



Security Team BigFix Agent Installation

Version 1.0

|  |  |
| --- | --- |
| Document last changed: | Apr/26/18 |
| Document Owner: | Tian Li PH He/China/IBM |
| Review and Approve: | Branden J Hartwell/Lansing/IBM  P&Q QA Specialist |
| Document Name: | AppOps – GB0193 - 1.5 Level Runbook Security Team BigFix Agent Installation v1.0.docx |

|  |  |
| --- | --- |
| Asset Type: | **Runbook** |
| Area: | ( ) Commercial Projects ( ) Internal Projects ( **X** ) Operations  ( ) Management |
| Level: | ( ) Common ( **X** ) Specific |
| Service/Technology: |  |

["THE ON-LINE VERSION IS THE MASTER VERSION”](https://dstassets.sby.ibm.com/ram/oslc/assets/EC907F1E-0D2E-6E40-CCED-A5633B430527)

Contents

1. Operation Specification 3

1.1 Description 3

1.2 Related Runbooks / Business Procedures 3

1.3 Participant Roles 3

1.4 Operation 4

1.4.1 Pre-conditions 4

1.4.2 Overview 4

1.4.3 Detailed Steps 4

2. References 10

3. Document History 11

# Operation Specification

BigFix is the core of a massive extensible ability of distributed processing system, which can be through a single policy-driven agent real-time continuous discovery, evaluation, repair and forced all desktop computers in the distributed enterprise, mobile terminals and services.

BigFix core services -- including the BigFix agent, the BigFix server, the BigFix console, the BigFix repeater and Fixlet policy messages. A lightweight, dynamic content driven messaging and management control system.

BES product function: Configuration management, Patch management, Terminal safety management, Vulnerability management, Network access control.

The Default port is 52311, Both the client and console use this port to connect to the server. The License Metric Tool server connects to the BigFix server using this port. License Metric Tool users from their computers using a Web browser to access the application server, provides the report interface, is used to display the BigFix endpoint management by collecting inventory and limited application usage data. A fixlet is composed of problem description, problem detection, and problem repair.

The design goal of the BigFix solution is not to deal with a preset environment, but to work in an unknown environment. BigFix has been working on creating a unified, common problem processing platform rather than just solving the current problems. Whatever the problem is, the platform can provide the infrastructure and methodology for solving the problem.

## Description

This Runbook provides a general overview of BigFix and introduces the BESClient installation.

## Related Runbooks / Business Procedures

N/A

## Participant Roles

* SOC Level 1.5 Team
* AppOps Security Team: responsible for BESClient installation, BESClient status check, BESClient Troubleshooting

## Operation

### Pre-conditions

* The client is allowed to install or configure during the operation.

### Overview

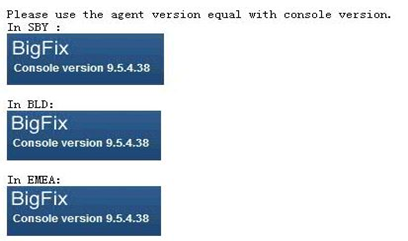
N/A

### Detailed Steps

1. **For Non-Windows installation:**
   1. Select the BESClient installation version:

There are four kinds of bigfix server: SBY, BLD, EMEA and SL(softlayer). Check server’s kind.

* + 1. Look to AdminSite in SADB
       1. If it started with SL, it’s SL.
       2. If it’s not SL server and if the AdminSite included DST MOP, DST RO, DST France, DSTAustralia, etc (all servers are from EMEA), it’s EMEA.
       3. If it’s DOU included BlueCloud, it’s BLD.
       4. Then it’s SBY.



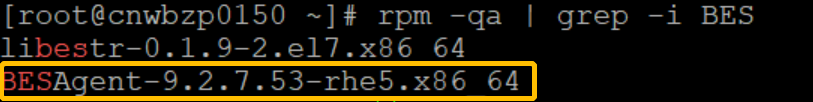
* 1. Use below command to check if the bigfix is installed：

Linux: rpm -qa | grep -i BES

Ubuntu: dpkg -l | grep BESAgent

AIX: lslpp -L | grep -i BESClient

For example: This Linux server has BESClient.

