



# BigFix Architecture

---

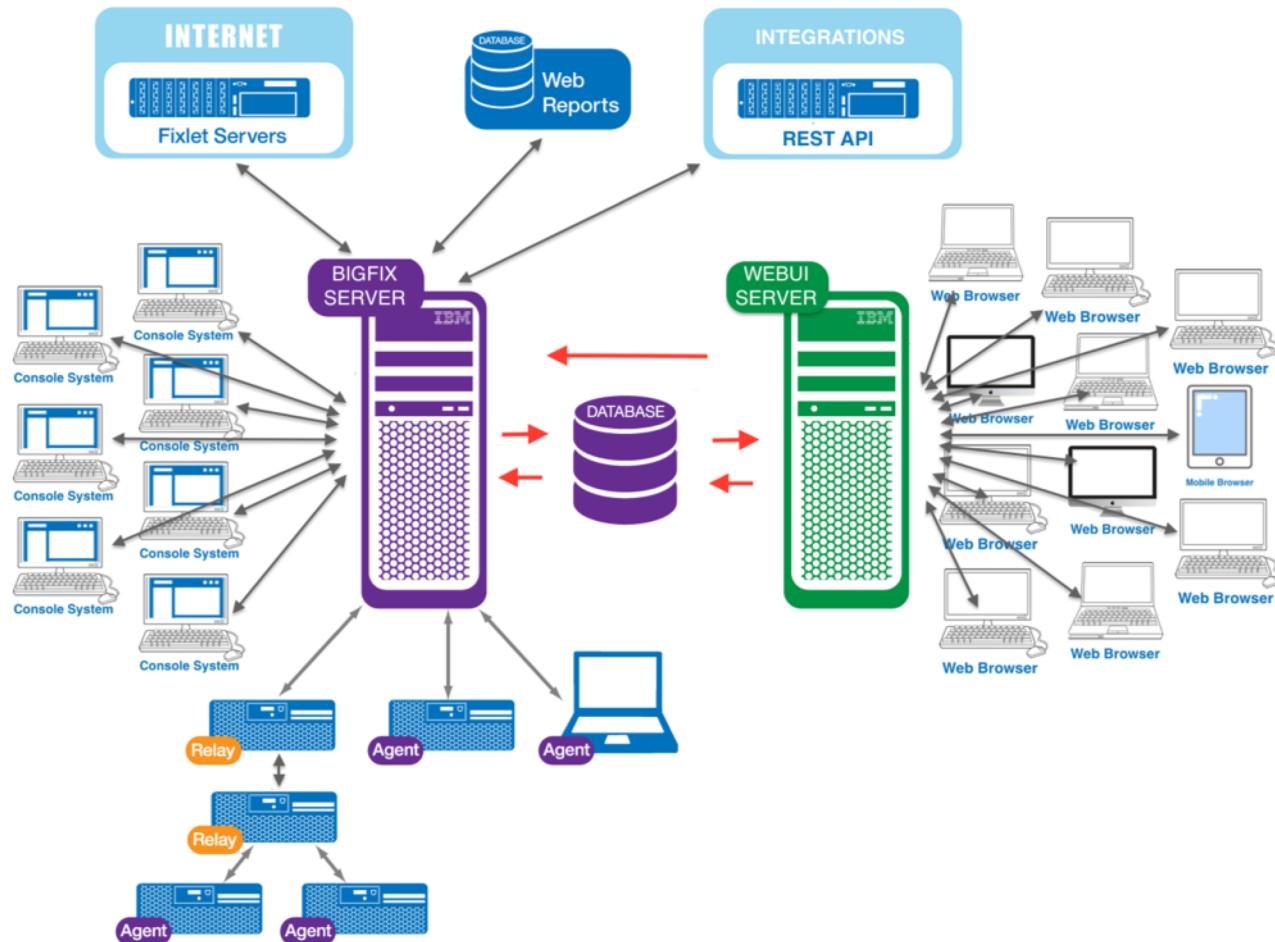
**Andrew Schmidt**  
BigFix Software Engineer

May 15, 2018



**HCL**

# Architecture – The Deployment as a whole



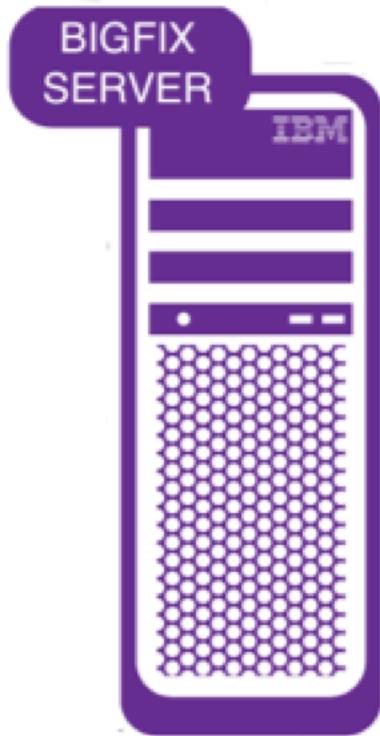
# BigFix Infrastructure Components

**01** ROOT SERVER

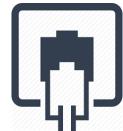
**02** WEBUI

**03** RELAYS

# 01 - Root Server - Basics



Site Gathering(sync.bigfix.com) & Downloading  
HTTP/HTTPS Ports 80/443



Infrastructure Communication  
HTTP/HTTPS TLS 1.2 TCP Port 52311



Client Communication  
HTTP/HTTPS TLS 1.0/1.2 TCP/UDP Port 52311



Database Communication  
ODBC



Windows 2008 SP2 or better 64 bit  
MS SQL 2008 or better



Red Hat Linux 6 or better 64 bit  
DB2 10.1 or better

# 01 - Root Server - Configuration

The server is very configurable so some settings to be aware of to make it perform the best in the environment you have are below

