.2.XX\hpe\Update" from HLH to "W:\Update_Migration".
5. Copy the following files and folders from HLH to"W:\HPEBackup".
    - C:\CDW\
    - C:\CDW.FINAL\
    - C:\hpe\admin-tools\Security\CustomerDefinedAcls.csv
    - C:\hpe\admin-tools\Security\CustomerDefinedFirewallRules.csv
    - C:\hpe\logs\

- C:\hpe\OneView\posh\
- C:\hpe\OneView\SPP\

Manually restoring files after installing Windows 2019

This procedure is optional for customers who want to create an additional backup of HLH files prior to beginning the OS migration, in the case that V: does not contain the HLH backup files.

Procedure

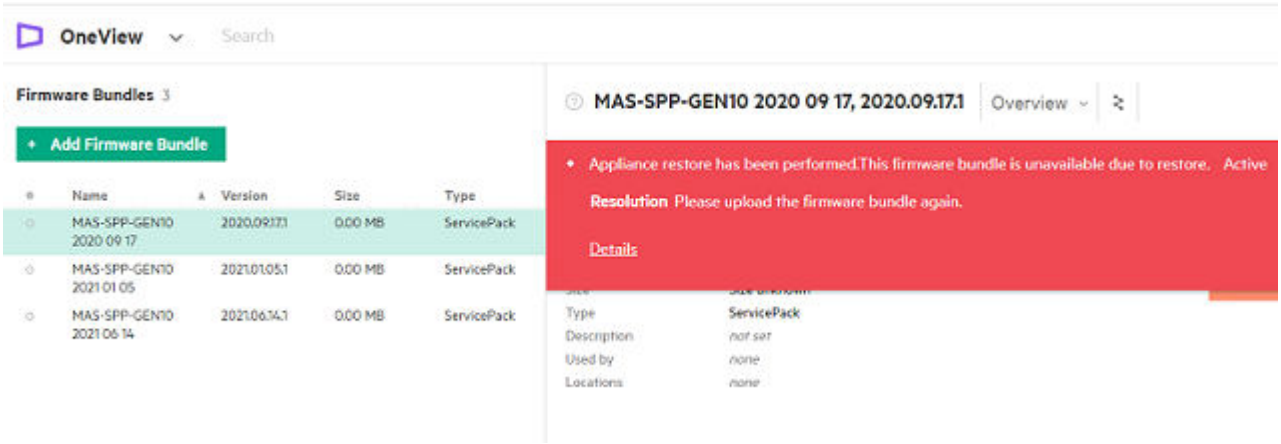
1. Copy the **HPEBackup** folder from “W:” to V:\HPEBackup. This folder needs to be created if it does not exist.
2. Copy the **Update_Migration** folder from “W:” to V:\ Update_Migration. This folder needs to be created if it does not exist.

Clearing stale/errored custom SPPs from the HPE OneView appliance

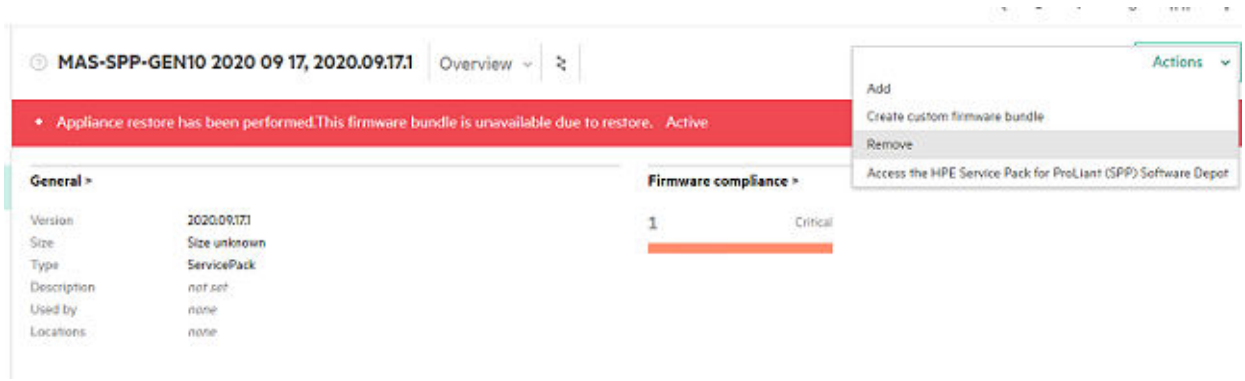
When the HPE OneView appliance is restored using its backup, it restores only configuration and settings, not the SPP’s. To restore the SPPs, use the procedure below to clear the errored entries on the Firmware Bundle page.

