IBM Security

Deploying BigFix® Patches for Red Hat®

IBM® SECURITY SUPPORT OPEN MIC

Reminder: You must dial-in to the phone conference to listen to the panelists.
The web cast does not include audio.

USA toll-free: 866-803-2141 USA toll: 1-203-607-0460
Participant passcode: 7402573
Slides and additional dial in numbers: https://ibm.biz/BdrQwL

Tuesday, 27 September 2016

IBM

Panelists

Presenter:
Adam McDonald – L2 Support Software Engineer for IBM BigFix

Panelists:
Ashwin Manekar – Product Manager for IBM BigFix Patch
Kenny Chow – Technical Lead for IBM BigFix Patch for Red Hat
Chuxin Zhao – Software Developer for IBM BigFix Patch for Red Hat

Moderator:
Kevin Reinstein – L2 Support Manager for IBM BigFix

Enabling Red Hat Patching Sites

- **The following Red Hat Patching (and supporting) sites are currently supported and should be enabled:**
  - Patches for RHEL5 - Native Tools
  - Patches for RHEL6 - Native Tools
  - Patches for RHEL 6 System Z
  - Patches for RHEL 7
  - Patching Support
  - Linux RPM Patching
- **The following Red Hat Patching sites have been deprecated and are not supported. These should not be enabled:**
  - Patches for RedHat
  - Patches for RedHat Enterprise Linux
  - Patches for RHEL 3
  - Patches for RHEL 4
  - Patches for RHEL 5/6 – Dependency Resolution

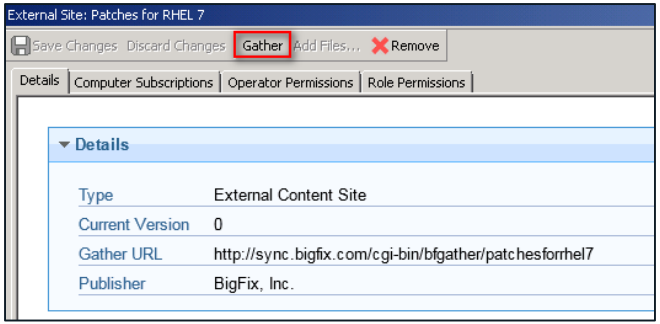
- **Note:** The designation of “Native Tools” at the end of the names of sites is going away and it is implicitly understood that RHEL 7 uses native tools (i.e. YUM) as part of its dependency resolution processes
- **Full List of Support Platforms:**
  - **https://ibm.biz/Bd4GWC**
- **Site Applicability Matrix:**
  - **https://ibm.biz/BdrtrT**

Enabling Red Hat Patching Sites

- Go to the License Overview Dashboard
- Click on the Enable link next to the site to enable

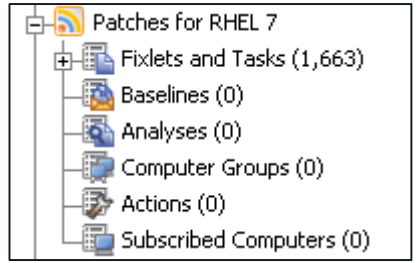
- Under Enabled Sites in the dashboard click on the site link

- Click the Gather button:



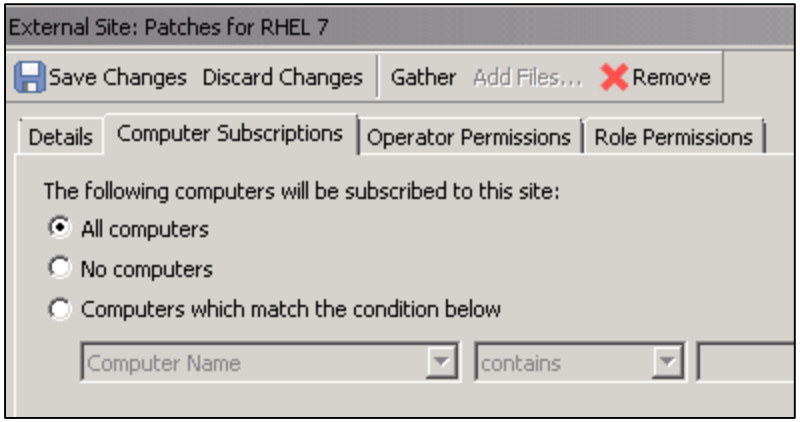
- The ..\BES Server\GatherDBData\GatherDB.log confirms successful gathering

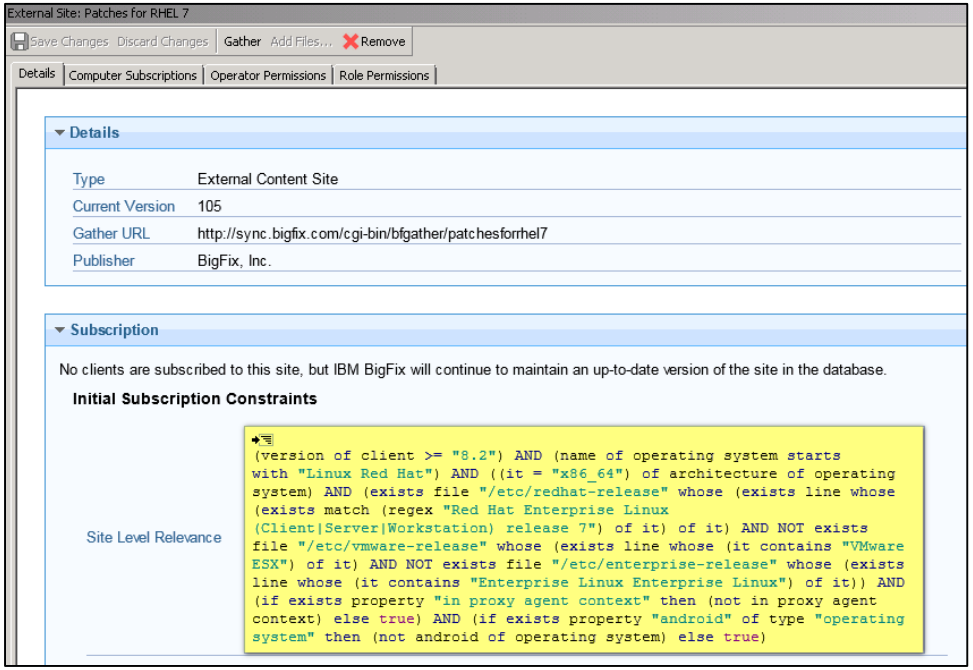
Wed, 21 Sep 2016 21:33:01 -0700 -- Beginning import of version 104 of site Patches for RHEL 7
Wed, 21 Sep 2016 21:33:42 -0700 -- Import of version 104 of site Patches for RHEL 7 completed successfully