## Global Settings

### Setting HTML data to a different location

```
[Software\BigFix\Enterprise Server]  
wwwRootFolder = /var/opt/BESServer/wwwrootbes  
  
[HKLM\Software\BigFix\Enterprise Server]  
wwwRootFolder = C:\Program Files (x86)\BigFix Enterprise\BESServer\wwwrootbes
```

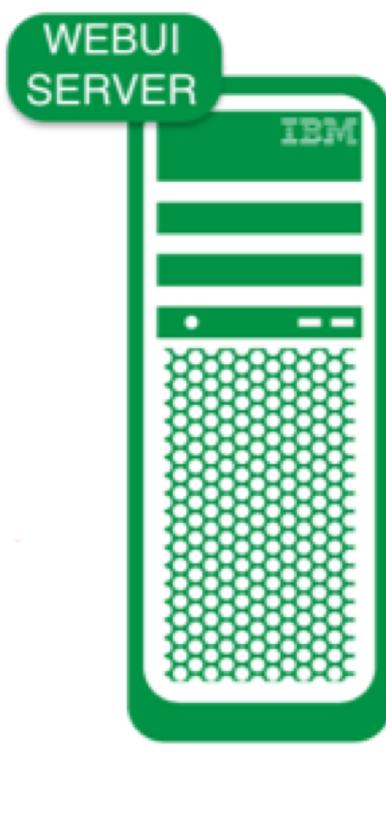
## Client Settings

Using HTTPS to Gather: \_BESGather\_Use\_Https (default 0)

Increasing server api thread usage: \_HTTPServer\_ThreadLimit\_api (default 250)



# 02 - WebUI - Basics



Browser Connectivity  
HTTP/HTTPS Ports 80/443

Root Server Communication  
HTTPS TLS 1.2 Ports 52311/52315

Database Communication  
ODBC

Windows 2008 R2 or better 64 bit

Red Hat Linux 6 or better 64 bit

# 02 - WebUI - Configuration

The server is very configurable so some settings to be aware of to make it perform the best in the environment you have are below  
Most of these are set during the deployment of the WebUI via Fixlet

## Client Settings

Base WebUI Directory: `_WebUIAppEnv_WebUI_DIR`

Sites WebUI Directory: `_WebUIAppEnv_WORK_DIR`

Task: Install IBM BigFix WebUI Service (Version 9.5.8)

Take Action |  Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description Details Applicable Computers (1) Action History (0)

**Description**

Deploy this Fixlet on a device to install the IBM BigFix WebUI Service

This Fixlet will:

- Install and start a service (Windows) or background process (Linux)
- Establish a secure connection with the IBM BigFix Server
- Set up the WebUI
- Send the database connection configuration to the WebUI server
- Encrypt the database credentials
- Create a new folder in the WebUI folder
- Extract and run the WebUI service

**Deployment configuration**

Specify WebUI HTTPS Port:

Specify WebUI HTTP Redirect Port:

Specify Hostname or IP of Targeted Endpoint:

Windows Only: Custom Directory for the WebUI Service (Optional):

**Database configuration**

Specify Database Username:

Specify Domain Name (see below):

Specify Database Password:

Confirm Database Password:

Specify BigFix Database Host (see below):

**Optional database configuration**

Specify SQL Server Named Instance:

Specify Database Port:

Follow this knowledgecenter [link](#) to view deployment requirements and detailed information on the inputs to this fixlet

**Deployment notes:**

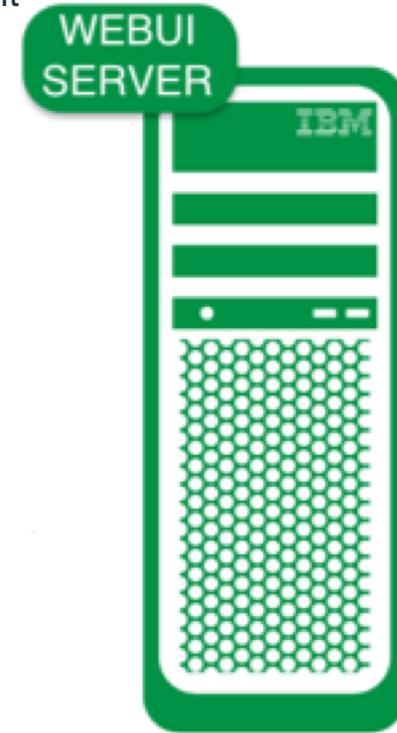
**Important Note:** IBM BigFix Server Version 9.5.8 is required to execute this Fixlet. Additionally only IBM BigFix Client Version 9.5.3 or later endpoints will be relevant for this Fixlet.

**Important Note:** An operating system patch is required for this Fixlet to become relevant for servers running Windows 2008 R2. This fixlet cannot be run automatically through a Fixlet. In order to apply the Hotfix, administrators must visit <http://support.microsoft.com/kb/257779>, request the patch from Microsoft and apply the patch.

