Hewlett Packard Enterprise

Cloud Service Automation

Software version: 4.70.0002
For Microsoft Windows® and Linux operating systems

Patch Read Me

Document Release Date:	December 2016
Software Release Date:	December 2016

Contents

Introduction

This readme describes the fixed issues and known issues in this patch and provides instructions for installing and configuring the patch on a Linux or Windows HPE Cloud Service Automation (CSA) server. The cumulative patch updates the CSA server to 04.70.002.

What's new with this Patch?

- **10 minutes delay for first time user login to CSA or MPP portal is resolved**

  Unlike CSA 4.7 and CSA 4.7 Patch 1, users belonging to a group added to an Organization's access control do not have to wait for 10 minutes for first time login to CSA or MPP portal.

- **The CSA or MPP portal is immediately accessible to users, once the group or the user is added to the Organization's access control**

- **Improved performance while saving designs, offerings and submitting requests for MS SQL Database**

  In CSA 4.7 and CSA 4.7 Patch 1, randomly located data could lead to filling up DB server memory and degradation of some data intensive operations like saving designs, offerings and submitting requests. With this patch, we are using related tabular data which are co-located in MSSQL database. This approach ensures that less memory is consumed for MSSQL caches.

- **Nested level property for LDAP nested groups should be explicitly set in aplicationContext.properties**

  From 4.7 Patch 2 onwards, nested groups should be enabled by setting the property **idm.ldap.nested_group_level** in %CSA_HOME%/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties file.

  The value set for the nested group level property denotes the nested group level instead of nested group depth unlike the previous versions.

  For example, idm.ldap.nested_group_level= <<value>>

  Where <<value>> denotes the nesting level. A value of 1 denotes the **top most group in the group hierarchy** as the maximum supported nested level.

  Users upgrading from CSA 4.7 and CSA 4.7 Patch1 should manually set the nesting level in **ApplicationContext.properties** file for nested groups to work properly.

Fixed Issues

The fixed issues in this patch are described in the table below.

Note: This patch includes several critical updates that are recommended for our customers apart from the items listed below.

Issue	Description
QCCR1D227441	The LDAP user is unable to login to CSA or Marketplace Portal immediately after access control configuration in the organization due to IdM - Async Roster API causing delay in the LDAP group and CSA sync.
QCCR1D227500	IdM - After creating an organization and configuring LDAP, the user should be able to login instead it takes around 10 mins to allow user to login.
QCCR1D228864	Exponential degradation in MPP Submit request (Order new subscription API) under load after 40 hours of load test.
QCCR1D228865	Exponential degradation in SMC Clone SO (Save as) under load after 40 hours of load test.
QCCR1D228866	Exponential degradation in SMC Clone SD (Save as) under load after 40 hours of load test.
QCCR1D229839	CSA/Propel: Transfer Subscription Failed.
QCCR1D230349	Unable to transfer ownership for service subscription from a user to an organization admin.
QCCR1D230418	IdM - Named Group Approver is not working when SAML is enabled on the Consumer Organization.
QCCR1D230521	When existing users are removed from catalogs and then added back in access control, 503 service unavailable error is displayed.
QCCR1D230556	Unable to transfer ownership of subscriptions from CSA/Propel.
QCCR1D230601	When consumer organization admin tries to add group approval policy in MPP, an error is displayed and gets logged out of MPP.
QCCR1D232011	When the user is on SMC dashboard, IdM - Session timeout error is displayed.
QCCR1D230273	When a lifecycle action fails due to an exception, the ActionProcessCallBackHandler is not handling error conditions by lifecycle actions. As a result, failed service instance/subscription get stuck in “Deploying” and “Pending” state instead of going to “Failed” and “Terminated”.
QCCR1D230777	When a flow is moved to a new location and an action is recreated pointing to that flow, the underlying process definition is not updated with the new location of the flow.
QCCR1D232562	CSA 4.7 Organization UI and MPP do not come up if host name has underscore.

Known issues

The remaining known issues in this patch are described in the below table.