Procedure

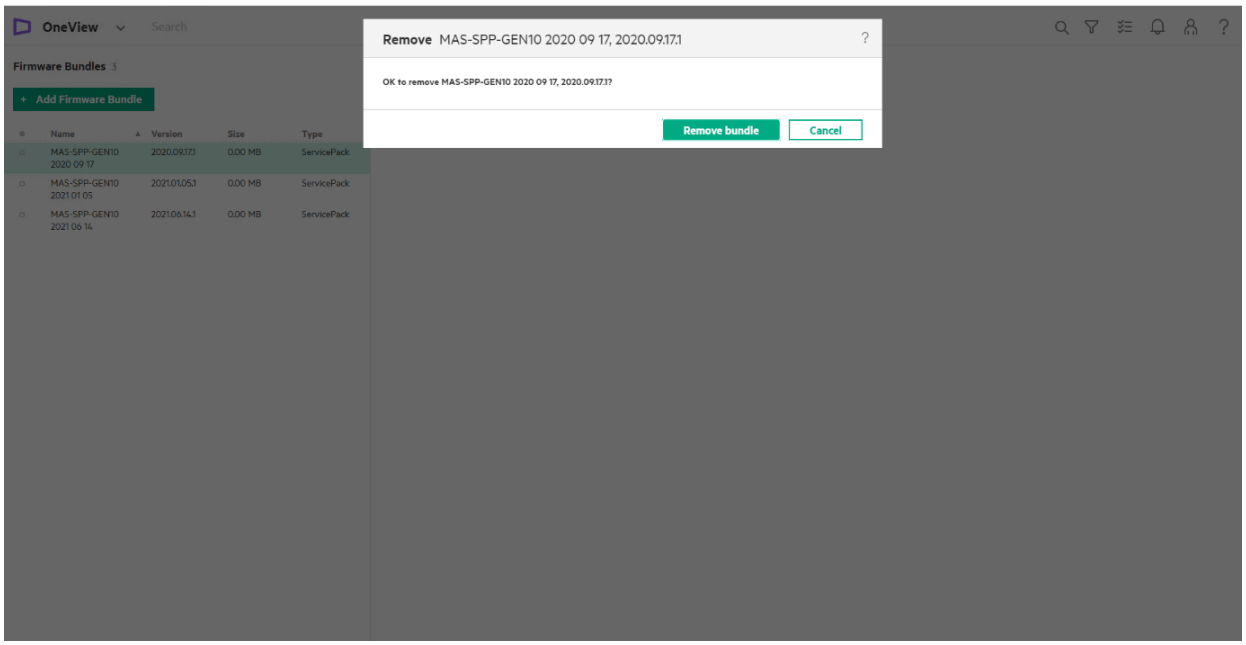
1. Log in to the HPE OneView appliance.
2. Navigate to the **Firmware Bundle** page.
3. Select the SPP error and follow the instructions below for each.



a. Click **Actions** > **Remove**.



b. Click **Remove bundle**.



c. Refresh the Firmware Bundle page to clear deleted entries.