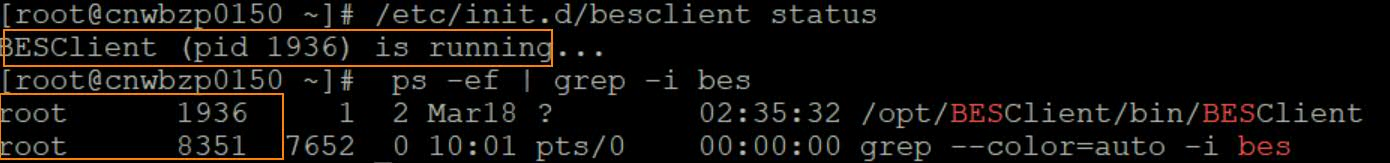


* 1. Use below command to check if the bigfix is running

ps -ef | grep -i bes

/etc/init.d/besclient status

For example:This linux server , BESClient is running…



* 1. If the bigfix haven’t been installed, install it
     1. Create directory

mkdir /etc/opt/BESClient

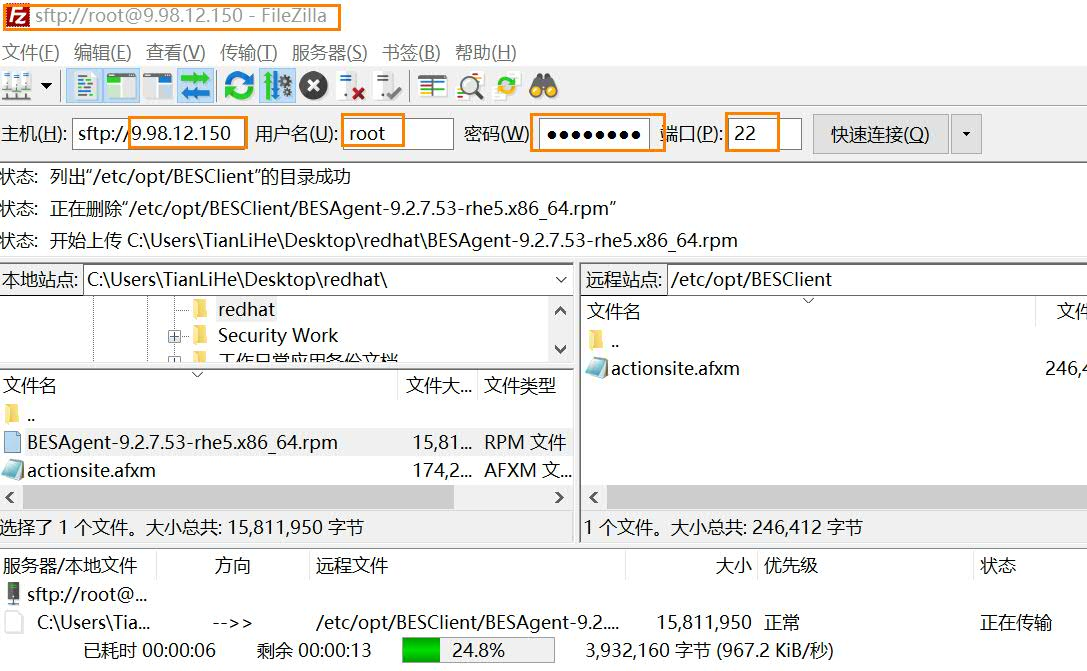
* 1. Use FZ or WinSCP to Upload installation package(BESAgent-9.5.4.38-rhe5.x86\_64.rpm，actionsite.afxm) to server or use command:‘scp BESAgent-9.5.4.38-rhe5.x86\_64.rpm actionsite.afxm root@severIP: /etc/opt/BESClient’.

