IBM BigFix Patch

Patching SUSE Systems Using BigFix

Best Practice Guide

28 March 2017
## Contents

1.0 Overview .......................................................................................................................... 4

2.0 Assumptions, Prerequisites, and Recommendations .......................................................... 5
    2.1 Supported Content ......................................................................................................... 5
    2.2 Required Packages ....................................................................................................... 5
    2.3 Disk Space .................................................................................................................. 5
        2.3.1 BigFix Server and Relays .................................................................................. 5
        2.3.2 BigFix Clients ................................................................................................. 5
    2.4 Network Configuration (Proxies and Whitelists) ......................................................... 6
    2.5 Baseline ..................................................................................................................... 6
        2.5.1 Multiple-Package Baseline Installation ............................................................ 7
    2.6 Custom Repositories ................................................................................................. 8
    2.7 SCC Download Plug-in ............................................................................................. 8
        2.7.1 BigFix Security Configuration - SHA256 checksum (Administration Tool) .... 8
    2.8 SCC Download Cacher .............................................................................................. 9
        2.8.1 Air-Gapped Environment Configuration .......................................................... 9

3.0 Testing Patches .................................................................................................................. 10
    3.1 Previewing Updates ..................................................................................................... 10

4.0 System Backup and Recovery .......................................................................................... 10

5.0 Reports ........................................................................................................................... 10

6.0 Tips .................................................................................................................................. 11
    6.1 Searching for a specific package ................................................................................ 11
    6.2 Locking packages to prevent installation ................................................................... 11

Appendix A: Logs .................................................................................................................... 12

Appendix B: Resources .......................................................................................................... 14
1.0 Overview

This document contains a compilation of best practices, assumptions, and requirements to help SUSE Linux Enterprise (SLE) system administrators and BigFix console operators adopt a smooth patch management strategy. The document describes how to set up and configure BigFix efficiently to patch SLE 11 and SLE 12 endpoints using IBM BigFix.

This document was written with the assumption that the readers possess the required knowledge of the SUSE operating system, the patch management lifecycle, and BigFix Patch.
2.0 Assumptions, Prerequisites, and Recommendations

2.1 Supported Content
BigFix Patch provides patch Fixlets for Mandatory, Recommended, and Optional updates in the following sites:

- Patches for SLE 11 Native Tools
- Patches for SLE 12 Native Tools
- Patches for SLE 11 on System z Native Tools

Fixlets are based on the packages that are made available in the supported SUSE repositories, which are listed in the BigFix Patch for SUSE User Guide.

**NOTE:** The available Fixlets do not upgrade the Service Pack level of the SUSE machines. You can create a custom Fixlet and use a custom repository to upgrade the Service Pack level of SUSE systems. To learn more, see [article](#).

2.2 Required Packages
Ensure that the required compression utilities are installed on the endpoints. Refer to the Patching using Fixlets section in the BigFix Patch for SUSE User's Guide.

2.3 Disk Space

2.3.1 BigFix Server and Relays
Ensure that the BigFix root server and BigFix relays have enough space to cache packages. A package is cached during its initial download, and subsequent downloads of that same package will come from the root cache or relay. It is recommended to set the BigFix server and BigFix relay cache size to 4 GB by using the BES Relay/ BES Server Setting: Download Cache Size Fixlet (ID #148) from the BES Support site.

2.3.2 BigFix Clients
Patching through the download plug-in directly from the BigFix server requires at least 4GB on the endpoint. If that much space is not available, the Custom Repository patching method can be considered.

Some guidelines:

- Ensure that you have at least 4GB of free disk space on each endpoint.
- Set the client download precache size (_BESClient_Download_PreCacheStageDiskLimitMB setting) to at least 2GB.
- Set the client download cache size (_BESClient_Download_DownloadsCacheLimitMB setting) to at least 2GB.
Set the download plug-in timeout
(_BESClient_ActionManager_PrefetchPlugInTimeoutSeconds setting) to a sufficiently large value. This client setting indicates how long the client should wait before blacklisting the script. You can use the Change Timeout for Prefetch Plugins task (ID #56), available from the Patching Support site, to set the setting to 30 minutes (1,800 seconds).