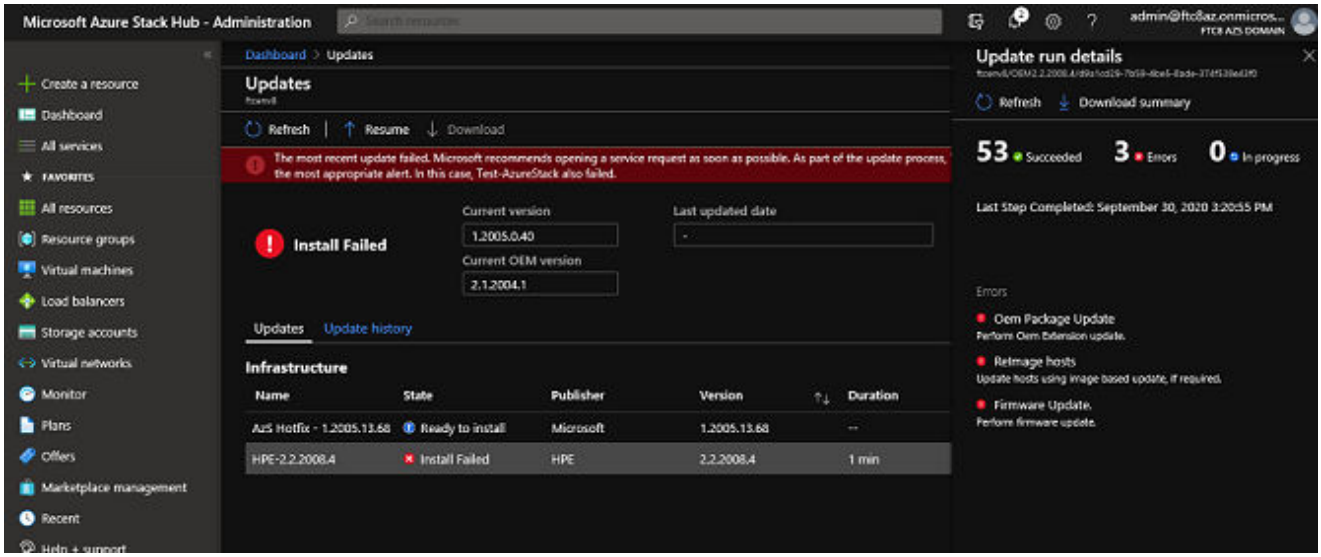
Known issues

This section includes information about known issues with the Solution Update Bundle. Where possible, suggested temporary fixes or workarounds are given.

OEM installation may fail during "Firmware Update" stage

Symptom

In the Admin portal, the OEM bundle installation may fail during the "Firmware update" stage and display the error message, "The RPC server is unavailable."



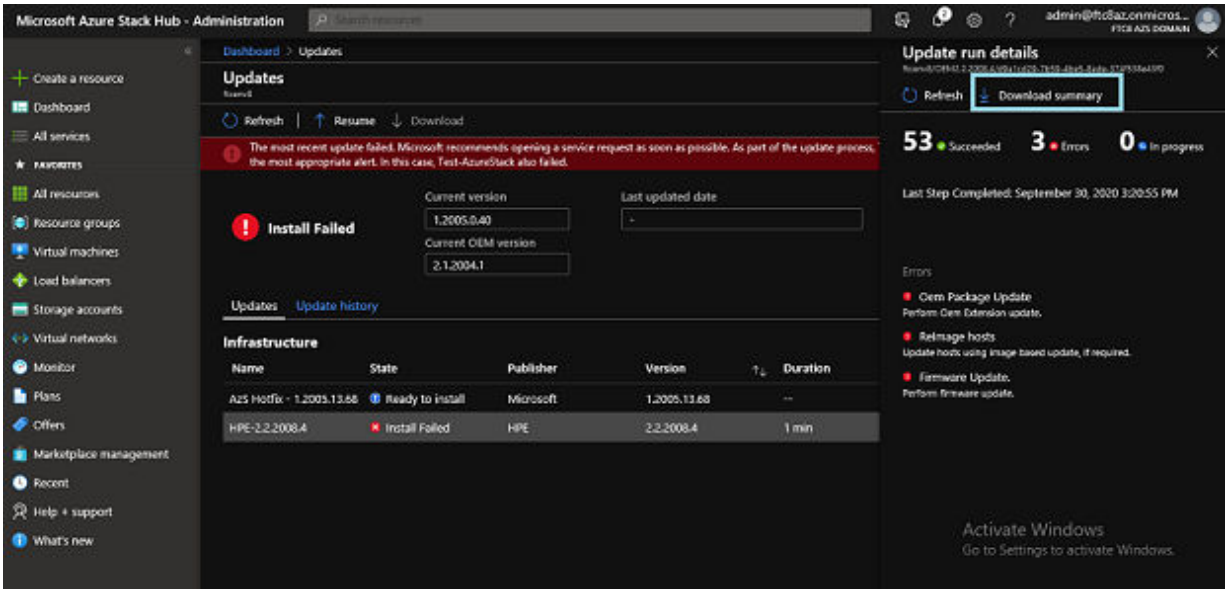
Cause

The OEM orchestration process is unable to shutdown the node, which is stopped by Azure Stack Hub during the installation procedure.

