BigFix Patch
Patch for Red Hat Enterprise Linux - User's Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page xcviii)*.

Edition notice

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview

BigFix® Patch for Red Hat Enterprise Linux™ keeps your Linux™ clients current with the latest updates and service packs.

Patch management is available through the *Patches for RHEL* Fixlet® sites from BigFix. For each new patch or update that becomes available, BigFix releases a Fixlet that can identify and remediate all the computers in your enterprise that need it. With a few keystrokes, the BigFix Console Operator can apply the patch to all the relevant computers and visualize its progress as it deploys throughout the network.

The BigFix agent checks the operating system version, file versions, the language of the system and other relevant factors to determine when and if a patch is necessary.

BigFix Patch for Red Hat Enterprise Linux Fixlet® often have notes that typically allow the Console Operator to work around problem, adding extra value to the patching process. BigFix Patch for Red Hat Enterprise Linux also incorporates user feedback into notes, ensuring that you receive the latest information.

Fixlets allow you to manage large numbers of updates and patches with comparative ease, enabling automated, highly targeted deployment on any schedule that you want. Large downloads can be phased to optimize network bandwidth and the entire deployment process can be monitored, graphed, and recorded for inventory or audit control.

New Features

This release of Patches for Red Hat Enterprise Linux includes support for Red Hat Enterprise Linux 7 for Power ppc64 (Big Endian). Red Hat Subscription Management (RHSM) download plug-in, RHSM download cacher, and the multiple-package baseline installation features are now supported for Patches for RHEL PPC64BE 7.

Supported platforms

BigFix Patch for Red Hat Enterprise Linux supports various versions of Red Hat Enterprise Linux.

BigFix Patch for Red Hat Enterprise Linux provides Red Hat Security Advisories, Fix Advisories, and Bug Fix Advisories. These advisories are based on errata advisories from Red Hat Enterprise Linux.

> **Note:** To receive Red Hat Subscription Management (RHSM) notifications, configure your errata notifications settings in the Red Hat Customer portal.

Red Hat Enterprise Linux 6 - Intel (32-bit x86 and 64-bit x86_64)

- Red Hat Enterprise Linux Client
- RHEL Client Supplementary
- RHN Tools for RHEL Client
- Red Hat Enterprise Linux Server
- Red Hat Enterprise Linux Server Supplementary
- RHN Tools for RHEL

- Red Hat Enterprise Linux Workstation
- RHEL Workstation Supplementary
- RHN Tools for RHEL Workstation

Red Hat Enterprise Linux 7 - Intel (32-bit x86 and 64-bit x86_64)

- Red Hat Enterprise Linux Workstation Supplementary
- Red Hat Enterprise Linux Workstation FasTrack
- Red Hat Enterprise Linux Workstation
- Red Hat Enterprise Linux Workstation Extras
- Red Hat Enterprise Linux Server Supplementary
- Red Hat Enterprise Linux Server FasTrack
- Red Hat Enterprise Linux Server
- Red Hat Enterprise Linux Server Extras
- Red Hat Enterprise Linux Desktop Supplementary
- Red Hat Enterprise Linux Desktop FasTrack
- Red Hat Enterprise Linux Desktop
- Red Hat Enterprise Linux Desktop Extras

Red Hat Enterprise Linux 8 - Intel (64-bit x86_64)

- Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
- Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
- Red Hat Enterprise Linux 8 for x86_64 - Supplementary (RPMs)

Red Hat Enterprise Linux 6 for System Z (s390x)

- Red Hat Enterprise Linux 6 for System Z - RH Common (RPMs)
- Red Hat Enterprise Linux 6 for System Z (RPMs)
- Red Hat Enterprise Linux 6 for System Z - Optional Fastrack (RPMs)
- Red Hat Enterprise Linux 6 for System Z - Optional (RPMs)
- Red Hat Enterprise Linux 6 for System Z - Fastrack (RPMs)
- Red Hat Enterprise Linux 6 for System Z - Supplementary (RPMs)
- Red Hat Enterprise Linux 6 for System Z - Extras (RPMs)
- RHN Tools for Red Hat Enterprise Linux 6 for System Z (RPMs)

Red Hat Enterprise Linux 7 for System Z (s390x)

- Red Hat Enterprise Linux 7 for System Z - RH Common (RPMs)
- Red Hat Enterprise Linux 7 for System Z (RPMs)
- Red Hat Enterprise Linux 7 for System Z - Optional Fastrack (RPMs)
- Red Hat Enterprise Linux 7 for System Z - Optional (RPMs)
- Red Hat Enterprise Linux 7 for System Z - Fastrack (RPMs)

- Red Hat Enterprise Linux 7 for System Z - Supplementary (RPMs)
- Red Hat Enterprise Linux 7 for System Z - Extras (RPMs)
- RHN Tools for Red Hat Enterprise Linux 7 for System Z (RPMs)

Red Hat Enterprise Linux 7 - IBM Power System PPC64LE (Little Endian)

- Red Hat Enterprise Linux 7 for IBM Power LE Supplementary (RPMs)
- Red Hat Enterprise Linux 7 for IBM Power LE Optional (RPMs)
- Red Hat Enterprise Linux 7 for IBM Power LE (RPMs)
- RHN Tools for Red Hat Enterprise Linux 7 for IBM Power LE (RPMs)

Red Hat Enterprise Linux 7 - IBM Power System PPC64 (Big Endian)

- Red Hat Enterprise Linux 7 for IBM Power Supplementary (RPMs)
- Red Hat Enterprise Linux 7 for IBM Power Optional (RPMs)
- Red Hat Enterprise Linux 7 for IBM Power (RPMs)
- RHN Tools for Red Hat Enterprise Linux 7 for IBM Power (RPMs)

Red Hat Enterprise Linux 8 for System Z (s390x)

- Red Hat Enterprise Linux for IBM z Systems 8 - BaseOS (RPMs)
- Red Hat Enterprise Linux for IBM z Systems 8 - AppStream (RPMs)
- Red Hat Enterprise Linux for IBM z Systems 8 - Supplementary (RPMs)

Red Hat Enterprise Linux 8 - IBM Power System PPC64LE (Little Endian)

- Red Hat Enterprise Linux 8 for Power, little endian - BaseOS (RPMs)
- Red Hat Enterprise Linux 8 for Power, little endian - AppStream (RPMs)
- Red Hat Enterprise Linux 8 for Power, little endian - Supplementary (RPMs)

Note: Patch for Red Hat Enterprise Linux supports only audit Fixlets on System z architecture.

Announcement sources

Patches for RHEL 6

Red Hat Enterprise Linux Workstation 6 x86_64: https://access.redhat.com/downloads/content/71/ver=/rhel---6/6.8/x86_64/product-errata

Red Hat Enterprise Linux Server 6 x86_64: https://access.redhat.com/downloads/content/69/ver=/rhel---6/6.8/x86_64/product-errata

Oracle Java (Restricted Maintenance) (for RHEL Server) 6 x86_64: https://access.redhat.com/downloads/content/435/ver=/rhel---6/6/x86_64/product-errata

Red Hat Enterprise Linux Desktop 6 x86_64: https://access.redhat.com/downloads/content/68/ver=/rhel---6/6.8/x86_64/product-errata

Red Hat Enterprise Linux Workstation 6 i386: https://access.redhat.com/downloads/content/71/ver=/rhel---6/6.8/i386/product-errata

Red Hat Enterprise Linux Server 6 i386: https://access.redhat.com/downloads/content/69/ver=/rhel---6/6.8/i386/product-errata

Oracle Java (Restricted Maintenance) (for RHEL Server) 6 i386: https://access.redhat.com/downloads/content/435/ver=/rhel---6/6/i386/product-errata

Red Hat Enterprise Linux Desktop 6 i386: https://access.redhat.com/downloads/content/68/ver=/rhel---6/6.8/i386/product-errata

Patches for RHEL 6 on System Z

Red Hat Enterprise Linux for IBM z Systems 6: https://access.redhat.com/downloads/content/72/ver=/rhel---6/6.8/s390x/product-errata

Patches for RHEL 7 on System Z

Red Hat Enterprise Linux for IBM z Systems 7: https://access.redhat.com/downloads/content/72/ver=/rhel---7/7.3/s390x/product-errata

Patches for RHEL 7

Red Hat Enterprise Linux Workstation 7: https://access.redhat.com/downloads/content/71/ver=/rhel---7/7.0/x86_64/product-errata

Red Hat Enterprise Linux Server 7: https://access.redhat.com/downloads/content/69/ver=/rhel---7/7.0/x86_64/product-errata

Oracle Java (Restricted Maintenance) (for RHEL Server) 7 x86_64: https://access.redhat.com/downloads/content/435/ver=/rhel---7/7/x86_64/product-errata

Red Hat Enterprise Linux Desktop 7: https://access.redhat.com/downloads/content/68/ver=/rhel---7/7.0/x86_64/product-errata

Patches for RHEL 7 PPC64LE

Red Hat Enterprise Linux for Power, Little Endian 7: https://access.redhat.com/downloads/content/279/ver=/rhel---7/7.3/ppc64le/product-errata

Patches for RHEL 7 PPC64BE

Red Hat Enterprise Linux for Power, Big Endian 7: https://access.redhat.com/downloads/content/74/ver=/rhel---7/7.3/ppc64/product-errata

Patches for RHEL 8

Red Hat Enterprise Linux Server 8: https://access.redhat.com/downloads/content/479/ver=/rhel---8/8.0/x86_64/product-errata

Patches for RHEL 8 on System Z

Red Hat Enterprise Linux for IBM z Systems 8: https://access.redhat.com/downloads/content/72/ver=/rhel---8/8.3/s390x/product-errata

Patches for RHEL 8 PPC64LE

Red Hat Enterprise Linux for Power, little endian 8: https://access.redhat.com/downloads/content/279/ver=/rhel---8/8.2/ppc64le/product-errata

Note: Red Hat requires Oracle Java users to enable a new content set to access the Oracle Java SE software. For more information, see the Red Hat Knowledge base site. BigFix users must create separate certificates for Oracle Java (Restricted Maintenance) with the Oracle Java Add-On (Physical or Virtual Nodes) subscription. To create certificate entitlements, see Creating the RHSM entitlement certificates.

Supported Red Hat repositories

BigFix® Patch for Red Hat Enterprise Linux™ supports the listed Red Hat repositories.

BigFix supports Red Hat 6, Red Hat 7, and Red Hat 8 repositories.

Table 1. Supported repositories for the RHEL 6 Native Tools site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 6 Server x86_64	• Red Hat Enterprise Linux 6 Server - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 6 Server - Fastrack (RPMs) • RHN Tools for Red Hat Enterprise Linux 6 Server (RPMs) • Red Hat Enterprise Linux 6 Server - RH Common (RPMs) • Red Hat Enterprise Linux 6 Server - Optional (RPMs) • Red Hat Enterprise Linux 6 Server - Extras (RPMs) • Red Hat Enterprise Linux 6 Server (RPMs) • Red Hat Enterprise Linux 6 Server - Supplementary (RPMs) • Red Hat Enterprise Linux 6 Server - Oracle Java (Restricted Maintenance) (RPMs)

Table 1. Supported repositories for the RHEL 6 Native Tools site (continued)

Red Hat version	Supported repository name
Red Hat Enterprise Linux 6 Server x86	• Red Hat Enterprise Linux 6 Server - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 6 Server - Fastrack (RPMs) • RHN Tools for Red Hat Enterprise Linux 6 Server (RPMs) • Red Hat Enterprise Linux 6 Server - RH Common (RPMs) • Red Hat Enterprise Linux 6 Server - Optional (RPMs) • Red Hat Enterprise Linux 6 Server - Extras (RPMs) • Red Hat Enterprise Linux 6 Server (RPMs) • Red Hat Enterprise Linux 6 Server - Supplementary (RPMs) • Red Hat Enterprise Linux 6 Server - Oracle Java (Restricted Maintenance) (RPMs)
Red Hat Enterprise Linux 6 Desktop x86_64	• Red Hat Enterprise Linux 6 Desktop - Oracle Java (Restricted Maintenance) (RPMs) • Red Hat Enterprise Linux 6 Desktop - Supplementary (RPMs) • Red Hat Enterprise Linux 6 Desktop - Extras (RPMs) • RHN Tools for Red Hat Enterprise Linux 6 Desktop (RPMs) • Red Hat Enterprise Linux 6 Desktop - Optional (RPMs) • Red Hat Enterprise Linux 6 Desktop - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 6 Desktop - RH Common (RPMs) • Red Hat Enterprise Linux 6 Desktop (RPMs) • Red Hat Enterprise Linux 6 Desktop - Fastrack (RPMs)

Table 1. Supported repositories for the RHEL 6 Native Tools site (continued)

Red Hat version	Supported repository name
Red Hat Enterprise Linux 6 Desktop x86	- Red Hat Enterprise Linux 6 Desktop - Oracle Java (Restricted Maintenance) (RPMs) - Red Hat Enterprise Linux 6 Desktop - Supplementary (RPMs) - Red Hat Enterprise Linux 6 Desktop - Extras (RPMs) - RHN Tools for Red Hat Enterprise Linux 6 Desktop (RPMs) - Red Hat Enterprise Linux 6 Desktop - Optional (RPMs) - Red Hat Enterprise Linux 6 Desktop - Optional Fastrack (RPMs) - Red Hat Enterprise Linux 6 Desktop - RH Common (RPMs) - Red Hat Enterprise Linux 6 Desktop (RPMs) - Red Hat Enterprise Linux 6 Desktop - Fastrack (RPMs)
Red Hat Enterprise Linux 6 Workstation x86_64	- Red Hat Enterprise Linux 6 Workstation (RPMs) - RHN Tools for Red Hat Enterprise Linux 6 Workstation (RPMs) - Red Hat Enterprise Linux 6 Workstation - Optional (RPMs) - Red Hat Enterprise Linux 6 Workstation - Fastrack (RPMs) - Red Hat Enterprise Linux 6 Workstation - Optional Fastrack (RPMs) - Red Hat Enterprise Linux 6 Workstation - Supplementary (RPMs) - Red Hat Enterprise Linux 6 Workstation - RH Common (RPMs) - Red Hat Enterprise Linux 6 Workstation - Extras (RPMs) - Red Hat Enterprise Linux 6 Workstation - Oracle Java (Restricted Maintenance) (RPMs)

Table 1. Supported repositories for the RHEL 6 Native Tools site (continued)

Red Hat version	Supported repository name
Red Hat Enterprise Linux 6 Workstation x86	• Red Hat Enterprise Linux 6 Workstation (RPMs) • RHN Tools for Red Hat Enterprise Linux 6 Workstation (RPMs) • Red Hat Enterprise Linux 6 Workstation - Optional (RPMs) • Red Hat Enterprise Linux 6 Workstation - Fastrack (RPMs) • Red Hat Enterprise Linux 6 Workstation - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 6 Workstation - Supplementary (RPMs) • Red Hat Enterprise Linux 6 Workstation - RH Common (RPMs) • Red Hat Enterprise Linux 6 Workstation - Extras (RPMs) • Red Hat Enterprise Linux 6 Workstation - Oracle Java (Restricted Maintenance) (RPMs)

Table 2. Supported repositories for the RHEL 7 Native Tools site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 7 Server x86_64	• Red Hat Enterprise Linux 7 Server - Fastrack (RPMs) • Red Hat Enterprise Linux 7 Server - Optional (RPMs) • Red Hat Enterprise Linux 7 Server - Extras (RPMs) • Red Hat Enterprise Linux 7 Server - RH Common (RPMs) • Red Hat Enterprise Linux 7 Server - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 7 Server (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 Server (RPMs)

Table 2. Supported repositories for the RHEL 7 Native Tools site (continued)

Red Hat version	Supported repository name
	• Red Hat Enterprise Linux 7 Server - Supplementary (RPMs) • Red Hat Enterprise Linux 7 Server - Oracle Java (Restricted Maintenance) (RPMs)
Red Hat Enterprise Linux 7 Desktop x86_64	• Red Hat Enterprise Linux 7 Desktop - Oracle Java (Restricted Maintenance) (RPMs) • Red Hat Enterprise Linux 7 Desktop - Extras (RPMs) • Red Hat Enterprise Linux 7 Desktop (RPMs) • Red Hat Enterprise Linux 7 Desktop - Fastrack (RPMs) • Red Hat Enterprise Linux 7 Desktop - Supplementary (RPMs) • Red Hat Enterprise Linux 7 Desktop - RH Common (RPMs) • Red Hat Enterprise Linux 7 Desktop - Optional Fastrack (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 Desktop (RPMs) • Red Hat Enterprise Linux 7 Desktop - Optional (RPMs)
Red Hat Enterprise Linux 7 Workstation x86_64	• Red Hat Enterprise Linux 7 Workstation - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 7 Workstation - Optional (RPMs) • Red Hat Enterprise Linux 7 Workstation - Extras (RPMs) • Red Hat Enterprise Linux 7 Workstation - RH Common (RPMs) • Red Hat Enterprise Linux 7 Workstation - Fastrack (RPMs) • Red Hat Enterprise Linux 7 Workstation - Supplementary (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 Workstation (RPMs)

Table 2. Supported repositories for the RHEL 7 Native Tools site (continued)

Red Hat version	Supported repository name
	• Red Hat Enterprise Linux 7 Workstation (RPMs) • Red Hat Enterprise Linux 7 Workstation - Oracle Java (Restricted Maintenance) (RPMs)

Table 3. Supported repositories for the Patches for RHEL RHSM 6 on System Z site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 6 Server s390x	• Red Hat Enterprise Linux 6 for System z - RH Common (RPMs) • Red Hat Enterprise Linux 6 for System z (RPMs) • Red Hat Enterprise Linux 6 for System z - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 6 for System z - Optional (RPMs) • Red Hat Enterprise Linux 6 for System z - Fastrack (RPMs) • Red Hat Enterprise Linux 6 for System z - Supplementary (RPMs) • Red Hat Enterprise Linux 6 for System z - Extras (RPMs) • RHN Tools for Red Hat Enterprise Linux 6 for System z (RPMs)

Table 4. Supported repositories for the Patches for RHEL RHSM 7 on System Z site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 7 Server s390x	• Red Hat Enterprise Linux 7 for System Z - RH Common (RPMs) • Red Hat Enterprise Linux 7 for System Z (RPMs) • Red Hat Enterprise Linux 7 for System Z - Optional Fastrack (RPMs) • Red Hat Enterprise Linux 7 for System Z - Optional (RPMs) • Red Hat Enterprise Linux 7 for System Z - Fastrack (RPMs)

Table 4. Supported repositories for the Patches for RHEL RHSM 7 on System Z site (continued)

Red Hat version	Supported repository name
	• Red Hat Enterprise Linux 7 for System Z - Supplementary (RPMs) • Red Hat Enterprise Linux 7 for System Z - Extras (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 for System Z (RPMs)

Table 5. Supported repositories for the Patches for RHEL 7 for IBM Power LE site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 7 PPC64LE	• Red Hat Enterprise Linux 7 for IBM Power LE - Supplementary (RPMS) • Red Hat Enterprise Linux 7 for IBM Power LE - Optional (RPMs) • Red Hat Enterprise Linux 7 for IBM Power LE (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 for IBM Power LE (RPMs)

Table 6. Supported repositories for the Patches for RHEL 7 for IBM Power site

Red Hat version	Supported repository name
Red Hat Enterprise Linux 7 PPC64 (Big Endian)	• Red Hat Enterprise Linux 7 for IBM Power - Supplementary (RPMS) • Red Hat Enterprise Linux 7 for IBM Power - Optional (RPMs) • Red Hat Enterprise Linux 7 for IBM Power (RPMs) • RHN Tools for Red Hat Enterprise Linux 7 for IBM Power (RPMs)

Table 7. Supported repositories for RHEL 8 x86_64

Red Hat version	Supported respository name
Red Hat Enterprise Linux 8 Server x86_64	• Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs) • Red Hat Enterprise Linux 8 for x86_64 - App-Stream (RPMs) • Red Hat Enterprise Linux 8 for x86_64 - Supplementary (RPMs)

Table 8. Supported repositories for RHEL 8 on System Z site

Red Hat Enterprise Linux 8 Server s390x	• Red Hat Enterprise Linux for IBM z Systems 8 - BaseOS (RPMs) • Red Hat Enterprise Linux for IBM z Systems 8 - AppStream (RPMs) • Red Hat Enterprise Linux for IBM z Systems 8 - Supplementary (RPMs)

Table 9. Supported repositories for Patches for RHEL 8 for IBM Power LE site

Redhat Version	Supported Repository Name
Red Hat Enterprise Linux 8 PPC64LE	• Red Hat Enterprise Linux 8 for Power, little endian - BaseOS (RPMs) • Red Hat Enterprise Linux 8 for Power, little endian - AppStream (RPMs) • Red Hat Enterprise Linux 8 for Power, little endian - Supplementary (RPMs)

Site applicability matrix

The various features of Patch for Red Hat apply differently for each Red Hat site.

