



Hewlett Packard
Enterprise

Cloud Service Automation

Software version: 4.80.0001

For Microsoft Windows® and Linux operating systems

Patch Read Me

Document release date: April 2017

Software release date: April 2017

Contents

Introduction	3
Fixed issues	3
Known issues	4
Patch installation	10
Check pre-installation requirements	10
Install the patch	11
Verify the patch installation	12
Patch removal - Linux	13
Before uninstalling the patch	13
Uninstall the patch on standalone and cluster CSA servers	13
Patch removal - Windows	14
Before uninstalling the patch	14
Uninstalling the patch on standalone and clustered environments	14
Patch removal verification	15
CSA modified files	15
Send documentation feedback	16
Legal notices	16

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 04.80.0001.

Fixed issues

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

The following table describes the issues that are fixed in this patch.

Issue	Description
QCCR1D235768	Existing Server 1.8 component - password output property - not usable.
QCCR1D235433	Jenkins Plug-in:- Deployment of a Sequenced Design does NOT utilize the Design Property Values provided from Jenkins Job.
QCCR1D235402	Pools Search Not working based on Filter Search criteria.
QCCR1D236121	Hyperlink is not working in IE 11 if the mouse is over the menu text, recognized only when the mouse is over the icon.
QCCR1D235756	Scroll Issue in Testrun (Multiple calls triggered when scrolled for more data).
QCCR1D235803	Automatic Reloading of Configurations in Log4j2.
QCCR1D235907	PCOE: Around 25% of Un-deploy with Scaling Designs are getting failed in OO Execution for Codar1.8 with ORACLE DB configuration.
QCCR1D235946	For CompositeDesign, the ContinuousPromote ReleaseGateDeployment done in final lifecycle stage does NOT use the property values configured in PackageProperties.
QCCR1D235133	XI Machine update API allows two machines to have a common IP Address.
QCCR1D235074	Codar Pilot: Release gate action with ignore on failure checked skips the approval action, promotes the package and creates multiple gate executions in parallel.
QCCR1D234984	Rolename should be displayed instead of Role ID when i try to add the Operator Users.
QCCR1D235717	Unable to execute ALM tests using test set release gate action after applying the latest hotfix.

Known issues

The following table describes the remaining known issues in this patch.

Issues	Description
QCCR1D234930	<p>Problem : Cloud Optimizer is not able to get CSA Organization LDAP details after fixing existing security vulnerability in HPE CSA</p> <p>Cause : Code fix is completed to close the security vulnerability. Please ensure to pass the userIdentifier to all the API calls as mentioned in CSA REST API Guide.</p> <p>Workaround : Hotfix available. Please contact support.</p>
QCCR1D228812	<p>Problem : The privacy statement does appear to show up on 4.8MR bits on the initial MPP login screen at /org/<ORG_NAME>. However, the next IDM screen you are navigated to when clicking Log in is where the issue lies. The screen apparently should, but does not show the privacy statement.</p> <p>Cause : Code defect.</p> <p>Workaround : The user could always manually go to the privacy link they have configured for the organizations privacy statement. This link is available in the Organizations > Organization Name > General Settings area. Or, the user could simply return back to the main portal login page to view the privacy link.</p>
QCCR1D235507	<p>Problem : Resuming a failed upgrade is failing on Oracle PCoE Environment because of the created_by and updated_by references in the scripts.</p> <p>Cause : Resuming a failed upgrade is failing and csa_CSA_4_80_0_installation\Logs\install.log contains error message that UPDATED_BY_ID columns is missing</p> <p>For example error message from Oracle database: PL/SQL: ORA-00904: "UPDATED_BY_ID": invalid identifier</p> <p>Workaround : Restore the database from backup taken prior upgrade and resume the upgrade again.</p>
QCCR1D227860	<p>Problem : Exception in log file, csa.log</p> <p>Cause : A bug in NodeJS. See https://github.com/nodejs/node/issues/712</p> <p>Workaround : A bug in NodeJS. See https://github.com/nodejs/node/issues/712</p>
QCCR1D229293	<p>Problem : Operation Orchestration displays: 403 Error when trying to use direct link from HPE CSA using menu Workflows -> Orchestration in case that LDAP Users does not Exist in OO.</p> <p>Cause : Caused by defect QCCR8C32250 in product HPE Operation Orchestration</p> <p>Workaround : Modify URL of HPE Operation Orchestration to end with /oo/login/login-form or use seeded user admin for login to HPE CSA.</p>
QCCR1D232747	<p>Problem : When CSA is configured with HPSSO which is a default in 4.8 (documentation contains steps how to disable it for FIPS mode), it will fail to logout user from CSA when the user performs logout action in other integrated product like HPE OO followed by login as different user in HPE OO.</p> <p>HPSSO does not have central server to handle logout. Programs using HPSSO do not need to know each other as long as shared secret used for encryption and validation of cookie is same.</p>