Issues	Description
QCCR1D233897	Problem : On logging in to an organization through CSA REST API after the DN to which the user belongs is added in access control, the system requires a minimum delay of 10 minutes for first time login. Workaround : No workaround available.
QCCR1D229855	Problem : CSANG Adapter Recipient need to be the Subscription Owner Not the Submitter. Workaround : Steps: 1. Login to propel provider UI. 2. Go to "Content Management". 3. Locate CSA request to fulfillment and download it. 4. Unpack the archive and navigate to *csa-ng-r2f\sx\templates*. 5. Edit the createReqUrl.ftl. 6. Locate line starting with */api/consumption/v2....* and Change line content to: */api/consumption/v2/request/?onBehalf=${message.inputEntity.summary.recipient}&onBehalfOrg=${instanceConfig.sxInfo.organization}*. 7. Pack the content. 8. Upload modified content pack back to Propel.
QCCR1D217764	Problem : Cannot launch the show performance page using SSO from MPP. Cause : Upload modified content pack back to Propel Workaround : No workaround available.
QCCR1D230291	Problem : Not able to bring up the MPP Login page in Cluster environment. Cause : This happens because of the double encryption of `the idm.encryptedSigningKey` in the standalone instance. Workaround : No workaround available.
QCCR1D228633	Problem : Login to Provider organization with LDAP is not working when SAML is enabled in 4.7 upgrade setup. Cause : When SAML is configured, LDAP representation with absolute DN is expected for successful login, but relative DN is available in upgrade setup. Workaround : Update the existing DN in access control of provider organization.
QCCR1D227922	Problem : Organization LDAP Configuration - Invalid Hostname or Port shows wrong error message. Workaround : Hewlett Packard Enterprise (HPE) has been unable to reproduce this issue. If the same behavior still exists and you can reproduce it, please contact Hewlett Packard Enterprise Software Support referencing this document. Be

Issues	Description
	prepared to provide the exact steps to reproduce and/or demonstrate the steps and environment details to Software Support. The current Change Request will remain in HPE's database for future reference.
QCCR1D230356	Problem : Cannot launch the show performance page using SSO from MPP. Cause : Cannot launch the show performance page using SSO from MPP. Workaround : User can login to Cloud Optimizer manually by entering username and password.

QCCR1D230507	Problem : Kafka service is not starting/stopping.
	Cause : Introduced new commands to enable/disable Kafka service in Cloud Optimizer.
	Workaround : To check Status/Enable/Disable kafka, please find below commands:
	
	<u>To check kafka status:</u>
	`# OVC`
	`hpcsrvd HPCS`
	`Server AGENT,OA (1213)`
	`Running`
	`hpekafka HPE Kafka`
	`Service CORE,SERVER (1364) Runn`
	`ing`
	`hpezookeeper HPE Zookeeper`
	`Service CORE,SERVER (989) Running`
	`ovbbccb OV Communication`
	`Broker CORE (1187) Running`
	`ovcd OV`
	`Control CORE (1115)`
	`Running`
	`ovtomcatB OV Tomcat(B) Servlet`
	`Container WEB,SERVER (1858) Running`
	`pvcd PV`
	`Core PV (6127)`
	`Running`
	
	<u>To Enable kafka:</u>
	# /opt/OV/bin/msgbus.sh -enable
	`========== Current Messagebus`
	`Configuration ==========`
	`HPEKafka and HPEZookeeper are disabled.`
	`==========`
	`==========`
	`Enabling Msgbus`
	`Registering HPEKafka and HPEZookeeper`
	`Starting HPEZookeeper and HPEKafka`
	`==========`
	`==========`
	
	<u>To Disable kafka:</u>

Issues	Description
	# /opt/OV/bin/msgbus.sh -disable ========== ========== Disabling Msgbus Stopping HPEZookeeper and HPEKafka Unregistering HPEKafka and HPEZookeeper ========== New Messagebus Configuration ========== HPEKafka and HPEZookeeper are disabled. ========== ==========
QCCR1D218883	Problem : Custom changes in Elasticsearch configuration may be discarded during an HA upgrade installation. Cause : Product defect. Workaround : Custom changes from upgraded installation are stored in a backup folder in `/elasticsearch/config/`. Transfer custom changes from the older installation file into the upgraded file.