The following matrix shows the Patch for Red Hat features that apply for each Red Hat site.

Table 10. Supported features for each Patches for Red Hat Enterprise Linux site

Site name	RHSM Download Plug-ins	Custom Repository Management dashboard	YUM Transaction History dashboard	RHSM Download Cacher
Patches for RHEL 6 - Native Tools site	Yes	Yes	Yes	Yes
Patches for RHEL 6 on System z	Yes	Yes	Yes	Yes
Patches for RHEL 7 on System z	Yes	Yes	Yes	Yes
Patches for RHEL 7 site	Yes	Yes	Yes	Yes
Patches for RHEL 7 PPC64LE	Yes	Yes	Yes	Yes
Patches for RHEL PPC64BE 7	Yes	Yes	Yes	Yes
Patches for RHEL 8	Yes	Yes	Yes	Yes
Patches for RHEL ppc64le 8	Yes	Yes	Yes	Yes
Patches for RHEL 8 on System Z	Yes	Yes	Yes	Yes

Fixlet fields

Fixlets contain fields of metadata that provide specific details. Some Fixlet fields are common across all domains, that is, categories of BigFix sites. Other fields are common to only one domain or product, such as Patch Management.

The following table lists the Fixlet fields and their descriptions.

Table 11. Fixlet fields and descriptions

Fixlet fields	Description	BigFix domain
ID	A numerical ID assigned to the Fixlet by the author.	All
Name	The name assigned to the Fixlet by the author.	All

Table 11. Fixlet fields and descriptions

(continued)

Fixlet fields	Description	BigFix domain
Applicable Computer Count	The number of BigFix clients in the network currently affected by the Fixlet.	All
Category	The type of Fixlet, such as a Security Patch or Update.	All
Download Size	The size of the remedial file or patch that the action downloads.	All
Source	The name of the source vendor that provides the Fixlet information.	All
Source ID	A numerical ID assigned to the Fixlet to relate it back to its source.	All
Source Release Date	The date when an upstream vendor releases the patch.	All
Source Severity	A measure of how critical a Fixlet is, assigned by the Fixlet author. Typical values are Critical, Important, Moderate, or Low.	All
Site	The name of the site that is generating the relevant Fixlet.	All
Unlocked Computer Count	The number of unlocked computers that are affected by the Fixlet.	All
Open Action Count	The number of distinct actions that are open for the given Fixlet.	All
X-Fixlet-product-family	The product family that the patch belongs to.	Windows Patching (Relates to BigFix Patch Management)
X-Fixlet-product	The product that the patch belongs to under a certain product family.	Windows Patching (Relates to BigFix Patch Management)
X-Fixlet-component	A component that the patch targets under a certain product family.	Windows Patching (Relates to BigFix Patch Management)
Modification Time	The time when a given Fixlet was last modified.	All
X-Fixlet-first-propagation	The Fixlet release date.	All

Chapter 2. Setup

Setting up your environment for patch management.

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by HCL, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by acquiring a Masthead file from a vendor or from HCL or by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the *BigFix Installation Guide*.

For more information about sites, see the *BigFix Console Operator's Guide*.

Subscribing to the Patches for RHEL sites

Subscribe to the Patches for RHEL sites through the License Overview dashboard.

RHEL 5.x requires the use of YUM utility version 3.2.19-18 or later.

> **Note:** The RHSMDownloadPlugin does not support patch deployment to RHEL 5. RHEL 5 reached its end of life (EOL) in March 2017. Subsequently, BigFix support of the earlier version of the RHEL plug-in and download cacher has ended. For BigFix notices about the RHEL 5 EOL, see http://bit.ly/2nEwWyT.

1. From the **BigFix Management** domain, click **License Overview** dashboard.
2. Scroll down to view the available content sites.
3. Click **Enable** to select the version of Patches for RHEL site to which you want to subscribe.
4. Open the **Manage Sites** node and select your newly subscribed site.
5. From the site dialog, click the **Computer Subscriptions** tab to assign the site to the appropriate computers.
6. From the **Operator Permissions** tab, select the operators that you want to associate with this site and their level of permission.
7. Click **Save Changes**.

You are now subscribed to a Patches for RHEL site.

Chapter 3. Using Patch Management for Red Hat Enterprise Linux

You can deploy patches from the BigFix console and view the Red Hat bulletin for a specific Fixlet. Activate an analysis to view the results of an action that is found in a log file on the endpoint.

Patch using Fixlets
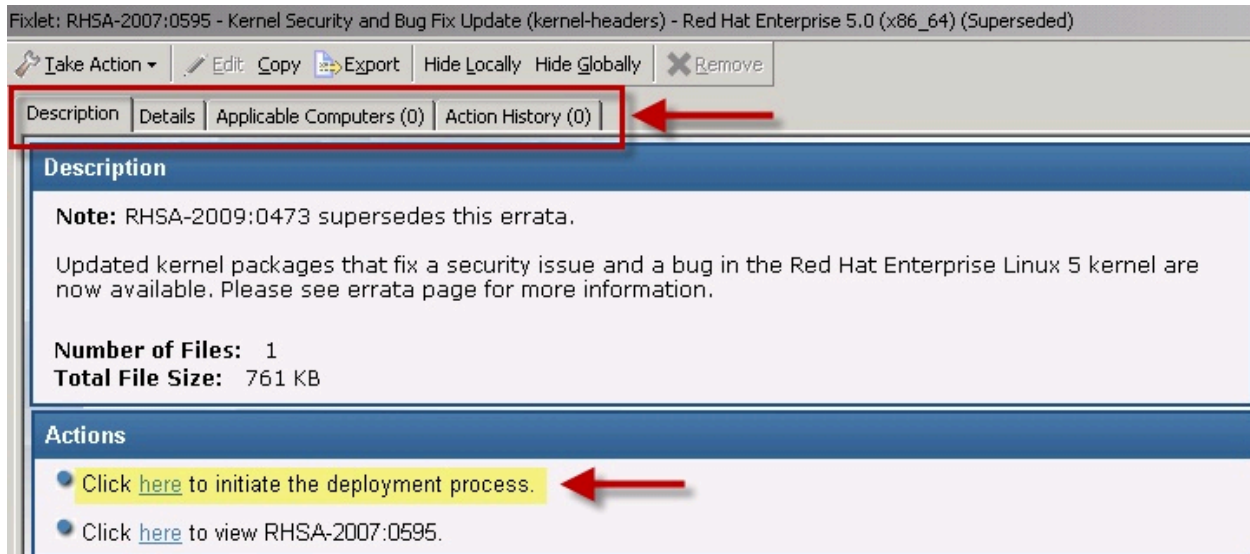
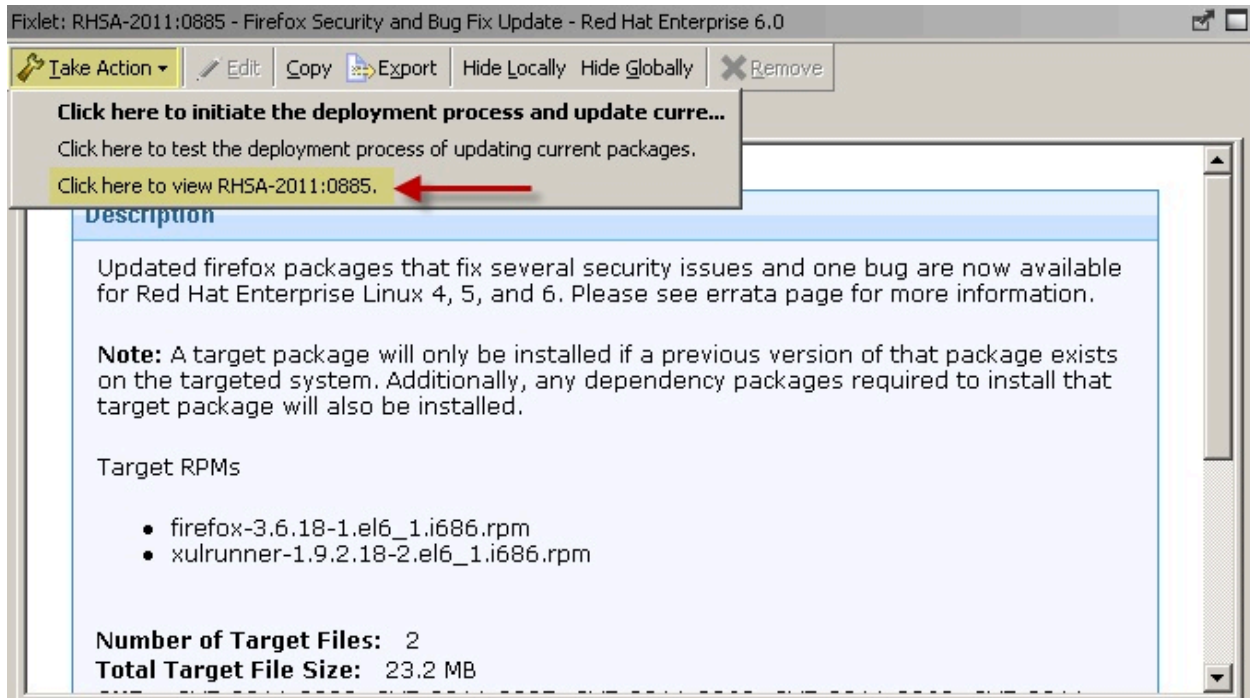You can deploy patches from the BigFix Console.

In the *Patch Management domain* in the console navigation tree, click *OS Vendors* and click Red Hat Enterprise Linux.
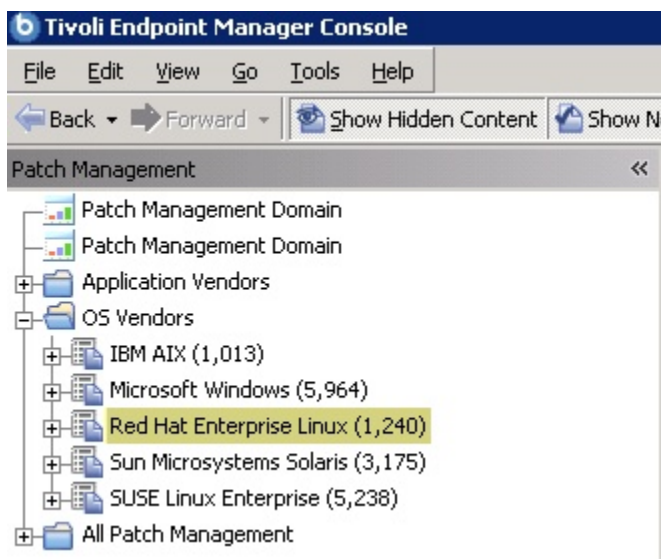
Double-click the Fixlet that you want to deploy. Click the tabs at the top of the Fixlet window to review additional details, and then click the appropriate link in the Actions box to start deployment. Click *OK*.

Fixlet: RHSA-2007:0595 - Kernel Security and Bug Fix Update (kernel-headers) - Red Hat Enterprise 5.0 (x86_64) (Superseded)

Take Action ▾   Edit Copy Export   Hide Locally Hide Globally   Remove

Description | Details | Applicable Computers (0) | Action History (0) |

Description

Note: RHSA-2009:0473 supersedes this errata.

Updated kernel packages that fix a security issue and a bug in the Red Hat Enterprise Linux 5 kernel are now available. Please see errata page for more information.

Number of Files: 1
Total File Size: 761 KB

Actions

● Click here to initiate the deployment process.

● Click here to view RHSA-2007:0595.

To view the Red Hat bulletin for a particular Fixlet, select the *Click here to view the patch page* action to view the patch page.

Fixlet: RHSA-2011:0885 - Firefox Security and Bug Fix Update - Red Hat Enterprise 6.0

Take Action ▾   Edit Copy Export   Hide Locally Hide Globally   Remove

Click here to initiate the deployment process and update curre...
Click here to test the deployment process of updating current packages.
Click here to view RHSA-2011:0885.

Description

Updated firefox packages that fix several security issues and one bug are now available for Red Hat Enterprise Linux 4, 5, and 6. Please see errata page for more information.

Note: A target package will only be installed if a previous version of that package exists on the targeted system. Additionally, any dependency packages required to install that target package will also be installed.

Target RPMs

● firefox-3.6.18-1.el6_1.i686.rpm
● xulrunner-1.9.2.18-2.el6_1.i686.rpm

Number of Target Files: 2
Total Target File Size: 23.2 MB

Patch by using the YUM utility

Yellow dog Updater, Modified (YUM), the default patch manager for Red Hat Enterprise Linux, replaces the Endpoint Dependency Resolver (EDR) utilities that Patch for Red Hat Enterprise Linux previously used. Patch for Red Hat Enterprise Linux that uses YUM applies to Red Hat Linux Enterprise versions 6 and later.

Previously, the Patch for Red Hat Enterprise Linux sites used a set of utilities that are called Endpoint Dependency Resolver utilities to handle package dependencies on the endpoint. YUM replaces these EDR utilities and gives you more flexibility in terms of patch deployment and providing results that are in parallel with Red Hat solutions.

YUM is a package management tool that updates, installs, and removes Red Hat Package Manager (RPM) packages. YUM uses a command-line interface and simplifies the process of installing, uninstalling, and updating packages, provided that there is access to the YUM repository.

It is highly suggested that users start to use the RHEL Native tools sites because YUM reduces dependency issues and improves performance. There is no marked difference in how the EDR and YUM native tools sites are used when deploying patches. To use YUM, users must subscribe to the Patches for RHEL Natives tool sites. To learn about subscribing to the Patches for RHEL Native tools sites, see Subscribing to the Patches for RHEL sites *(on page 20)*.

Note: The Patch Management for Red Hat Enterprise Linux site for RHEL 6 continues to use the EDR utilities, which use RPM.

YUM utility configuration settings

The Patch Management for Red Hat sites that apply the YUM utility use Fixlet settings in `/etc/yum.conf.` except for the following YUM configuration settings:

- `cachedir`
- `keepcache`
- `plugins`
- `reposdir`
- `pluginpath`
- `pluginconfpath`
- `metadata_expire`
- `installonlypkgs`

Identifying file relevance with Native tools content

Native tools content capture file relevance differently from EDR. EDR checks for packages that are earlier than a certain version, by using the relevance `clause not exist lower version of file`. Native tools content is more restrictive and checks for packages that are earlier than a specific version, as well as not later than a specific version. Native tools content uses the relevance clause checks for `exist lower version of file, but not exist higher version of file`.

If both tools are applied to the same deployment, the difference of the EDR and Native tools methods might lead to a difference in relevance results. It is highly suggested that users use the Native tools sites.

Supersedence

Please refer to Supersedence in Non-Windows to know more about the supersedence.

Deployment of Modular Fixlets on RHEL8

This topic describes how to deploy a modular Fixlets on RHEL8.