Issues	Description
	<p>Cause : In CSA the Management Console in <code>csa.war</code> uses IdM tokens as means to authenticate users. HPSSO tokens are recognized only by Identity Management (IdM) component, but not by CSA Management Console. When there is no session with Management console, the <code>csa.war</code> will redirect user to IdM which will validate and consume HPSSO cookie to produce IdM token for Management Console.</p> <p>CSA Management Console will perform logout when it is accessed while the HPSSO cookie is missing (due to logout in other product which deletes the cookie).</p> <p>But if CSA Management Console is accessed after logout followed by login in other product, then it will not detect the logout (it does not inspect cookie contents, it cannot decrypt it, in CSA only IdM component can decrypt it) and keep session established with original user identified by IdM token.</p> <p>Sessions are still limited by token expiration. IdM tokens expire after 30 minutes by default, though there is process to extend their lifetime if done within these 30 minutes.</p> <p>Workaround : Multiple options:</p> <ul style="list-style-type: none"> • Turn off HPSSO if its functionality is not desirable. • Perform logout in CSA, not in HP E OO. • After performing logout in HPE OO, access HPE CSA so HPE CSA notices the cookie got deleted and it will perform logout, before continuing in to login as different user in HPE OO.
QCCR1D235119	<p>Problem : upgrade fails with "Read timed out" during processing "<code>csa_remove_createdby_updatedby.plsql</code>" file on SQL Server (check <code>CSA\CSA_4_80_0_installation\Logs\install.log</code> to ensure it)</p> <p>Cause : <code>csa_remove_createdby_updatedby.plsql</code> contains ALTER TABLE ... REBUILD statements that goes through all rows in table. So the REBUILD operation could timeout on huge databases.</p> <p>Workaround :</p> <ol style="list-style-type: none"> 1. Edit <code>CSA\scripts\mssql\csa_remove_createdby_updatedby.plsql</code> and comment out all "ALTER TABLE ... REBUILD" statements at the end of the file. You can comment it out by enclosing all REBUILD statements to <code>/*</code> and <code>*/</code> (SQL comments). Save the file. 2. Restart the upgrade process. It should end successfully. 3. After upgrade it is recommended to apply the commented REBUILD statements manually, For example, using Microsoft SQL Server Management Studio. <p>Note: It could take several hours on big databases with millions of artifacts.</p>
QCCR1D235209	<p>Problem : If <code>[CLIENT:<prop>]</code> token is used as parameter value of semantic validation parameters, then test (validation) fails with following error message:</p> <p>Option property with the name <code><prop></code> is not found. If this refers to a new property, ensure that it is saved.</p> <p>Test fails even if the <code>[CLIENT:<prop>]</code> is used on property <code><prop></code> and user filled "Input Validation" input fields.</p> <p>Note: it is test issue only. In runtime tokens are resolved correctly.</p> <p>Cause :</p> <ol style="list-style-type: none"> 1. If token <code>[CLIENT:<prop>]</code> is used as parameter value of validation parameter on user operation parameter <code><prop></code> and user filled Input Validation field input <ul style="list-style-type: none"> • It is caused by UI, which does not replaces the <code>[CLIENT:<prop>]</code> token with string entered to Input Validation input field. 2. If token <code>[CLIENT:<prop>]</code> refers to another parameter of user operation <ul style="list-style-type: none"> • It is caused by backend, which does not resolve tokens pointing to parameters of user operation when test is requested