QCCR1D219172	Problem : Logging to MPP using a personal identity verification (PIV) card fails after upgrading from CSA 4.5 to CSA 4.6. This issue is seen only in Linux environments.
	Cause : The default HPE SSO value is incorrect in the CSA 4.5 environment prior to the upgrade. The upgrade process does not properly update the idm.war file, resulting in HP SSO not functioning correctly after the upgrade.
	Workaround : Edit the `idm.war/WEB-INF/web.xml` file.
	Find the section below:
	`<listener>`
	`<listener-class>com.hp.hpsso.HpSsoContextListener</listener-class>`
	`</listener>`
	`<context-param>`
	`<param-name>com.hp.sw.bto.ast.security.lwsso.conf.fileLocation</param-name>`
	`<param-value>/usr/local/hp/csa/jboss-as/standalone/deployments/idm-service.war/WEB-INF/web.xml</param-value>`
	`</context-param>`.
	Now change - `web.xml`
	To
	`hpssoConfig.xml`. and then restart the CSA service

QCCR1D222070 (225115)	Problem : Providers not defined in a resource environment are used during provisioning when internal actions for building and selecting from a resource provider list are not used.

Issues	Description
	Cause : Filtering is not done when internal actions are not used to identify providers that can be used during provisioning. This is a product limitation. Workaround : No workaround available.
QCCR1D224553	Problem : When creating or editing a string property on a component type or component template in the Designs / Sequenced / Components areas of the Cloud Service Management Console, the **Property Value** input may not be visible. Cause : Product defect. Workaround : Close the dialog and refresh the current page. Re-open the dialog again.
QCCR1D225958	Problem : Missing data points when VM is powered Off or Suspended. Cause : Unable to plot the graph for missing data points. Workaround : No workaround available.
QCCR1D226184	Problem : In Operation Console for Service Instance upgrade: • Existing actions display name get changed after upgrade. • Source column shows original Resource Offering display name for upgrading actions instead of its own Resource Offering display name. Cause : If the Resource Offering for upgrade was created by doing save as from the original Resource Offering and Initializing, Reserving, and Deploying lifecycle actions are kept as is, but display name is being modified for them. In that case all the existing actions would get new display name from new Resource Offering. Workaround : No workaround available.
QCCR1D226494	Problem : The Featured Category list is empty for a newly created organization. Cause : The organization data synchronization is not complete after a new organization is created in IDM tables. Workaround : After the synchronization is completed, the catalogs and featured category list will appear. (~30 seconds).
QCCR1D227598	Problem : SAML authorization does not work if the access control is configured with the LDAP sub tree. Cause : CSA does not support the LDAP sub tree for Access Control (ACL) when SAML is enabled. Workaround : No workaround available.
QCCR1D227675	Problem : Infrastructure monitoring health status information is not available for infrastructure servers in Market place portal and Server Management Console even after configuring the Cloud Optimizer provider.