1. Modular streams must be enabled on client before deploying the modular Fixlets.
2. Modular stream can be enabled on the endpoint using Fixlet "`dnf module commands execution on endpoint - RHEL 8 - x86_64`" or by manually running dnf module commands (reset, enable) on the endpoint (this commands will run successfully only when the client is registered with subscription manager).
3. Added a new prerequisite Fixlet "`List enabled modules to file on client - RHEL 8 - x86_64 (Prerequisite)`". This Fixlet must be deployed first before deploying modular Fixlets on client. As a good practise, this Fixlet should be deployed before the modular Fixlets are deployed.
4. Once the above prerequisite Fixlet is deployed, the same Fixlet will be re-deployed automatically once a day to read the information about the modular streams.
5. If the modular Fixlets are applicable, you can deploy modular Fixlets on the endpoint. If it is not applicable, you need to enable modular stream version on the endpoint and rerun our prerequisite Fixlet.
6. **Example**

   Perform the following steps to deploy the modular Fixlet "`RHSA-2021:2584 - Ruby:2.7 Security, Bug Fix, and Enhancement Update - Red Hat Enterprise Linux 8 (x86_64)`":

   a. The Fixlet "`RHSA-2021:2584 - Ruby:2.7 Security, Bug Fix, and Enhancement Update - Red Hat Enterprise Linux 8 (x86_64)`" is not applicable because ruby version of **2.7** is not enabled on the endpoint as shown in the following figures:

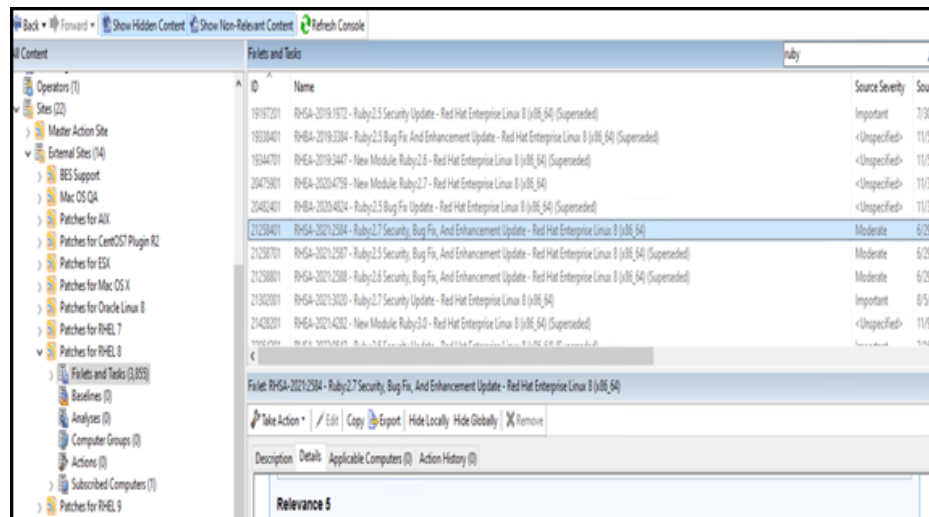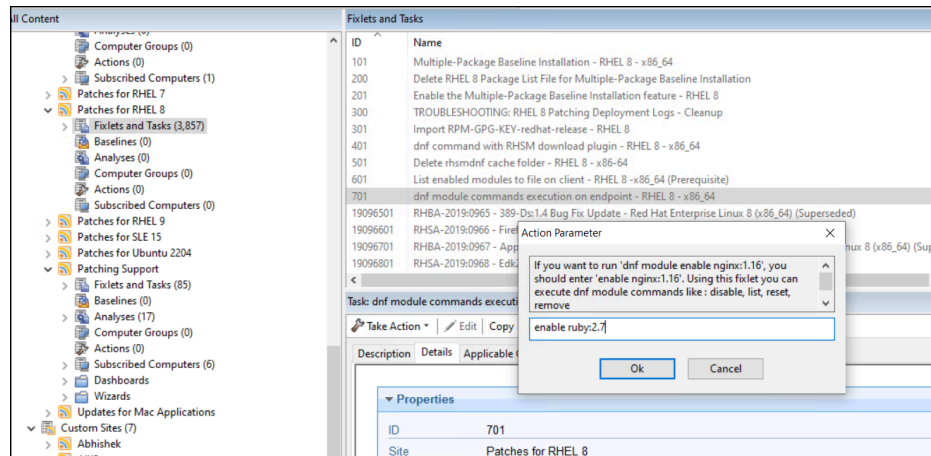   Figure 1. Fixlet is not relevant

Figure 2. Ruby 2.7 (disabled)

b. To enable ruby modular stream version of **2.7**, you must deploy the Fixlet "`dnf module commands execution on endpoint - RHEL 8 - x86_64`" as shown in the following figures:

Figure 3. Reset command on ruby module

Figure 4. Enable ruby module with stream 2.7

c. The Fixlet "`List enabled modules to file on client - RHEL 8 - x86_64 (Prerequisite)`" must be deployed before deploying the modular Fixlet. Once it is deployed, the modular Fixlet become relevant on the client where ruby **2.7** has been enabled, as shown in the following figure:

Figure 5. Relevant Fixlet
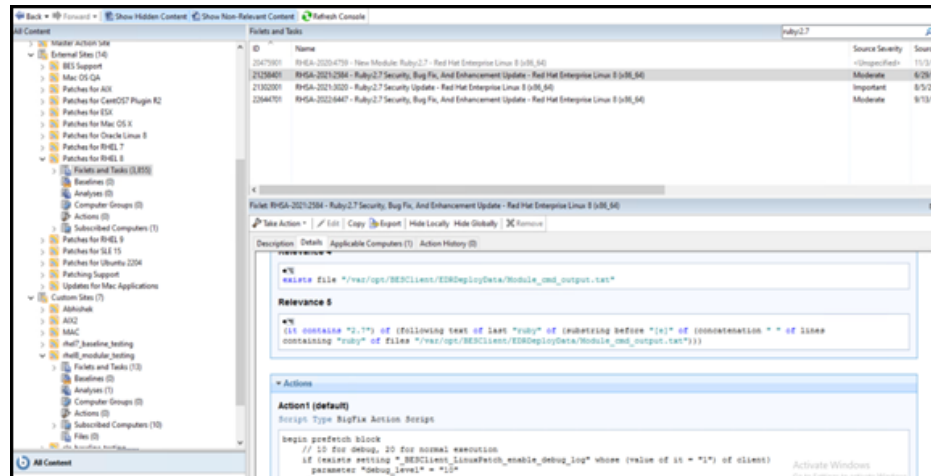
d. Now, modular Fixlet "`RHSA-2021:2584 - Ruby:2.7 Security, Bug Fix, and Enhancement Update - Red Hat Enterprise Linux 8 (x86_64)`" is applicable and can be deployed on the client.

> **Note:** An errata for a specific module stream is used to patch only the specific stream and not to be used as an update for other module streams. Follow this general practice for all the modular streams. For example, an endpoint is usually configured to one module stream, such as nodejs:10 and the packages from the same stream should be applied as an update. For some reason, however, if you want to switch the module stream that is installed on an endpoint from nodejs:10 to nodejs:12 then you must remove all the nodejs:10 packages or

dependencies manually and update the endpoint with nodejs:12 packages. This scenario cannot be covered through BigFix, as this is limitation from **RED HAT**.

For more information related to modular steams, refer to following links:

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/ installing_managing_and_removing_user-space_components/managing-versions-of-appstream-content_using-appstream
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/ installing_managing_and_removing_user-space_components/red_hat_enterprise_linux-8-installing_managing_and_removing_user-space_components-en-us.pdf

Chapter 4. Manage custom repositories

Use the RHEL Custom Repository Management dashboard to register and manage standard repositories and satellite repositories.

With the RHEL Custom Repository Management Support, users of Patch Management for Red Hat Native tools sites can:

- Use the dashboard to register, unregister, add, delete, and import custom repositories and Red Hat Network satellites.
- Deliver custom software through BigFix. Support for custom repositories leverages on existing local repositories to save bandwidth and improve performance.

Instead of following the current BigFix infrastructure which allows Fixlets in the RHEL native tools to download the patches directly from the Red Hat servers, the Fixlets now allow YUM to download from local repositories.

Ensure that you have met the following requirements:

- BigFix 9.2 and later versions.
- RHEL versions 6 and later.
- Minimum YUM version: YUM 3.2.19-18
- Subscribe to the Patching Support site.
- Activate the Repository Configuration - Red Hat Enterprise Linux analysis from the Patching Support site to access the dashboard.
- Enable the following tasks:
    - Enable custom repository support - Red Hat Enterprise Linux
    - Disable custom repository support - Red Hat Enterprise Linux
- Users of the custom repository must register the RHSM download plug-in to avoid download errors. Registration is required though the data that the download plug-in generates will not be used. You can register the download plug-in through the Manage Download Plugins dashboard. There is no need to set up the certificates.

Note: The dashboard does not support the creation and maintenance of local repositories. You must create local repositories separately.

Using custom repositories can give you the flexibility to control what can be deployed to the endpoints in your deployment. For example, you can deploy custom software that you are hosting in your custom repositories.

Use the Install packages by using the YUM task from the Patching Support site to install custom software that are in your custom repositories.

Differentiating between repository and satellite

You can use standard and Red Hat Network satellite repositories in the dashboard. For both types of repositories, ensure that the repositories and satellites are updated. Actions might fail if the packages are not available.

Repository

This type refers to standard software repositories, which are storage locations from which users can retrieve packages. The RHEL Custom Repository dashboard does not add physical repositories. You must do this separately. To learn about creating repositories, see the Red Hat documentation: https://access.redhat.com/site/documentation/en-US/.

Satellite

This type refers to the Red Hat Network (RHN) Satellite, a Red Hat product which manages patches and subscriptions. These satellite repositories can mirror the patches from Red Hat. Satellite repositories provide a local copy of the Red Hat patch content repositories which are synched to the Red Hat network.

Note: The dashboard only runs the bootstrap channels. Satellite channels cannot be configured through the dashboard.The channels that the endpoints use must be configured through the satellite servers.

Registering a repository

Using the dashboard, you can register and connect your existing repositories to endpoints.

1. Activate the Repository Configuration - Red Hat Enterprise Linux analysis.
2. Enable the following task: Enable custom repository support - Red Hat Enterprise Linux.

1. From the All Content domain, go to **Sites > External Sites > Patching Support > Dashboards > RHEL Custom Repository Management**.
2. Click the **Endpoints** tab and select an endpoint. The repositories of the selected endpoints are listed in the lower part of the window. When a repository is named as unspecified, it means that it is not listed in the Repository list.
3. Click **Register a new repository**.
4. From the Register a New Repository window, select the repository then click **Next**. The next window shows the name and the URL of the repository that you are registering.
5. This step is optional. You can also add more configuration information in **Additional Fields**. This information is saved in the YUM configuration files.

    Note: Users who have custom repositories that are not just mirrors of the vendor sites must add `gpgcheck=0` in **Additional Fields**. When the gpg signature files are excluded, the rpm files are not checked for authenticity and might cause the installation to fail.

6. Click **Save**.
7. From the **Take Action** window, select the computer and click **OK** to run the action.

Registering a satellite repository

Using the dashboard, you can register and connect your existing satellite repositories to endpoints.

1. Activate the Repository Configuration - Red Hat Enterprise Linux analysis.
2. Enable the following task: Enable custom repository support - Red Hat Enterprise Linux.

1. From the All Content domain, go to **Sites > External Sites > Patching Support > Dashboards > RHEL Custom Repository Management**.
2. Click the **Endpoints** tab and select the endpoint. The repositories of the selected endpoints are listed in the lower part of the window. When a repository is named as unspecified, it means that it is not listed in the Repository list.
3. Click **Register a new repository**. From the **Register a New Repository** window, select the repository then click **Next**. A window opens showing the name and the URL of the repository that you are registering.
4. Enter the values in the following fields:
   For Satellite5
   - Bootstrap URL
   - Activation Keys

   Activation keys are generated by Red Hat Network Satellite. For more information about activation keys, see https://access.redhat.com/site/documentation/en-US/.

   For Satellite6

   > 📝 **Note:** When you register or unregister the satellite6 server using BigFix, it will remove all the preconfigured subscription and identity data from the client machine.

   - Activation Keys
   - Organization
   - Auto-attach(y/n)

   Activation keys and Organization are created by Red Hat Network Satellite. For more information about activation keys, see https://access.redhat.com/documentation/en-us/red_hat_satellite/6.7/html/content_management_guide/managing_activation_keys.

5. Click **Save**.
6. From the **Take Action** window, select the computer and click **OK** to run the action.

Unregistering a repository from an endpoint

When you unregister a repository, the dashboard removes the system ID file from the computer you selected. You must log in to the satellite server and delete the computer manually.

1. From the All Content domain, go to **Sites > External Sites > Patching Support > Dashboards > Custom Repository Management**.
2. Click the Endpoints tab and click **Unregister a new repository**.
3. From the **Unegister a New Repository** window, select the repository and click **Save**.
4. From the Take Action window, select the computer and click **OK**.

> **Note:** When you unregister a repository, the YUM configuration file is not deleted, but just disabled.

Adding repositories

You can add standard or satellite repositories with the RHEL Custom Repository Management dashboard.

1. From the All Content domain, go to **Sites > External Sites > Patching Support > Dashboards > RHEL Custom Repository Management**.
2. From the **Repositories** tab, select the repository that you want to add and click **Add**.
3. From the Add a New Repository window, select the repository type and enter values for the following fields.
   - For standard repositories:
     - Name
     - Repository URL
   - For Satellite5 repositories
     - Satellite Name
     - Satellite URL
     - Bootstrap URL

     > **Note:** When you enter the satellite URL, the bootstrap URL is entered automatically. Bootstraps are created on the satellite server.

   - For Satellite6 repositories
     - Satellite6 Name
     - Satellite6 URL
4. Click **Save**.

You added a repository to the dashboard. To have an endpoint use the repository that you added, go to the **Endpoints** tab and register the repository.

Importing a repository

Users can import their existing repositories using this feature.

Activate the Repository Configuration - Red Hat Enterprise Linux analysis to populate the dashboard with endpoint and repository information.

When importing existing repositories, ensure that the following entries are entered in the following order in the .repo files.

```
name=
baseurl=
enabled=
gpgcheck=
```

1. From the All Content domain, go to **Sites > External Sites > Patching Support > Dashboards > RHEL Custom Repository Management**.
2. Click the Repositories tab and click **Import**.
3. From the **Import Existing Repositories** window, select and name the repository.
4. Click **Save**.

The repository is now imported and added to the list of repositories in the dashboard.

Chapter 5. Manage YUM transactions

View YUM transaction history and manage transactions through the YUM Transaction History dashboard, which works with Red Hat Enterprise Linux version 6 and later versions.

The dashboard displays the YUM transaction history and can be used to roll back, undo, and redo transactions in your deployment.

Rollback

The rollback feature undoes all transactions up to the point of the specified transaction.

Undo

The undo feature reverts a selected transaction only.

Redo

The redo feature repeats the recent transaction action.

Note: Active kernel cannot be rolled back for a kernel update.

The YUM Transaction History dashboard supports the use of the RHSM download plug-in with the following Red Hat versions: RHEL 6, RHEL 6 for System z, RHEL 7, RHEL 7 PPC64LE, RHEL 7 PPC64BE, and RHEL 8.

Requirements

To use the YUM Transaction History dashboard, ensure that you have the following requirements.

- Use BigFix version 9.0 and later.
- Use Red Hat Enterprise Linux 6 and later versions.
- Use YUM version 3.2.28 and later. The rollback functionality is not supported for the YUM versions 3.2.28 to 3.2.29-22.

Note: In the dashboard, if the YUM version of a selected endpoint is earlier than version 3.2.29-22, a warning sign next to the YUM version will indicate that the version does not support the rollback action. The **Rollback** button is disabled for all transactions if the version is not supported.

- Subscribe to the Patching Support site.
- Activate the YUM Transaction History analysis.

YUM transaction actions

The **Actions** column identify the YUM transaction actions in the dashboard. The following table give details of the actions for every transaction.

Table 12. Description of transaction actions

Action	Abbreviation	Description
Downgrade	D	At least one package has been downgraded to an older version.
Erase	E	At least one package has been removed.
Install	I	At least one new package has been installed.
Obsoleting	O	At least one package has been marked as obsolete.
Reinstall	R	At least one package has been reinstalled.
Update	U	At least one package has been updated to a newer version.

For more information about YUM history, go to Red Hat Product Documentation site.

YUM transaction analyses

The dashboard uses the following analyses:

YUM Transaction History analysis

Patch for Red Hat Enterprise Linux generates a log which records the results of the actions that are taken in the YUM Transaction History dashboard. The YUM History Transaction analysis retrieves the content of the action log `yum_history.log`. The log is located in `/var/opt/BESClient/EDRDeployData/yum_history.log`

YUM rollback capable field

YUM Logs analysis

YUM log is the official log that YUM generates by default in `/var/log/yum.log`. To change the default location, modify the log file settings in `/etc/yum.conf`. The YUM log analysis is very useful for troubleshooting purposes.

The analysis has 2 properties.

YUM Log property

Logs all the operations that are performed and identifies the transactions that are modified. This log retrieves the last 40 lines of the YUM log file.

YUM History Dashboard action log

This log lists the action logs for the redo, undo, and rollback operations from the action. The actions write the logs to `/var/opt/BESClient/EDRDeployData/yum_history.log`. The YUM History Dashboard action records the latest 5 actions.

Troubleshooting

To perform troubleshooting for the YUM Transaction History dashboard, you can check the `yum_history.log` file in `var/opt/BESClient/EDRDeployData`.

Rolling back a YUM transaction

Ensure that you meet the following requirements:

- Use BigFix version 9.0 and later.
- Use Red Hat Enterprise Linux 6 and later versions.
- Use YUM version 3.2.28 and later. The rollback functionality is not supported for the YUM versions 3.2.28 to 3.2.29-22.

  Note: In the dashboard, if the YUM version of a selected endpoint is earlier than version 3.2.29-22, a warning sign next to the YUM version will indicate that the version does not support the rollback action. The **Rollback** button is disabled for all transactions if the version is not supported.

- Subscribe to the Patching Support site.
- Activate the YUM Transaction History analysis.

Note: Active kernel cannot be rolled back for a kernel update.

1. Using the BigFix console, go to **External Sites > Patching Support > Dashboards > YUM Transaction History**.
2. Select the endpoint whose YUM history you want to view.

   Note: If the YUM version of a selected endpoint is earlier than version 3.2.29-22, a tooltip will indicate that the version is not supported.

3. Select the transaction that you want to roll back to.
4. Click **Rollback**.
5. The **Rollback Up To Transaction** window opens. OPTION: You can add flags in the field.Click **Apply**.
6. From the **Take Action** window, select the computer and click **OK** to run the action.

Undo a YUM transaction

Use this feature to revert to a single, specific transaction.

Ensure that you meet the following requirements:

- Use BigFix version 9.0 and later.
- Use Red Hat Enterprise Linux 6 and later versions.
- Use YUM version 3.2.28 and later.

> ✎ **Note:** In the dashboard, if the YUM version of a selected endpoint is earlier than version 3.2.29-22, a warning sign next to the YUM version will indicate that the version does not support the rollback action. The **Undo** button is disabled for all transactions if the version is not supported.

- Subscribe to the Patching Support site.
- Activate the YUM Transaction History analysis.

> ✎ **Note:** Active kernel cannot be rolled back for a kernel update.

1. Using the BigFix console, go to **External Sites > Patching Support > Dashboards > YUM Transaction History**.
2. Select the endpoint whose YUM history you want to view.
3. Select the transaction whose rollback that you want to undo.
4. Click **Undo**.
5. In the **Undo Transaction** window, click **Apply**.
6. From the **Take Action** window, select the computer and click **OK** to run the action.

Redo a YUM transaction

Use this feature to repeat the recent transaction action.

Ensure that you meet the following requirements:

- Use BigFix version 9.0 and later.
- Use Red Hat Enterprise Linux 6 and later versions.
- Use YUM version 3.2.28 and later.

> ✎ **Note:** In the dashboard, if the YUM version of a selected endpoint is earlier than version 3.2.29-22, a warning sign next to the YUM version will indicate that the version does not support the rollback action. The **Redo** button is disabled for all transactions if the version is not supported.

- Subscribe to the Patching Support site.
- Activate the YUM Transaction History analysis.

> ✎ **Note:** Active kernel cannot be rolled back for a kernel update.

1. Using the BigFix console, go to **External Sites > Patching Support > Dashboards > YUM Transaction History**.
2. Select the endpoint whose YUM history you want to view.
3. Select the transaction that you want to redo.
4. Click **Redo**.
5. In the **Redo Transaction** window, click **Apply**.
6. From the **Take Action** window, select the computer and click **OK** to run the action.

Chapter 6. Checking for YUM package updates

You can identify YUM package updates that you must install in your deployment by using a task.

You can refer to a list that details the YUM package updates that are applicable to your Red Hat Enterprise Linus endpoints. When you run the **ID 39: YUM: Check Available Package Updates** task, the **YUM Logs** analysis shows the results in a new column. The task uses the `yum check-update` to determine which updates are available for your installed packages.

The task uses the repository in your deployment. Ensure that the YUM packages are available in your repository when you run the task.

Using the YUM: Check Available Package Updates task

- Subscribe to the **Patching Support Beta** site.
- Ensure that the **YUM Logs** analysis is activated.
- Ensure that your endpoint uses a repository and that the YUM packages are available in the repository.

1. From the console, go to **Patching Support Beta** site, select the following task: **ID 39: YUM: Check Available Package Updates**.
2. Click **Take Action** to run the task.
3. Click **OK**.
4. When the action completes, go to **Patching Support Beta > Analyses > Analysis: YUM Logs** and select the **Results** tab.

   The **YUM check-update output** column is added and you can check if your endpoints have updates that must be installed.

Chapter 7. Using RHSM download plug-ins

The download plug-in is an executable program that downloads relevant packages directly from the patch vendor. Fixlets use an internal protocol to communicate with the download plug-in to download files. These Fixlets are based on updates made by the vendor.