Issues	Description
	<p>3. If token [CLIENT:<prop>] refers option model property</p> <ul style="list-style-type: none"> • Such token cannot be resolved because <ul style="list-style-type: none"> a. User operation does not have access to option model (e.g., user operation is on resource offering), b. Option model can define more than one property of the name, so it is not possible to identify the property <p>Workaround : For all causes 1), 2), and 3) the workaround is * enter value instead of token [CLIENT:<prop>] used as user operation parameter value - once tested, change parameter value back to the token.</p>
QCCR1D234010	<p>Problem : The increment and decrement quantity field in Marketplace Portal shopping cart does not show increment/decrement buttons in Internet Explorer.</p> <p>Cause : Standard UI widget for number input type does not include increment/decrement buttons in Internet Explorer.</p> <p>Workaround : Enter quantity manually.</p>
QCCR1D235356	<p>Problem : CSA 4.8 Content Store, after installing the content from file system, if we try installing the same content through HPLN, it does not prompt for re-install dialog box in the first attempt.</p> <p>Cause : Product Limitation.</p> <p>Workaround : 1. Install the content from file system. 2. Install the same content from the HPLN site (it will fail for the first time). 3. Re-attempt because all subsequent attempts to install the same content from HPLN site will succeed and the re-install dialog box will appear. Refresh the browser after every attempt in case the browser is slow or lagging.</p>
QCCR1D235590	<p>Problem : Import Preview fails while previewing the import of a design from an upgraded CSA instance into a fresh CSA 4.8 instance.</p> <p>Cause : A constraint violation is indicated in the Preview</p> <p>Workaround : Result of Import Preview can be ignored, and the design can be imported by clicking on Import button instead.</p>
QCCR1D234938	<p>Problem : CO URL in csa.war/dashboard/config.json file has changed to default value after Upgrade to CSA 4.8.</p> <p>Cause : Structural changes to the config.json file that is the New Dashboard changes</p> <p>Workaround : If you have made customizations to the config.json for the CSA launchpad/dashboard you will need to manually re-apply those after upgrade due to structural changes to the config.json file with the addition of the new interactive dashboard.</p>
QCCR1D234038	<p>Problem : SAML configuration is lost after upgrade to CSA 4.8 from CSA 4.7</p> <p>Cause : Process Limitation</p> <p>Workaround : If SAML is configured in CSA 4.7 and you have upgraded to CSA 4.8, you need to configure SAML again.</p>
QCCR1D225958	<p>Problem : Missing data points when VM is powered OFF or Suspended.</p> <p>Cause : Unable to plot the graph for missing data points.</p>