Issues	Description
	Cause : This feature cannot be enabled with the current version of Cloud Optimizer. Workaround : If you are subscribed for email notifications of CSA 4.7 documentation updates, you will be notified when the CSA 4.7 Support Matrix is updated with information about the supported version of Cloud Optimizer.
QCCR1D228220	Problem : Health status is not updated for servers deployed on Helion Openstack (HOS) provider. Cause : CSA is unable to retrieve the health status since Cloud Optimizer (CO) is not supporting HOS 3.0. Workaround : It is a product limitation. No workaround available.
QCCR1D228293	Problem : Unable to launch MPP Organization created with special character-2894. Cause : Customers with already existing special character organization names will not be able to access MPP after upgrading to 4.7. Workaround : Change the organization name and ensure not to have any special characters in the name.
QCCR1D228421	Problem : When SSO is enabled, Operation Orchestration (OO) does not prompt for login after CSA tokenGlobaltimeout is elapsed. Cause : SSO configuration differs in CSA and OO and settings is not fully compatible. Workaround : Steps: 1. SSO in CSA is configured in CSA\jboss-as\standalone\deployments\idm-service.war\WEB-INF\hpssoConfig.xml, • See tokenGlobalTimeout and tokenIdleTimeout parameters. 2. SSO in OO is configured in OO\central\tomcat\webapps\oo\WEB-INF\classes\lwssofmconf.xml, • See expirationPeriod parameter, which corresponds to tokenIdleTimeout in CSA. 3. Check if both values are in sync. **Note:** However, there is no counterpart for tokenGlobalTimeout in OO.
QCCR1D228600	Problem : Cannot use groups in Service Management Console that were created through Artifact API with name containing characters other than alphanumeric and hyphen (-). Cause : There is no group name validation in Artifact API. Workaround : Use only alphanumeric characters or '-' for group name when creating group through Artifact API.
QCCR1D228619	Problem : Global search from MPP portal does not work in a Linux CSA installation.

Issues	Description
	Cause : CSA Search service fails to update the Elastic search indices as a result of which Global search from MPP returns nothing. Workaround : After CSA installation is complete, or after restarting CSA, stop the CSA Search service and restart it manually by following the steps below: If CSA was installed in a location other than /usr/local/hp/csa, adjust the path accordingly.
QCCR1D228672	Problem : Cannot launch the show performance page using SSO from MPP. Cause : SSO token is not passed correctly. Workaround : User can login to Cloud Optimizer manually by entering username and password.
QCCR1D228716	Problem : Transfer ownership operation fails even after the ownership is successfully transferred. It happens only when the user has different name and display name. Cause : It is caused by implementation of checkTransferOwnershipResponse.ftl * input message contains user's full name (User15), but user's name (user15) - comparison fails (upper case vs lower case), so request is marked as failed. Input message : "flatFields" : [{ "id" : "transferTo", "value" : "User15", "type" : "DROPDOWN_LIST" }], Workaround : This is not a functional problem. Only the message about the result of the ownership transfer is wrong but the transfer is successful. Therefore workaround is either ignoring the "failed status" of the transfer ownership or avoiding usage of users with different name and display name.
QCCR1D228726	Problem : Launching help content for adding upgrade path in offerings throws page not found error. Cause : No topic ID is defined for the help icon on that dialog box. Workaround : Open the help and navigate to Deploy > Offerings > Upgradability for a topic on upgradability.
QCCR1D229537	Problem : Cannot upgrade to CSA 4.7 when Base DN in LDAP tab in the Organization detail is empty (Oracle only). Cause : Software defect.

Issues	Description
	Workaround : If upgrade has already started and stopped with an error, update the Base DN directly in the Database. Set the base_dn column in the csa_ldap_access_point table for each record that is present in the table. The Base DN is last part of the LDAP Full DN. It can be "dn=company,dn=com" if full dn of some group is "cn=group1,dn=company,dn=com". It depends on the LDAP settings. Stop CSA and install upgrade again.
QCCR1D220470	Problem : After applying the patch, custom changes related to cluster are not retained. Cause : Cluster environment fails after installation of patch if CSA is configured in high-availability mode. Workaround : From %CSA_HOME%/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext.xml Replace this: <!--START HA Mode Configuration--> <!-- <jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/> <!--END HA Mode Configuration--> With this: <!--START HA Mode Configuration--> <jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/> <!--END HA Mode Configuration--> Restart the services of CSA after all the above changes made.
QCCR1D233719	Problem : Market Place Portal organization fails to load with invalid tenant when the created organization has $ symbol in Org Name. Workaround : No workaround available.

Patch Installation

This section describes how to install the patch.