You must create and download identification certificates through the Red Hat Subscription Management system to use the RHSM Download Plug-in. For the Fixlet to be able to use the protocol, register the download plug-in on the BigFix server or BigFix relay. Use the Manage Download Plug-ins dashboard to register the appropriate plug-in.

The Red Hat Subscription Management (RHSM) download plug-in is an enhanced version of the download plug-in for Red Hat that uses the RHSM to download and cache patches from a vendor's website to the BigFix server. The enhanced download plug-in enable the following possibilities.

- Customize available repositories through a user extensible repository list.
- Installation and dependency resolution can easily be extended to all repositories, not just those that are shipped out of the box.
- Customers and service teams can easily extend functionalities.
- Eliminates dependencies on utilities such as bzip2, gzip, and similar.

You can do the following tasks with the RHSM download plug-in:

- Register *(on page 40)*

  📝 **Note:** To view this topic, see Registering the RHSM download plug-in *(on page 40)*

- Unregister *(on page 54)*
- Configure basic settings *(on page 51)*
- Configure advanced settings *(on page 51)*
- Unregister *(on page 54)*
- Upgrade *(on page 54)*
- Extend to use unsupported RHSM repositories *(on page 54)*

📝 **Note:**

The RHSM download plug-in does not work when the Require SHA-256 Downloads option in the BigFix Administration tool is enabled. When this option is enabled, all download verification use only the SHA-256 algorithm. However, there are certain Red Hat repository metadata, which do not contain SHA-256 values for packages in the repository that are used by the plug-in.

Consider disabling the Require SHA-256 Downloads option to successfully deploy a patch. Security and package integrity is not compromised as another layer of checking and verification is done using the GPG

signature of the package. For more information about the download option, see BigFix Platform Installation Guide at https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Installation/c_security_settings.html.

The YUM Transaction History dashboard supports the use of the RHSM download plug-in with the following Red Hat versions: RHEL 6, RHEL 6 for System z, RHEL 7 for System z, RHEL 7, RHEL 7 PPC64LE, and RHEL 7 PPC64LE. Endpoints must be subscribed to the Patching Support site.

Setting up RHSM download plug-in

You must create and download identification certificates through the Red Hat Subscription Management system to use the RHSM Download Plug-in.

Before you use the RHSM Download Plug-in, you must do the following steps to set up the RHSM certificate.

- Ensure that you have met the prerequisites to using the RHSM Download Plug-in. The prerequisites are found in Registering the RHSM Download Plug-in *(on page 40)*.
- Register the RHSM Download Plug-in. *(on page 40)*
- Create RHSM certificates through access.redhat.com *(on page 42)*
- Add the certificates to the download plug-in *(on page 47)*. It is possible to add multiple certificates.
- Verify that the RHSM download plug-in certificate has access to Red Hat repositories *(on page 49)*

- Import the GPG keys to endpoints

  Red Hat requires the use of GPG keys. Before deploying patches, you must apply the applicable task to import the GPG keys to the endpoints.

  - **Import RPM-GPG-KEY-redhat-release - RHEL 6** (from the Patches for RHEL6 Native Tools site)
  - **Import RPM-GPG-KEY-redhat-release - RHEL 7** (from the Patches for RHEL 7 site)

  You only need to deploy the Import GPG key Fixlet once to the endpoints. The following tasks are optional.

  - Use the **Change Timeout for Prefetch Plugins** task, which is found in the Patching Support site, to avoid an error with the execution of the prefetch plug-in. The error is caused by a short prefetch timeout setting. To remedy this, run the task to change the timeout to 30 minutes.
  - After running the task to change the timeout settings, restart the BES client with the **TROUBLESHOOTING: Restart BES Client on RHEL/SUSE** task. The task is found in the BES Support site.
- When configuring the download plug-in, the BigFix server and the BigFix client on the BigFix server must have the same version to avoid a null error. At a minimum, the version must be on the same major version level, for example 9.x.

For more information about what other tasks you can do with the download plug-in, including configuring, extending, and unregistering the download plug-in, see Using the RHSM download plug-in *(on page 38)*.

Registering the RHSM download plug-in

Use the Manage Download Plug-ins dashboard to register the RHSM download plug-in on the BigFix server or BigFix relay.

You must complete the following tasks:

- For Linux BigFix servers, install the following packages and their dependencies:
    - GLIBC 2.2.5
    - GLIBC 2.3
    - GNU/Linux kernel version 2.6.31 and later
- Subscribe to the **Patching Support** site to gain access to the Manage Download Plug-ins dashboard.
- From the BES Support site, enable the **Enable Encryption for Clients** Fixlet on servers and relays for which you want to register the download plug-in.
- The RHSM download plug-in will need to access cdn.redhat.com at port 443, with HTTPS client certificate authentication. Ensure that the network, proxy, or firewall is configured with these settings.
- Activate the following analyses:

Table 13. Analyses that must be activated

ID	Analysis	Site
977	Encryption Analysis for Clients	BES Support
45	Download Plug-in Versions	Patching Support

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server on which the download plug-in is to be registered.

    Important: You can register the download plug-in on the BigFix server or BigFix relays.

3. From the Plug-ins table, select **RHSM Plug-in**.
4. Click **Register**.

    The Register Red Hat Plug-in wizard displays.
5. Enter the proxy parameters if the downloads must go through a proxy server.

    Proxy URL

    The URL of your proxy server. It must be a well-formed URL that contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

    Proxy Username

    Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

    Proxy Password

Your proxy password if your proxy server requires authentication. Note that only basic authentication is supported.

Confirm Proxy Password

Your proxy password for confirmation.

6. Click **OK**.

The Take Action dialog displays.

7. Select the target computer.

8. Click **OK**.

You successfully registered the RHSM download plug-in. The `plugin.ini` configuration file is created in the following locations:

On Windows systems

`%PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins\RHSMProtocol`

On Linux systems

`/var/opt/BESServer/DownloadPlugins/RHSMProtocol`

After you have registered the RHSM download plug-in, create a folder named 'certs' in the RHSM Protocol folder.

On Windows systems

`%PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins\RHSMProtocol`

On Linux systems

`/var/opt/BESServer/DownloadPlugins/RHSMProtocol`

Note: For Linux systems, ensure that the new **certs** folder is in lower case to avoid issues.

Note: If you are registering the RHSM download pug-in on the BigFix relay, you need to perform the additional tasks. See Registering the RHSM download plug-in for BigFix Relays *(on page 41)*

Registering the RHSM download plug-in for BigFix Relays

Use the Manage Download Plug-ins dashboard to register the RHSM download plug-in on the BigFix Relays.

1. To register and configure the RHSM download plug-in, see Registering the RHSM download plug-in *(on page 40)*

2. You need a repository list file in the suitable format. You can create a new format or use the existing format form the Patch Support site.

- If you are creating a new format, see Extending the RHSM download plug-in (Optional) *(on page 54)* for more information on the appropriate formats.
- If you are using the existing format from the Patch Support site, BigFix Server machine must be subscribed to the Patch Support site.

  a. After the subscription, on the BigFix Server machine locate `DLRHELRepoList.json` file in this path `%PROGRAM FILES%\BigFix Enterprise\BES Server\GatherDBData \gather\Patching Support\CurrentSiteData\DLRHELRepoList.json` for Windows and this path `/var/opt/BESServer/GatherDBData/gather/Patching Support/ CurrentSiteData/DLRHELRepoList.json` for Linux.

  b. Copy the file into the target BigFix Relay machine.

3. Locate the `plugin.ini` file in this path `%PROGRAM FILES%\BigFix Enterprise\BES Relay \DownloadPlugins\RHSMProtocol` for Windows and this path for `/var/opt/BESRelay/ DownloadPlugins/RHSMProtocol` for Linux.

4. In the `plugin.ini` file, update the path of **primaryRepoListFile**. For more information on plug-in settings, see Configuring the advanced RHSM download plug-in settings *(on page 51)*.

> ⚠️ **Important:** The updated value of the path must be corresponding to the location of the repository list file.

> ⚠️ **Important:** The RHSM download plug-in must be registered in both the BigFix Relay and BigFix Server to work as intended.

Creating the RHSM entitlement certificates

You must create and download certificates through the Red Hat Subscription Management system. From the Red Hat portal, you must register a system then attach your subscriptions (entitlements) to that system.

This section describes the steps you need to create RHSM certificates through the Red Hat Subscription Management system. This entails registering a system then attaching your subscriptions (entitlements) to that system.

You must have at least one set of certificates that you need to download. You only need to register at least one system and attach the subscriptions (entitlements) to cover your machines.

> 📝 **Note:** The System Identity Certificate is no longer required from v1.0.2.0 of the RHSM Download Plug-in and RHSM download Cacher.

> 📝 **Note:** Red Hat requires Oracle Java users to enable a new content set to access the Oracle Java SE software. To deploy Oracle Java patches, create separate certificates for Oracle Java (Restricted Maintenance) with the Oracle Java Add-On (Physical or Virtual Nodes) subscription. The steps for creating the certificate and

attaching them to a subscription are detailed in this section. For more information about Red Hat requirement to enable the new content set, see the Red Hat Knowledge base site.

1. Log in to the Red Hat Customer Portal at https://access.redhat.com/.
2. Go to the **Subscription Overview** page at https://access.redhat.com/management/. Click **Systems**.
3. Click **New** to create a new system.
4. Fill in the form with the following information then click **Create**.
   - System type: Virtual system type
   - Name
   - Architecture: x84_64

     If you are using System z, select s390x.

   - Number of Sockets or LPARS - this field displays when you select Physical system type
   - Number of vCPUs - this field displays when you select Virtual system type
   - Red Hat Enterprise Linux version: 7.2

Selecting Red Hat Enterprise Linux version 7.2 will create entitlement certificates that also work with RHEL 6. The RHSM download plug-in does not support RHEL 5.

Note: This should not affect the entitlement but only the cert format.

5. When the page has refreshed, click the **Subscriptions** tab and click **Attach Subscriptions**.
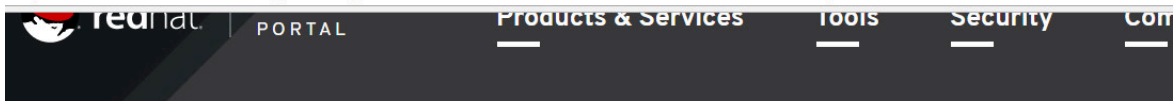
6. Select the subscriptions that will be attached to the system that you created and click **Attach Subscriptions**.
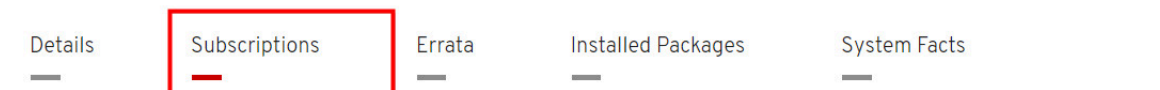
7. The page displays the subscriptions attached to the system. Click **Download Certificates**.
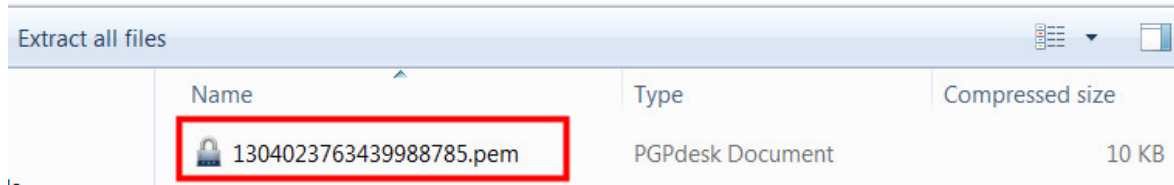
8. Unzip the downloaded certificate. Red hat now uses a single certificate instead of the earlier RHSM version which required having both an entitlement certificate and an identity certificate.

> **Note:** Ensure that your Red Hat subscriptions are active to avoid errors.

9. Go to <BES Server>\DownloadPlugins\RHSMProtocol\certs and create a folder. Place the unzipped certificates in the newly-created folder. Ensure that your Red Hat subscriptions are active to avoid errors.

> **Note:** In the plugin.ini, the "rootCertDir" value should be "certs", which is the default value. This is the relative path from the RHSMDownloadPlugin.exe to the rootCertDir called "certs".

You can run verify access to the repos when you run RHSMPlugin.exe --check-baserepos. For more information, see the Verifying RHSM download plug-in certificate access to Red Hat repositories section.

Adding the RHSM entitlement certificates to the download plug-in

To add certificates to the download plug-in, create a folder in <BES Server>\DownloadPlugins\RHSMProtocol\certs and copy the entitlement certificates and the system identity certificates in the created folder.

Take note of the following guidelines when adding the certificates.

- You must create sub-folders under the certs folder. For example, cert_set_1, cert_set_2.
- Once you have created the new folder under <BES Server>\DownloadPlugins\RHSMProtocol\certs, ensure that the following guidelines are followed within the new folder.
  - Only files with .pem extension are allowed. There are 2 types of ".pem" files that can be placed in the newly created folder:

    Entitlement Certificates

    You can have one or more entitlement certificates. An example of an entitlement certificate is 443229635427054308.pem.

    System Identity Certificate

    You can place only one system identify certificate. System identity certificates are typically identifiable by the dash in its file name. An example of a system identity certificate is 2916b776-ab7f-432f-b8a9-b39c812542a7.pem.

◦ Different sets of certificates must be kept in separate sub-folders in the <rootCert> folder.

> 🛈 **Tip:** Adding the expiration date to the file name of each certificate can help with tracking and debugging.

1. Create a new folder in `<BES Server>\DownloadPlugins\RHSMProtocol\certs`. For example, if the new folder is called cert_set_1, then the path would be `<BES Server>\DownloadPlugins \RHSMProtocol\certs\cert_set_1`.
2. Copy all the entitlement certificates and the system identity certificate to the new folder. For example, the .pem files should be placed in `<BES Server>\DownloadPlugins\RHSMProtocol\certs \cert_set_1`. In the plugin.ini, the "rootCertDir" value should be "certs", which is the default value. This is the relative path from the RHSMDonwloadPlugin.exe to the rootCertDir called "certs".

> ✎ **Note:** If you have more than one set of certificates, ensure that only one set of certificates go to one folder.
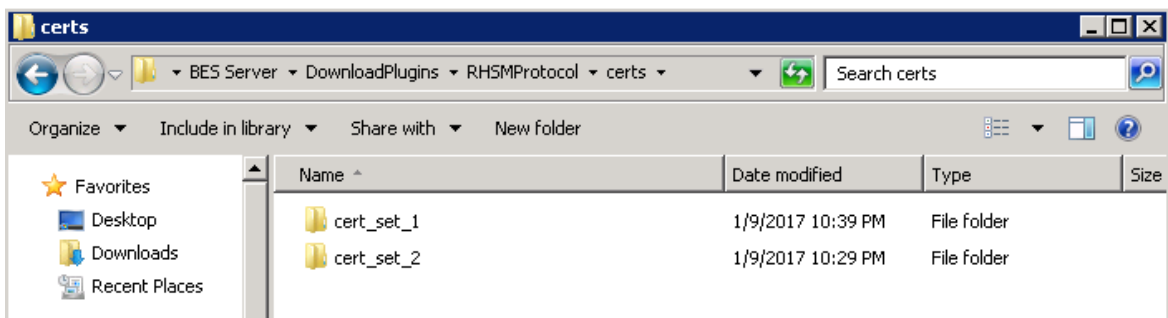
> ⚠ **Important:** To avoid errors, ensure that only the files of the entitlement certificate and system identity certificates are in the newly-created folder.
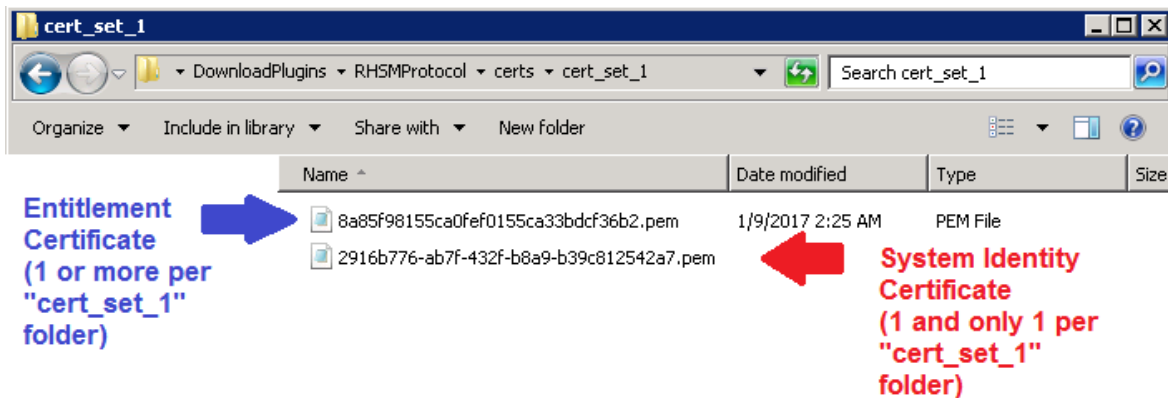
> ✎ **Note:** Different sets of certificates must be kept in different sub-folder in the <rootCert> folder.

Verifying RHSM download plug-in certificate access to Red Hat repositories

From the command line, you can use the --check-baserepos and the --check-allrepos commands to check that the entitlement certificates, which are in the 'certs' folder, have access to the supported Red Hat repositories.

Use the following commands to verify if the entitlement certificate found in `<BES Server>\DownloadPlugins \RHSMProtocol\certs` can access the Red Hat repositories.

The results, which are displayed in the command prompt and printed to the RHSMPlugin.log, identify the number of accessible repositories which the certificate is entitled to against the available Red Hat repositories that BigFix supports.

--check-baserepos

Checks if the entitlement certificates in the 'certs' folder has access to the base repositories.

--check-allrepos

Checks if the entitlement certificates in the 'certs' folder has access to the base repositories and the sub-repositories.

For a list of Red Hat repositories that BigFix supports, see https://help.hcltechsw.com/bigfix/9.5/patch/Patch/Patch_RH/c_supported_rhel_repos.html.

Configuring the blacklist repository function to allow only entitled repositories

The repository blacklist function blocks access to Red Hat repositories that are not needed for patching.

Identify the Red Hat repositories that your subscription covers. You can run the --check-baserepos command on the RHSMPlugin.exe. For more information, see Verifying RHSM download plug-in certificate access to Red Hat repositories.

The repository blacklist, which is drawn from the allowrepos.cfg, lists which repositories the download plug-in can access. The repository blacklist improves the performance of the download plug-in and the download cacher. It also reduces the amount of errors that are logged in RHSMDownloadCacher.log and RHSMPlugin.log.

Automatic configuration

Starting from v1.0.1.2, after running --check-baserepos, users are prompted if they want to automatically update the allowrepos.cfg.

Manual configuration

Manual configuration of the functionality is available from version 1.0.0.x of the RHSM download plug-in and RHSM download cacher.

The functionality works around a limitation in how the BES server processes downloads. The limitation might result to unnecessary errors being logged and to longer processing time of the download plug-in and download cacher.