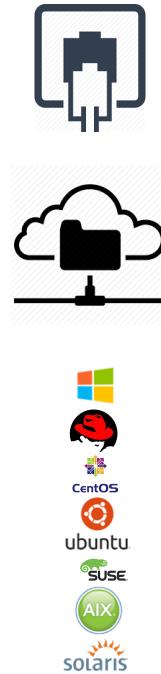
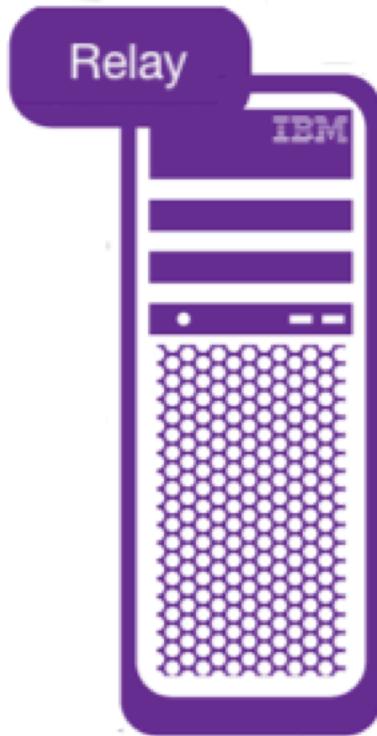
**Important Note:** Targeted Endpoint should be the same OS type as the IBM BigFix Server.

**Important Note:** Only install WebUI Service on one Endpoint per deployment.

**Important Note:** If upgrading from a previous WebUI instance, existing SSL certificates from the old WebUI location should be manually copied to the new WebUI location.