Action

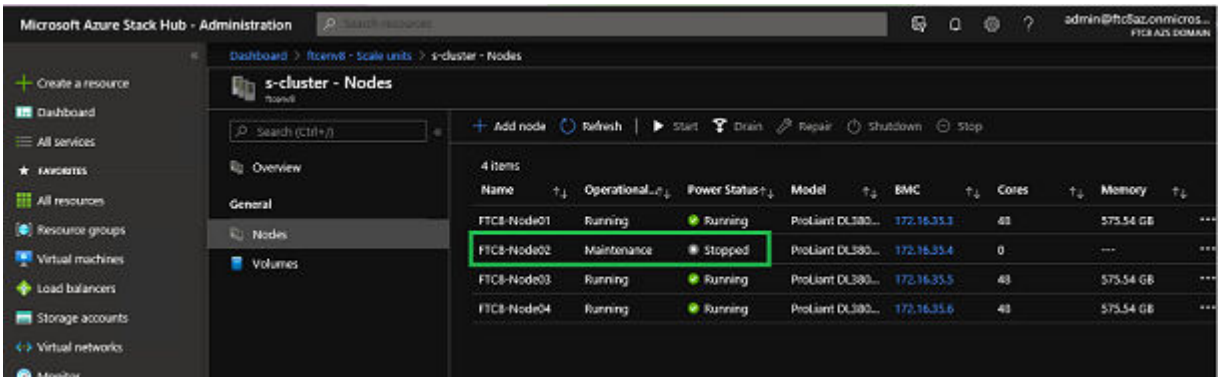
1. Confirm the issue.

    a. Download the update summary from the admin portal.

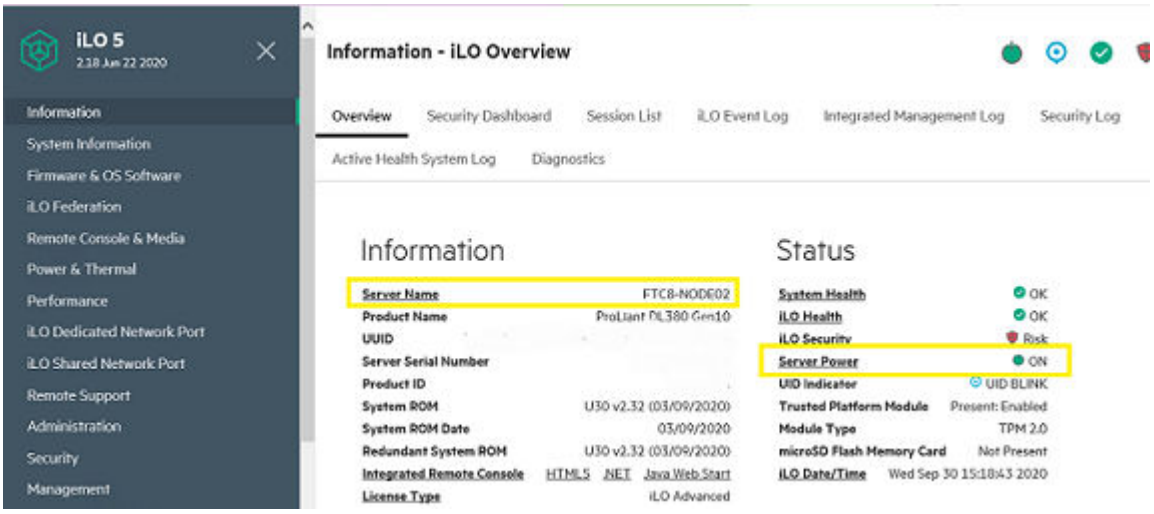


b. Open the update summary in Notepad and search for "**The RPC server is unavailable**".

c. In the Admin portal, go to **Dashboard** > **Scale Units** > **S-cluster** > **Nodes**, check for the "Stopped" node power status.