Check Pre-installation Requirements

Ensure the below prerequisites are fulfilled before installing:

1. Check minimum hardware requirements:
   - CPU: 4 CPU, 3.0 GHz
   - RAM: 8 GB
   - Hard Drive: 20 GB
2. Check the CSA 4.70 Support Matrix to verify operating-system requirements.
3. Check minimum software requirements:
   - CSA version 4.70.0000
4. Set the CSA_HOME environment variable:

   In case of remote MPP installation, please ensure that CSA_HOME environment variable is set.
   - **Windows:** Set the CSA_HOME environment variable to point to the CSA installed location.

     Eg: C:\Program Files\HPE\CSA
   - **Linux**: Set the CSA_HOME environment variable to point to the CSA installed location

     `Eg: /usr/local/hpe/csa`
5. Back up your CSA environment.
6. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, the installation might fail and CSA might be left in an unstable state.
7. Stop the following CSA services: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service and Elasticsearch 1.6.1 (elasticsearch-service-x64).

   Important: You must stop these services on each node in a cluster.
   Note: If you do not stop these services manually, the following folders will not be cleared and will cause UI issues after installing the patch:

   - **Windows**: `<CSA_HOME>\jboss-as\standalone\tmp`
   - **Linux**: `/usr/local/hpe/csa/jboss-as/standalone/tmp`

Install the Patch

Use the following procedure to install the patch in a standalone configuration or on *each* node of a cluster:

1. Download the CSA patch file:

   - **Linux:** https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00037
   - **Windows:** https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00036

For Linux:

Note: For clusters, perform all steps on each node in a cluster.

a. Extract the downloaded file: `HPE_CSA_Patch_04.70.0002.bin` file from the patch file.
b. Ensure that the `csauser` user is the owner of the file and has full privileges.
c. Log in as `csauser` and run `HPE_CSA_Patch_04.70.0002.bin` to open the CSA patch installer console mode.
d. Enter `./HPE_CSA_Patch_04.70.0002.bin` to run the patch installer.
e. Select **Enter** in the introduction, warnings, and prerequisites screens.
f. In the environment dialog screen, select **Standalone** or **Cluster** environment, then click **Enter**.
g. In the set-up screen, select your set-up option:
   - CSA and MPP are installed
   - Only MPP is installed

   Note: If you select **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
h. Click **Enter**.
i. In the pre-installation summary dialog screen, click **Enter**.

   The patch installer begins the installation.
j. When prompted, click **Enter** to exit the installation.

For Windows:

a. Extract the `HP_CSA_Patch_04.70.0002.exe` file from the patch zip file.
b. Run `HP_CSA_Patch_04.70.0002.exe` to launch the installation wizard.
c. Click **Next** to open the CSA Environment Selection wizard.
d. Select **Standalone** or **Cluster** environment, then click **Next**.
e. Select your set-up option:
   - CSA and MPP are installed
   - Only MPP is installed

   Note: If you select **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
f. Click **Install** to run the patch installation.
g. When prompted, click **Done** to exit the installation.

Verify the Patch Installation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the installation on each node.

1. Check for errors in the log files:

   - **Windows:** `<CSA_HOME>\_CSA_4_70_2_installation\Logs`
   - **Linux:** `$CSA_HOME/_CSA_4_70_2_installation/Logs`
     Log files include `csa_install.log` and `csa_InstallPatch.log`.

   Note: If there are errors, create a backup of the log files, restore the backup of the `CSA_HOME` directory, and contact HPE Support.

2. Clear the browser cache.
3. Ensure the HPE Cloud Service Automation, Marketplace Portal, HPE Search, and Elasticsearch services 1.6.1 (elasticsearch-service-x64) are running:

   - **Windows:** Installer automatically starts these services.
   - **Linux:** Start the services manually. In a cluster environment, manually start the services on all nodes.

4. Launch the CSA Console, log in and check for the updated version.

Patch Removal - Linux

This section provides the steps to uninstall the patch on a Linux server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

Before Uninstalling the Patch

Complete the following preparation steps before you uninstall the patch:

1. Backup the CSA environment.
2. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, uninstallation might fail and CSA might be left in an unstable state.