# 03 - Relays - Basics

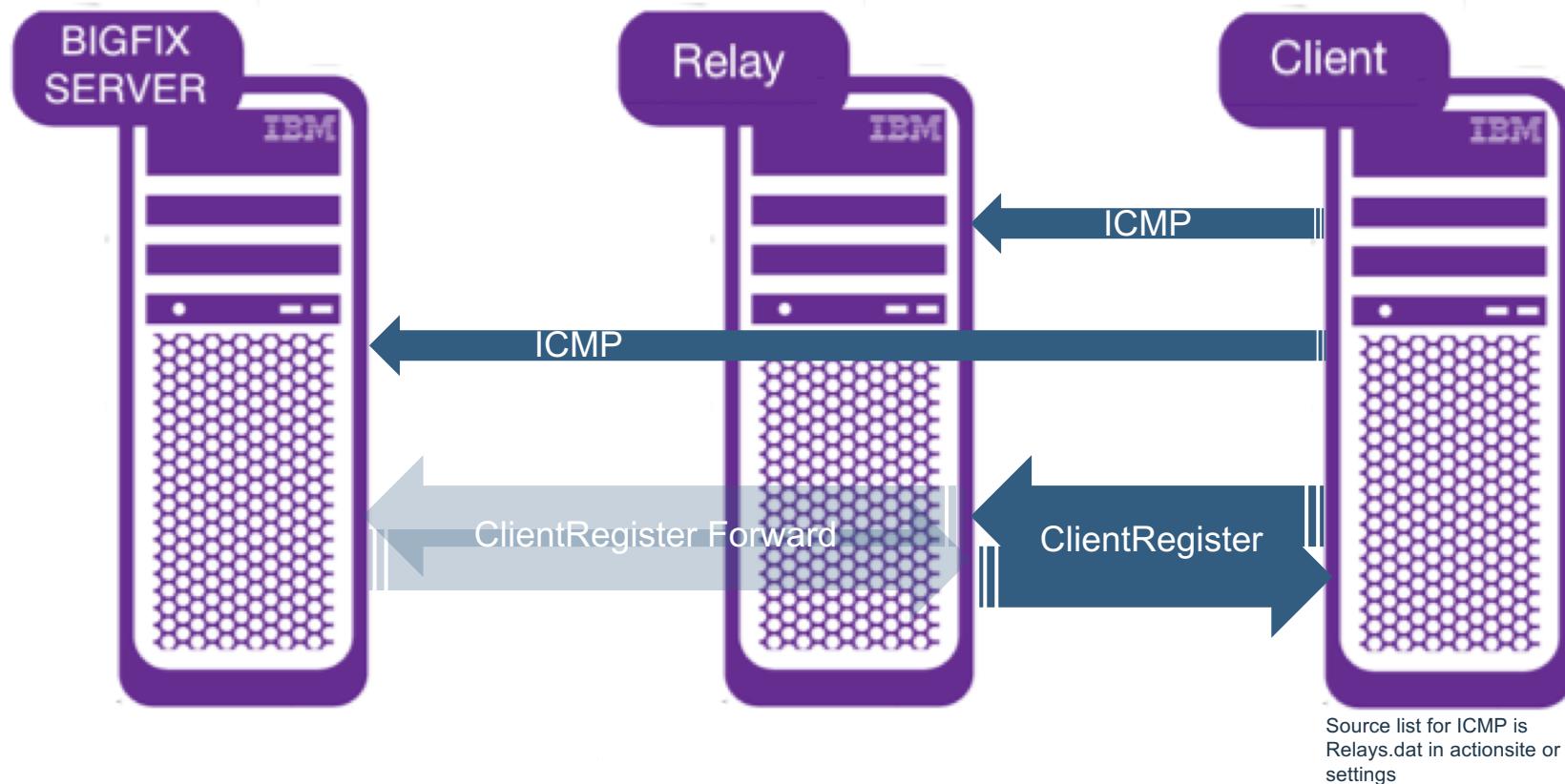


Infrastructure Communication  
HTTP/HTTPS TLS 1.2 TCP Port 52311

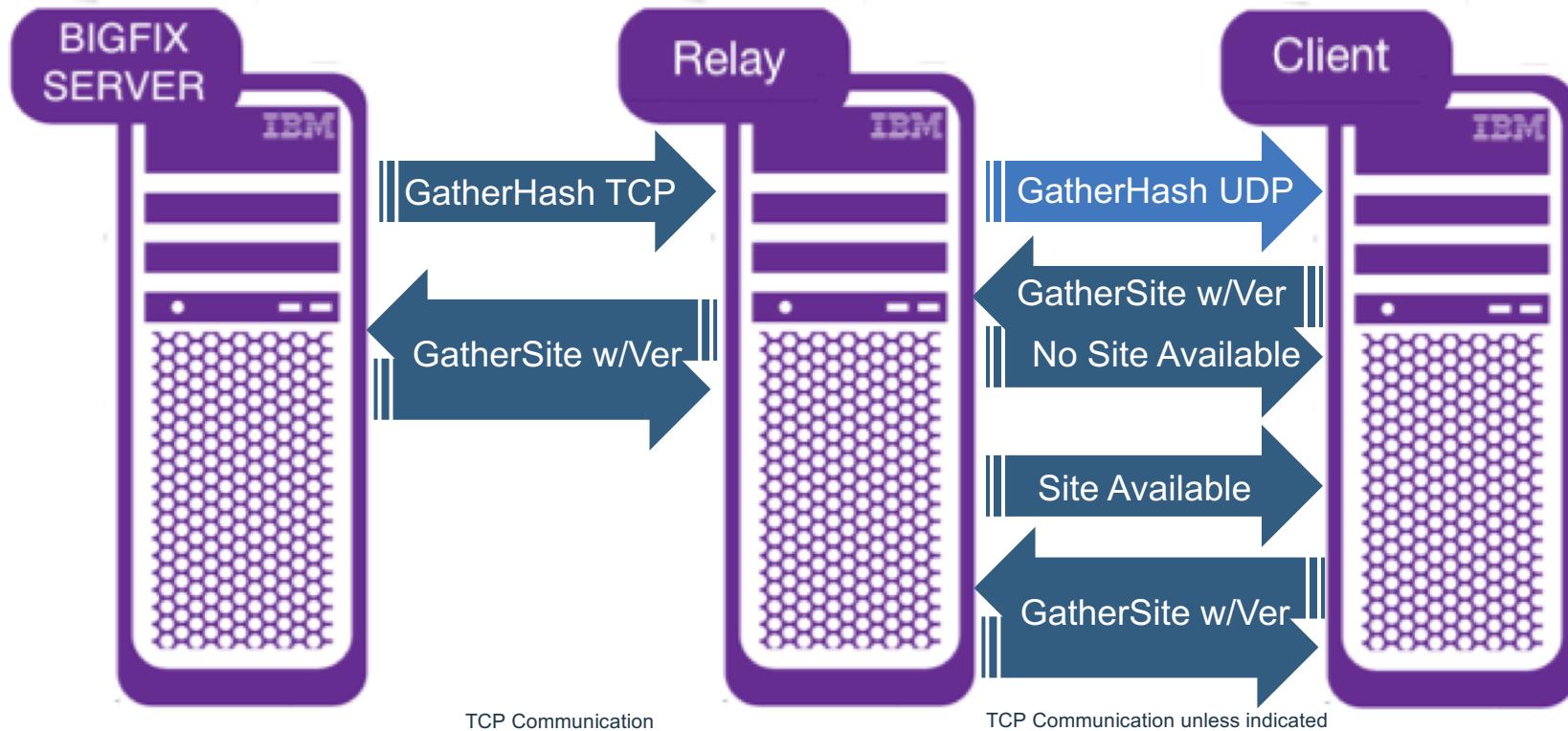
Client Communication  
HTTP/HTTPS TLS 1.0/1.2 TCP/UDP Port 52311

Windows 2008 SP2 or better (PIII or better)  
Red Hat Enterprise Linux 5 or better (i686, x86\_64)  
CentOS Linux 5 or better (i686, x86\_64)  
Ubuntu 14.4 or better (amd64)  
SuSE Linux Enterprise 10 or better (i686, x86\_64)  
AIX 6.1 or better TL4  
Solaris 10 or better (i386, Sparc)

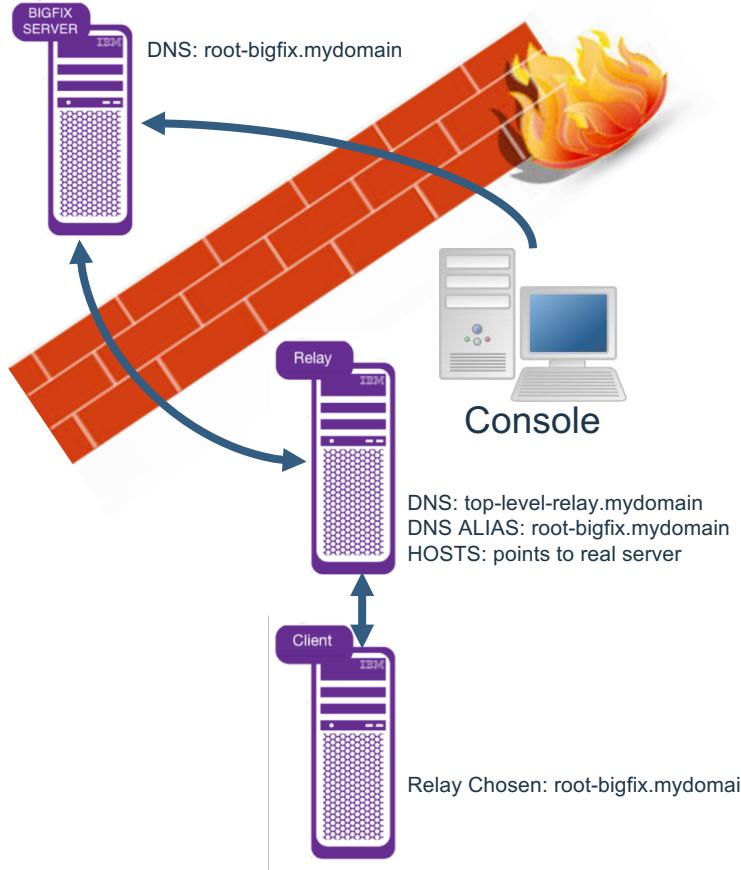
# 03 - Relays – Relay Select and Registration



