



Hewlett Packard Enterprise

Cloud Service Automation
Edition

Patch ReadMe

Software version: CSA 4.60.0001
Document release date: March 2016
Software release date: March 2016

Contents

Introduction	2
What's New	2
Fixed Issues	3
Known Issues	4
Install the patch	4
Check preinstallation requirements	4
Install the patch	5
Verify the installation	6
Linux - Uninstall the patch	6
Uninstall Preparation	6
Uninstall the patch on standalone and cluster CSA servers	6
Windows – Uninstalling the patch	7
Uninstall Preparation	7
Uninstalling the patch on standalone and clustered environments	7
Verify the uninstall	7
CSA modified files	8
Send documentation feedback	9
Legal notices	9

Introduction

This readme provide lists of known and fixed issues, includes a [What's New](#) section, provides [installation/uninstallation](#) instructions, and provides configuration steps for the Linux and Windows HPE Cloud Service Automation server (CSA server). The cumulative patch updates CSA server to 04.60.0001.

What's New

This section lists what is new in this patch.

- Support for SELinux
- In addition to TLS 1.0 and 1.1 (already supported), this patch adds support for TLS version 1.2.
 - To restrict support to TLS 1.2 only (optional), modify the following files:

File	Modification
<code><CSA_HOME>\jboss-as\standalone\configuration\standalone.xml</code> file (for standalone servers) and <code><CSA_HOME>\jboss-as\standalone\configuration\standalone.full.xml</code> (for clusters)	Insert the yellow-highlighted information shown below: <pre><https-listener name="https" socket-binding="https" security-realm="SSLRealm" enabled-protocols="TLSv1.2" enabled-cipher-suites="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,..." /></pre>
<code><CSA_HOME>\portal\conf\mpp.conf</code>	Insert the yellow-highlighted information shown below: <pre>"provider": { "url": "https://<LB node>:<lb csa port>", "contextPath": "/csa/api/mpp", "strictSSL": true, "TLSVersions": "1.2", "ca": "C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/apache_csa.crt" }, "idmProvider": { "url": "https://<LB node>:<lb csa port>", "returnUrl": "https://<LB node>:<lb mpp port>", "contextPath": "/idm-service", "username": "idmTransportUser", "password": "ENC (F9za+OiGOC11PmTgef2EUQ\u003d\u003d)", "strictSSL": true, "TLSVersions": "1.2", "ca": "C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/apache_csa.crt" }, "https": { "enabled": true, "options": { "pfx": "../conf/.mpp_keystore", "passphrase": "ENC (Rp1mUoWY05TdgwAGofCRiw\u003d\u003d)", "TLSVersions": "1.2" } } },</pre> <p>Note: You must make sure that your integrated products also support the version of TLS you choose to use (TLS 1.0, 1.1, or 1.2).</p>

- To enable CSA support for Apache 2.4, add these parameters and corresponding values to the <path_to>\Apache2.2\conf\extra\mpp.conf file after the entry SSLProxyEngine:
 - SSLProxyEngine **on**
 - SSLProxyVerify **none**
 - SSLProxyCheckPeerCN **off**
 - SSLProxyCheckPeerName **off**

Note: CSA 4.60.0001 has been verified on clusters using Apache 2.4 and BIG-IP F5 11.5.1 LB. Support for TLS 1.1 and TLS 1.2 only has been verified with CSA 4.60.0001 and OO 10.50.

Fixed Issues

Issue	Symptom/Resolution
QCCR1D204370/219207	Support for TLS v1.2 added. This patch also supports TLS v1.1. See the What's New section for configuration requirements.
QCCR1D212900	CSA API incorrectly validates Property Values with Custom Validators.
QCCR1D217168	Support a list of service offerings associated with a selected Service Design.
QCCR1D217514	Display shows <code>pending</code> state even after a deletion/cancellation. A new Refresh button was added to reload data.
QCCR1D218397	The Cancel and Delete buttons should not be located in the same place. The subscription-cancellation alert message was modified.
QCCR1D218404	CSA Category Filter Option is not displayed in the drop-down list.
QCCR1D218526	Some subscriptions in Canceled/Expired state still have Cancel buttons. Provided retry button for failed subscriptions.
QCCR1D218711	Some JSPs that are loading dynamic-subscription options are shown as invalid as the default option is empty.
QCCR1D219208/213229	During subscription modification using CSA MPP, users can modify nested subscriber option Initialorderonly ON.
QCCR1D220177	The status of the approval is not displayed in the Approval Review Requests List page.
QCCR1D220292	Requests in the process of deployment can be deleted, resulting in the following error message: <code>Delete Subscription Error. Your request to delete subscription failed.</code> Failure can occur for multiple reasons. Delete button is displayed <i>after</i> the instance is created.
QCCR1D220602	Groups/user used in catalog access control earlier (not used now), don't get listed to provide access to other catalogs until added to the Org level. Earlier added groups/user should be available in drop down list of available groups under "Add groups to provide access control of catalogs".
QCCR1D220683	Make it possible to disable dashboard-widget editing. Disabled (default): <code>csa.ui.organizations.dashboardwidgets.enableEditingMashup=f</code> <code>alse</code> Enabled: <code>csa.ui.organizations.dashboardwidgets.enableEditingMashup=t</code> <code>rue</code>

Known Issues

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

Issues	Symptom	Resolution
QCCR1D221285	MPP Modify Subscription Details page erroneously shows a property as quantify multiplier.	None.

Install the patch

This section describes how to install the patch.

Check preinstallation 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 4.60 Support Matrix](#) to verify operating-system requirements:
3. Check minimum software requirements:
 - CSA version 4.60.0000
4. **Windows:** Set the CSA_HOME environment variable to the following (remote MPP node):
`C:\Program Files\HPE\CSA`
Linux: Set the CSA_HOME environment variable for the remote MPP node to the default path :
`/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: CSA Provider Console and Marketplace Portal, Search, 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_00031

Windows:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00032

2. **Linux:**

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

- a. Extract the downloaded file: `HPE_CSA_Patch_04.60.0001.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_04.60.0001.bin` to open the CSA patch installer console mode.
- d. Enter `./HPE_CSA_Patch_04.60.0001.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. Enter the CSA database password for the CSA user and click **Enter**.
- j. 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_04.60.0001.exe` file from the patch zip file.
- b. Run `HP_CSA_Patch_04.60.0001.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. Enter the CSA database user password and click **Next**.
- g. Click **Install** to run the patch installation.
- h. When prompted, click **Done** to exit the installation.

Verify the 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_60_1_installation\Logs

Linux: \$CSA_HOME/_CSA_4_60_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 CSA, 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.

Linux - Uninstall the patch

This section explains how to prepare to uninstall, how to uninstall, and how to verify patch uninstall.

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

Uninstall Preparation

To prepare for the uninstall:

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: CSA Provider Console and Marketplace Portal, HPE search, and Elasticsearch 1.6.1.
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_60_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. Click **Enter** to exit the uninstall.

Windows – Uninstalling the patch

This section describes how to uninstall the patch in both standalone and clustered environments.

Uninstall Preparation

To prepare for the uninstall:

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: CSA Provider Console and Marketplace Portal, HPE search, and Elasticsearch 1.6.1.
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 in a standalone environment using either of the following methods:

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

Note: 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_60_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.

Verify the uninstall

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

1. Check for errors in the log files:

Windows: `<CSA_HOME>_CSA_4_60_1_installation\Logs`

Linux: `$(CSA_HOME)/_CSA_4_60_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 CSA, 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>/portal/*
```

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.hp.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.hp.com>.