Subscribing Computers

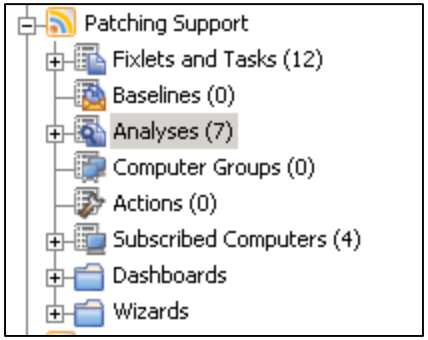
- Within the site go to the **Computer Subscriptions** tab and select **All Computers**
- In the **Operator Permissions** tab select the operators that you want to associate with this site and their level of permission
- Click **Save**
- **Site Level Relevance** in the site will take care of the rest:





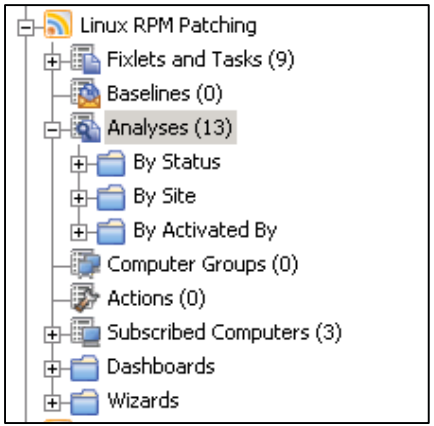
Activate analyses within the **Patching Support** and **Linux RPM Patching** sites

- The following analyses are useful for gaining information during the deploying patches for Red Hat systems



Analyses

ID	Status	Name	Site
1829	Activated Globally	"Shell Shock" bash Vulnerability (CVE-2014-7169) Status	Patching Support
45	Activated Globally	Download Plug-in Versions	Patching Support
49	Activated Globally	Overview of the Custom Repository Setting (Windows)	Patching Support
344	Activated Globally	Patch and Update Rollback Information	Patching Support
12	Activated Globally	Repository Configuration - Red Hat Enterprise Linux	Patching Support
28	Activated Globally	YUM Logs	Patching Support
27	Activated Globally	YUM Transaction History	Patching Support



Analyses

ID	Status	Name	Site
33	Activated Globally	Bootable Kernel Status - CentOS Linux	Linux RPM Patching
4	Activated Globally	Bootable Kernel Status - Red Hat Enterprise Linux	Linux RPM Patching
6	Activated Globally	Bootable Kernel Status - SuSE Linux Enterprise	Linux RPM Patching
38	Activated Globally	Bootable Kernel Status - Ubuntu	Linux RPM Patching
14	Activated Globally	Endpoint Dependency Resolution - Deployment Results	Linux RPM Patching
43	Activated Globally	Endpoint Dependency Resolution - Missing Prerequisite Packages	Linux RPM Patching
18	Activated Globally	Endpoint Dependency Resolution - Preference Lists	Linux RPM Patching
44	Activated Globally	Endpoint Dependency Resolution - Unsupported Packages	Linux RPM Patching
39	Activated Globally	Installed .deb Package List - Ubuntu	Linux RPM Patching
32	Activated Globally	Installed RPM Package List - CentOS Linux	Linux RPM Patching
2	Activated Globally	Installed RPM Package List - Red Hat Enterprise Linux	Linux RPM Patching
3	Activated Globally	Installed RPM Package List - SuSE Linux Enterprise	Linux RPM Patching
16	Activated Globally	RPM Deployment - View Results	Linux RPM Patching

Network Considerations

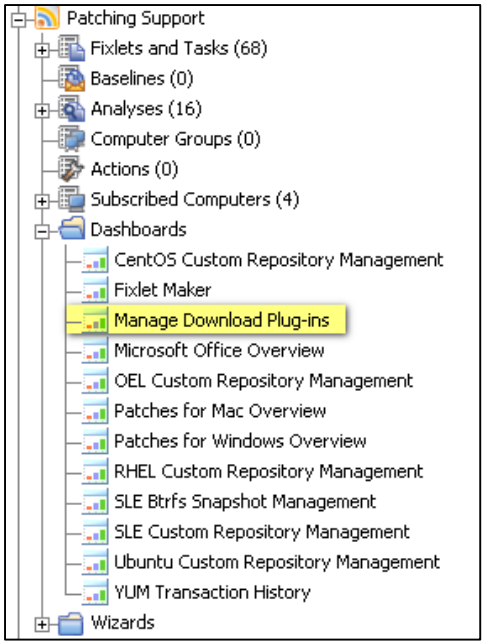
- The following sites will/may be access during Red Hat patching by the BigFix server or BigFix relays. Firewalls and proxies need to allow traffic from these sites through on ports 80 and 443:
  - software.bigfix.com
  - support.bigfix.com
  - sync.bigfix.com
  - sso.redhat.com
  - rhn.redhat.com
  - www.redhat.com
  - Your custom repository site if using a custom repository