# 03 - Relays – Propagation



# 03 - Relays – Fake Root



Tricks clients into thinking a relay is actually the root server

- Accomplished by pointing the root server DNS alias (masthead name) to a top level Relay that serves as the False Root which is isolated
- Protects root server from direct access
- Lowers connection demands on the real server but still allows clients to connect to the “root” server when it is the last option available
- Clients operate as normal, however steps must be taken to allow machines that need access to the root server (i.e. WebUI, Console, Web Reports, SCA, SUA and DSA) through host entries or other name resolution manipulation
- Easy detection of clients failing over to root without the root server taking the load directly

# BigFix Applications

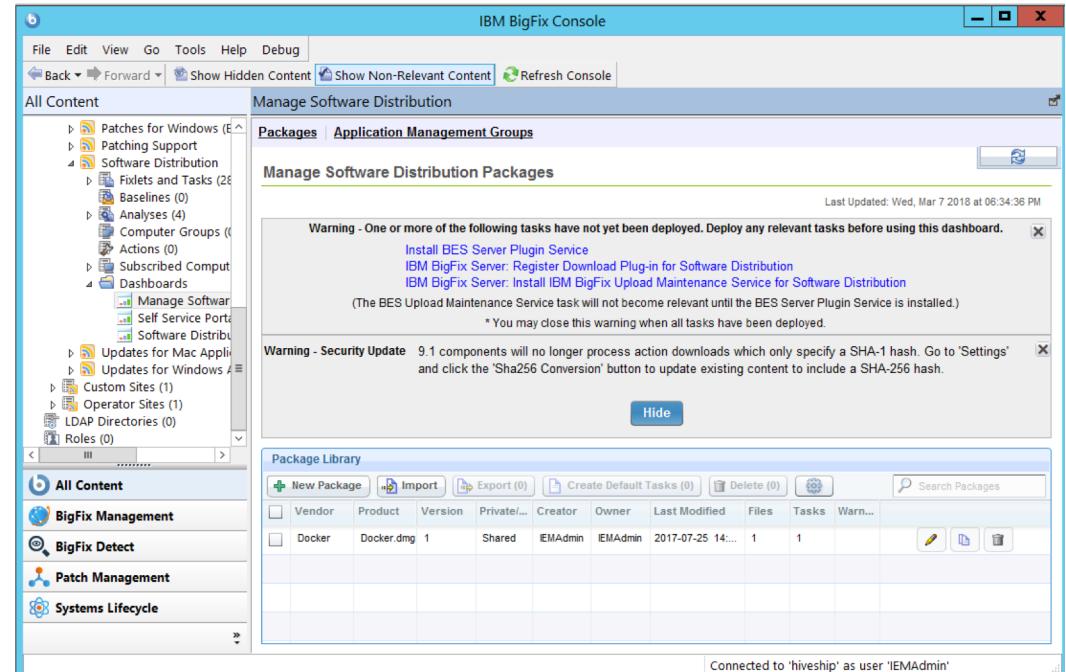
**01** LEGACY

**02** WEBUI

**03** INTEGRATION

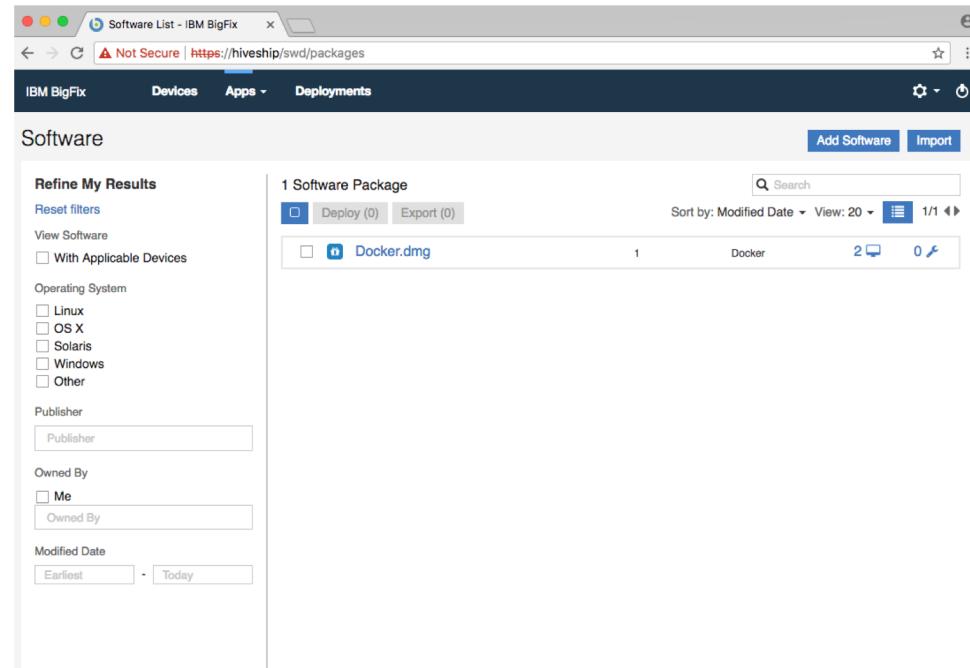
# 01 – Legacy Application Example (SWD)

- SWD setup registers a Download Plugin with the Server and installs a Upload Maintenance Service (UMS) plugin
- Operators interact with the SWD Dashboard in the Console to create and deploy new SWD packages
- UMS plugin monitors for new packages and completes upload/processes pkg metadata
- Deployed packages are fixlet actions executed by Agents, and utilize SWD Download plugin for downloads



## 02 – WebUI Application Example (SWD)

- SWD setup registers a Download Plugin with the Server and installs a Upload Maintenance Service (UMS) plugin
- Node.js Application on browser allows managing SWD packages and can form more complicated SWD objects in DBMS
- Packages are deployed to endpoints through WebUI
- Deployed packages are fixlet actions executed by Agents, and utilize SWD Download plugin for downloads



# 03 – Integration Application Example (QRadar)

- REST interface can provide all data flow from external applications to root server
- Legacy connection often meant dashboard work in Console
- WebUI integrations planned

The screenshot shows the IBM QRadar Security Intelligence dashboard. At the top, there are four main statistics: Endpoints (105k), Vulnerabilities (1k), Antivirus okay (5k), Not running (0), Quarantine (25k), and Patches (340). Below this is a table titled "Details" with columns for IP address, Device name, OS type, Antivirus status, Patches, and Compliance. The table lists six endpoints with various operating systems and patch levels.