After the RHSM download plug-in is run for the first time, a file called allowrepos.cfg is created in the same folder as the download plug-in and the cacher. The file lists the Red Hat repositories that BigFix supports. By default, all repositories are allowed.

- YES or Y = the repository is allowed to be accessed by the plug-in
- NO or N = the repository is not allowed to be accessed by the plug-in

Note: You only need to run the RHSM download plug-in once to generate the file.

1. If you have not done so, run the RHSM download plug-in. The allowrepos.txt file is generated in the same folder as the RHSM download plug-in and the RHSM download cacher.
2. Open allowrepos.txt in a text editor. The file contains a list of repositories which are set to YES by default.
   - YES or Y = the repository is allowed to be accessed by the plug-in
   - NO or N = the repository is not allowed to be accessed by the plug-in

   client-6-x86 = yes

   client-6-x86_64 = yes

   client-7-x86_64 = yes

   server-6-s390x = yes

   server-6-x86 = yes

   server-7-x86_64 = yes

   server-7-ppc64le = yes

   server-7-ppc64be = yes

   workstation-6-x86 = yes

   workstation-6-x86_64 = yes

   workstation-7-x86_64 = yes

3. Set the values of the repositories. Set YES or Y to the Red Hat repositories to which you have access and NO or N to repositories to which you have no access.
4. Save your changes.

Configuring the basic RHSM download plug-in settings

Use the Manage Download Plug-ins dashboard to configure the basic properties, such as proxy settings of the Red Hat Subscription Management (RHSM) download plug-in.

The BigFix server and the BigFix client on the server must have the same version to avoid a null error.

The scope of this task only covers the basic RHSM plug-in configuration from the BigFix console.

You might want to take note of your existing configuration for the download plug-in. Existing configurations are overwritten when you configure the download plug-in.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be configured.
3. From the Plug-ins table, select **RHSM Plug-in**.
4. Click **Configure**.
   The Configure Red Hat Plug-in wizard displays.
5. Enter the proxy parameters if the downloads must go through a proxy server.

   Proxy URL

   > The URL of your proxy server. It must be a well-formed URL that contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

   Proxy Username

   > Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

   Proxy Password

   > Your proxy password if your proxy server requires authentication.

   Confirm Proxy Password

   > Your proxy password for confirmation.

6. Click **OK**.
   The Take Action dialog displays.
7. Select the target computer.
8. Click **OK**.

Once the action completes successfully, you have successfully applied the settings that you configured.

Configuring the advanced RHSM download plug-in settings

For advanced configurations, manually edit the RHSM download plug-in configuration file called `plugin.ini`.

The `plugin.ini` file is automatically created when the download plug-in is registered from the Manage Download Plug-in dashboard. It contains the settings for logging and caching, as well as custom configurations for extending the repository list file.

On Linux systems, the file is in the root directory tree occupied by the download plug-in. For example, `/var/opt/BESServer/DownloadPlugins/RHSMProtocol`.

On Windows systems, the file is in the BigFix server installation directory. For example, `%PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins\RHSMProtocol`.

> **Note:** The `plugin.ini` is divided into sections, which are denoted by square brackets. Ensure that the options are under the correct sections. Moving the options to a different section might result in errors.

primaryRepoListFile

This list file contains the repositories that BigFix supports by default. Use either an absolute path or relative path.

extendedRepoListFile

This optional repository list is for extensions to the **primaryRepoListFile**, the default repository list. It has the same format as **primaryRepoListFile**. Use either an absolute path or relative path.

onlyUseExtendedRepoListFile

This is an optional configuration list file to limit downloads to only custom repositories as stated in the "**extendedRepoListFile**". Its value can be "yes" or "no". No is the default value.

localCache

This setting is used when the RHSM download plug-in is used in an air-gapped environment. The **localCache** field is a full path to the download directory, (--download_dir) that is specified when using the RHSM Download Cacher. Use an absolute path. For example,

```
localCache = C:\RHEL_Cache
```

localCacheOnly

This setting is used when the RHSM download plug-in is used in an air-gapped environment. By default, its value is set to "no". When this setting is set to "yes", the RHSM download plug-in will get its files from the localCache and will not attempt to get files from the Internet.

rootCertDir

This setting stores the relative path of the rootCertDir folder.

The following options require paths. Relative paths are relative to the download plug-in executable directory. By default, the executable file is in the DownloadPlugins\RHSMProtocol folder. Use the required corresponding path types as indicated in the following list:

- file: Use either an absolute path or relative path
- primaryRepoListFile: Either an absolute path or relative path
- extendedRepoListFile: Either an absolute path or relative path
- localCache: Use an absolute path

Setting the logging level

The logging level determines the amount of detail that is written to the `RHSMPlugin.log` file.

The available logging levels are as follows:

ERROR

Contains errors related to the execution of the download plug-in, which might indicate an impending fatal error.

WARNING

Contains information about failed downloads, and reasons for failure.

INFO

Contains general information outlining the progress and successful downloads, with minimal tracing information.

DEBUG

Contains fine-grained information used for troubleshooting issues. This is the most verbose level available.

You can change the logging level option from the `[Logger]` section of the `plugin.ini` file.

```
[Logger]
file = logs/RHSMPlugin.log
level = INFO
```

For example, if the logging is set to INFO, the logger outputs any logs for that level and any level above it. In this case, it outputs the INFO, WARNING, and ERROR logs.

Note: Setting the logging level to DEBUG increases the amount of information to log, which might impact performance. Only increase the logging level to DEBUG when investigating an issue, and switch back to INFO or WARNING after the issue is resolved.

Adding an extended repository list file

The RHSM download plug-in can be configured to work with repositories that are not officially supported by BigFix, such as debuginfo repository, if required. For more information, see Extending the RHSM Download Plug-in (Optional) (on page 54).

Unregistering the RHSM download plug-in

Use the Manage Download Plug-ins dashboard to unregister the RHSM download plug-in.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be unregistered.
3. From the Plug-ins table, select **RHSM Plug-in**.
4. Click **Unregister**.
5. Select the target computer.
6. Click **OK**.

You successfully unregistered the RHSM download plug-in.

Upgrading the RHSM download plug-in

Use the Manage Download Plug-ins dashboard to upgrade the RHSM download plug-in to the latest version available.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be upgraded.
3. From the Plug-ins table, select **RHSM Plug-in**.
4. Click **Upgrade**.
   The Take Action dialog displays.
5. Select the target computer.
6. Click **OK**.

> 📝 **Note:** It is mandatory to re-configure the Download Plug-ins.

> 📝 **Note:** The latest versions of Download Plug-ins are enhanced to strengthen the security of storing Proxy Password and Vendor Password.

You now have the latest version of the RHSM download plug-in installed.

Extending the RHSM download plug-in (Optional)

You can configure the RHSM download plug-in to download and cache packages from repositories that are not officially supported by BigFix.

The RHSM download plug-in can resolve package dependency for unsupported RHSM repositories, allowing the installation of unsupported dependent packages. This extended solution allows you to use BigFix to deploy packages from repositories that are not shipped out of the box, such as debuginfo repositories.

Before you begin, you must complete the following tasks:

- Ensure that appropriate licenses are registered and that your Red Hat subscription is active.
- Review the BigFix Patch for Red Hat support information and verify the list of supported repositories: Red Hat Repositories that BigFix supports.

Creating an extended repository list file

The Red Hat download plug-in can use an extended repository list file, which contains additional repositories for both base and extension products that are included in your subscription.

The extended repository list file must meet the following criteria:

- It must be a valid `.json` file.
- It must be accessible to the Red Hat download plug-in. Ensure that the Administrator or root user can read the file.
- It must contain the following format:

```
{
    "<OS_key>":[
        {"name": "<name>", "baseurl": "<url>"},
        {"name": "<name>", "baseurl": "<url>"}
    ]
}
```

For example:

```
{
    "x86":[
        {"name": "Red Hat Enterprise Linux 6 Server - Oracle Java (Source RPMs)",
"baseurl": "https://cdn.redhat.com//content/rhel/server/6/6Server/
x86/oracle-java/source/SRPMS"}
    ]
}
```

> **Note:** It uses the same format as the `DLRHELRepoList.json` file, which is set for `repoListFile` in the `plugin.ini` file.

You must replace the placeholders, which are enclosed in angle brackets <>, with the actual values.

OS_key

To use the unsupported repositories with the BigFix RHEL Patching content, use the following OS keys as listed in the `DLRHELRepoList.json` file. This might not be the full list as later versions of the download

plug-in are released. To get the latest and complete copy of the repository list, complete the following actions:

1. Check whether your endpoints are registered to the latest download plug-in. The Manage Download Plug-ins dashboard indicates when the plug-in is up-to-date or when a new version is available.
2. View the `DLRHELRepoList.json` file from the following locations:

   On Windows Systems

   ```
   %PROGRAM FILES%\BigFix Enterprise\BES Server\GatherDBData
   \gather\Patching Support\CurrentSiteData
   ```

   On Linux Systems

   ```
   /var/opt/BESServer/gatherDBData/gather/Patching Support/
   CurrentSiteData
   ```

> ⚠️ **Important:** Use the correct OS key for each repository to avoid download and dependency resolution issues.

name

> You can retrieve the name from the Red Hat Customer Portal; see Retrieving the repository information *(on page 56)*.

baseurl

> You can retrieve the distribution target name from the Red Hat Customer Portal; see Retrieving the repository information *(on page 56)*. In the baseurl, replace the architecture `$basearch` and `$releasever` values.

Retrieving the repository information

To retrieve repository information from the Red Hat Customer Portal, complete the following steps:

1. Log in to the Red Hat Customer Portal at https://access.redhat.com/.
2. Go to the **Subscription Overview** page at https://access.redhat.com/management/.
3. Click the appropriate subscription. The Subscription Information page is displayed.
4. From the Manage section, under **Subscriber Inventory**, you can see the number of subscribed systems and hypervisors. Click **Systems**.
5. From the **Content Sets** tab, go to the row of the repository and click **View**.

6. You can derive the values for the name and baseurl keys based on the following guidelines:

   name

   > Select the repository name value from the **Name** column. An example of the name value is Red Hat Enterprise Linux 6 Server - Oracle Java (Source RPMs)

baseurl

The baseurl starts with `https://cdn.redhat.com/`. You can see the repository baseurl from the **Content details** column, in the **Content Download URL** field. For example,

```
/content/rhel/server/6/$releasever/$basearch/

oracle-java/source/SRPMS
```

Replace the values for $releasever and $basearch. See the table for examples of values. When the values are replaced, an example of the baseurl is:

```
https://cdn.redhat.com//content/rhel/server/6/6Server/

x86/oracle-java/source/SRPMS
```

Architecture in baseurl	Possible values
$releasever	◦ 6Server ◦ 6Client ◦ 6Workstatsion ◦ 7Server ◦ 7Client ◦ 7Workstation
$basearch	x86_64, i386, ppc64le, ppc64be

> ✎ **Note:** This table contains examples of values. For more updated and complete values, see the Red Hat Customer Portal at https://access.redhat.com/

To verify if the certificate has access to the repository that you chose to setup, import the certificate to the browser, then use the URL to check if it can be accessed.

Updating the RHSM download plug-in configuration file

Configure the RHSM Download Plug-in to use an extended repository list file. The `plugin.ini` configuration file is overwritten when the RHSM download plug-in is unregistered or configured from the Manage Download Plug-in dashboard. Any change that you make in the configuration file is lost, therefore take note of the previous changes.

The configuration file includes the following:

primaryRepoListFile

This list file contains the repositories supported by default by BigFix.

extendedRepoListFile

This optional repository list is for extensions to the default repository list. It has the same format as the default repository list.

onlyUseExtendedRepoListFile

This is an optional configuration list file to limit downloads to only custom repositories.

1. Use a text editor to open the `plugin.ini` file from the following locations:

    On Windows systems

    ```
    %PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins
    \RHSMProtocol
    ```

    On Linux systems

    ```
    /var/opt/BESServer/DownloadPlugins/RHSMProtocol
    ```

2. In the **extendedRepoListFile** field, enter the absolute path or relative path to the extended repository list file. If it is set to a relative path, the path must be relative to the location of the RHSM download plug-in executable.

    For example:

    ```
    extendedRepoListFile  = C:\Program Files (x86)\BigFix Enterprise\
                  BES Server\DownloadPlugins\RHSMProtocol\<extendedRepoList>.json
    ```

3. If you want set the RHSM Download Plug-in to only use the extended repository list, set the **onlyUseExtendedRepoListFile** field to yes.

    For example:

    ```
    onlyUseExtendedRepoListFile= yes
    ```

    If you want to set RHSM Download Plug-in to use both repository list files, configure the setting to no. In cases where the same OS key is used in both files, the repositories will be combined.

4. Save the file.

In the following examples, the EPEL 6 repo was added to server-6-x86_64 and the EPEL 7 repo was added to server-7-x86_64. Running the `RHSMPlugin.exe --check-allrepos` command will have the following output.

Example: When EPEL 6 repo is added to server-6-x86_64

```
4496 : 2018-02-28 15:26:31 : INFO : Testing Certs access to: server-6-x86_64
```

```
4496 : 2018-02-28 15:26:31 : INFO : EPEL_6
```

```
4496 : 2018-02-28 15:26:31 : INFO : Success!
```

```
4496 : 2018-02-28 15:26:31 : INFO : Red_Hat_Enterprise_Linux_6_Server_(RPMs)
```

```
4496 : 2018-02-28 15:26:31 : INFO : Success!
```

Example: When EPEL 7 repo is added to server-7-x86_64

```
4496      : 2018-02-28 15:26:31 : INFO      :  Testing Certs access to: server-7-x86_64
```

```
4496      : 2018-02-28 15:26:31 : INFO      :  EPEL_7
```

```
4496 : 2018-02-28 15:26:31 : INFO : Success!
```

```
4496 : 2018-02-28 15:26:31 : INFO : Red_Hat_Enterprise_Linux_7_Server_(RPMs)
```

```
4496 : 2018-02-28 15:26:31 : INFO : Success!
```

Chapter 8. Using the RHSM download cacher

Use the RHSM download cacher to download and cache x86, x86_64, S390x, ppc64le, ppc64 Red Hat patches in air-gapped environments.

The RHSM download cacher supports the following Red Hat versions:

- RHEL 6 x32
- RHEL 6 x64
- RHEL 7 x32
- RHEL 7 x64
- RHEL 6 s390x
- RHEL 7 s390x
- RHEL 7 PPC64LE
- RHEL 7 PPC64BE
- RHEL 8 x64
- RHEL 8 s390x
- RHEL 8 PPC64LE

You can run the RHSM download cacher on a Windows system or a Linux system. For information about requirements, see BigFix - System Requirements.

The RHSM download cacher is available from the BigFix Support site.

- For Windows systems, download the tool from https://software.bigfix.com/download/bes/util/ RHSMDownloadCacher.exe
- For Linux systems, download the tool from

  https://software.bigfix.com/download/bes/util/RHSMDownloadCacher-linux.tar.gz.

  > **Note:** To use the tool successfully, ensure to install the following packages and their dependencies: GLIBC 2.2.5, GLIBC 2.3, and GNU/Linux 2.6.31 and later

> **Note:** The RHSM download cacher will need to access cdn.redhat.com at port 443 and access sync.bigfix.com at port 80.

> **Note:** For illustration purposes, this section indicates the steps to run the RHSM download cacher in Windows. However, the parameters and subcommands to run the RHSM download cacher are the same for both Windows and Linux systems.

You can run the tool `RHSMDownloadCacher.exe` to perform additional operations. To run this tool from the command prompt, use the following command:

```
RHSMDownloadCacher.exe [-h] --rootCertDir <rootcertdir>
```

```
[parameters...] {subcommand} [-h]  [subparameters...]
```

where:

-h

Specifies the help message of a command instead of running the command.

--rootCertDir

Specifies the root directory where the entitlement certificates and system identity certificates are located. Each set of entitlement certificates and system identity certificates must be placed in their own folder. You can configure the rootCertDir in the plugin.ini file.

check-baserepos

Checks if the entitlement certificates under the certs folder can access the base Red Hat repositories that BigFix supports. The results are displayed in the console and printed in the RHSMDownloadCacher.log.

check-allrepos

Checks if the entitlement certificates under the certs folder can access the Red Hat base repositories and its sub-repositories that BigFix supports. The results are displayed in the console and printed in the RHSMDownloadCacher.log.

parameters

Specifies the optional parameters to be used to configure the download cacher.

> **--proxyServer**
>
> Specifies the URL of the proxy server to use. It must be a well-formed URL that contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: http://192.168.100.10:8080.
>
> **--proxyUser**
>
> Specifies the proxy user name if your proxy server requires authentication. It is usually in the form of *domain\username*.
>
> **--proxyPass**
>
> Specifies the proxy password if your proxy server requires authentication.
>
> **--download_dir**
>
> Specifies the directory where the repository metadata and the packages are cached. This directory must be transferred to the BES Server. The localCache of the RHSM plug-in's plugin.ini must be updated to reference this directory.

If this parameter is not defined, the files are downloaded to the directory that is relative to the download cacher executable directory.

If this parameter is not defined, a default download_dir folder is used.

--sha1_download_dir

With effect from version 1.0.1.0, specifies the directory where the sha1 packages are cached. The repository metadata is still cached in the --download_dir. The sha1_download_dir option stores the sha1 packages in a flat directory structure which can result to significant space saved when caching multiple repositories from the same Red Hat versions. Space-saving benchmarks are established with the use of the `--sha1_download_dir` through the `check-storagereq` subcommand.

To learn about the storage space benchmark, see .

--redownload

Specifies the flag to re-download and overwrite existing RPM files that are in the download directory.

If this parameter is not defined, RPM files are not re-downloaded. However, metadata are, by default, downloaded and overwritten.

--verifyExistingPkgChecksum

Specifies the flag to enforce a checksum check for existing RPM files when trying to download packages using the "buildRepo", "downloadPkg", or "downloadbypatchid" subcommands.

Note: The checksum is set to 'off' by default.

--loglevel

Specifies the log level. You can choose among DEBUG', 'INFO', 'WARNING', or 'ERROR'. By default, the value is set to 'INFO'.

INFO

Contains general information outlining the progress and successful downloads, with minimal tracing information.

WARNING

Contains information about failed downloads, and reasons for failure.

ERROR

Contains errors related to the execution of the download plug-in, which might indicate an impending fatal error.

DEBUG

Contains fine-grained information used for troubleshooting issues. This is the most verbose level available.

--help

Specifies the full description and help of a command instead of running the command.

subcommand subparameter

Specifies the subcommand and subparameters to be used to run the download cacher.

> **Note:** The subcommand and subparameter names are case-sensitive.

The *subparameter* varies for each *subcommand* as follows:

showKeys

Outputs the list of OS keys for the supported repositories in the `<cacher directory>\logs\RHSMDownloadCacher.log` file. An OS key indicates the Red Hat operating system version, architecture, and service pack of a single Red Hat repository.

The syntax to run this subcommand is:

```
RHSMDownloadCacher.exe -rootCertDir <rootcertdir> --download_dir <download_dir>
 [parameters] showsKeys
```

For example, `RHSMDownloadCacher.exe --rootCertDir certs --download_dir C:\downloads showKeys`

buildRepo

Builds a local mirrored repository and downloads all the relevant files based on the specified OS key.