This client setting varies based on the endpoint and the Fixlet being installed. To get the desired value, take the slowest endpoint and increase the setting to a high number, such as 3,000 seconds, then run a large Fixlet and see how long it takes. You can then take that number and multiple it by two. Alternatively, set the client setting to 600 seconds and adjust it accordingly if the suggested value does not work for you.

- The /var cannot be mounted as noexec. For more information, see http://www-01.ibm.com/support/docview.wss?uid=swg21698951.

2.4 Network Configuration (Proxies and Whitelists)
Contact your Network Administrator to have the following URLs included in your network's whitelist, firewall, or proxy settings:

- https://scc.suse.com:443
- https://updates.suse.com:443
- http://sync.bigfix.com:80

The SCC Download Plug-in and the SCC Download Cacher access the listed URLs. Therefore, allowing traffic through the listed hosts and ports help prevent download errors.

2.5 Baseline
Some guidelines on using baselines when patching SUSE Linux Enterprise endpoints:

- Keep the baseline small (around 150 Fixlets).
- Avoid running multiple baselines from the same site on the same endpoint. Follow the Baseline Best Practices that is documented in the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21636385.
- Allow enough time for a Fixlet, which is using the multiple-package installation method, to complete all zypper transactions and refresh the status on the endpoints before individually deploying the same Fixlet.
- The repositories that are registered on the endpoint must contain the target packages and all the required dependency packages.
- Do not include multi-year Fixlets.
- Do not include Fixlets with packages that are in different repositories.
Patch zypper with the latest update to ensure successful installation of Fixlets for SUSE Linux Enterprise release packages, such as `sled-release-12-5.1.x86_64.rpm` or `sles-release-12-5.1.x86_64.rpm`.

You can find more guidelines for baselines in the [BigFix devWorks wiki](http://www-01.ibm.com/support/docview.wss?uid=swg21636385).

### 2.5.1 Multiple-Package Baseline Installation

BigFix Patch for SUSE offers the Multiple-Package Baseline Installation solution to help improve performance by reducing the execution time of the baseline. It can run a baseline patching time by up to eight times faster than a regular baseline execution.

This solution combines the installation of updates for multiple packages that are in a baseline into a single task, instead of having separate installation for each Fixlet. For detailed information about this solution, see [here](http://www-01.ibm.com/support/docview.wss?uid=swg21636385).

Some requirements for using the Multiple-Package Baseline Installation solution:

- Pay special attention to SLE release packages and apply the zypper patches. As older versions of zypper cannot resolve dependency conflict issues, ensure that you patch zypper with the latest update. By doing so, you can ensure that Fixlets for SUSE Linux Enterprise release packages, such as `sled-release-12-5.1.x86_64.rpm` or `sles-release-12-5.1.x86_64.rpm`, can be installed successfully in the baseline. For details about how to search for certain Fixlets with the zypper patch update, see [Creating a search filter for zypper](http://www-01.ibm.com/support/docview.wss?uid=swg21636385).

- Set the client download precache and cache sizes to at least 2GB. See the guidelines discussed in [2.3.2 BigFix Clients](http://www-01.ibm.com/support/docview.wss?uid=swg21636385).

- 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 zypper 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 that is documented in the following technote: [http://www-01.ibm.com/support/docview.wss?uid=swg21636385](http://www-01.ibm.com/support/docview.wss?uid=swg21636385)

Packages with broken dependencies are skipped whenever possible. Packages with dependency issues with a SUSE product, such as `SLED-12-0.x86_64`, cannot be skipped. Another scenario where packages are not skipped is when a dependency error occurs during installation, as indicated by the following error message:

```
File conflicts happen when two packages attempt to install files with the same name but different contents.
```

In such cases, the installation is canceled and no patches are installed on the endpoints.
2.6 Custom Repositories

Use custom repositories to manage packages according to your needs. You can stage patches; block a certain package from installing, such as kernel updates; and do other customizations.

Repositories must be registered on the endpoint through the SLE Custom Repository Management dashboard.