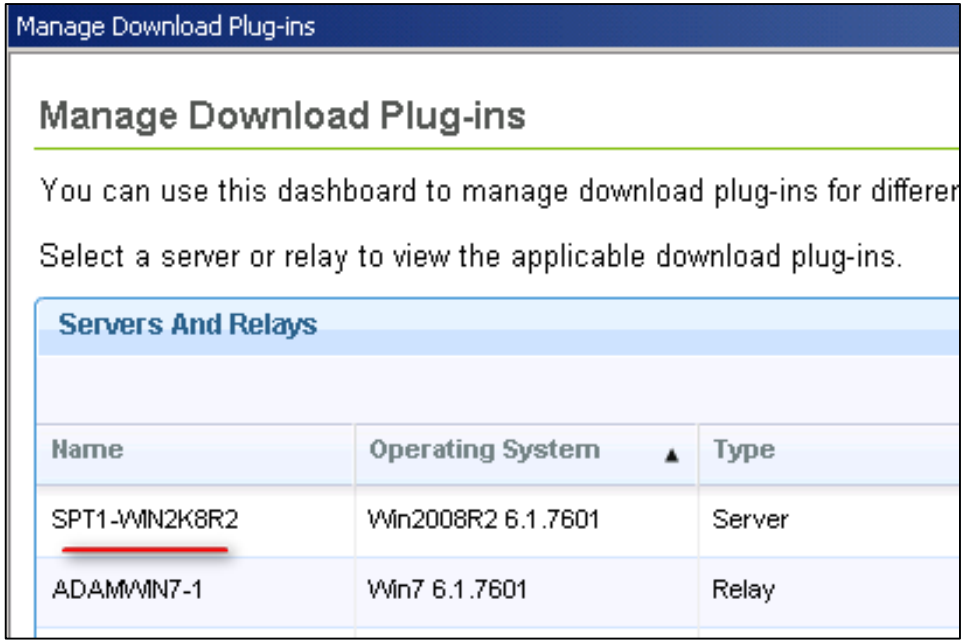
Two Setup Methods

Download Plug-in Method

Registering the Download Cacher Plug-in

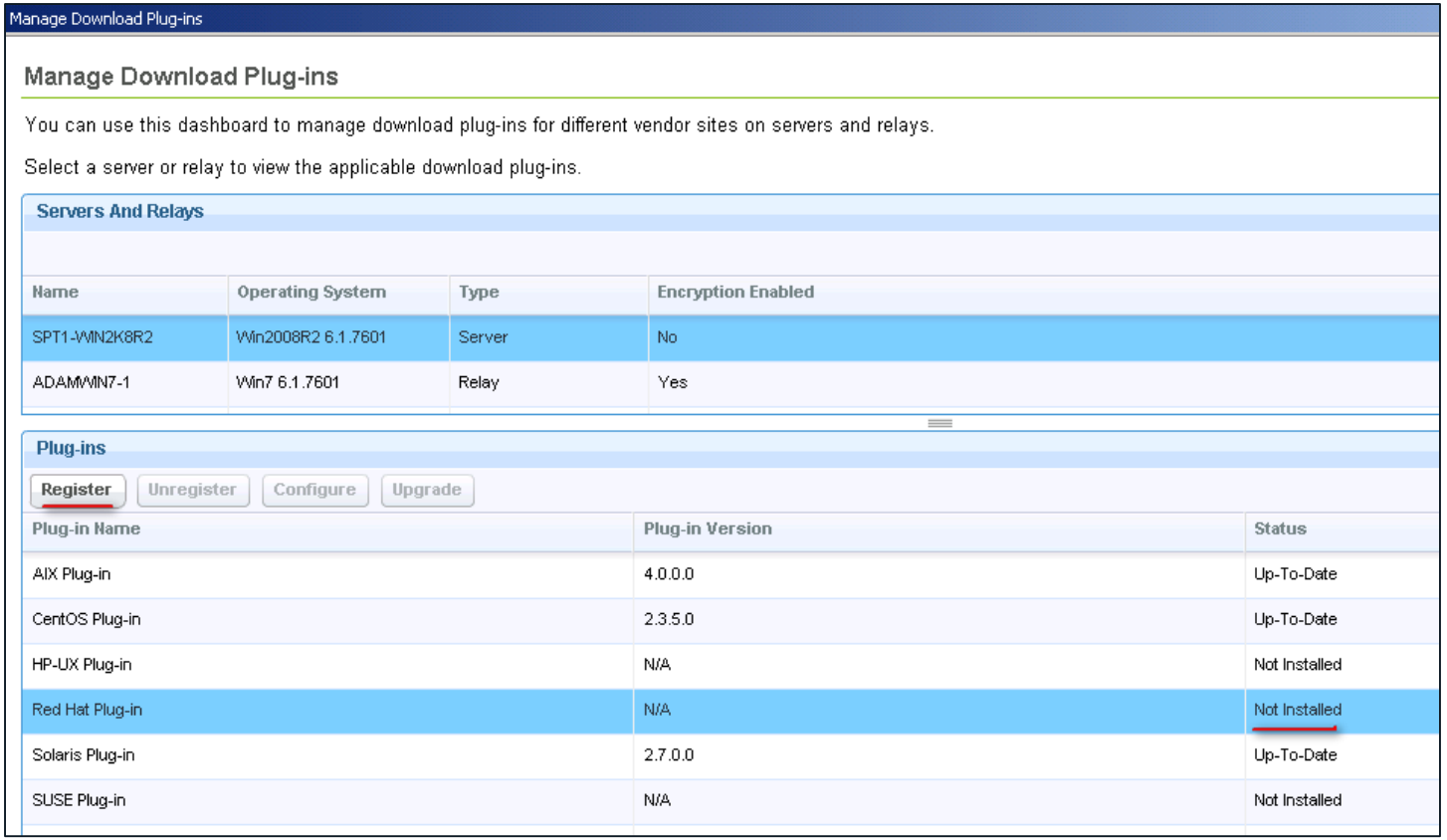
- **Go to the All Content > Sites > Patching Support > Dashboards > Manage Download Plug-ins dashboard**
- **And, choose your primary BigFix server**