Issues	Description
	Workaround : No workaround available.
QCCR1D228220	<p>Problem : Health status is not updated for servers deployed on Helion Openstack (HOS) provider.</p> <p>Cause : CSA is unable to retrieve the health status since Cloud Optimizer (CO) is not supporting HOS 3.0.</p> <p>Workaround : It is a product limitation. No workaround available.</p>
QCCR1D228619	<p>Problem : Global search from MPP portal does not work in a Linux CSA installation.</p> <p>Cause : CSA Search service fails to update the Elasticsearch indices as a result of which Global search from MPP returns nothing</p> <p>Workaround : After CSA installation is complete, or after a CSA restart, 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.</p>
QCCR1D234418	<p>Problem : Upgrade from 4.6 to 4.8 is failing for windows with MS-SQL database</p> <p>Cause : Snapshot Isolation not enabled for idm</p> <p>Workaround : For Microsoft SQL Server, it is mandatory to enable the snapshot isolation for Identity management database which can be achieved through following two database statements: ALTER DATABASE idmdb SET ALLOW_SNAPSHOT_ISOLATION ON; ALTER DATABASE idmdb SET READ_COMMITTED_SNAPSHOT ON;</p>
QCCR1D218883	<p>Problem : Custom changes in Elasticsearch configuration may be discarded during an HA upgrade installation.</p> <p>Cause : Product defect.</p> <p>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.</p>
QCCR1D227598	<p>Problem : The SAML Authorization does not work if the access control is configured with the LDAP sub tree.</p> <p>Cause : CSA does not support the LDAP sub tree for Access Control (ACL) when SAML is enabled.</p> <p>Workaround : None</p>
QCCR1D235063	<p>Problem : "Subscription Status", "Service Instance Status", and "Upgradable To" fields go out of focus and get shifted to the bottom of the Operations Overview page.</p> <p>Cause : This is a Chrome browser issue in version 52 through version 55.</p> <p>Workaround : Use Chrome 56 and above version to avoid this problem.</p>
QCCR1D234562	<p>Problem : SMC login fails if we disable HP SSO configuration manually on CSA 4.8 HA</p> <p>Cause : Product limitation</p> <p>Workaround : Open the file \$CSA-HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-security.xml and set checkSSOCookie value to false in the below mentioned section of bean and restart CSA service. <beans:bean id="tokenValidityFilter" class="com.hp.csa.security.TokenValidityFilter"></p>

Issues	Description
	<pre data-bbox="581 153 1328 220"><beans:property name="checkSSOCookie" value="true" /> </beans:bean></pre>
QCCR1D230155	<p data-bbox="370 254 1276 285">Problem : SMC portal does not get logged out upon HP SSO timeout.</p> <p data-bbox="370 300 797 331">Cause : Product limitation.</p> <p data-bbox="370 346 992 378">Workaround : No workaround currently available.</p>
QCCR1D230605	<p data-bbox="370 411 1593 474">Problem : Manage User Subscriptions under Administration of MPP lists few users unauthorized to access the MPP.</p> <p data-bbox="370 489 797 520">Cause : Product limitation.</p> <p data-bbox="370 535 992 567">Workaround : No workaround currently available.</p>
QCCR1D235314	<p data-bbox="370 600 1593 663">Problem : Even if the undeploy/unreserving actions fails during cancellation, the subscription will go offline. However the resources may not be completely deallocated.</p> <p data-bbox="370 678 1588 741">Cause : This is because of a limitation in the architecture that does not allow to pause/resume the failed actions during cancellation.</p> <p data-bbox="370 756 883 787">Workaround : No workaround available.</p>
QCCR1D232661	<p data-bbox="370 816 1503 848">Problem : Currently we do not support hybrid Cloud Slang-AFL flows in any combination.</p> <p data-bbox="370 863 862 894">Cause : It is a product limitation.</p> <p data-bbox="370 909 1544 1003">Workaround : The procedure on 'Creating a topology Design with CloudSlang' is available in the Topology Components Guide (Whitepaper). Refer to this guide for a workaround information.</p>
QCCR1D186068	<p data-bbox="370 1033 1598 1253">Problem : When importing an Operations Orchestration flow in the Designs / Topology / Components area of the Cloud Service Management Console, if that flow contains an Input property with Type value of List of Values and From value of Prompt User from List – Selection List, the resulting component imported into CSA will have a property value of type String for this Input property. Instead of a list of values from which one or more can be selected, a single text input will be presented to the user for this property in both the Components and Designer areas.</p> <p data-bbox="370 1268 1598 1362">Cause : The Designs / Topology / Components and Designs / Topology / Designer areas of the Cloud Service Management Console do not have graceful support for multi-select properties such as these.</p> <p data-bbox="370 1377 1598 1587">Workaround : In the text input for such a property, encode the property values using the appropriate delimiter, which is determined by the method the flow uses to parse the Input property. If the flow uses the Selection List Iterate operation that is provided with the Base content pack in Operations Orchestration, the delimiter (separator) is configurable and has a default of ' '. For example, the values 'red', 'green', and 'blue' would be specified as 'red green blue' (unquoted) if using the Selection List Iterate operation with the default separator value.</p>
QCCR1D187711	<p data-bbox="370 1614 1606 1835">Problem : Topology components imported from Chef include an attributes parameter in their deploy operation, allowing customization of the provisioning of the Chef recipe. Properties passed in the attributes parameter are automatically converted to Strings. For example, an Integer component property of 3306 will be converted to "3306", and a Boolean component property of true will be converted to "true". If the Chef recipe is written to expect an Integer or Boolean input and not a String, the provisioning of the component will fail.</p> <p data-bbox="370 1850 797 1881">Cause : Product limitation.</p> <p data-bbox="370 1896 1398 1927">Workaround : The Chef recipe should be written or modified to expect String inputs.</p>