The syntax to run this subcommand is:

```
RHSMDownloadCacher.exe --rootCertDir <rootcertdir> --download_dir <download_dir>
[parameters] buildRepo --key <OS_key1,OS_key2,…>
```

For example, `RHSMDownloadCacher.exe --rootCertDir certs --download_dir C:\downloads buildRepo --key server-7-x86_64`

where:

--key *OS_key1,OS_key2,…*

Specifies the Red Hat operating system version, architecture, and service pack. Entries must be separated by a comma and must not include spaces. It must use the following format:

```
<product>-<version_number>-<architecture>-<sp_level>
```

For example, `--key server-7-x86_64`.

check-storagereq

Checks the storage space requirement when using the `builRepo` command with and without the `--sha1_download_dir` option. The results are displayed in the console and in the RHSMDownloadCacher.log.

downloadMetadataOnly

Downloads the metadata of the specified OS keys.

The syntax to run this subcommand is:

RHSMDownloadCacher.exe --rootCertDir --download_dir C:\downloads downloadMetadataOnly --key server-7-x86_64

```
RHSMDownloadCacher.exe --rootCertDir <rootcertdir> --download_dir <download_dir>

[parameters] downloadMetadataOnly --key <OS_key1,OS_key2,…>
```

For example, `RHSMDownloadCacher.exe --rootCertDir certs --download_dir C:\downloads downloadMetadataOnly --key server-7-x86_64`

where:

--key *OS_key1,OS_key2,…*

Specifies the Red Hat operating system version, architecture, and service pack. Entries must be separated by a comma and must not include spaces. It must use the following format:

```
<product>-<version_number>-<architecture>-<sp_level>
```

For example, `--key server-7-x86_64`.

downloadPkg

Downloads the listed RPM files for the specified OS key.

📝 **Note:** If the package that you are downloading has dependencies, it is suggested that that buildrepo be used instead to avoid dependency issues

The syntax to run this subcommand is:

```
RHSMDownloadCacher.exe --rootCertDir <rootcertdir> --download_dir <download_dir>

[parameters] downloadPkg --key <OS_key1,OS_key2…>

--pkg <pkg1,pkg2,…>
```

For example, `RHSMDownloadCacher.exe --rootCertDir certs --download_dir C:\temp --redownload downloadPkg --key server-7-x86_64 --pkg python-qrcode-core-5.0.1-1.el7.noarch.rpm`

where:

--key *OS_key1,OS_key2,...*

Specifies the Red Hat operating system version, architecture, and service pack. Entries must be separated by a comma and must not include spaces. It must use the following format:

```
<product>-<version_number>-<architecture>-<sp_level>
```

For example, `--key python-qrcode-core-5.0.1-1.el7.noarch.rpm`.

--pkg *pkg1,pkg2,...*

Indicates the package name.

Each entry must be separated by a comma and must not include spaces. For example, `--pkg liblcms1-1.17-77.12.1.x86_64.rpm,liblcms1-32bit-1.17-77.12.1.x86_64.rpm`.

downloadByPatchId

Downloads files based on the patch ID for one or more OS keys. The RHSM cacher replaces the reference to the bulletins with the patch_id. The first two digits of the patch_id typically refers to the year. For example, the RHSA-2016-2573 bulletin is replaced with patch_id 162573, with '16' referring to the year.

Note: If the package that you are downloading has dependencies, it is suggested that that buildrepo be used instead to avoid dependency issues

The syntax to run this subcommand is:

```
RHSMDownloadCacher.exe --rootCertDir <rootcertdir>
--download_dir <download_certdir>[parameters] downloadByPatchId
 --key <OS_key1,OS_key2…>
--patch_id <patch_id1,patch_id2,…>
```

For example, `RHSMDownloadCacher.exe --rootCertDir certs --download_dir C:\downloads downloadByPatchId --key server-7-x86_64 --patch_id 162516`

where:

--key *OS_key1,OS_key2,...*

Specifies the Red Hat operating system version, architecture, and service pack. Entries must be separated by a comma and must not include spaces. It must use the following format:

```
<product>-<version_number>-<architecture>-<sp_level>
```

For example, `--key server-7-x86_64`.

--patch_id *patch_id1,patch_id2,…*

Indicates the patch ID of a Fixlet, which is the first six digits in the Fixlet title.

Each entry must be separated by a comma and must not include spaces. For example, `--patch_id 162516`.

Using –sha1_download_dir with air-gapped and internet-enabled BES Server

Previously, using the "buildRepo –key server-7-x86_64" with RHSMDownloadCacher mirrors the Red Hat Repo "server-7-x86_64" structure offline. This might result to duplication of packages if they are found in multiple repositories. Using –sha1_download_dir will download all packages from all repositories (keys) as files with a sha1 filename into a single, flat directory. The use of –sha1_download_dir varies, depending on whether the BES Server is air-gapped or internet-enabled.

The use cases indicated in this section require version v1.0.1.0 and later.

Storage space savings benchmark

Space-saving benchmarks have been established with the use of the --sha1_download_dir. Using the --sha1_download_dir have shown significant decrease in storage size, download size, and time when caching multiple repositories of the same RHEL version. This is because many packages are duplicated among repositories with the same RHEL version (server-6-x86_64, workstation-6-x86_64, client-6-x86_64). Space is not saved if you only cache a single repository for each RHEL version, such as caching server-6-x86_64, server-7-x86_64.

Caching server-6-x86_64, workstation-6-x86_64 (with --sha1_download_dir)

Total Repo Metadata and Packages will take up 84.2 GB of space instead of 158.3 GB (45% space saved)

Caching server-6-x86_64, workstation-6-x86_64, client-6-x86_64 (with --sha1_download_dir):

Total Repo Metadata and Packages will take up 85 GB of space instead of 235 GB (63% space saved).

Air-gapped BES Server

1. Increase the BES Server's sha1 folder size limit.

   From the BES Console, right click the computer and select **Edit Computer Setting**. Increase the _BESGather_Download_CacheLimitMB size. The suggested size is the current BES Server's sha1 folder size plus the size of sha1_download_dir.

   If the size of the sha1_download_dir cannot be determined beforehand the suggested size of the sha1_download_dir is a minimum of 60GB per repository. Note that the minimum size of 60GB might increase over time.

2. Use the RHSM download cacher to cache packages to "sha1_download_dir" and the Repo metadata to "download_dir".

   ```
   RHSMDownloadCacher --rootCertDir "certs" --download_dir "download_dir" --sha1_download_dir "
   sha1_download_dir" buildRepo --key server-7-x86_64
   ```

3. Transfer the "download_dir" to the air-gapped BES Server and the sha1 files in "sha_download_dir" to the sha1 folder of the BES Server.

4. Configure the values in the plugin.ini file.

   The plugin.ini file is located in C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins\RHSMProtocol\plugin.ini.

   Configure the values to the following settings:

   ```
   localCache = "location of the transferred download_dir"
   ```

   ```
   localCacheOnly = yes
   ```

   localCacheOnly is set to 'yes' so that the air-gapped BES Server will not get the repository metadata online but only from the localCache.

   Repository metadata:

   The BES Server will only get the Repo Metadata from the localCache.

   Packages:

   The BES Server will only get the packages from the localCache.

> **Note:** Ensure that the path for the **localCache** parameter is different from the RHSM Download Plugin cache folder path. By default, the RHSM Download Plugin cache is located at `C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins\RHSMProtocol\cache`.

Internet-enabled BES Server

1. Increase the BES Server's sha1 folder size limit.

   From the BES Console, right click the computer and select **Edit Computer Setting**. Increase the _BESGather_Download_CacheLimitMB size. The suggested size is the current BES Server's sha1 folder size plus the size of sha1_download_dir. If the size of the sha1_download_dir cannot be determined beforehand, the suggested size of the sha1_download_dir is a minimum of 60GB per repository. Note that the minimum size of 60GB might increase over time.

2. Use the RHSM download cacher to cache the package to BES Server's sha1 folder.

   ```
   RHSMDownloadCacher --rootCertDir "C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins
   \RHSMProtocol\certs" --download_dir "C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins
   \RHSMProtocol\download_dir" --sha1_download_dir "C:\Program Files (x86)\BigFix Enterprise\BES Server
   \wwwrootbes\bfmirror\downloads\sha1" buildRepo --key server-7-x86_64
   ```

3. Configure the values in the plugin.ini file.

   The plugin.ini file is located in C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins \RHSMProtocol\plugin.iniConfigure the values to the following settings:

   localCache = local

   CacheOnly = nolocal

   Cache is not specified as the packages are saved directly in the BES Server's sha1. localCacheOnly is set to 'no' as the BES Server is internet-enabled and can get the repository metadata and packages from the Internet.

   Repository metadata: The BES Server will get the repository metadata from the RHSMPlugin's cache folder first, and then the internet if it is expired.

   Packages: The BES Server will check its sha1 folder for the package first, and then get it from the internet if the package is not found.

Internet enabled BES Server (no sha1_download_dir)

Since v1.0.1.0, using the --sha1_download_dir to cache the packages is considered best practice. Users that have their BES Server in an internet-enabled environment might want to store the packages in a separate folder instead of the BES Server' sha1 folder. This is useful if the BES Server's sha1 folder size inflates. Since the BES Server only stores the latest download, the packages stored there might be replaced by newer files if the BES Server sha1 folder size limit that is set is too small.

Storing the packages in the localCache will allow the RHSMPlugin to use it instead of getting it from the internet.

Using the localCache to cache packages instead of the sha1_download_dir might take up additional space as the package will also be cached in the BES Server's sha1 folder when the BES Server requests the package from the localCache.

1. Use the RHSM download cacher to cache packages to "download_dir".

```
RHSMDownloadCacher --rootCertDir "certs" --download_dir "download_dir" buildRepo --key
    server-7-x86_64
```

2. Configure the values in the plugin.ini file.

   The plugin.ini file is located in `C:\Program Files (x86)\BigFix Enterprise\BES Server \DownloadPlugins\RHSMProtocol\plugin.ini.`

   Configure the values to the following settings:

   ```
   localCache = "location of the transferred download_dir"
   ```

   ```
   localCacheOnly = no local
   ```

   CacheOnly is set to 'no' since the BES Server is internet-enabled and can get repository metadata and packages from the internet.

   Repository metadata: The BES Server will get the repository metadata from the RHSMPlugin cache folder first, and then the internet if the repository metadata is expired.

   Packages: The BES Server checks for the package in the following sequence: its sha1 folder for the package first, the localCache, and then gets it from the internet.

Chapter 9. Multiple-Package Baseline Installation

BigFix Patch provides a solution to combine the installation of updates for multiple packages in a baseline into a single task, which can reduce the execution time of the baseline.

Baselines can help you gather multiple Fixlets into groups, which you can apply immediately to any set of target computers. It is a powerful way to deploy a group of actions across an entire network. However, each Fixlet in a baseline creates a separate update transaction when the baseline is run. A single baseline can have numerous calls, which can severely impact performance as it increases the time taken to complete all the transactions.

The multiple-package baseline installation solution helps improve the performance that is due to the dependency resolution and package installation that is done separately for each Fixlet. This solution requires you to enable the feature at the start of the baseline and append the installation task to install the relevant packages from a single call.

Use the **Enable the Multiple-Package Baseline Installation feature** task to set the flag that instructs Fixlets to add packages to a list instead of installing them. The flag is cleared after the baseline is completed. You must add the appropriate task at the start of the baseline to allow the installation of multiple packages from a single command.

A multiple-package installation task is made available for each Red Hat distribution, operating system version, service pack level, and architecture. You must add the appropriate installation task at the end of your baseline to complete the dependency resolution, download the packages, and then install them on the endpoints.

Use the appropriate task to install the relevant packages listed on the `MultiPkgInstall.txt` file, located in the following directory locations from a single yum call.

> **On Windows systems**
>
> `%PROGRAM FILES%\BigFix Enterprise\BES Client\EDRDeployData`
>
> **On Linux systems**
>
> `/var/opt/BESClient/EDRDeployData`

The task action skips packages with broken dependencies.

These tasks must be run at the end of the baseline to do dependency resolution and package installation for the entire baseline in a single instance.

> **Note:** Ensure that the following option is unchecked for the related tasks: **Baseline will be relevant on applicable computers where this component is relevant**.

You can also do a dry run of the installation to preview the changes on the packages to avoid broken dependencies, which might be due to undesired packages updates. The test action outputs to the following file at `/var/opt/BESClient/EDRDeployData`.

> `PkgToInstallList.txt` **file**
>
> This file contains packages that are to be installed after a dependency check.

Installing multiple packages in a baseline

The multiple-package baseline installation feature helps you to save time when deploying Fixlets with multiple unique packages from a baseline.

To install or update packages for all Fixlets in the baseline, you must add the task to enable the feature and add the appropriate multiple-package baseline installation task into the baseline.

Note: The multiple-package baseline installation feature does not support the pre-cache option **Start download before all constraints are met** in **Take Action**.

1. Create a baseline.

   From the console, select **Create New Baseline** from the **Tools** menu. You can also highlight the Fixlets from a Fixlet site and select **Add to New Baseline** from the context menu.

2. Add the related tasks to the new baseline. The order of the tasks as listed in the tables is important.

   RHEL 6

   Table 14. Tasks for RHEL 6

Fixlet ID	Task
200	Delete RHEL 6 Package List File for Multiple-Package Baseline Installation
300	TROUBLESHOOTING: RHEL 6 Patching Deployment Logs - Cleanup
301	Import RPM-GPG-KEY-redhat-release - RHEL 6
201	Enable the Multiple-Package Baseline Installation feature - RHEL 6

   RHEL 7

   Table 15. Tasks for RHEL 7

Fixlet ID	Task
200	Delete RHEL 7 Package List File for Multiple-Package Baseline Installation
300	TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup
301	Import RPM-GPG-KEY-redhat-release - RHEL 7
201	Enable the Multiple-Package Baseline Installation feature - RHEL 7

RHEL 6 on System z

Table 16. Tasks for RHEL 6 on System z

Fixlet ID	Task
200	Delete RHEL 6 Package List File for Multiple-Package Baseline Installation - s390x
300	TROUBLESHOOTING: RHEL 6 Patching Deployment Logs - Cleanup - s390x
301	Import RPM-GPG-KEY-redhat-release - RHEL 6 s390x
201	Enable the Multiple-Package Baseline Installation feature - RHEL 6 - s390x

RHEL 7 on System z

Table 17. Tasks for RHEL 7 on System z

Fixlet ID	Task
200	Delete RHEL 7 Package List File for Multiple-Package Baseline Installation - s390x
300	TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - s390x
301	Import RPM-GPG-KEY-redhat-release - RHEL 7 s390x
201	Enable the Multiple-Package Baseline Installation feature - RHEL 7 - s390x

RHEL 7 PPC64LE

Table 18. Tasks for RHEL 7 PPC64LE

Fixlet ID	Task
200	Delete RHEL 7 Package List File for Multiple-Package Baseline Installation - PPC64LE
300	TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - PPC64LE
301	Import RPM-GPG-KEY-redhat-release - RHEL 7 PPC64LE
201	Enable the Multiple-Package Baseline Installation feature - RHEL 7 - PPC64LE

RHEL 7 PPC64BE

Table 19. Tasks for RHEL 7 PPC64BE

Fixlet ID	Task
200	Delete RHEL 7 Package List File for Multiple-Package Baseline Installation - PPC64BE
300	TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - PPC64BE
301	Import RPM-GPG-KEY-redhat-release - RHEL 7 PPC64BE
201	Enable the Multiple-Package Baseline Installation feature - RHEL 7 - PPC64BE

RHEL 8 x86_64

Table 20. Tasks for RHEL 8 x86_64

Fixlet ID	Task
200	Delete RHEL 8 Package List File for Multiple-Package Baseline Installation
300	TROUBLESHOOTING: RHEL 8 Patching Deployment Logs - Cleanup
301	Import RPM-GPG-KEY-redhat-release - RHEL 8
201	Enable the Multiple-Package Baseline Installation feature - RHEL 8

RHEL 8 PPC64LE

Table 21. Tasks for RHEL 8 PPC64LE

Fixlet ID	Task
200	Delete RHEL 8 Package List File for Multiple-Package Baseline Installation - PPC64LE
300	TROUBLESHOOTING: RHEL 8 PPC64LE Patching Deployment Logs - Cleanup
301	Import RPM-GPG-KEY-redhat-release - RHEL 8 PPC64LE
201	Enable the Multiple-Package Baseline Installation feature - RHEL 8 - PPC64LE

RHEL 8 on System z

Table 22. Tasks for RHEL 8 on System z

Fixlet ID	Task
200	Delete RHEL 8 Package List File for Multiple-Package Baseline Installation - s390x
300	TROUBLESHOOTING: RHEL 8 s390x Patching Deployment Logs - Cleanup - s390x
301	Import RPM-GPG-KEY-redhat-release - RHEL 8 s390x
201	Enable the Multiple-Package Baseline Installation feature - RHEL 8 - s390x

Note: The following tasks are optional but it is suggested that these tasks are added to the new baseline.

- TROUBLESHOOTING: RHEL 6 Patching Deployment Logs - Cleanup
- TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup
- TROUBLESHOOTING: RHEL 6 Patching Deployment Logs - Cleanup - s390x
- TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - s390x
- TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - PPC64LE
- TROUBLESHOOTING: RHEL 7 Patching Deployment Logs - Cleanup - PPC64BE
- TROUBLESHOOTING: RHEL 8 Patching Deployment Logs - Cleanup
- TROUBLESHOOTING: RHEL 8 Patching Deployment Logs - Cleanup - PPC64LE
- TROUBLESHOOTING: RHEL 8 Patching Deployment Logs - Cleanup - s390x
- Import RPM-GPG-KEY-redhat-release - RHEL 6
- Import RPM-GPG-KEY-redhat-release - RHEL 7
- Import RPM-GPG-KEY-redhat-release - RHEL 6 - s390x
- Import RPM-GPG-KEY-redhat-release - RHEL 7 - s390x
- Import RPM-GPG-KEY-redhat-release - RHEL 7 - PPC64LE
- Import RPM-GPG-KEY-redhat-release - RHEL 7 - PPC64BE
- Import RPM-GPG-KEY-redhat-release - RHEL 8
- Import RPM-GPG-KEY-redhat-release - RHEL 8 - PPC64LE
- Import RPM-GPG-KEY-redhat-release - RHEL 8 - s390x

3. Selectively add the patch Fixlets in the baseline.

   Ensure that for all Fixlets the **Baseline will be relevant on applicable computers where this component is relevant** option is selected.

   Note: If you add two or more Fixlets to the baseline that affect different versions of the same package, the installation task will skip the older versions of the package and install the latest one only.

4. Add the appropriate **Multiple-Package Baseline Installation** task at the end of the baseline. With this task, you can deploy any of the following actions:

- Run a preview of the installation, without actually installing the packages, to check for possible issues.
- Install all the RPMs in a single transaction.

Ensure that the **Baseline will be relevant on applicable computers where this component is relevant** option is not selected.

Before running the baseline, ensure that you meet the following requirements:

- The repositories that are registered on the endpoint must contain the target packages and all the required dependency packages.
- Allow enough time for a Fixlet, which is using the multiple-package installation method, to complete all transactions and refresh the status on the endpoints before individually deploying the same Fixlet.
- Do not run multiple baselines from the same site on the same endpoint.
- Follow the Baseline Best Practices documented in the following technote: https://hclpnpsupport.service-now.com/csm?id=kb_article&sys_id=d288c2021b098c9477761fc58d4bcbdf.