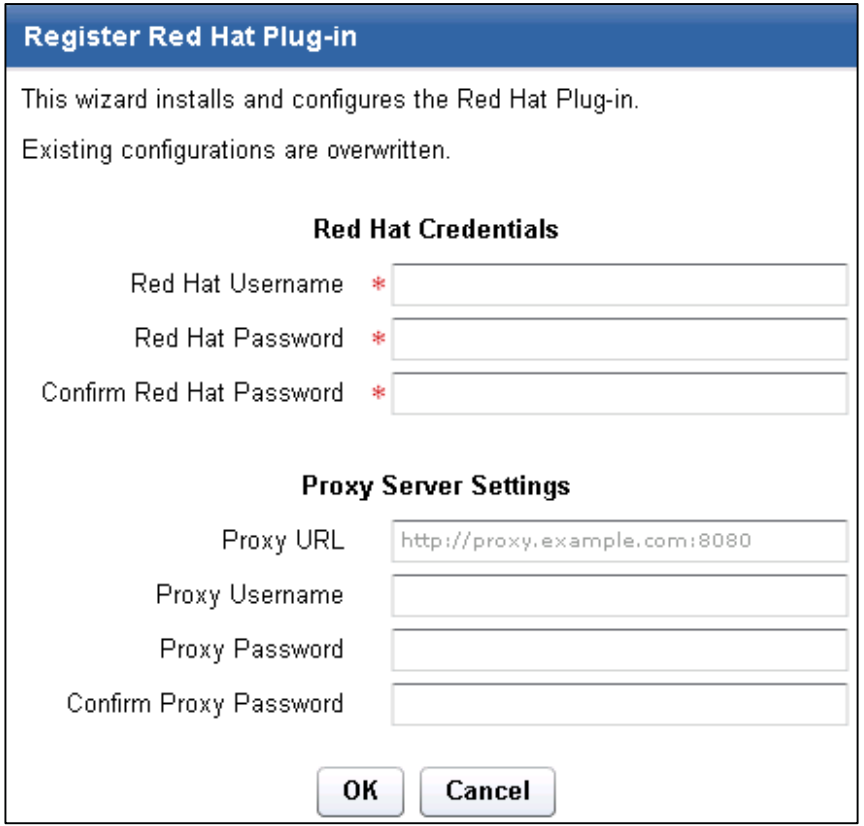
Registering the Download Cacher Plug-in

- **Choose the primary BigFix server and then click Register**



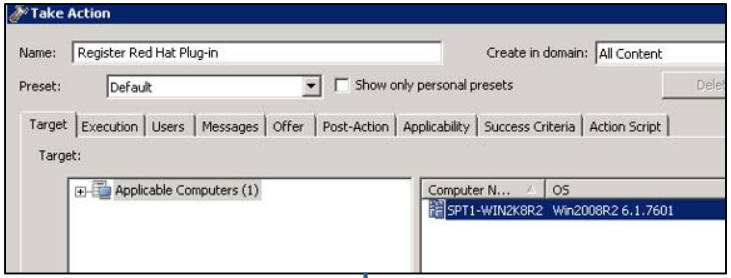
Registering the Download Cacher Plug-in

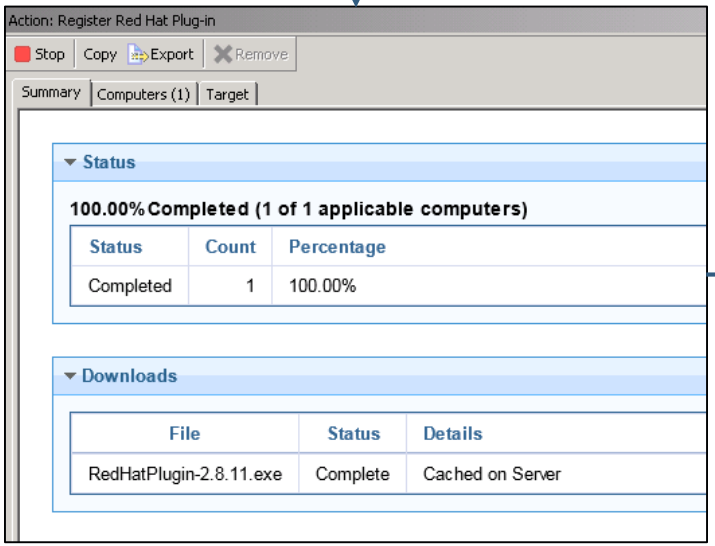
- **Enter your Red Hat credentials and your proxy credentials (if needed) and click OK**

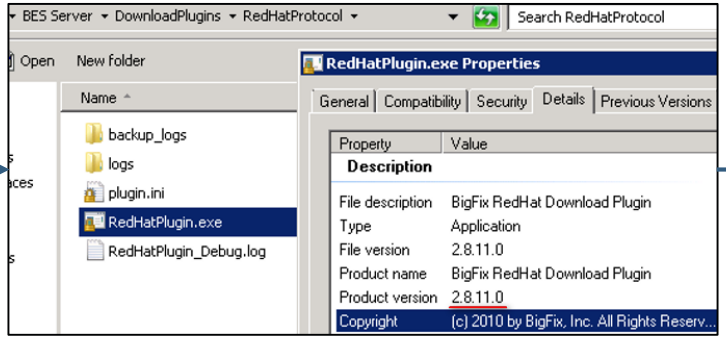


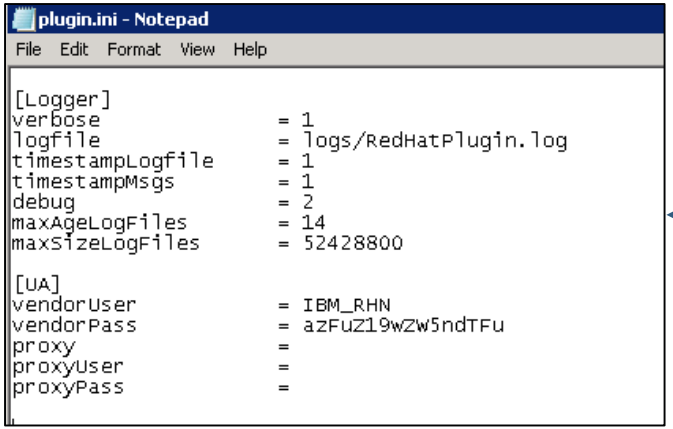
Registering the Download Cacher Plug-in

- **Once the action is completed, you can verify the plug-in is installed on the BigFix server from the following directory: <BES SERVER>\DownloadPlugins\RedHatProtocol**