3. Sign out of all open instances of the CSA Provider Console and Marketplace Portal.
4. Stop the following CSA services: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service, and Elasticsearch 1.6.1 (elasticsearch-service-x64).

   Important: You must stop these services on each node in a cluster.

Uninstall the Patch on Standalone and Cluster CSA Servers

To uninstall the patch:

1. Navigate to `$CSA_HOME/_CSA_4_70_2_installation/Uninstaller`.
2. Run `./Uninstall HPE Cloud Service Automation Patch` to start the uninstaller console mode.
3. Click **Enter** for the introductory and warning screens.
4. Click **Enter** to run the patch uninstaller.
5. When the patch uninstallation is complete, click **Enter** to exit the uninstallation process.

Patch Removal - Windows

This section provides the steps to uninstall the patch on a Windows server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

Before Uninstalling the Patch

Complete the following preparation steps before you uninstall the patch:

1. Backup the CSA environment.
2. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, the uninstallation might fail and CSA might be left in an unstable state.
3. Sign out of all open instances of the CSA Provider Console and Marketplace Portal.
4. Stop the following CSA services: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service, and Elasticsearch 1.6.1 (elasticsearch-service-x64).

   Important: You must stop these services on each node in a cluster.

Uninstalling the Patch on Standalone and Clustered Environments

You can uninstall the patch using either of the following methods:

- Using the Control Panel
- Using the Uninstall Cloud Service Automation Patch wizard

Note: For clustered environments, perform the steps on each node of the cluster after stopping the services on all nodes.

To uninstall the patch using the Control Panel:

1. In the Control Panel, choose **Uninstall a program**.
2. Select **Cloud Service Automation Patch** and click **Uninstall**.

3. Follow the instructions on the uninstall wizard to uninstall the patch.

To uninstall the patch using the Uninstall Cloud Service Automation Patch wizard:

1. Navigate to `<CSA_HOME>\_CSA_4_70_2_installation\Uninstaller`.
2. Execute `Uninstall HPE Cloud Service Automation Patch.exe` to open the Uninstall Cloud Service Automation Patch wizard.
3. Click **Uninstall** to uninstall the patch.
4. Click **Done** to exit the uninstall wizard.

Patch Removal Verification

After uninstalling the patch, perform the following steps to verify the patch was removed. These verification steps apply to both standalone and clustered environments.

Note: For clustered environments, complete these steps on each node.

1. Check for errors in the log files:
   - **Windows:** `<CSA_HOME>\_CSA_4_70_2_installation\Logs`
   - **Linux:** `$CSA_HOME/_CSA_4_70_2_installation/Logs`
     Log files include `csa_uninstall.log`, and `csa_unInstallPatch.log`.

   Note: If there are errors, create a backup of the log files, restore the backup of the `CSA_HOME` directory, and contact HPE Support.
2. Clear the browser cache.
3. Ensure the HPE Cloud Service Automation, Marketplace Portal, HPE Search, and Elasticsearch 1.6.1 services are running:
   - **Windows:** The installer automatically starts these services.
   - **Linux:** Start the services manually. In a cluster environment, manually start the services on all nodes.

CSA Modified Files

```
<CSA_HOME>/jboss-as/standalone/deployments/csa.war/*
<CSA_HOME>/jboss-as/standalone/deployments/csa.war/idm-service.war/*
<CSA_HOME>/portal/*
<CSA_HOME>//CSAKit-4.7/Content Archives/topology/Jenkins plugin/HPE_Codar.hpi
<CSA_HOME>//CSAKit-4.7/Lib/service manager/HPSM_CSA_Integration_file.unl
<CSA_HOME>/Tools
```

Send Documentation Feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

Legal Notices

Warranty

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. The information contained herein is subject to change without notice.

Restricted Rights Legend

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.

Copyright Notice

© Copyright 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.
Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.
UNIX® is a registered trademark of The Open Group.
RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.
The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hpe.com.
Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.
You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hpe.com.