IP address	Device name	OS type	Antivirus status	Patches	Compliance
192.168.1.100	Server01	AIX 7.1	Unknown	59	-
192.168.1.101	Server02	Win2008R2 6.1.7601	Outdated	111	-
192.168.1.102	Server03	Linux Red Hat Enterprise Server 6.4 (2.6.32-358.18.1.el6.x86_64)	Unknown	57	-
192.168.1.103	Server04	Mac OS X 10.12.6 (16Q29)	Okay	1	-
192.168.1.104	Server05	Win2012R2 6.3.9600	Unknown	16	-
192.168.1.105	Server06	SunOS 5.10 (Generic_135656-08)	Unknown	101	-

# BigFix Details

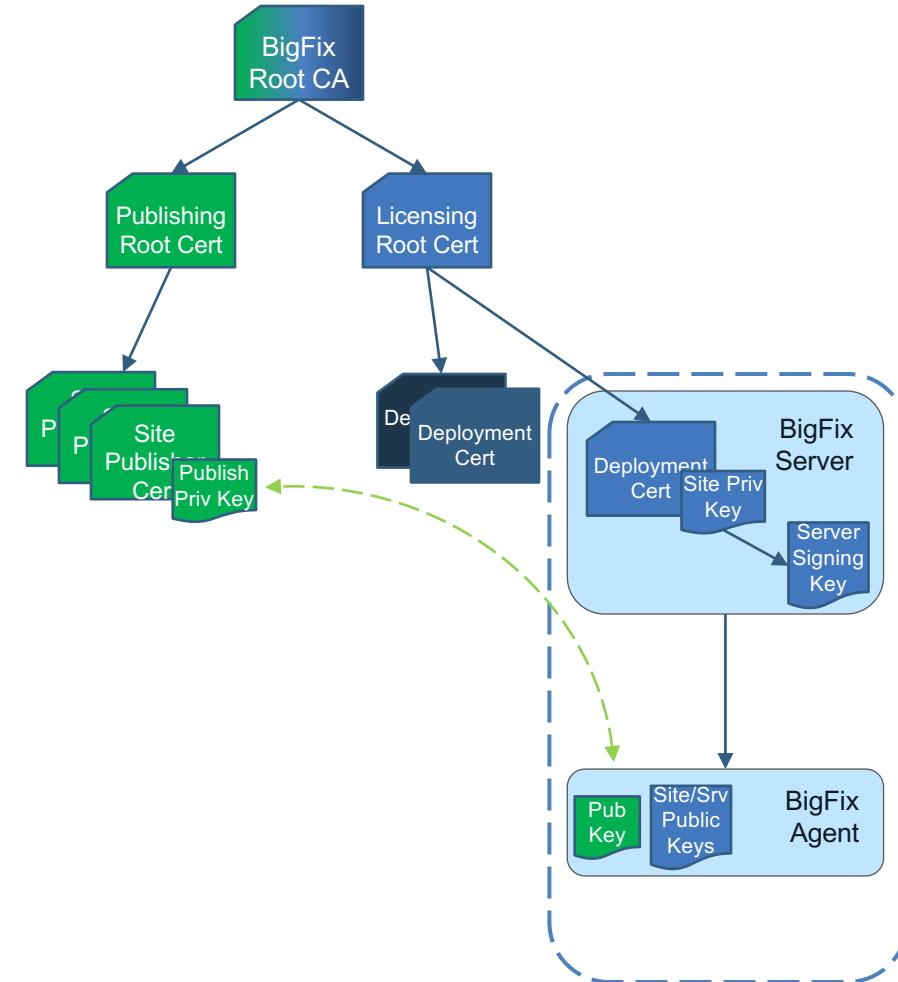
**01** SECURITY MODEL

**02** SETTINGS  
MANAGEMENT

**03** CLIENTS

# 01 - Security Model

- All cryptographic functions provided by OpenSSL (FIPS 140-2 certified)
- All content (External & Custom) protected by digital signatures, AES SHA-256 w/ 2048 or 4096 bit keys
  - External content signed by Publishing keys and trusted by all deployments
  - Custom content signed by Root Server private key and only valid within deployment
- Deployment cert & pub/priv keys generated during install establishes trust chain for the environment
  - Only local operators can revoke or publish to this part of the chain
- Deployment/server cert is also the basis of the HTTPS (TLS) communication between components, client certs signed by the server are used for two-way SSL
- Downloads are also validated by size and SHA1/SHA-256



# 02 – Settings Management

ActionScript usually performs settings changes to endpoints

<https://developer.bigfix.com>

setting "<name>="value" on "<date>" for client

Settings order controlled by the “on” segment of the command, only newer settings will override older ones guaranteeing order.

Don’t use “{now}” as this date as you have no control over order.