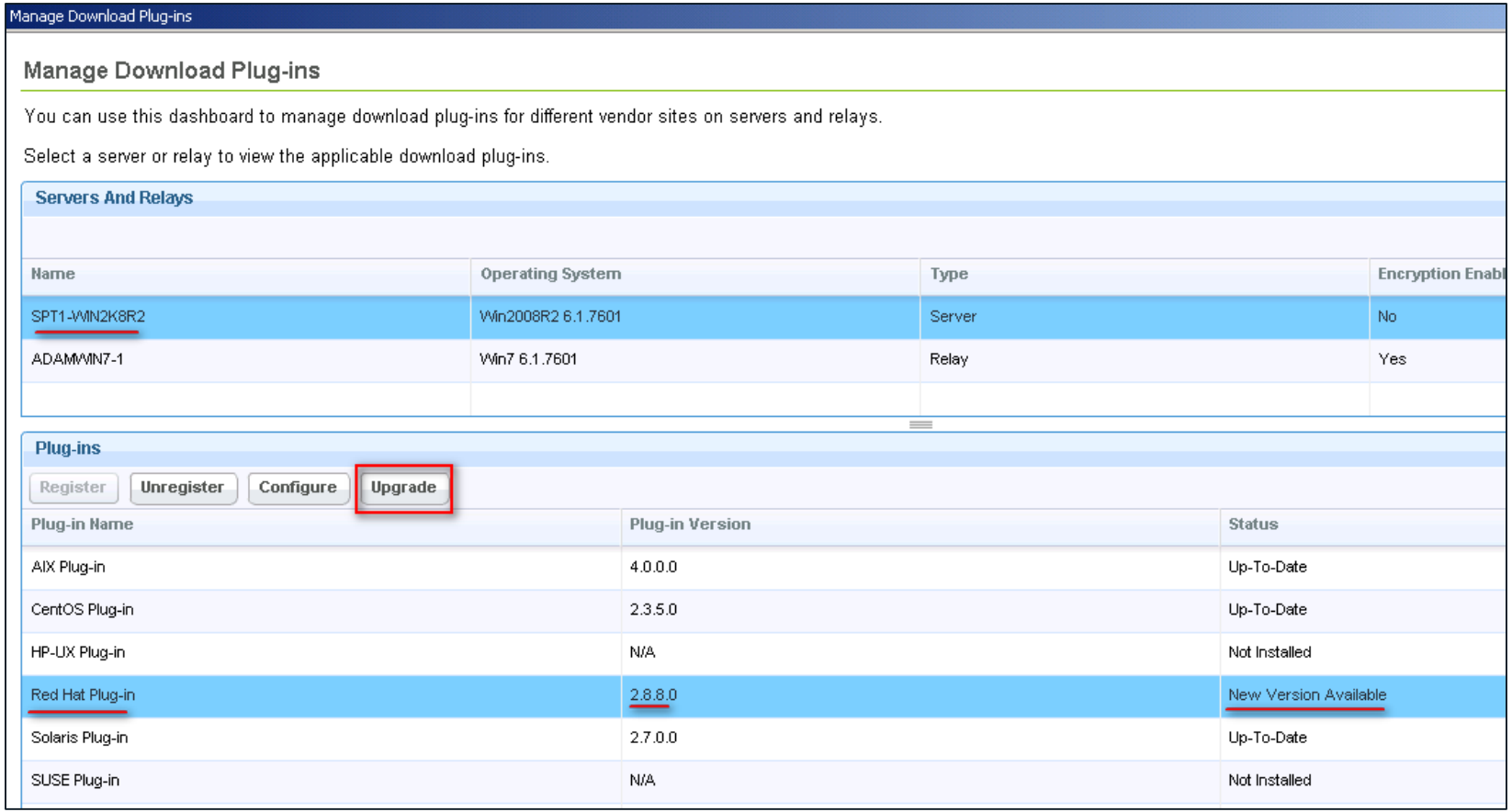




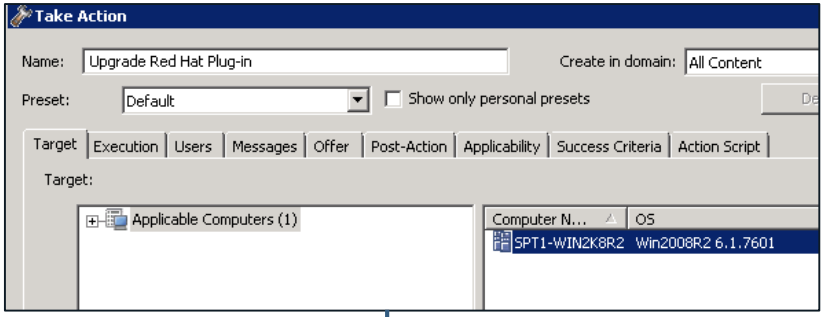


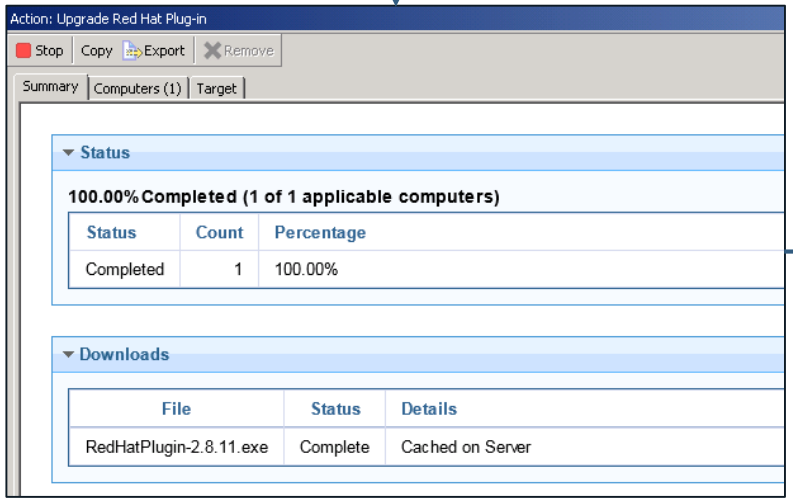


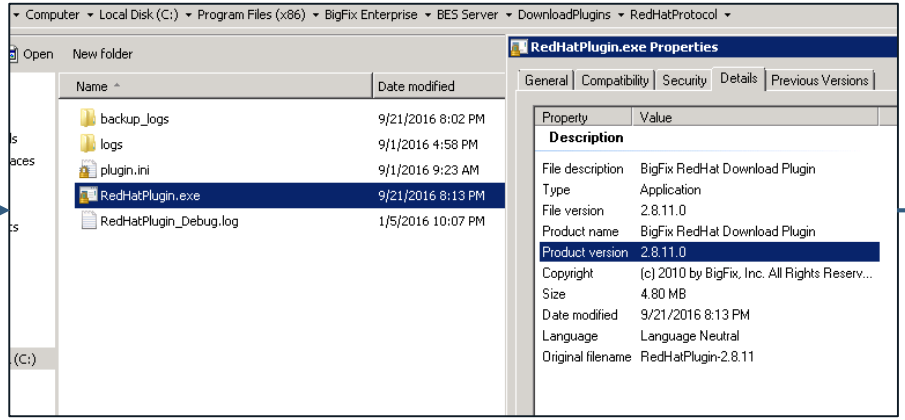
Upgrade Download Plug-in

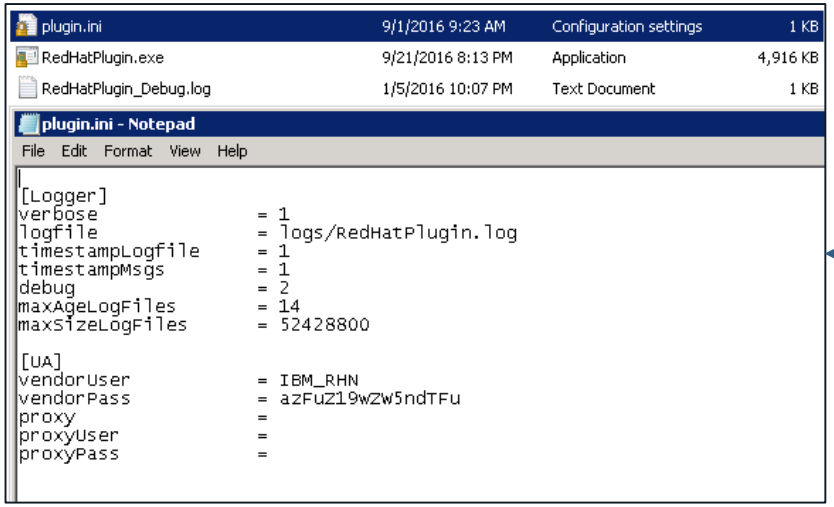


Upgrade the Download Plug-in



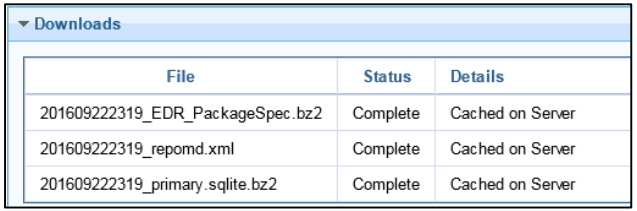






The Download Process

- Action is taken on a Red Hat patching fixlet
- Client receives action, evaluates it, and starts to execute it
- Native tool dependency resolution files are cached to the BigFix server and downloaded by the client to be used in the dependency resolution process on the client endpoint:
  - <BES SERVER>\wwwrootbes\bfmirror\downloads\sha1

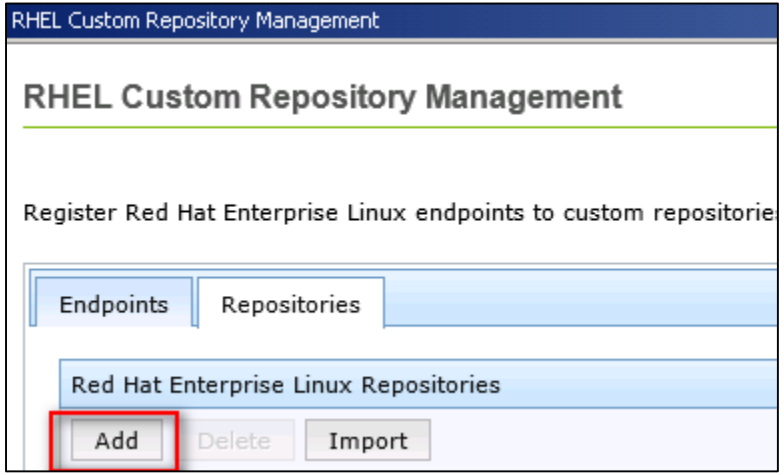


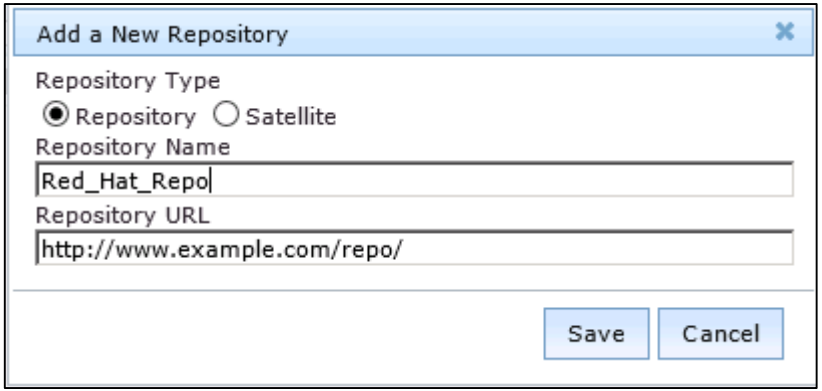