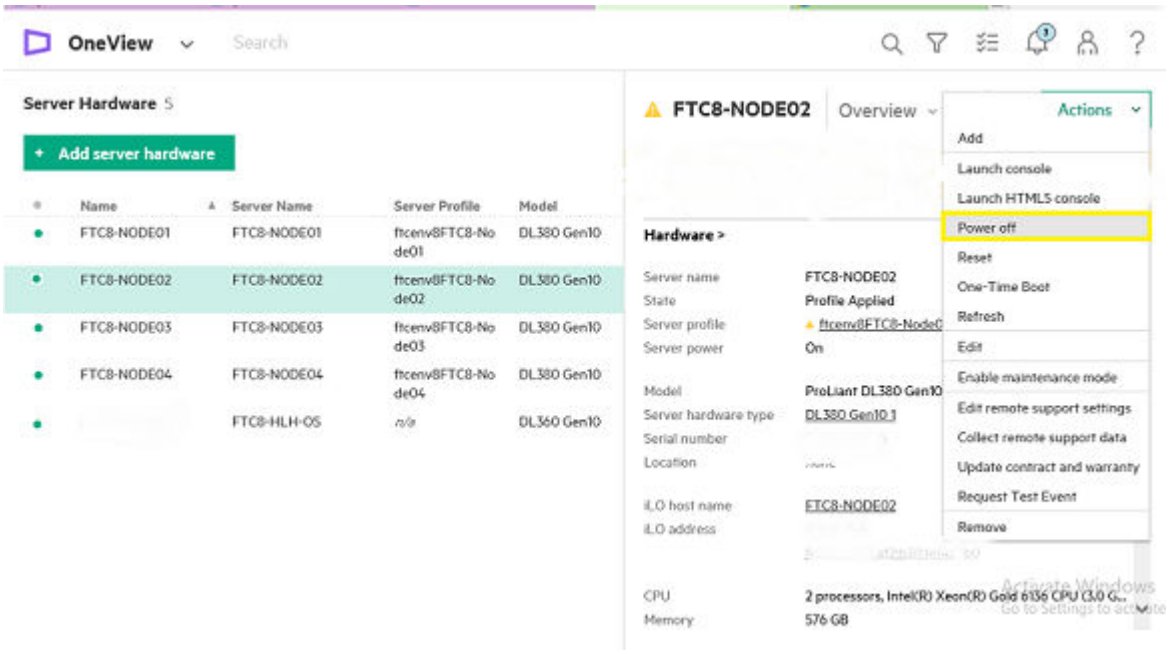
d. Open the iLO of the "Stopped" node and check to see that the node power status is "On".



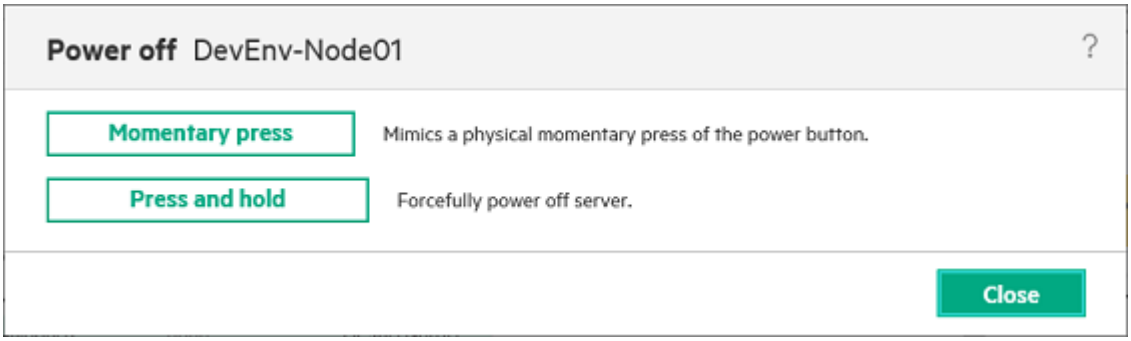
2. If the conditions above match, then proceed with the following:

   OEM installation can be resumed after changing the power state of the "Stopped" node to "Off" from HPE OneView.

   a. Log in to HPE OneView and go to **OneView** > **Server Hardware**. Select **Power off** from the **Actions** dropdown menu.



   b. Select the **Press and hold** option.



c. Verify that no critical alarms are present in HPE OneView.

d. Resume the OEM installation from the Admin portal.