For BigFix Package Download Address and related files, please check [References Section.](#_References)

Different kinds server has different actionsite.afxm, please get it from folder

* SL: linux/SL/actionsite.afxm
* EMEA: linux/EMEA/actionsite.afxm
* SBY: linux/SBY/actionsite.afxm
* BLD: linux/BLD/ActionSite.afxm

For example: Use FZ to transfer files to a specified folder:



* 1. Install the bigfix client, get the package from folder linux/Install package
     1. For EMEA and SL server:

Linux : rpm -ivh BESAgent-9.2.7.53-rhe5.x86\_64.rpm

zlinux SUSE : BESAgent-9.5.6.63-sle10.s390x.rpm

Other SUSE: rpm -ivh BESAgent-9.2.7.53-sle10.s390x.rpm

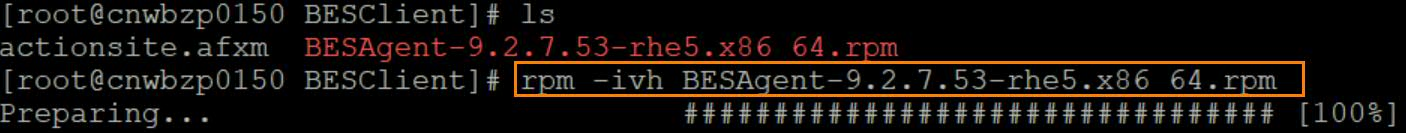
Ubuntu: dpkg -i BESAgent-9.2.7.53-ubuntu10.amd64.deb

AIX : installp -agqYXd ./BESAgent-9.2.7.53.ppc64\_aix61.pkg BESClient

* + 1. For SBY and BLD server:

Linux : rpm -ivh BESAgent-9.5.4.38-rhe5.x86\_64.rpm

For example (Linux Server): Use command install and Check if BES has been installed:



* 1. Put the besclient to server.
     1. This Step is only for SL server:

Linux：

/etc/init.d/besclient start && /etc/init.d/besclient stop

mv /var/opt/BESClient/besclient.config /var/opt/BESClient/besclient.config.bk

cp /etc/opt/BESClient/besclient.config /var/opt/BESClient

AIX：

/etc/rc.d/rc2.d/SBESClientd start && /etc/rc.d/rc2.d/SBESClientd stop

mv /var/opt/BESClient/besclient.config /var/opt/BESClient/besclient.config.bk

cp /etc/opt/BESClient/besclient.config /var/opt/BESClient

* 1. Start the bigfix service

Linux : /etc/init.d/besclient start

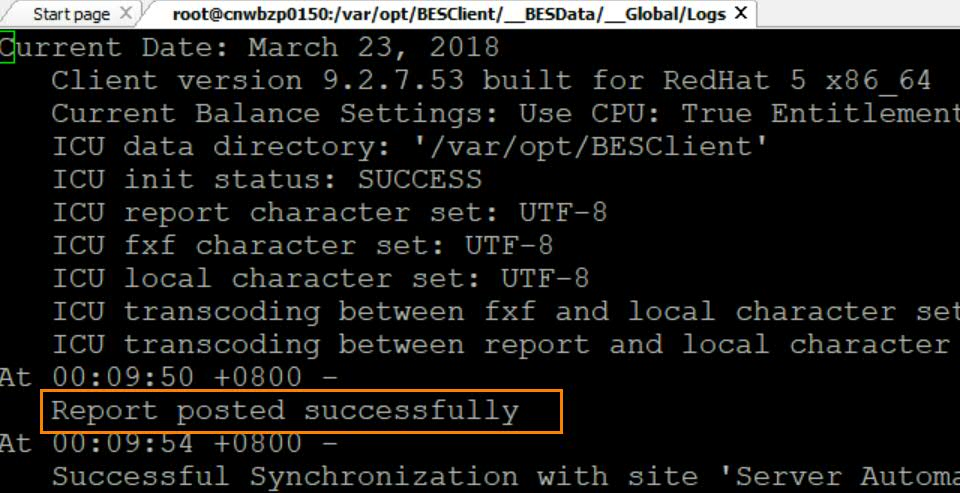
AIX: /etc/rc.d/rc2.d/SBESClientd start

* 1. Check the log on directory to see if any error or fail

cd /var/opt/BESClient/\_\_BESData/\_\_Global/Logs

lf in the report appears “Report posted successfully” it proves that bigfix is successfully running and successfully connected to the server.