- The client calculates any needed dependencies on the client endpoint and sends these requests along with request for the payload patch package to Download Cacher plug-in on the server
- Download Cacher plug-in authenticates to Red Hat site, searches, and requests these items from the Red Hat for download
- The downloads are retrieved and cached to the BigFix server
  - <BES SERVER>\wwwrootbes\bfmirror\downloads\sha1
- Lastly, the client downloads them from the BigFix server (and through the relays) and installs them.

Custom Repository Method

Add a New Repository

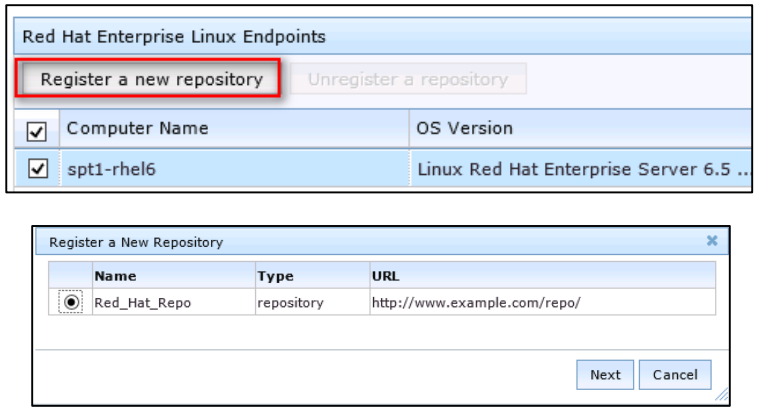
- Go to Sites > Patching Support > Dashboards > RHEL Custom Repository Management
- On the Repositories tab
- Choose the Repository Type and enter the details



