Hewlett Packard Enterprise

Cloud Service Automation

Software version: 4.70.0003
For Microsoft Windows® and Linux operating systems

Patch Read Me

Document release date: June 2017
Software release date: June 2017

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 04.70.003.

What's new with this Patch?

- **MPP provide users an option to renew a subscription before it expires.**

  This patch provides the ability to perpetually renew a particular subscription with restriction on the max term period. Please refer to the online help for further details.

- **Ability to set Subscription Start Time**

  With this patch we will be able to specify the Subscription Start Time, along with the Start Date.

- **Add Child Service Component API honor the Component Template parameter allowing us to create a child component based on an existing component template.**

- **HTML Notifications are supported for Service Instance Upgrade and Modify Subscription**

  Note: If we want the subscribers to know what are the additional features that are available as part of the Service Instance Upgrade, we need to include the required details in the description of the Service Offering.

- We have included a Tool named **Hotfix Deployer Tool**, to simplify the Deployment of hotfixes in this patch. The too is available at %CSA_HOME%/hotfixes/hotfixDeployer directory.

  Please refer to **Appendix A** of the **Patch Read Me** file for further details.

Fixed Issues

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

Issue ID	Description
QCCR1D226667	Add Child ServiceComponent API does not honor the Component Template parameter and hence cannot create a child component based on a component template
QCCR1D228276	While mentioning the reason for denying a subscription we are unable to use space characters once we press carriage return and move to a new line.
QCCR1D228706	Deployment cancellation failed (cancellation flows didn't start)
QCCR1D229381	When user request a service in MPP, after selecting an environment and provider, there is a delay with the dynamic list.
QCCR1D229434	Uploading a 15MB file to MPP request shows service unavailable
QCCR1D229750	CSA flow "Select Resource Provider" returns incorrect Resource Provider
QCCR1D229798	Component Property getting reset to empty on Modify Actions
QCCR1D230278	While trying to resubmit a failed Modification Request for a Subscription, no flows are launched and the action returns as a success.
QCCR1D230465	Most Requested Services fails for normal Consumer Users
QCCR1D230494	CSA Artifact API does not always return the createdOn timestamp in the expected format, when the milliseconds are .000
QCCR1D230501	Modification of service instances fails after deletion of Service Offering.
QCCR1D231730	Cannot see Service Offerings from a Service Design
QCCR1D232619	Provide users an option to renew subscription before it expires
QCCR1D232710	Constraint check for property fails in Service Offering module
QCCR1D232932	Link in email notifications from Server Deployments is incorrect
QCCR1D233049	Timeout not configurable for communication between CSA and Search Service. Currently timeout is Infinite PS: The default value of timeout between csa and search service is 30000ms (30s). This can be changed by modifying "csa.provider.msvc.esRequestTimeout" in csa.properties. The timeout is to be provided in milliseconds.
QCCR1D233486	User is able to delete a service offering based on which there are active service instances and thus break the upgrade chain.
QCCR1D233768	Token parameters on dynamic lists in user operations are not resolved
QCCR1D234224	Reduce the time taken for computing the association detail data during an import operation for Service Offering/Design
QCCR1D234559	MPP Regex validation passes on Modify page but fails during checkout.
QCCR1D234622	Error when trying to use the deployment function

Issue ID	Description
QCCR1D234919	Email notifications display subscriber.userId where subscriber.name is used
QCCR1D234923	Garbled Japanese characters in the csa organization page
QCCR1D235113	Ability to set Subscription Start Time
QCCR1D235803	Automatic Reloading of Configurations in Log4j2
QCCR1D235804	When use delegated approval to reject a request, reason for rejection is not displayed in the HTML Notification PS: When we use delegated approval template the reason for rejection is shown in the html email notification, but the approver names will not be present.
QCCR1D235824	MPP API requests with LDAP group DN are not working PS: Please set the property "csa.useLDAPNameForOwnerGroup" to true in csa.properties file for the changes to be effective after applying the patch.
QCCR1D236221	IDM Dependency (236224) - Tracking Defect - StaleObjectStateException in IDM during group user synchronization
QCCR1D236226	IDM Dependency (236215) - Tracking Defect - NPE is thrown when IDM cannot find the manager information provided by the LDAP server leading to thread leakage
QCCR1D236230	IDM Dependency (236231) - Tracking Defect - Reduce the serverity of messages printed by the authentication providers for a failed authentication from ERROR to WARNING
QCCR1D236247	IDM Dependency (236248) - Tracking Defect - Constraint key violation error messages are thrown in a cluster environment when IDM tries to acquire lock on the group representation object
QCCR1D236249	IDM Dependency (236251) - Tracking Defect - Lock issues on group object in cluster environment
QCCR1D236405	Can't import Service Design: error importing service design archive
QCCR1D236601	It is not possible to set the default value of a Static list option property at the offering layer
QCCR1D237111	Check of permissions which user is having by groupmembership missing in 4.70
QCCR1D237221	State of the service instance is sometimes shown as deploying when service health is enabled
QCCR1D237393	CSA api/mpp/mpp-subscription - response - changes between CSA4.2 and CSA4.7
QCCR1D237512	CSA cluster duplicate events problem
QCCR1D238248	Cannot import Ressource Offering from 4.60 in 4.70
QCCR1D239248	user/mycomponents API for a particular user returns the subscriptions details of other organization that the user does not belong to