Prior to patching, the repositories must contain the target packages and all the required dependency packages to avoid dependency issues.

For more information about Custom Repository Management, see https://ibm.biz/BdsCgY.

2.7 SCC Download Plug-in

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

For the Fixlet to be able to use the protocol, register the SCC download plug-in on the BigFix server. Use the Manage Download Plug-ins dashboard to register the SCC Plug-in. More information is available in the SCC Download Plug-in section of the BigFix Patch for SUSE User Guide.

By default, packages are downloaded from the vendor site via the SCC download plug-in for SLED/SLES 11 and SLED/SLES 12.

Depending on the package size and the network speed, you may need to configure some client settings to ensure efficiency in caching files. For more information, see section 3.2.2 BigFix Clients.

2.7.1 BigFix Security Configuration - SHA256 checksum (Administration Tool)

Do not enable the Enhanced Security mode with the SHA-256 downloads requirement.

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

If your environment requires SHA-256 to verify the integrity of the patches for security reasons, consider doing the following actions:

- Open a request to SUSE directly to request them to generate the repository metadata with SHA-256 checksum.
- Use the custom repository feature. BigFix Patch for SLED/SLES 11 and SLED/SLES 12 ships with support for using an SMT server as a custom repository. Using the SMT to act as a custom repository would bypass the download request from the BigFix client and directly use zypper to download the packages. For more information about this feature, see Custom Repositories Management in IBM Knowledge Center.
2.8 SCC Download Cacher

The SCC Download Cacher is a standalone command-line tool that is designed to be used for air-gapped environments to download and cache files required for patching. The pre-cached files can be used by the download plug-in to patch the endpoints. By pre-caching the files, execution of actions is faster because files don't need to be downloaded from the Internet before distributing them to BigFix clients.

The latest SCC Download Cacher is available from IBM Knowledge Center. You can access the Windows and Linux installers here.

The system running the SCC Download Cacher must meet the required packages and disk space that are specified in the previous link.

The SCC Download Cacher does not support repositories that are not officially supported by BigFix Patch, such as LTSS and similar. For a list of the supported repositories, see here.

To ensure successful access to the SUSE repositories, use the correct mirror credentials during the registration of the download plug-in registration and execution of the download cacher. The mirror credentials refer to the Organization Credentials that are listed in the SUSE Customer Center or Novell Customer Center. For more details, see Mirroring Credentials.

2.8.1 Air-Gapped Environment Configuration

A typical air-gapped environment has no internet connectivity but can access shared drives or portable hard disks.

To patch endpoints in an air-gapped environment, you will have to cache the files needed on an internet-accessible machine and then move those files to the BigFix server in the air-gapped environment.

Ensure to register the SCC Download Plug-in and use the SCC Download Cacher to download and manage the packages in a local repository.

The network share or portable drive that is used by the SCC Download Cacher must contain sufficient space for all the repositories used for patching. Each repository could be up to 60GB large. If you have enough bandwidth and disk space, it is recommended to cache as much as possible with the Download Cacher prior to your patching window.

You can reduce the download time during the Fixlet deployment process by configuring the SCC SCC Download Cacher with the SCC Download Plug-in. The Download Plug-in can be configured to look for the packages locally first (from the Download Cacher folders) before going to the internet to find packages from SUSE's servers. This may give a faster and more reliable patching experience, as the amount of internet traffic should be reduced considerably during the actual patching window.

Complete the following steps to set up the local patch repository for an air-gapped environment:

1. Run the SCC Download Cacher by using the buildRepo subcommand to download all patches for a repository to a specified directory.

   Example command line to cache:

   SCCDownloadCacher.exe --mirrorUser user_name --mirrorPass password --proxyServer http://someproxy:8080 --download_dir "E:\some_folder_for_storage" buildRepo --key sles-12-x86_64-sp0

2. Transfer the entire download directory to the air-gapped server.
3. Configure the Download Plug-in to use the directory on the air-gapped server by editing the plugin.ini file in the SCCPlugin folder and modifying the following line (change the path accordingly):

```
localCache = E:some_folder_for_storage
localCacheOnly = yes
```

### 3.0 Testing Patches

It is recommended to test the patches through the released Fixlets before installing them on the endpoints. This is to ensure that all possible conflicts have been identified in a test environment before installing them in the production environment.