For example:



* 1. For SL servers, if there are errors in log, check the communication with bigfix servers; it’s connected time out. It is needed that PA to open a ticket to open the port:

SBY：

ping dstsecubigfix.sby.dst.ibm.com //ping SBY server 9.45.222.231

telnet dstsecubigfix.sby.dst.ibm.com:52311 //telnet SBY server 9.45.222.231

SBY SL：

ping atlnocbigfix01.atl.edst.ibm.com //ping SBY relay

telnet atlnocbigfix01.atl.edst.ibm.com:52311 //telnet SBY relay

ping atlnocbigfix02.atl.edst.ibm.com //ping SBY relay

telnet atlnocbigfix02.atl.edst.ibm.com:52311 //telnet SBY relay

ping 10.255.255.9 //atlbyzbigfix01.atl.dst.ibm.com 9.220.160.9

BLD：

ping dstsecubigfix07.bld.dst.ibm.com //ping BLD server 9.220.3.27

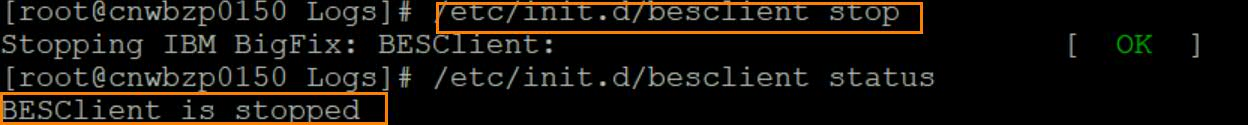
telnet dstsecubigfix07.bld.dst.ibm.com:52311 //telnet BLD server 9.220.3.27

* 1. If there are some error in the log, there may be needed to stop the bigfix services or to uninstall the bigfix client.
     1. Stop bigfix services command:

Linux: /etc/init.d/besclient stop

AIX: /etc/rc.d/rc2.d/SBESClientd stop

For example:



* + 1. Uninstallation steps for linux:

rpm -ev BESAgent-9.2.7.53-rhe5.x86\_64

rm -rf /var/opt/BESClient

rm -rf /etc/opt/BESClient

rm -rf /tmp/BES

rm -rf /opt/BESClient

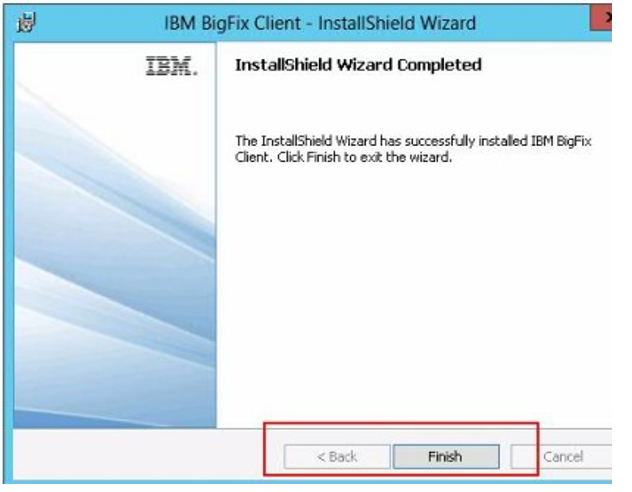
* + 1. Uninstallation steps for AIX：

AIX 6 7：installp -C BESAgent-9.2.7.53.ppc64\_aix61.pkg

AIX 6 7：smit remove BESAgent-9.2.7.53.ppc64\_aix61.pkg

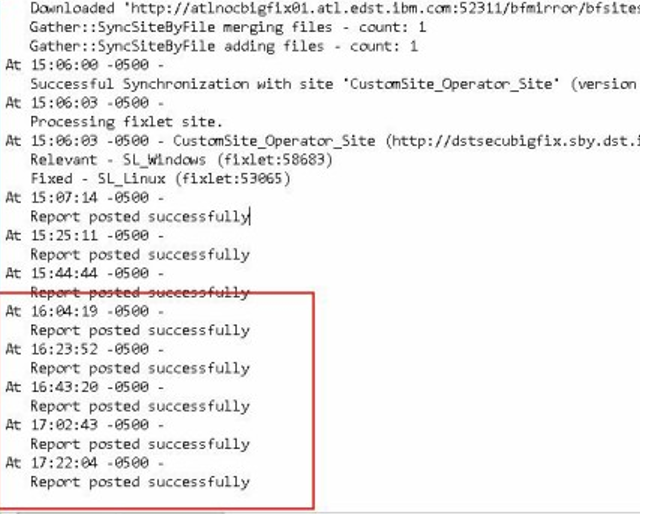
1. **For Windows installation:**
   1. Install the package:
      1. For SL: put three files (masthead.afxm, clientsettings.cfg and setup\_agent.exe) in windows\SL in the same directory in server and then run setup\_agent.exe
      2. For SBY: put the windows\SBY\ BigFixAgent\_SBY.msi to server and then run it
      3. For BLD: put the windows\BLD\ BigFixAgent\_BLD.msi to server and then run it