Use "{parameter "action issue date" of action}"

The screenshot shows a web browser window with the URL <https://developer.bigfix.com/action-script/reference/client/setting.html>. The page title is "setting | BigFix Developer". The main content area contains the following sections:

- setting**: A brief description stating "This command sets a BigFix client setting. Settings are named values that can be applied to individual sites or to client computers. Each setting has a timestamp associated with it. This timestamp is used to establish priority – the latest setting will trump any earlier ones."
- Syntax**: Three examples of the command syntax:

```
setting "<name>="value" on "<date>" for client
setting "<name>="value" on "<date>" for current site
setting "<name>="value" on "<date>" for site "<sitename>"
```
- Where**: A note explaining that `name=value` describes the setting, and `date` is a timestamp used to establish priority between conflicting setting commands.
- Examples**: A table showing examples of setting values:

Setting	Type	Description
<code>ab</code> (Default)	REG_SZ	(value not set)
<code>ab effective date</code>	REG_SZ	Wed, 07 Mar 2018 17:39:43 -0800
<code>ab value</code>	REG_SZ	<a href="http://hiveship:52311/cgi-bin/bfgather.exe/actionsite">http://hiveship:52311/cgi-bin/bfgather.exe/actionsite</a>
[Software\BigFix\EnterpriseClient\Settings\Client\__RelayServer1]		
<code>value</code>	= ""	
<code>effective date</code>	=	Wed, %2007%20Mar%202018%2017:39:35%20-0800

Manual edits can be complex on some platforms

- Windows uses registry
- UNIX/Linux config files are complex and owner process must be stopped
- macOS uses a plist and requires privileged editing

<code>ab</code> (Default)	REG_SZ	(value not set)
<code>ab effective date</code>	REG_SZ	Wed, 07 Mar 2018 17:39:43 -0800
<code>ab value</code>	REG_SZ	<a href="http://hiveship:52311/cgi-bin/bfgather.exe/actionsite">http://hiveship:52311/cgi-bin/bfgather.exe/actionsite</a>
[Software\BigFix\EnterpriseClient\Settings\Client\__RelayServer1]		
<code>value</code>	= ""	
<code>effective date</code>	=	Wed, %2007%20Mar%202018%2017:39:35%20-0800

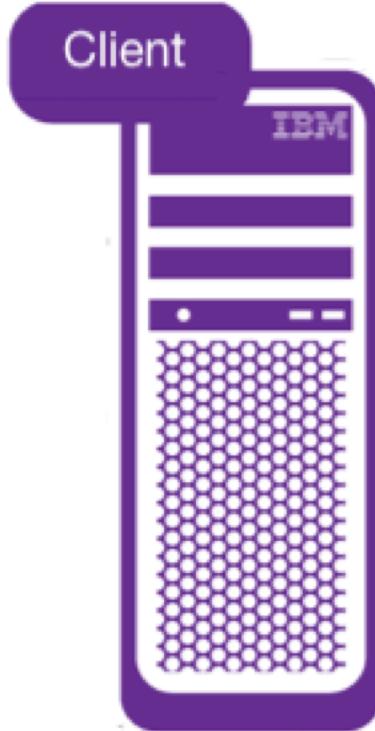
# Some useful settings

- Client command polling
  - \_BESClient\_Comm\_CommandPollingEnable
  - \_BESClient\_Comm\_CommandPollingIntervalSeconds (6 hours or 90 minutes)
- Relay Authentication
  - \_BESRelay\_Comm\_Authenticating
- Relay Diagnostics
  - \_BESRelay\_Diagnostics\_Enable
  - \_BESRelay\_Diagnostics\_Password
- HTTP Communication timeouts
  - \_BESData\_Comm\_ConnectTimeoutSeconds (Console 10 secs)
  - \_BESData\_Comm\_Timeout (Console 10 minutes)
  - \_HTTPRequestSender\_Connect\_TimeoutSeconds (Most things other than client 10 secs)
- External Site Gathering over HTTPS:
  - \_BESGather\_Use\_Https
- Server/Relay thread limits:
  - \_HTTPServer\_ThreadLimit\_api (RESTAPI thread pool, 250)

# Verbose logs (Debug log)

- Root server (also relay)
  - \_BESRelay\_Log\_Verbose
  - \_BESRelay\_HTTPServer\_LogFileSizeLimit
  - \_BESRelay\_HTTPServer\_LogFileRotationLimit
  - \_BESRelay\_HTTPServer\_HttpLogDirectoryPath
  - \_BESRelay\_HTTPServer\_HttpLogExpirationDays
- GatherDB
  - HKLM\Software\BigFix\Enterprise Server\GatherDB\VerboseDebugOut [DWORD] 1
- FillDB
  - HKLM\Software\BigFix\Enterprise Server\FillDB\EnableLogging [DWORD] = non-zero
  - HKLM\Software\BigFix\Enterprise Server\FillDB\EnabledLogs [SZ] = “critical” or “debug”
- WebUIService
  - \_WebUIService\_Logging\_Verbose
- WebReports
  - HKLM\Software\BigFix\Enterprise Server\BESReports\LogOn [DWORD] 1
  - HKLM\Software\BigFix\Enterprise Server\BESReports\LogPath
  - HKLM\Software\BigFix\Enterprise Server\BESReports\EnabledLogs [SZ] = “critical” or “debug”