#### 3.1 Previewing Updates

All the patch Fixlets and tasks, such as Multiple-Package Baseline Installation, provide an action for a dry run of the installation. This option helps avoid broken dependencies due to undesired package updates by providing a preview of the changes on the packages.

Doing a dry run caches the metadata and packages on the BigFix server, which optimizes the actual patch deployment.

### 4.0 System Backup and Recovery

One of the most important aspects of patching is to have a backup and recovery plan in place. When things go wrong (power outages, disk drive failures, and so on), the aim is to decrease the downtime and bring the system back up to a stable state at the soonest possible time.

BigFix Patch offers the following solutions to help with data recovery:

- Native tools rollback command
- SLE Btrfs snapshot management solution

More information about these solutions can be found [here](#).

Using the Multiple-Package Baseline Installation feature can have effects on how patches are rolled back. Everything in the baseline will be rolled back. Therefore, consider splitting the Fixlets into different baselines based on the need to allow for fine-grained management on rollbacks.

### 5.0 Reports

There are several Web Reports that are capable of providing what patches were applied to a computer, and which ones are still relevant.

Some example Web Reports that could be useful:

- Action List
- Missing Patch Report (SLE 11)
Apart from web reports, BigFix provides analyses which can help you in preparing for the compliance reports.

6.0 Tips
This section discusses a few deployment tips that may come in handy.

6.1 Searching for a specific package
You can create a custom Filter in the BigFix console to search for the package name that is listed in the Fixlet description.

To display the Custom Filter dialog, press **CTRL-F** or click **Edit > Find** from the menu bar. Then, use the appropriate properties to filter the content that you need.

Here is an example filter that searches the Patches for SLE 12 Native Tools site for the sssd package:

6.2 Locking packages to prevent installation
You can use the **Hide a Fixlet** feature in the console to stop other operators from installing certain types of packages.

Also, the native tools command **zypper lock** can lock packages from being upgraded. For more information, refer to **zypper help**.
Appendix A: Logs
Logs and data to collect for troubleshooting IBM BigFix Patch for SUSE issues.

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

- **SCCPlugin.log**
  Lists the results of the downloads related to the execution of the SCC download plug-in.
  The amount of information depends on the logging level, which can be configured in the [Logger] section of the plugin.ini file.

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

  The available logging levels are listed in the order of increasing amount of information logged:

  - **ERROR**
    Contains errors that are 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. The amount of information to log, which might impact performance, so only use this level when investigating an issue.

  The SCCPlugin.log file can be found in the following locations:

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

The following logs 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 Zypper output. The log file indicates if the normal Zypper process is used for either a standard repository or SMT. To enable debug logs for the EDR_DeploymentResults.txt file, set the debug_level of a Fixlet action to 10 and rerun the Fixlet.
- **register-repo.log**
  Lists the results of the repository registration action of the SLE Custom Repository Management dashboard.

- **register-SMT.log**
  Lists the results of the SMT registration action of the SLE Custom Repository Management dashboard.

- **unregister-repo.log**
  Lists the results of the unregister repository action of the SLE Custom Repository Management dashboard.

- **unregister-SMT.log**
  Lists the results of the unregister SMT action of the SLE Custom Repository Management dashboard.

- **snapper_rollback.log**
  Lists Btrfs snapshot rollback feature that is available from the SLE Btrfs Snapshot Management dashboard.
Appendix B: Resources

BigFix Patch 9.5 Documentation in IBM Knowledge Center:

BigFix Forum: https://forum.bigfix.com

BigFix Blog: https://ibm.biz/BdsCpN

BigFix Developer: https://developer.bigfix.com/

BigFix Support: https://support.bigfix.com/

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

BigFix.me Community: https://bigfix.me

BigFix Videos and OpenMics: https://ibm.biz/Bdrcscs

BigFix Patch Beta Program: https://ibm.biz/BdsCpG

SUSE Customer Center: https://scc.suse.com/login