Start-UpdateBundle.cmd occasionally fails in rerun scenarios

Symptom

A failure displays in the Start-preOSUpgrade PowerShell window log, although all steps in the UberInstaller window show success.

Cause

Uberinstaller.exe returns an invalid process ID on a rerun (sporadic issue).

Action

1. Close the Installer dashboard window.
2. On the PowerShell window, press Enter to exit the update bundle installation process.
3. Rerun Start-UpdateBundle.cmd.

Start-postOSUpgrade.ps1 occasionally fails in rerun scenarios

Symptom

A failure displays in the Start-postOSUpgrade PowerShell window log, although all steps in the UberInstaller window show success.

Cause

Uberinstaller.exe returns an invalid process ID on a rerun (sporadic issue).

Action

1. Close the Installer dashboard window.
2. On the PowerShell window, press Enter to exit the update bundle installation process.
3. Rerun Start-postOSUpgrade.ps1.
4. After successful completion of the last action, the OS reboots and Complete-Migration.ps1 is automatically invoked.

The restored user account is disabled during postOSUpgrade

Symptom

After restoring users/groups during the postOSUpgrade phase, the users/groups will be in disabled state.

Cause

While exporting users/groups, user passwords are not migrated. This is the design of Windows Server Migration Cmdlets. Only the "User Name" and "Account is Disabled" properties are migrated.

Action

User passwords are not migrated. Create a password when logging in to the server for the first time.

Start-UpdateBundle.cmd fails to initiate Start-UpdateBundle.ps1 after CDS

Symptom

Start-UpdateBundle.cmd fails to start Start-UpdateBundle.ps1, and displays the error “FullyQualifiedErrorId : DotSourceNotSupported”.

Cause

“FullyQualifiedErrorId : DotSourceNotSupported”.

Action

1. Disable Device Guard.
   a. Go to `c:\hpe\admin-tools\DeviceGuard\`.
   b. Execute Toggle-PolicyRestrictions.ps1 -Action Disable.

2. Reboot the HLH to deactivate device guard.
3. Rerun Start-UpdateBundle.cmd.

Software version of "Identifiers for Intel Xeon Scalable Processors (First and Second Generation) for Windows" doesn't match expected versions on HLH from TestHPENodes report

Symptom

Software version of "Identifiers for Intel Xeon Scalable Processors (First and Second Generation) for Windows" doesn't match expected versions on HLH from TestHPENodes report, even though the software has been updated successfully.

Action

This is a known issue with this component. No action needed.

Enhancements and fixed issues

These issues have been fixed since the previous version of this system Update Bundle Installation Guide.

Enhancements

- Updated HPE OneView appliance to version 7.00.00.
- Refined OS Migration workflow the HLH OS upgrade from Windows Server 2016 to Windows Server 2019.
- Optimized log messages and log modules.
- Enhanced OAW creation with CDW input parameters.
- Enhanced Invoke-HPEAzureStackDeployment.ps1 by adding precheck for password length and complexity.

Fixes

- Fixed Reset option on Start-MainFactoryInstall script.
- Removed unwanted warning messages in Start-UpdateBundle.cmd execution and improved log messages.

- Fixed Admin Portal credentials validation.
- Fixed HPE iLO version mismatch on HLH.
- HPE OneView POSH library fix on 5.4.
- Security Fix for exception handling.
- Fixed cleanup schedule task from 4.0 update bundle.

Additional resources and helpful links

HPE ProLiant for Microsoft Azure Stack documentation

http://hpe.com/info/PL-MSFT-Azure-docs

Microsoft Azure Stack operator documentation

https://docs.microsoft.com/en-us/azure/azure-stack/

Microsoft Azure Stack updates

https://docs.microsoft.com/en-us/azure-stack/operator/release-notes

Microsoft Azure Stack node actions

https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-node-actions

Learn more

http://www.hpe.com/info/PL-MSFT-Azure-docs

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

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

  Hewlett Packard Enterprise Support Center: Software downloads

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

My HPE Software Center

https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

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

> **IMPORTANT:**
> Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Onepass set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Pointnext Tech Care

https://www.hpe.com/services/techcare

HPE Complete Care

https://www.hpe.com/services/completecare

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider.

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

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 (located 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. All document information is captured by the process.