# 03 - Clients – Officially Supported Platforms (9.2 and 9.5)

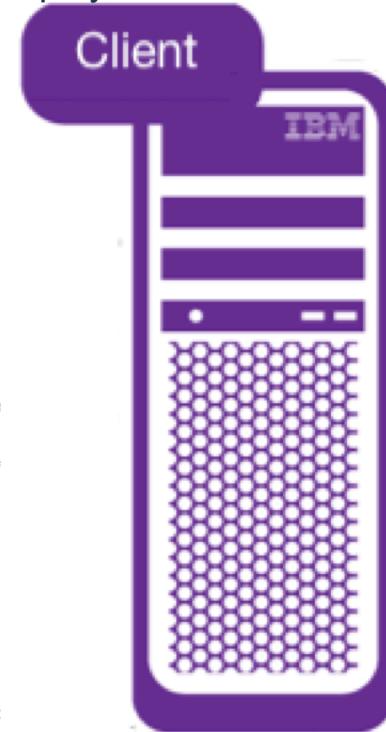


AIX 6.1	Solaris 9 SPARC
AIX 7.1	Solaris 10 i86
AIX 7.2	Solaris 10 SPARC
CentOS 5 i686	Solaris 11 i86
CentOS 5 x86_64	Solaris 11 SPARC
CentOS 6 i686	SUSE 10 i686
CentOS 6 x86_64	SUSE 10 x86_64
CentOS x86_64	SUSE 10 s390x
Debian 6 i386	SUSE 10 PPC64BE
Debian 6 amd64	SUSE 11 i686
Debian 7 i386	SUSE 11 x86_64
Debian 7 amd64	SUSE 11 s390x
Debian 8 i386	SUSE 11 PPC64BE
Debian 8 amd64	SUSE 12 x86_64
Debian 9 i386	SUSE 12 s390x
Debian 9 amd64	SUSE 12 PPC64LE
ESX 4	Ubuntu 10 LTS i386
HPUX 11.11	Ubuntu 10 LTS amd64
HPUX 11.23	Ubuntu 12 LTS i386
HPUX 11.31	Ubuntu 12 LTS amd64
OEL 6 i686	Ubuntu 14 LTS i386
OEL 6 x86_64	Ubuntu 14 LTS amd64
OEL 7 x86_64	Ubuntu 14 LTS PPC64LE
OSX 10.7	Ubuntu 16 LTS i386
OSX 10.8	Ubuntu 16 LTS amd64
OSX 10.9	Ubuntu 16 LTS PPC64LE
OSX 10.10	Windows XP
OSX 10.11	Windows XPe
OSX 10.12	Windows XP-2003
OSX 10.13	Windows 2003
Power KVM	Windows Vista
RHEL 5 i686	Windows 2008
RHEL 5 x86_64	Windows 7
RHEL 5 s390x	Windows 7 embedded
RHEL 5 PPC64BE	Windows 2008 R2
RHEL 6 i686	Windows 8
RHEL 6 x86_64	Windows 2012
RHEL 6 s390x	Windows 8.1
RHEL 6 PPC64BE	Windows 2012 R2
RHEL 7 x86_64	Windows 10
RHEL 7 s390x	Windows 10 Anniversary and later
RHEL 7 PPC64BE	Windows 2016
RHEL 7 PPC64LE	

# 03 - Clients – Logs

Default logs show a lot about the system and can often expose issues with the deployment

```
Current Date: March 8, 2018
Client version 9.5.8.38 built for WINVER 6.0 i386 running on WINVER 6.3.9600 x86_64
Current Balance Settings: Use CPU: True Entitlement: 0 WorkIdle: 10 SleepIdle: 400
ICU 54.1 init status: SUCCESS
Agent internal character set: UTF-8
ICU report character set: UTF-8 - Transcoding Disabled
ICU fxf character set: windows-1252 (Latin 1 / Western European) - Transcoding Enabled
ICU local character set: windows-1252 (Latin 1 / Western European) - Transcoding Enabled
At 11:11:35 -0800 -
Starting client version 9.5.8.38
FIPS mode disabled by default.
Cryptographic module initialized successfully.
Using crypto library libBEScrypto - OpenSSL 1.0.2j-fips 26 Sep 2016
Initializing Site: actionsite
Restricted mode
Processing Download plugins
Adding custom site (CustomSite_Test)
Beginning Relay Select
At 11:11:36 -0800 -
RegisterOnce: Attempting secure registration with 'https://rhe6compute:52311/cgi-bin/bfenterprise/clientregister.exe?RequestType=RegisterMe'
Unrestricted mode
Configuring listener without wake-on-lan
Registered with url 'https://rhe6compute:52311/cgi-bin/bfenterprise/clientregister.exe?RequestType=RegisterMe&ClientVersion=9.5.8.38&Body=
Registration Server version 9.5.8.38 , Relay version 9.5.8.38
Relay does not require authentication.
Client has an AuthenticationCertificate
Created mailboxsite and marking to gather
Relay selected: rhe6compute. at: 192.168.40.223:52311 on: IPV4 (Using setting IPV4ThenIPV6)
At 11:11:38 -0800 -
PollForCommands: Requesting commands
PollForCommands: commands to process: 3
Entering Service Loop.
Starting Service Loop.
A2AServer::Start().
At 11:11:38 -0800 - actionsite (http://hiveship:52311/cgi-bin/bfgather.exe/actionsite)
Downloaded 'http://rhe6compute:52311/bfmirror/bfsites/manydirlists_1/_fullsite_2bfba6b3b2af0ccf35dcc4f6166d474cb91266e8' as '__TempUpdateFile'
Gather::SyncSiteByFile adding files - count: 72
At 11:11:38 -0800 -
Successful Synchronization with site 'actionsite' (version 571) - 'http://hiveship:52311/cgi-bin/bfgather.exe/actionsite'
Successful Synchronization with site 'mailboxsite' (version 62) - 'http://hiveship:52311/cgi-bin/bfgather.exe/mailboxsite12241621'
```



# THANK YOU

FOLLOW US ON:

-  [www.bigfix.com](http://www.bigfix.com)
-  [forum.bigfix.com](http://forum.bigfix.com)
-  [developer.bigfix.com](http://developer.bigfix.com)
-  [www.hcltech.com/products-and-platforms](http://www.hcltech.com/products-and-platforms)