Note: When you deploy the baseline, the initial sub-action status for all the patch Fixlets will show that they failed. This is the expected behavior. The process for downloading and installing the packages in the baseline is not done at the Fixlet action level, but in the **Multiple-Package Baseline Installation** task. When the baseline completes, the baseline sub-action status of the Fixlets will reflect the final state of each patch installation.

Appendix A. Support

For more information about this product, see the following resources:

- Knowledge Center
- BigFix Support Center
- BigFix Support Portal
- BigFix Developer
- BigFix Wiki
- HCL BigFix Forum

Appendix B. Frequently asked questions

The questions and answers in the section can help you to better understand Patch for Red Hat Enterprise Linux.

The Manage Download Plug-ins dashboard is not reflecting any data. What do I do?

Here are some steps you can do to troubleshoot the issue:

- Gather the latest **Patching Support** site.
- Activate the **Download Plug-in Versions** analysis, available from the **Patching Support** site.
- Clear the BigFix console cache.

What are superseded patches?

Superseded Fixlets are Fixlets that contain outdated packages. If a Fixlet is superseded, then a newer Fixlet exists with newer versions of the packages. The newer Fixlet ID can be found in the description of the superseded Fixlet.

Where are the deployment logs located in the endpoints?

The logs are in the EDRDeployData folder, under the client folder: `/var/opt/BESClient/EDRDeployData`.

Endpoint Dependency Resolution - Deployment Results in the Linux RPM Patching site can be used to view the deployment logs on the BigFix Console.

If the latest plug-ins are registered, why do downloads still fail?

Patch number 8.0.627 has a known issue of not recognizing the whitelist for dynamic downloads. Upgrade to the latest version of BigFix to resolve the issue. You can also add the following lines in the download whitelist on your server:

- RHSMProtocol://.*
- http://software.bigfix.com/download/bes/dep/rhel/.*
- http://software.bigfix.com/download/bes/dep/pkgdeps/.*
- http://software.bigfix.com/download/bes/yum/rhel/6Servers390x/.*

What needs to be done when the action reports back with EDR Plug-in failure, Invalid set of initially installed packages?

There is at least one conflict between the packages that exist on the system. The resolver does not work until the conflicting packages are removed.

Why is there XML in the deployment results?

The XML is from the error output of the resolver when the resolver fails to produce a solution. You can look at the description in the 'errorType' tag to gain a better understanding of why the failure occurred.

What must be done when the deployment results display a 'Dependency Resolver Failure, noSolution"?'

If the resolver finds that there is no solution, the system cannot install all targets and dependencies. This is caused by a conflict between these files and the endpoint files.

How often are new dependency graphs generated?

Dependency graphs are generated every Monday, Wednesday, and Friday.

What steps must be taken when an action reports back with an installation failure?

Check to see whether the conflict is caused by a vendor-acquired package. These packages must be removed for the installation to occur.

Why does the resolver function select a lower priority package over a higher priority one?

The resolver does not select a preferred package when selecting that package creates a conflict with another package. Therefore, it is possible for a lower priority package to be selected.

What are the dependency issues in RHEL 3 and 4, and how do they affect the deployment?

See the **Dependency Issues** section of this document.

How do I verify that the download plug-in was registered correctly?

Run a Fixlet with an action task to verify that the download plug-in is registered correctly. Verify that the patch download is successful. Otherwise, you might need to unregister the download plug-in and register it again.

How do I register a download plug-in? Do I use the register download plug-in task or the Manage Download Plug-in dashboard?

To register a download plug-in, you must use the Manage Download Plug-in dashboard in the Patching Support site. Existing register download plug-in tasks are being deprecated. To learn more about plug-in registration, see Registering the RHSM download plug-in *(on page 40)*.

> 📝 **Note:** You must also use the Manage Download Plug-in dashboard to unregister, configure, and upgrade download plug-ins. The existing unregister and edit download plug-in tasks are being deprecated. For more information about the dashboard, see Using RHSM download plug-ins.

The password should be obfuscated, but is still in clear text. Why is that?

If your download plug-in version is earlier than 2.1, you are still using an old version of the download plug-in that stores credentials in clear text. To encrypt credentials, upgrade your download plug-in to version 2.1 or later from the Manage Download plug-ins dashboard in the Patching Support site.

Which version of the YUM native tools must be used?

The Patches for RHEL native tools site requires version 3.2.19-18 or later.

An action failed and the logs contain YUM-specific errors. How do I troubleshoot the failed action?

For more information about YUM and errors that are related to it, see the YUM documentation at http://yum.baseurl.org and the YUM-related articles in the Red Hat Customer Portal.

What version of YUM is required to use the RHEL Custom Repository dashboard?

You must have a minimum YUM version of 3.2.19-18.

Which Red Hat Enterprise Linux is supported by the RHEL custom repository dashboard?

The dashboard supports Red Hat Enterprise Linux versions 5 and 6.

Which version of the BigFix server supports the RHEL Custom Repository dashboard?

The RHEL Custom Repository dashboard supports version 8.2 and later of BigFix.

When deploying patches, should I use the existing method or go through the custom repository? Can the two methods co-exist?

The two methods can exist together. However, when deploying patches for single clients, you must choose between using the native tools or through the custom repository method.

How are dependencies resolved the RHEL Custom Repository dashboard is used?

YUM uses the metadata to resolve the dependencies to know which packages are needed.

Can the custom repositories be used for software installation?

Yes, you use custom repositories for software installation. To use custom repositories for software installation, follow these steps:

1. Ensure that the clients are registered through the Custom Repository dashboard.
2. Create a Fixlet in the custom site with the action `yum install<space><package name>`. Ensure that you set the correct relevance or success criteria, that is, whether the Fixlet takes action against that client or endpoint. To learn more about creating Fixlets, see the *Console Operator's Guide*.

> **Note:** It is important to ensure that the repositories and satellites are updated. Actions can fail if the packages are not available.

For satellites: The dashboard only helps to run bootstrap scripts and the `rhnreg_ks` command to subscribe the endpoints to satellite servers. The channels that the endpoints use must be configured through the satellite servers.

While registering a repository, I was prompted to enter an activation key. Where can access this activation key?

Red Hat Network Satellite administrators create and manage these activation keys. For more information about activation keys, see https://access.redhat.com/site/documentation/en-US/.

Can previously configured repositories be configured again?

Yes, you can configure again a previously configured repository.

From the logs, can I tell if I am using the normal YUM process to the satellite or repository in the log?

Yes, the log indicates whether the normal YUM process in the satellite or repository is used.

What is the difference between registering a repository and importing a repository?

Use the import feature if you have existing repositories that are not included in the Repositories list in the dashboard. Use the register feature if you already have a repository in the Repository list, but you still need to link the repository with the endpoint.

What happens when the repository does not contain the package?

When a package is not found, the Fixlet fails. You can troubleshoot from `EDR_DeploymentResult.txt`, which is where the YUM output is logged.

What happens if there are issues with the custom repository solution?

Users that encounter issues with the custom repository resolution can revert to the standard BES server solution. Users can run the task that is called Disable custom repository support - Red Hat Enterprise Linux.

In the Endpoints tab of the RHEL Custom Repository Management dashboard, are the repositories that are listed in the lower part of the window that is used in sequence?

There is no sequence in the repositories that are listed in the Endpoints tab. When YUM queries the repositories, the repository that first gets the fetch query replies, including the package and its dependencies.

Through the RHEL Custom Repository Management dashboard, a patch was deployed through a custom repository that is not a mirror of the manufacturer site. The deployment failed and the EDR logs indicate that the rpm files could not be opened. What should I do?

When a custom repository that is not a mirror of the vendor site is used, it is possible that the default gpgcheck is being done as part of the installation and the gpg signature files might not be included. The rpm files might not be checked for authenticity and the installation might fail. To resolve this, ensure that when you register the endpoints in the RHEL Custom Repository Management dashboard, you added 'gpgcheck=0' to Additional fields.

Does BigFix support Red Hat satellite servers?

BigFix does not support nor provide Fixlets for Red Hat Satellite servers. For more information about the scope of BigFix support for Red Hat Enterprise Linux, see: https://help.hcltechsw.com/bigfix/9.5/patch/Patch/Patch_RH/c_supported_platforms.html.

BigFix does have the capability to register and connect your existing satellite repositories to endpoints using the Custom Repository feature. For more information about custom repositories, see https://help.hcltechsw.com/bigfix/9.5/patch/Patch/Patch_RH/c_manage_custom_repositories.html.

Can I install several packages using 'Task: Install packages by using YUM'?

Yes, you can install several packages with the task. Use a space to separate the rpm names.

I'm trying to deploy Fixlets and received the following warning message: Warning: execute prefetch plug-in command taking more than 2 seconds to complete. It took 4 seconds. ActionLogMessage: (action:1343) Missing required argument size=. What is causing the error and how could I remedy this?

Users who are subscribed to EDR and native sites might also encounter this message. Try the following actions to troubleshoot the failed deployment.

- Check if the gpg keys are installed and enabled.
- Gather the latest version of the Patches for RHEL site.
- Delete the `/var/opt/BESClient/yum folder` and run the action again.
- Check if sha1 is present in the EDR_PackageSpec files. The EDR_PackageSpec files can be found in the /var/opt/BESClient/_BESDATA/Patches for RHEL 7 folder.
- Check if bzip2 is available in the environment. If not, install bzip2.

What version of YUM does the YUM Transaction History dashboard support?

You must have a minimum YUM version of 3.2.28.

Which version of Red Hat Enterprise Linux does the YUM Transaction History dashboard support?

The dashboard supports Red Hat Enterprise Linux 6 and later versions.

In the YUM Transaction History dashboard, what is the difference between rollback and undo?

The rollback command will undo all transactions up to the point of the specified transaction. The undo command will revert the selected transaction only.

What is the difference between the YUM Transaction History log and YUM Logs analyses?

Patch Management for Red Hat Enterprise Linux generates the YUM Transaction History log, which records the results of the actions that are taken in the YUM Transaction History dashboard. The log is located in `/var/opt/BESClient/EDRDeployData/yum_history.log`.

The YUM log is the official log that is generated by YUM in `/var/log/yum.log` by default. To change the default location, modify the log file settings in `/etc/yum.conf`.

Does the YUM Transaction History dashboard show only `yum -update all`?

Aside from `yum -update all`, the **Command Line** column in the dashboard also shows the different transactions such as the following installation commands.

- `install bzip2`
- `install net-tools`
- `install vim enhance`
- `install wget`

To learn more about YUM commands, see the Red Hat Enterprise Linux website: https://access.redhat.com/.

How does the YUM Transaction History dashboard work if you have configured the BigFix client to use YUM repository or satellite servers?

The YUM Transaction History dashboard does not adversely affect your deployment if you have configured the BigFix client to use YUM repositories or satellite servers. If you already use a local YUM repository or satellite server, it might be easier to provide the packages for rollback.

I'll be using the RHSM download plug-in and I saw that it is highly suggested that a few tasks be applied before deploying Fixlets. Why do I need to do this?

Users are highly suggested to apply the tasks described before deploying Fixlets to avoid issues with GPG keys and the execution of the prefetch plug-in.

Red Hat requires the use of GPG keys. The following two tasks import the GPG keys to the endpoints.

- **Import RPM-GPG-KEY-redhat-release - RHEL 6** (from the Patches for RHEL6 Native Tools site)
- **Import RPM-GPG-KEY-redhat-release - RHEL 7** (from the Patches for RHEL 7 site)

Use the **Change Timeout for Prefetch Plugins** task, which is found in the Patching Support site, to avoid an error with the execution of the prefetch plug-in. The error is caused by a short prefetch timeout setting. To remedy this, run the task to change the timeout to 30 minutes.

After running the task to change the timeout settings, restart the BES client with the **TROUBLESHOOTING: Restart BES Client on RHEL/SUSE** task. The task is found in the BES Support site.

What to do when Fixlets fail to install with the following message in the EDR log? "Warning: Nothing to install. Please check if you are using the latest kernel."

This message appears only in case of Fixlets that deploy kernel packages. A kernel Fixlet becomes relevant if the endpoint does not have the target kernel package installed or if the endpoint's active kernel is at a lower version than the target kernel package. An endpoint is still considered subject to kernel vulnerabilities even if it has the latest kernel installed but not using it actively.

To remediate the issue, restart the endpoint and ensure it is using the latest kernel available.

Appendix C. Troubleshooting

You can try several ways to troubleshoot Patch for Red Hat Enterprise Linux. This section also has references that are specific to the RHSM enhancements.

Troubleshooting actions

The action reported back as a failed download

Make sure your download plug-in is updated to the latest version and is registered with the correct credentials.

The action reports back with "EDR Plug-in failure, Invalid set of initially installed packages"

There is at least one conflict between the packages that exist on the system. The resolver does not work until the conflicting packages are removed.

An action reports back with an installation failure

Check to see whether the conflict is caused by a vendor-acquired package. These packages must be removed for the installation to occur.

An action has failed and the EDR logs state that the private key is missing for some RPM files

When the EDR logs show the following entry when the action fails, this suggests that the RedHat Release Key is not accepted by the rpm command on the system where the action failed:

```
rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 37017186 Public key for <RPM files> is
not installed.
```

You can resolve the issue in two ways:

- Use rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release.
- Set gpgcheck=0 in /etc/yum.conf. This option only for the native tools sites.

It is suggested that you use the first command. The second command `gpgcheck` allows other unsigned packages to be installed.

An action has failed and the EDR logs do not give any information about the failing action

The last six lines of the deployment and test actions are intended to delete the temporary files that are created during the action execution. If the deployment logs do not give information about the reason for the failure, delete the following two lines to troubleshoot:

- To see the YUM configuration used during the action, delete `"{parameter "EDR_YumConfig"}"`

- To see the YUM output that is generated during the dependency resolution, delete `"{parameter "EDR_YumResolveOutput"}"`

When these two lines are deleted out, the following files are placed in the site folder for the Patches for RHEL Native tools site:

- EDR_YumConfig_<fixlet id>
- EDR_YumResolveOutput_<fixlet id>

An action failed and the logs contain YUM-specific errors.

For more information about YUM and errors related to it, see the YUM documentation at http://yum.baseurl.org and the YUM-related articles in the Red Hat Customer Portal.

Troubleshooting the RHEL Custom Repository Management dashboard

Try the following steps to troubleshoot failed deployments in the RHEL Custom Repository Management dashboard.

- Ensure that you enable the task that is called Enable custom repository support - Red Hat Enterprise Linux task from the Patching support site.
- Ensure that when you register the endpoints, you added `gpgcheck=0` to Additional fields.
- Check that the client setting _BESClient_RHEL_AllowYumDownloads in the endpoints is set to 1.
- Verify that the downloads went through the custom repository through the https service logs in the custom repository.
- Refer to the following logs:
    - /var/opt/BESClient/EDRDeployData/register-repo.log
    - /var/opt/BESClient/EDRDeployData/register-satellite.log
    - /var/opt/BESClient/EDRDeployData/unregister-repo.log

  The following example shows a log for a standard repository:

  ```
  Processing /etc/yum.repos.d/test-repo.repo/etc/yum.repos.d/test-repo.repo

  Done with /etc/yum.repos.d/test-repo.repo
  ```

- Check the repository configurations that are stored in `/etc/yum.repos.d/`. The configurations include the user name and password of the repositories that the users have.

To check the deployment logs in the endpoints, go to `/var/opt/BESClient/EDRDeployData`. Endpoint Dependency Resolution - Deployment Results in the Linux RPM Patching site can be used to view the deployment logs on the BigFix Console.

Note: BigFix does not support nor provide Fixlets for Red Hat Satellite servers. For more information about the scope of BigFix support for Red Hat Enterprise Linux, see: https://help.hcltechsw.com/bigfix/9.5/patch/Patch/Patch_RH/c_supported_platforms.html. BigFix does have the capability to register and connect your existing satellite repositories to endpoints using the Custom Repository feature. For more information about custom repositories, see https://help.hcltechsw.com/bigfix/9.5/patch/Patch/Patch_RH/c_manage_custom_repositories.html.

Troubleshooting the RHSM Download Plug-in

When problems occur, you can determine what went wrong by viewing messages in the appropriate log files that provide information about how to correct errors.

- Download plug-in log and configuration files

Enhanced logging with clearer error reporting and error handling to improve troubleshooting.

RHSMPlugin.log

Lists the results of the downloads related to the execution of the RHSM download plug-in. The amount of information depends on the logging level.

The log can be found in the following locations:
- On Windows systems: `%PROGRAM FILES%\BigFix Enterprise\BES Server \DownloadPlugins\RHSMProtocol`
- On Linux systems: `/var/opt/BESServer/DownloadPlugins/RHSMProtocol`

plugin.ini

The configuration log can be found in the following location: `<BES Server install location>\DownloadPlugins\RHSMProtocol\plugin.ini`.
- On Windows systems, the file is in the BigFix server installation directory. For example, `%PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins\ RHSMProtocol`.
- On Linux systems, the file is in the root directory tree occupied by the download plug-in. For example, `/var/opt/BESServer/DownloadPlugins/RHSMProtocol.`

- Client log file

The following log file can be found in the client folder in the directory `/var/opt/BESClient/ EDRDeployData`.

EDR_DeploymentResults.txt

Lists the results of the EDR deployment and the Yum output.

Error when /var is mounted as noexec

All available Fixlets use an executable that by default runs directly from the `/var` directory, a partition on the endpoint. The Fixlets will not work when `/var` is set with the `noexec` option, regardless of whether the RHSM Download Plug-in or Custom Repository solution is used. Therefore, ensure that the `/var` directory is not set with the `noexec` option by doing the following steps:

1. Check the client log to see if the prefetch plug-in returned the `exit code 126`. For example:
2. Run `mount` as the root user to check the mount option that is currently used:

```
[root@host ~]# mount

/dev/mapper/vg_data-lv_root on / type ext4 (rw)

proc on /proc type proc (rw)

sysfs on /sys type sysfs (rw)

devpts on /dev/pts type devpts (rw,gid=5,mode=620)

tmpfs on /dev/shm type tmpfs (rw)

/dev/sda1 on /boot type ext4 (rw,nodev)

/dev/mapper/vg_data-lv_var on /var type ext4 (rw,noexec,nosuid,nodev)

none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
```

If `/var` is set to `noexec`, you must take one of the following actions:

- Remove the `noexec` mount option.
- Move `/var/opt/BESClient` to a different partition, which is not `noexec`, and create a symbolic link to it in its place.
- Run the **Set the path for _BESClient_LinuxPatch_executable_directory** Fixlet and specify an alternative directory to run the executable for patching. The directory path must be a valid, absolute path name. It can contain only alphanumeric characters, forward slashes, and underscores.

Reference logs for troubleshooting RHSM enhancements

Download plug-in log and configuration files

Enhanced logging with clearer error reporting and error handling to improve troubleshooting.

RHSMPlugin.log

Lists the results of the downloads related to the execution of the RHSM download plug-in. The amount of information depends on the logging level.