Known issues

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

Issues	Description
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 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.

Issues	Description
	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: To check kafka status: # 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 To Enable kafka: # /opt/OV/bin/msgbus.sh -enable ====================== Current Messagebus Configuration ====================== HPEKafka and HPEZookeeper are disabled. ========== ========== Enabling Msgbus Registering HPEKafka and HPEZookeeper Starting HPEZookeeper and HPEKafka ========== ========== To Disable kafka: # /opt/OV/bin/msgbus.sh -disable ========== ========== Disabling Msgbus Stopping HPEZookeeper and HPEKafka Unregistering HPEKafka and HPEZookeeper

Issues	Description	
		===================== 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.
	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.

Issues	Description		
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.
	Cause	:	This feature cannot be enabled with the current version of Cloud Optimizer.

Issues	Description
	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. Cause : CSA Search service fails to update the Elastic search indices as a result of which Global search from MPP returns nothing.

Issues	Description		
	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.
	Workaround	:	If upgrade has already started and stopped with an error, update the Base DN directly in the Database.

Issues	Description	
		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.

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`
    Clustered environment: `<CSA_HOME>\jboss-as\domain\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_00047
   - **Windows**: https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00046

For Linux:

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

a. Extract the downloaded file: `HPE_CSA_Patch_04.70.0003.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_04.70.0003.bin` to open the CSA patch installer console mode.
d. Enter `./HPE_CSA_Patch_04.70.0003.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_04.70.0003.exe` file from the patch zip file.
b. Run `HP_CSA_Patch_04.70.0003.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_3_installation\Logs`
   - **Linux:** `$CSA_HOME/_CSA_4_70_3_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_3_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_3_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_3_installation\Logs`
   - **Linux:** `$CSA_HOME/_CSA_4_70_3_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
```

Appendix A

How to Use the HotfixDeployer tool

Windows:

a) Place the hotfixes zip files inside %CSA_HOME% /hotfixes folder.
b) Open a command prompt to the %CSA_HOME% /hotfixes/hotfixDeployer directory.

To deploy a fix :
../../node.js/node hotfixManger.js -deploy "hotfixName.zip"

e.g. C:\Program Files\HPE\CSA\hotfixes\hotfixDeployer>../../node.js/node hotfixManger.js –deploy QCCR1D23451.zip >> <QCCR ID>.zip

To undeploy the fix :

../../node.js/node hotfixManger.js -undeploy "hotfixName"

e.g. C:\Program Files\HPE\CSA\hotfixes\hotfixDeployer>../../node.js/node hotfixManger.js -undeploy QCCR1D23451 >> <QCCR ID>

List the hotfixes deployed:

../../node.js/node hotfixManger.js –list

List all the hotfixes – deployed and undeployed

../../node.js/node hotfixManger.js -listAll

Help - Displays the list of commands supported and their syntax
../../node.js/node hotfixManger.js -help

Linux:

a) Place the hotfixes zip files inside %CSA_HOME% /hotfixes folder.
b) Open a command prompt to the %CSA_HOME% /hotfixes/hotfixDeployer directory.

To deploy a fix :

../../node.js/bin/node hotfixManger.js -deploy "hotfixName.tar" >> hotfiName.zip

e.g. $../../node.js/bin/node hotfixManger.js -deploy QCCR1D23451.tar >> <QCCR ID>.zip

To undeploy the fix :
../../node.js/node hotfixManger.js -undeploy "hotfixName"
e.g. $../../node.js/node hotfixManger.js -undeploy QCCR1D23451 >> <QCCR ID>

List the hotfixes deployed:
../../node.js/bin/node hotfixManger.js -list

List all the hotfixes – deployed and undeployed

../../node.js/bin/node hotfixManger.js -listAll

Help - Displays the list of commands supported and their syntax

../../node.js/bin/node hotfixManger.js -help

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

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.