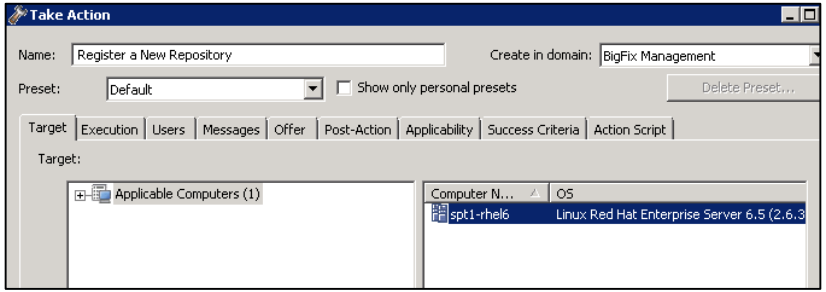


Register the Repository to your Endpoints

- On the Endpoints tab select the Red Hat endpoints to register with the repository and click **Register a new repository**:



- Choose the repository and click Next and click Save, then take action:

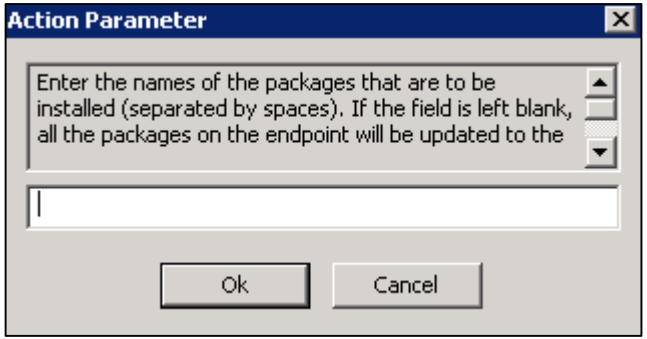


Enable custom Repository Support on your Red Hat Endpoints

- Take action on:
  - Task # 13 – “Enable custom repository support - Red Hat Enterprise Linux” in the Patching Support site
    - This task adds the following client setting on the endpoints:
      - "_BESClient_RHEL_AllowYumDownloads"="1"
- You should now be able to take actions on the patching fixlets and have the Red Hat endpoints download the patch packages

You can also update specific YUM packages

- You could also take action on Task # 18 – “Install packages by using yum” in the Patching Support site if there was a specific YUM update you wanted to update on the endpoint. Simply enter the name of the package(s) separated by spaces.
- **Note:** If you leave it black, the action will it updates all installed packages on the endpoint.



Common Problems

Download Plug-In Problems

- The Red Hat download plug-in needs to be registered on the server
- A new Red Hat download plug-in is available and needs to be updated
- The Red Hat site has changed and a new plug-in needs to be released by IBM BigFix
- Incorrect or invalid username/password is being used:
  - Test logging in via a browser @ https://sso.redhat.com/
- The Red Hat user does not have sufficient subscription privileges on the Red Hat site
  - Try manually searching for and downloading the package via http://access.redhat.com/errata/<errata id> in a browser.
- Your Internet proxy may be blocking the connection or download from occurring.
  - Consult with your network administrators. Wireshark packet captures.
- Download Plug-in logs are located at:
  - ..\BES Server\DownloadPlugins\RedHatProtocol\logs\RedHatPlugin_YYYY-M-D_HH-MM-SS.log
- Client logs can help to troubleshoot issues on the client endpoint: https://ibm.biz/BdrtsS

Example: A Change to Red Hat's Download Site

A change in the Red Hat site can cause a break in the download cacher plugin process.

Entries in the Red Hat plugin log:

..\BES Server\DownloadPlugins\RedHatProtocol\logs\RedHatPlugin_YYYY-M-D_HH-MM-SS.log

Which look similar to:

```
[Thu Sep  1 16:58:06 2016] BigFix RedHat Download Plugin v2.8.8
[Thu Sep  1 16:58:06 2016] Please make sure you have the latest version of this utility.
[Thu Sep  1 16:58:06 2016] Running plugin with DLoad::LWPUAIface
[Thu Sep  1 16:58:06 2016] (1) Logging in to Red Hat...
[Thu Sep  1 16:58:07 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:07 2016] Forbidden[Thu Sep  1 16:58:07 2016] (1) Logging in to Red Hat (try 2)...
[Thu Sep  1 16:58:07 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:07 2016] Forbidden[Thu Sep  1 16:58:07 2016] (1) Logging in to Red Hat (try 3)...
[Thu Sep  1 16:58:07 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:07 2016] Forbidden[Thu Sep  1 16:58:07 2016] (1) Logging in to Red Hat (try 4)...
[Thu Sep  1 16:58:08 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:08 2016] Forbidden[Thu Sep  1 16:58:08 2016] (1) Logging in to Red Hat (try 5)...
[Thu Sep  1 16:58:08 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:08 2016] Forbidden[Thu Sep  1 16:58:08 2016] (1) Logging in to Red Hat (try 6)...
[Thu Sep  1 16:58:08 2016] ERROR: Failed to log in to Red Hat
[Thu Sep  1 16:58:08 2016] Forbidden[Thu Sep  1 16:58:08 2016] ERROR: FATAL Failed to log in to vendor's site: Failed after 6 tries.
RHN may be down
```

Indicate either a problem with the Red Hat username/password or the Red Hat site has updated and broken the plug-in download process.

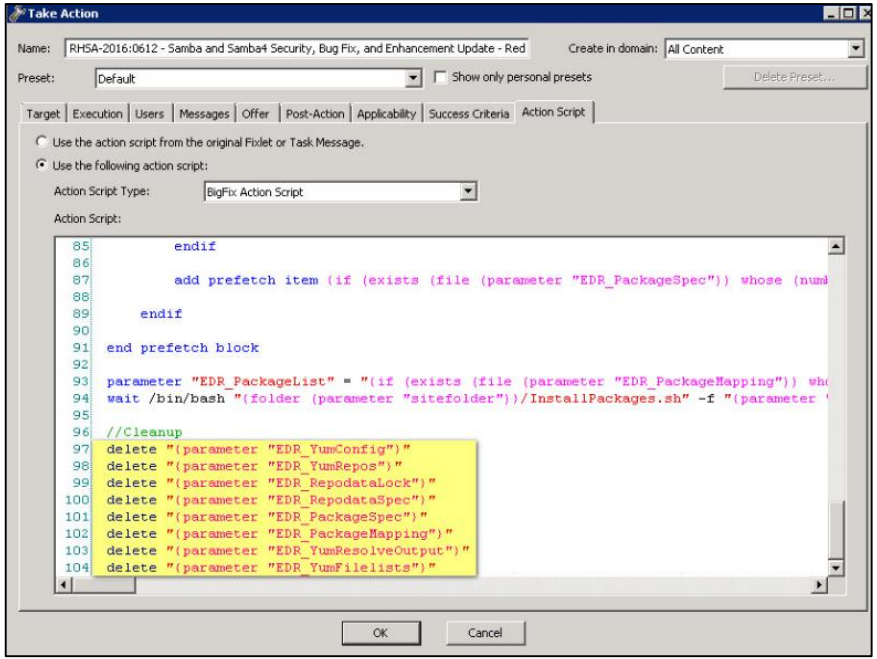
Test your username and password credentials via a browser @ https://sso.redhat.com/

