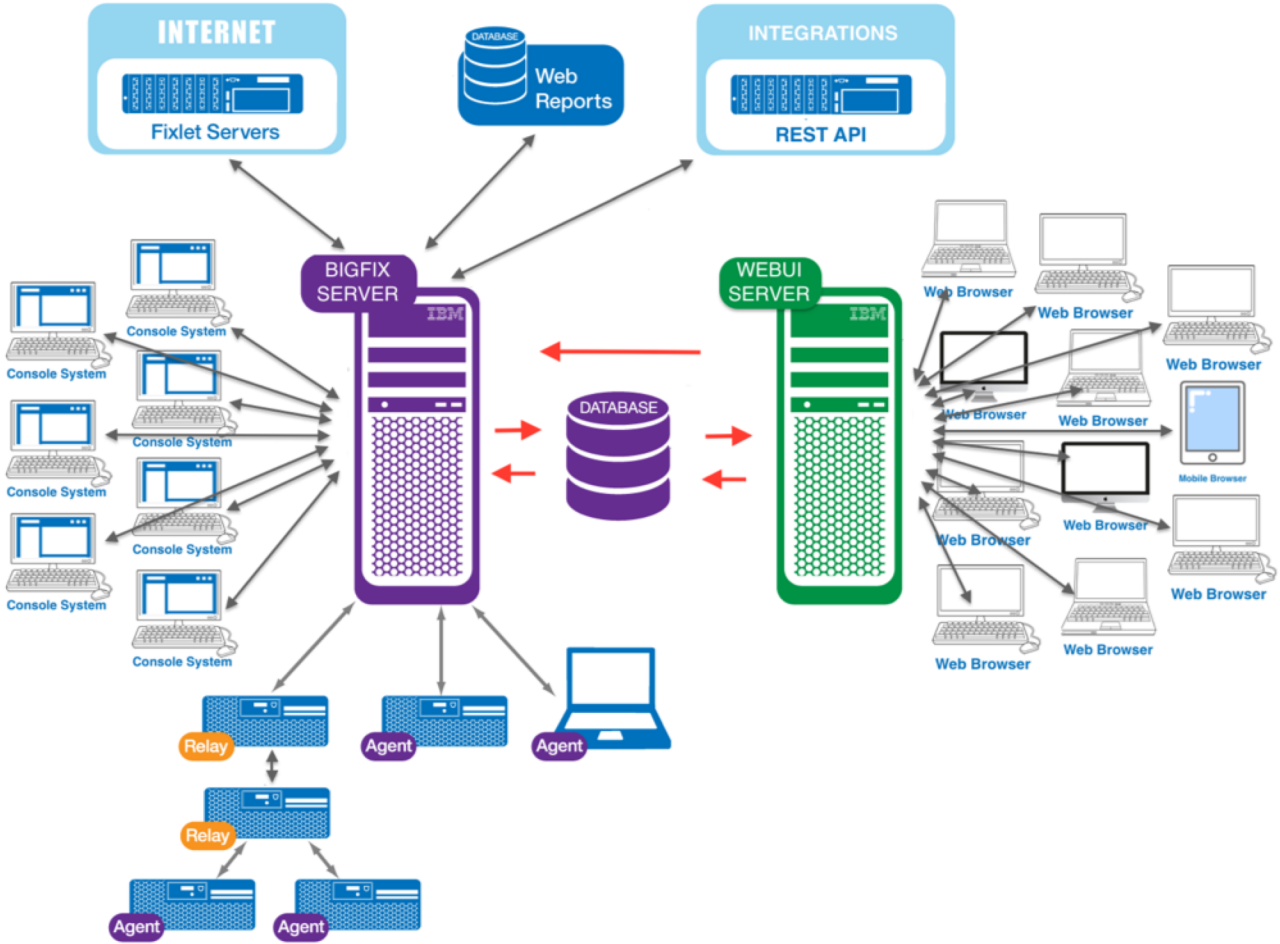
BigFix Architecture

Andrew Schmidt
BigFix Software Engineer

May 15, 2018

HCL

Architecture – The Deployment as a whole



BigFix Infrastructure Components

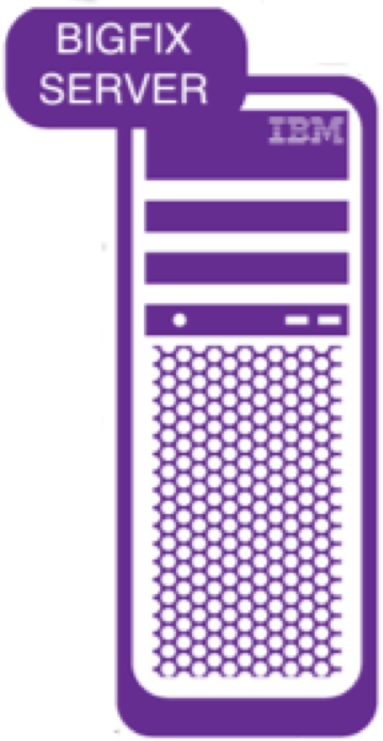
01 ROOT SERVER

02 WEBUI

03 RELAYS

HCL

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