Issues	Description
CR1D226494	<p>Problem : The Featured Category list is empty for a newly created organization.</p> <p>Cause : The organization data synchronization is not complete after a new organization is created in IDM tables.</p> <p>Workaround : After the synchronization is completed, the catalogs and featured category list will appear. (~30 seconds)</p>
QCCR1D233354	<p>Problem : In MPP Service checkout page for an offering, the group list shows only the DNs that are added in the access control of the organization, it does not list all the groups to which the user belongs in LDAP.</p> <p>Cause : This behavior is currently unsupported in CSA. In order to show the group in group list, all the groups need to be explicitly mentioned in the organization access control.</p> <p>Workaround : None.</p>
QCCR1D234644	<p>Problem : Misleading icon displayed in MPP.</p> <p>If an organization is set to Pause Subscriptions on Provisioning error and a subscription fails, MPP shows right status as Paused but the icon is wrong.</p> <p>Spinner is displayed in MPP instead of Pause icon.</p> <p>Cause : Wrong HTML in MPP code base.</p> <p>Workaround : No workaround is required. Inappropriate icon is displayed.</p>
QCCR1D228672	<p>Problem : Cannot launch the show performance page using SSO from MPP.</p> <p>Cause : SSO token is not passed correctly.</p> <p>Workaround : User can login to Cloud Optimizer manually by entering username and password.</p>

Patch installation

This section describes how to install the patch.

Check pre-installation requirements

Make sure you fulfill these prerequisites before installing:

1. Check minimum hardware requirements:
 - CPU: 4 CPU, 3.0 GHz
 - RAM: 8 GB
 - Hard Drive: 20 GB
2. Check the [CSA 4.80 Support Matrix](#) to verify operating-system requirements.
3. Check minimum software requirements:

CSA version 4.80.0000

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.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00045

Windows:

https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00046

2. **Linux:**

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

- a. Extract the downloaded file: `HPE_CSA_Patch_04.80.0001.bin` file from the patch file.
- b. Make sure that the `csauser` user is the owner of the file and has full privileges.
- c. Log in as `csauser` and run `HPE_CSA_Patch_04.80.0001.bin` to open the CSA patch installer console mode.
- d. Enter `./HPE_CSA_Patch_04.80.0001.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.

3. When prompted, click **Enter** to exit the installation.

4. **Windows:**

- a. Extract the `HP_CSA_Patch_04.80.0001.exe` file from the patch zip file.
- b. Run `HP_CSA_Patch_04.80.0001.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_80_1_installation\Logs

Linux: \$CSA_HOME/_CSA_4_80_1_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. Make sure 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, the uninstall 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_80_1_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_80_1_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_80_1_installation\Logs

Linux: \$CSA_HOME/_CSA_4_80_1_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. Make sure 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>/CSAKit-4.7/Content Archives/topology/Jenkins plugin/HPE_Codar.hpi
<CSA_HOME>\Tools\CSLContentInstaller\ existing-infra.zip
<Deployments_home>/csa-codar-provider-help.war/en_US
<Deployments_home> /csa-provider-help.war/en_US
<Deployments_home> /codar-provider-help.war/en_US
```

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>.