Custom Repository Problems

- A custom repository or satellite server for Red Hat has not been setup or configured properly in your deployment
- The custom repository has not been added to your BigFix deployment
- Your Red Hat endpoints have not been registered to your custom repository
- Client setting "_BESClient_RHEL_AllowYumDownloads"="1“ has not been set on your client endpoints
- Client logs can help to troubleshoot issues on the client endpoint: https://ibm.biz/BdrtsS

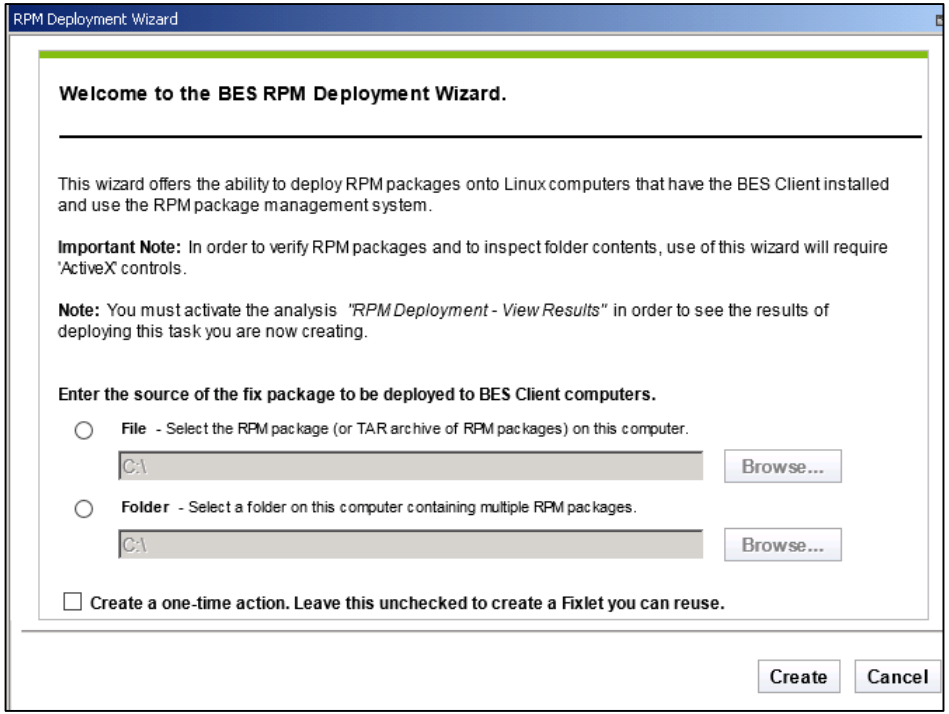
Problems with Dependency Resolution

- Check the /var/opt/BESClient/EDRDeployData/EDR_DeploymentResults.txt file on the endpoint for issues.
  - Certain kernel drivers and third party libraries may need to be updated ahead of deployment of a specific patch
  - You may need to take a secondary action, and remove the delete commands in the //Cleanup section at the bottom of the fixlet's Action Script. This will preserve all the EDR files which can be collected from the endpoint for troubleshooting.
    - Steps: https://ibm.biz/BdrkuZ
- Example: Dependency resolution fails because of third party dependency libraries
  - https://ibm.biz/Bdrkuj



You can use the RPM Deployment Wizard

- You can use the RPM Deployment Wizard in the Linux RPM Patching site to deploy an RPM to the endpoint via an action. You must have downloaded the RPM already.
- **Note:** This will process will not perform dependency resolution for the RPM



Other Potential Problems

- Problem with decompression of packages on the endpoint:
  - Ensure latest bzip2 application is installed on the endpoints.
- GPG error message on the endpoint during patch deployment:
  - Error in the EDRDeploymentResults file:
    - rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 37017186 Public key for <RPM files> is not installed.
  - Ensure gpg keys are installed and enabled on the endpoints or set the gpgcheck to 0
    - Use rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release.
    - Or, set gpgcheck=0 in /etc/yum.conf. This option only for the native tools sites.
- Important Note about the RHEL 7:
  - The BigFix patching process is similar among the versions and flavors for Red Hat Enterprise Linux. However, the change in the management services for Red Hat Enterprise Linux 7 might have an impact on how the patches are retrieved. Please see the following article for some additional steps you may need to take to ensure RHEL 7 downloads are accessible
    - RHEL 7 Patching: https://ibm.biz/BdHnFU

Resources

- **Patch for Red Hat Enterprise Linux Guide:**
  - https://ibm.biz/BdrkuY
- **Patch for Red Hat FAQ's:**
  - https://ibm.biz/Bdrku2
- **Best Practices for Patching Red Hat Linux:**
  - https://ibm.biz/BdrGJP
- **Additional Troubleshooting:**
  - https://ibm.biz/Bdrtjc

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Press *1 to ask a question over the phone

or

Type your question into the IBM Connections Cloud Meeting chat

To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum on this topic: https://developer.ibm.com/answers/questions/304559/openmic-deploying-bigfix-patches-for-redhat-septem/

Where do you get more information?

Questions on this or other topics can be directed to the product forum:

https://developer.ibm.com/answers/topics/bigfix/

Useful links:

Get started with IBM Security Support

IBM Support Portal | Sign up for “My Notifications”

Follow us:

IBM Security

THANK YOU

FOLLOW US ON:

https://www.facebook.com/IBM-Security-Support-221766828033861/

youtube/user/ibmsecuritysupport

@askibmsecurity

securityintelligence.com

xforce.ibmcloud.com

IBM