The log can be found in the following locations:

- On Windows systems: `%PROGRAM FILES%\BigFix Enterprise\BES Server \DownloadPlugins\RHSMProtocol`
- On Linux systems: `/var/opt/BESServer/DownloadPlugins/RHSMProtocol`

Note: Due to a no hash download limitation, some errors which are not relevant to your deployment might display in the log.

RHSMDownloadCacher.log

Displays the results of the entitlement certificate access check to Red Hat repositories that BigFix supports.

- On Windows systems: `%PROGRAM FILES%\BigFix Enterprise\BES Server \DownloadPlugins\RHSMProtocol`
- On Linux systems: `/var/opt/BESServer/DownloadPlugins/RHSMProtocol`

> **Note:** Due to a no hash download limitation, some errors which are not relevant to your deployment might display in the log.

You can set logging levels for RHSMDownloadCacher.log. For more information, see Using the RHSM download cacher *(on page 60)*.

plugin.ini

The RHSM configuration log can be found in the following location: `<BES Server install location>\DownloadPlugins\RHSMProtocol\plugin.ini`.

- On Windows systems, the file is in the BigFix server installation directory. For example, `%PROGRAM FILES%\BigFix Enterprise\BES Server\DownloadPlugins\ RHSMProtocol.`
- On Linux systems, the file is in the root directory tree occupied by the download plug-in. For example, `/var/opt/BESServer/DownloadPlugins/RHSMProtocol.`

To retrieve information that can be used for troubleshooting issues, update the logger level value to DEBUG.

Client log file

The following log file can be found in the client folder in the directory `/var/opt/BESClient/EDRDeployData`.

EDR_DeploymentResults.txt

Lists the results of the EDR deployment and the Yum output.

RHSM troubleshooting checklist

Troubleshooting RHSM errors

Table 23. Overview of the RHSM troubleshooting checklist

What to check	Errors or warnings encountered	Possible causes and remediation steps
GPG key is imported.	If the GPG is not imported in an endpoint, you might find this entry in the EDR log: `warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY Public key for httpd-devel-2.2-`	The GPG is not imported in an endpoint. Check the EDR log of the endpoint. The log displays if the GPG is not imported. If it is not, import the GPG through the command line or by using Fixlets specific to either the

Table 23. Overview of the RHSM troubleshooting checklist (continued)

What to check	Errors or warnings encountered	Possible causes and remediation steps
	`.15-56.el6_8.3.x86_64.rpm is not installed.`	Patches for RHEL 6 Native tools site or the Patches for RHEL site.
The prefetch plug-ins timeout settings is set too low.	You might encounter a failed Fixlet deployment and with "fail" indicated at the `execute prefetch plug-in` line.	Use a task to set the timeout to 30 minutes.
Ensure that your certificates can access Red Hat repositories.	`Error: Certs cannot access any Repos` or the certificates are only able to access some of the required repositories.	Run a quick repository access check.
Ensure that the entitlement certificates are placed in the correct folders.	Patch deployment fails.	The certificates might not be placed in the correct folders and sub-folders. Unnecessary metadata files must be removed. For more information, see the guidelines in the following section: Entitlement certificates and system identity certificate are placed in the correct folders.
Ensure that the entitlement certificates have the correct format.	Patch deployment fails.	The user might have entitlements that have the old formats. To check the certificate format, see the steps detailed in the following section: The version of RHSM entitlement certificates have the correct format.
Entitlement certificates are active and have not expired.	Patch deployment fails one day after creating an entitlement certificate.	Follow the methods in the section to verify that the certificates have not expired. If the subscription is expired, you must generate or attach a new subscription (entitlement) to the entitlement certificate. Regenerate the identity certificate if it is expired.
Entitlement certificates have the correct subscriptions (entitlements) attached.	Certificates cannot access the required Red Hat base repositories.	Attach the correct subscription (entitlement) to the Entitlement Certificate to get access to the required repositories. Follow the methods in

Table 23. Overview of the RHSM troubleshooting checklist (continued)

What to check	Errors or warnings encountered	Possible causes and remediation steps
		the section to verify the subscription entitlements that are attached to your entitlement certificates.
Entitlement certificate can access the Red Hat base repositories.	Certificates cannot access the Red Hat base repositories.	Possible causes: • The certificates have expired. • The required subscription were not properly attached when the system was registered through Red Hat Subscription Management portal. • The network or proxy is blocking RHSMPlugin.exe from accessing the repositories. Run an access test which is described in the section.

Error messages in RHSMPlugin.log	You might find the following entry in the log:
	
	`ERROR : All Key and Cert pairs in 'rootCertDir' cannot access: https://cdn.redhat.com/content/dist/rhel/client/7/`
	
	`7Client/x86_64/os/repodata/repomd.xml`
		• If you don't need to deploy patches to any such endpoints, you may safely ignore this message. This might be caused by a no hash limitation.
		• If the error message is associated with a repository that you need for your patch deployment, this error might be due to several reasons. Refer to the following section: Entitlement certificates are not able to access the repositories

The GPG key is imported

A GPG key must be imported from Red Hat to download Red Hat content. After deploying a patch, check the EDR log of the endpoint, which is located at `var\opt\BESClient\EDRDeployData\EDR_DeploymentResults.txt`.

If the GPG key for an endpoint is not imported, you might see the following warning in EDR_DeploymentResults.txt.

```
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key ID fd431d51:
NOKEY Public key for httpd-devel-2.2.15-56.el6_8.3.x86_64.rpm is not installed
```

To import the GPG key for the endpoint, use the following command: `rpm --import /mnt/cdrom/RPM-GPG-KEY-redhat-release`.

You may also use the following Fixlets to import the GPG key for the endpoint:

- Patches for RHEL 6 Native Tools: 301 Import RPM-GPG-KEY-redhat-release - RHEL 6
- Patches for RHEL 7: 301 Import RPM-GPG-KEY-redhat-release - RHEL 7

These steps usually only needs to be done once on each newly-set up endpoint.

Ensure that the timeout setting is sufficient to execute the prefetch plug-in

You might need to configure the plug-ins timeout setting if the Fixlet deployment fails and from the Action Script Execution Detail in the console, "fail" is indicated in the `execute prefetch plug-in` line.

From the Patching Support site, use this task to set the timeout to 30 minutes: **Change Timeout for Prefetch Plugins**.

After applying the task, restart the BES client with the following task from the BES Support site: **TROUBLESHOOTING: Restart BES Client on RHEL/SUSE.**

Your certificates can access Red Hat repositories

You can run a quick test to check if your certificates can access Red Hat repositories. Typically, the test runs less than 10 seconds.

The RHSM plug-in is usually located in `C:\Program Files (x86)\BigFix Enterprise\BES Server \DownloadPlugins\RHSMProtocol`.

Run the following repository access test.

```
RHSMPlugin.exe --check-baserepos
```

There are three possible outcomes when running the repository access test. Possible outcomes from Repo Access Test:

None of the certs can be accessed

```
INFO      :  Base Repos Test Summary

INFO      :  Certs in <rootCertDir> can access 0 / 12 Base Repos:


ERROR     :  Error: Certs cannot access any Repos.
```

The certificates were not set up properly. Continue with the checklist. For more information about setting up and downloading both certificates, see Setting Up RHSM Certificates.

Certificates are able to access all required repositories.

```
INFO      :  Base Repos Test Summary

INFO      :  Certs in <rootCertDir> can access 3 / 12 Base Repos:


INFO      :  server-7-x86_64:       Red Hat Enterprise Linux 7 Server (RPMs)

INFO      :  server-6-x86:          Red Hat Enterprise Linux 6 Server (RPMs)

INFO      :  server-6-x86_64:       Red Hat Enterprise Linux 6 Server (RPMs)
```

Certificates are able to access only some required repositories.

You might need to patch endpoint types that do not appear in the list of successfully accessed repositories. For example, you have Workstaton endpoints but the output only shows access to the Server repositories. In such cases, you must attach the required subscriptions to the certificates through the Red Hat portal.

The list of repositories that are tested are derived from the RepoList ("primaryRepoListFile", "extendedRepoListFile") file that is referenced in the plugin.ini. At the time of writing, the list of repositories in[1]

are as follows.

- client-6-x86
- client-6-x86_64
- client-7-x86_64
- server-6-x86
- server-6-x86_64
- server-7-x86_64
- workstation-6-x86
- workstation-6-x86_64
- workstation-7-x86_64
- server-6-s390x
- server-7-s390x
- server-7-ppc64le
- server-7-ppc64be

1. primaryRepoListFile

Entitlement certificates are placed in the correct folders

Ensure that the certificates are in the correct folders. Follow these guidelines to avoid errors.

- The following path is the relative path where the rootCertDir is located. This can be left at its default value ("certs") in the plugin.ini

```
^^^^^^^^^^^^^^^^^^^^^^^^^

rootCertDir = certs

^^^^^^^^^^^^^^^^^^^^^^^^^
```

- The "certs" folder must only contain subfolders. For example, cert_set_1, cert_set_. Remove metadata files.
- Within the "cert_set_1" folder only files ending with ".pem" are allowed. There can be any no. of Entitlement Certificates in "cert_set_1". For example, 443229635427054308.pem. Only Entitlement Certificates with the new format are allowed.

  Note: Earlier versions of the RHSM subscription interface had an option to download the system identity certificate. This is no longer the case with the current RHSM subscription interface version. The System Identity Certificate is no longer required from v1.0.2.0 of the RHSM download plug-in and RHSM download cacher.

- If you have more than one set of certificates, ensure that only one set of certificates go to one folder.

The version of RHSM entitlement certificates have the correct format

When creating RHSM certificates in the RHSM customer portal, and you are at the step in which you need to register a system, you must specify the Red Hat Enterprise Linux version.

To avoid errors, select version 7.2. Red Hat Enterprise Linux versions that are earlier than version 7.2 have a different entitlement certificate format that the RHSM download plug-in does not read. The new entitlement certificate format has "BEGIN ENTITLEMENT DATA" in the .pem file.

To verify the format version of the entitlement format, do the following steps:

1. Open the .pem file in a text editor.
2. Search for "BEGIN ENTITLEMENT DATA". Only the new entitlement format will have this; neither the old entitlement certificate format and the system identify certificate will have "BEGIN ENTITLEMENT DATA".

Note: Ensure that the Entitlement Certificates with the old format is deleted from <BES_Server> \DownloadPlugins\RHSMProtocol\certs\cert_set_1.

The entitlement certificates are active and have not expired

Certificates usually expire in 1 year to a few years. There have been some cases where patch deployment would fail one day after the entitlement certificates were created. The entitlement certificates were found to have an expiry date set 1 day after they were created. There are several ways to check the expiry date of the certificates.

- Through a Red Hat machine.
- Through the Red Hat portal. You must access the account in https://access.redhat.com that generated the entitlement certificates.
- Through OpenSSL

If the subscription is expired, you must generate or attach a new subscription (entitlement) to the entitlement certificate. Regenerate the identity certificate if it is expired. Place the downloaded certificates in the correct folder.

Verifying the correct subscription (certificate) attachments using a Red Hat machine

From the command line in a Red Hat machine, run `> rct cat-cert <entitlement cert> > output.txt` to print the certs metadata to the ouput.txt file. Repeat this for each Entitlement Certificate and the System Identity Certificate using a different output.txt filename. Open the file in a text editor and the certs expiry date will be in the **End Date** field `End Date: 2018-05-25 12:50:11+00:00`.

Verifying the correct subscription (certificate) attachments through the Red Hat portal

1. Log in to https://access.redhat.com.
2. Go to https://access.redhat.com/management/consumers?type=system
3. Click the system that you previously created. A list of Entitlement Certificates displays.
4. For each Entitlement Certificate, click **View**. Go to the **Order Info** tab. In the **End Date** column, verify that the subscription are not expired.
5. Click Back in the browser and repeat steps 4 to 6 for each Attached Subscription in your system.

Verifying the correct subscription (certificate) attachments through OpenSSL

If you are able to use openssl, open a command line at this folder: **\DownloadPlugins\RHSMProtocol \certs\cert_set_1**

Use this command and replace the name of the ".pem" file:

```
$ openssl x509 -enddate -noout -in 7a8337a5-eb47-4a52-a161-9635d5691996.pem
```

This results to the expiry date of the certificate. For example,

```
notAfter=Jan 10 15:19:14 2018 GMT
```

Entitlement certificates with the attached subscription (entitlement) with `Name: Red Hat Enterprise Linux for Virtual Datacenters` has been known to stop working after 1 day. If you are having issues with patch deployment after 1 day, we suggest avoiding this subscription and using a non-Virtual Datacenters subscription like `Red Hat Enterprise Linux 7 Server (RPMs)` instead.

Entitlement Certificates have the correct Subscriptions (Entitlements) attached

There are two ways to verify if the correct subscription (entitlement) is attached to the entitlement certificate. This is needed to get access to the required repositories. The first method requires having a Red Hat machine. The second method requires access to the account in https://access.redhat.com that generated the entitlement certificates.

Verifying the correct subscription (certificate) attachments using a Red Hat machine

From the command line in a Red Hat machine, run `> rct cat-cert <entitlement cert>`. This displays the entitlement certificate metadata, including the expiry date of the certificate and the repositories that the certificate can access.

In the following example, Certificate: `End Date: 2017-01-17 13:30:47+00:00` shows the expiry date. Content: `Name: Red Hat Enterprise Linux 7 Server (RPMs)` lists the repositories that the certificate it can access.

```
=========================================

Certificate:

Path: 7a85f98153c2eb950153c73d2fb159e5.pem

Version: 3.2

Serial: 3689711437028903897

Start Date: 2016-03-31 04:00:00+00:00

End Date: 2017-01-17 13:30:47+00:00

Content:

Type: yum

Name: Red Hat Enterprise Linux 7 Server (RPMs)

Label: rhel-7-server-rpmsVendor: Red Hat

URL: /content/dist/rhel/server/7/$releasever/$basearch/os

GPG: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

Enabled: True

Expires: 86400

Required Tags: rhel-7-server

Arches: x86_64

=========================================
```

You might need the following base repositories, depending on the endpoint that you deploy patches to.

- Red Hat Enterprise Linux 6 Desktop (RPMs)
- Red Hat Enterprise Linux 6 Workstation (RPMs)
- Red Hat Enterprise Linux 6 Server (RPMs)
- Red Hat Enterprise Linux 7 Desktop (RPMs)
- Red Hat Enterprise Linux 7 Server (RPMs)
- Red Hat Enterprise Linux 7 Workstation (RPMs)

If the base repository name of the RHEL version that you deploy patches for was not found in all the metadata of the entitlement certificates, it means that the required subscriptions were not attached. Entitlement certificates with the attached subscription (entitlement) with `Name: Red Hat Enterprise Linux for Virtual Datacenters` has been known to stop working after 1 day. If you are having issues with patch deployment after 1 day, we suggest avoiding this subscription and using a non-Virtual Datacenters subscription like `Red Hat Enterprise Linux 7 Server (RPMs)` instead.

Verifying the correct subscription (certificate) attachments by accessing the account on https://access.redhat.com that generated the entitlement certificates

1. Log in to https://access.redhat.com.
2. Go to https://access.redhat.com/management/consumers?type=system
3. Click the system you previously created. A list of list of attached subscriptions displays.
4. For each subscription, in the **Entitlement Certificate** column, click **View > Content Sets > Export All as CSV**.
5. Click Back in the browser and repeat Step 4 for each Attached Subscription in your system.
6. Open each export.CSV that was downloaded from RedHat. Under the **Name** column, search for the Base repository name of the repositories that you need access to for patch deployment.

You might need the following base repository names, depending on the endpoint that you deploy patches to.

- Red Hat Enterprise Linux 6 Desktop (RPMs)
- Red Hat Enterprise Linux 6 Workstation (RPMs)
- Red Hat Enterprise Linux 6 Server (RPMs)
- Red Hat Enterprise Linux 7 Desktop (RPMs)
- Red Hat Enterprise Linux 7 Server (RPMs)
- Red Hat Enterprise Linux 7 Workstation (RPMs)

If the base repository name of the RHEL version that you deploy patches for was not found in all the export.csv, it means that the required subscriptions were not attached.

Entitlement certificate can access the Red Hat base repositories

Before you begin, ensure that Check 1 (Ensure that the entitlement certificates have the correct format) and 2 (Ensure that the entitlement certificates are placed in the correct folders) are completed before following the steps in this check.You can run commands that will help identify Red Hat repository access. The RHSMPlugin.exe uses the entitlement certificate to do the following:

- Test the access to the Red Hat base repositories.
- Determine if the proper subscriptions have been attached to the entitlement certificate.

Run the following:

- For RHSMPlugin.exe (v1.0.0.2 and later): >>>RHSMPlugin.exe --check-baserepos
- For RHSMDownloadCacher.exe (v1.0.0.2 and later) : >>> RHSMDownloadCacher.exe --rootCertDir certs check-baserepos

This will test all base repos in the "primaryRepoListFile" as specified in the plugin.ini. Depending on network conditions, this should take around 10 to 60 seconds. After the commands are run, the results are printed to the console as a "Base Repos Test Summary", and to the logs which will state which base repositories the certificates are able to access.

There are several possible reasons why the Entitlement Certificate are not able to access the repositories:

- The certificates have expired. To remedy this, see CHECK 5: Entitlement Certificates and System Identity Certificate are not expired.
- The required subscription were not properly attached when the system was registered through Red Hat Subscription Management portal. To remedy this, see CHECK 4: Entitlement Certificates have the correct Subscriptions (Entitlements) attached.
- The network or proxy is blocking RHSMPlugin.exe from accessing the repositories. Check that your network firewall or proxy is not blocking the RHSMPlugin.exe. If the problem persists, you might need to contact Support.

Error messages in RHSMPlugin.log

The RHSMPlugin.log is located in <BES_Server>\DownloadPlugins\RHSMProtocol\logs.

You might encounter the following error in the log:

```
ERROR : All Key and Cert pairs in 'rootCertDir' cannot access: https://cdn.redhat.com/content/dist/rhel/
client/7/7Client/x86_64/os/repodata/repomd.xml
```

This error message indicates that RHSMplugin was not able to access RedHat's Client RHELClient 7 Repo ("rhel/client/7/7Client/x86_64/os").

This happens when the same package is found in multiple repositories. This will prompt the RHSM download plug-in to access all the repositories where the package is located. When the download plug-in tries to access a repository

that it does not have access to and when there is a lack of entitlement of the Entitlement Certificate, it will the indicate the error in the log.

If you do not need to deploy patches to any endpoints, as for example, RHEL Client 7 machines

If you do need to deploy patches to any such endpoints, you may safely ignore this message. This error might be due to the client script nohash limitation which the RHSM download plug-in cannot avoid. For more information, see: https://developer.bigfix.com/action-script/reference/download/add-nohash-prefetch-item.html.

If the error message is associated with a repository that you need for your patch deployment, for example if you have a RHEL 7 Server endpoint that requires patching

This might be caused by any of the following reasons:

- The certificates have expired or were revoked. To remediate this, see the steps in "Ensure that entitlement certificates are not expired."
- The required subscriptions were not properly attached when registering the system through RedHat. To remediate this, see the steps in "Entitlement certificates are not able to access the repositories."
- The network or proxy is blocking the RHSMPlugin.exe from accessing the repositories. Check that your network firewall or proxy is not blocking the RHSMPlugin.exe. If the problem persists, you might need to contact Support.

.

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.