For example:



* 1. Check the logs: C:\Program Files (x86)\BigFix Enterprise\BES Client\\_\_BESData\\_\_Global\Logs

The report appears “Report posted successfully” proves bigfix is successfully running and successfully connected to the server.



For related installation files (clientsettings.cfg and masthead.afxm), please check [References Section.](#_Toc506564567)

# References

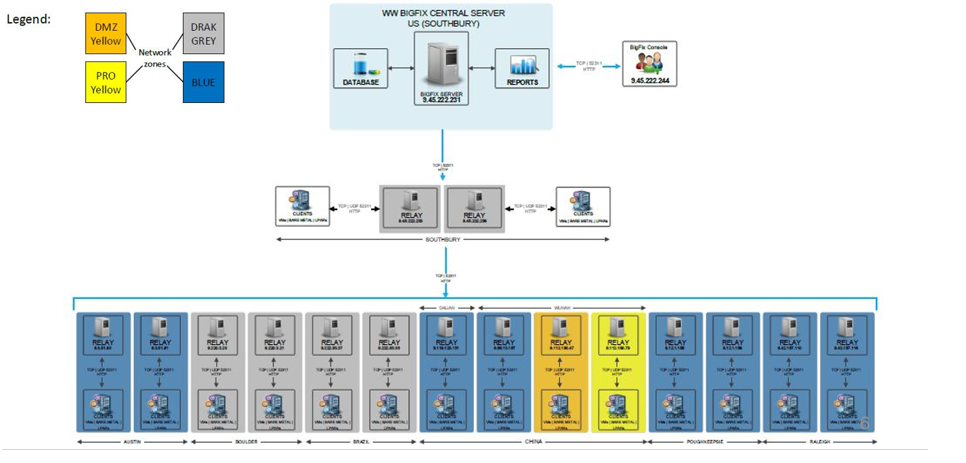
1. The relevant introduction and process are thought to refer to the following links: <https://www.ibm.com/support/knowledgecenter/zh/SSMNRU_9.5.0/com.ibm.bigfix.detect.doc/welcome/BigFix_Detect_welcome.html>
2. BigFix Package Download Address and related files:
3. SBY & BLD: <http://support.bigfix.com/bes/release/9.5/patch4/>

1. Related installation files (clientsettings.cfg and masthead.afxm):



1. All version bigfix client, relay and server installation package, you can download from: http://support.bigfix.com/bes/release/9.5/patch6/
2. All configuration files and installation package for BLD, SBY and SL, you can get from: <http://dst.lexington.ibm.com/install/BigFix_Client/>
3. EMEA actionsite. afxm from: <https://ibm.ent.box.com/s/0p8jfdkw3k30qaso9vhu95xo5oks1isk/folder/40695466137>
4. Softlayer installation steps in wiki: <https://w3-connections.ibm.com/wikis/home?lang=en#!/wiki/W73bc53e9309c_4801_a5e7_4bc3c4f15c56/page/BigFix>
5. DST BigFix Architecture Diagram:



# Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Release | Date | Summary of Changes | Author | Reviewer |
| 0.1 | Mar/30/18 | Creation | AppOps Security Team  Tian Li PH He/China/IBM | Branden J Hartwell/Lansing/IBM |
| 0.2 | Apr/18/18 | Modification | AppOps Security Team Branden J Hartwell | Roxana Manta |
| 1.0 | Apr/26/18 | Release | Roxana Manta |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Approvals**

| Release | Approver Name | E-mail ID |
| --- | --- | --- |
| 1.0 | Branden J Hartwell | Branden J Hartwell/Lansing/IBM |
|  |  |  |