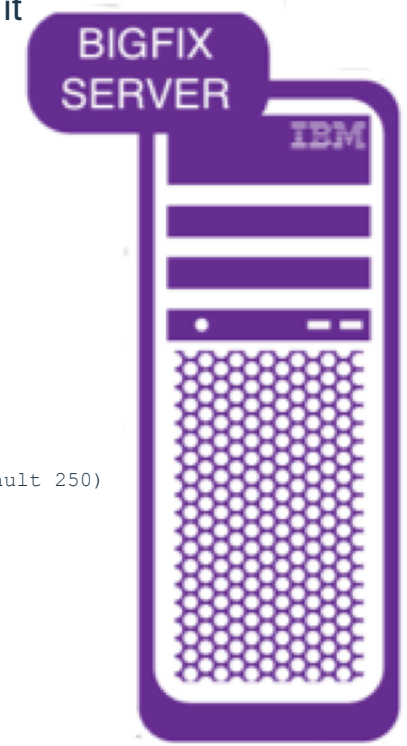
Database Communication
ODBC

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

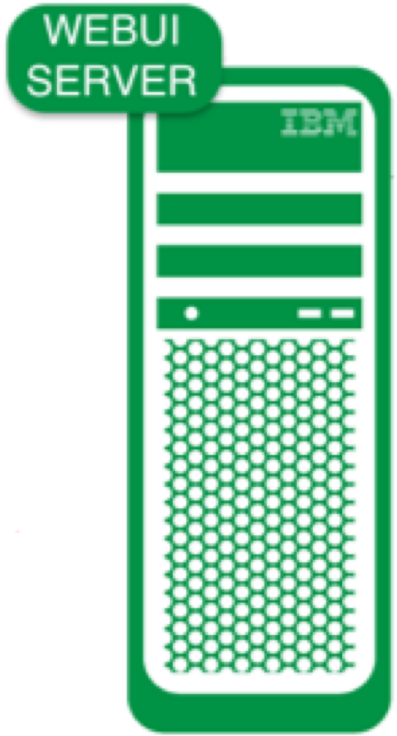
```
[Software\BigFix\Enterprise Server]
wwwRootFolder                  = /var/opt/BESServer/wwwrootbes

[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

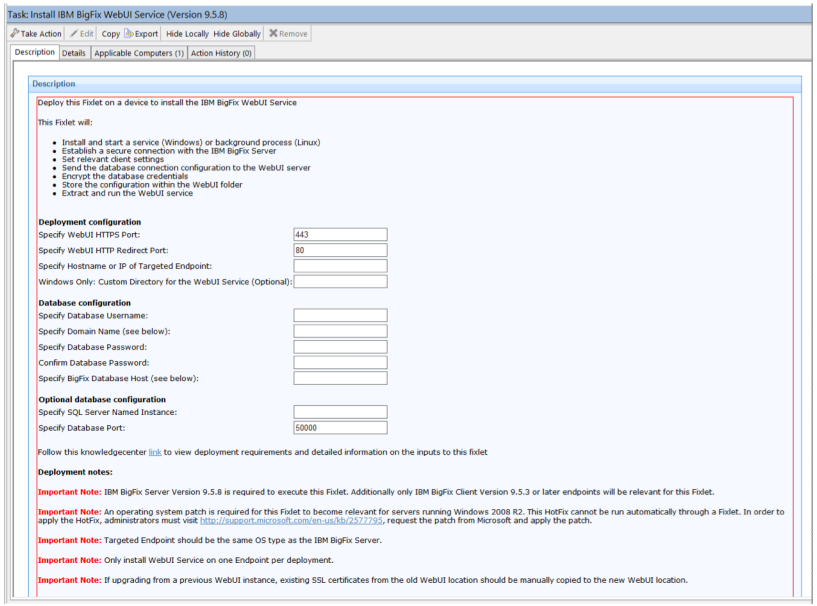
Red Hat Linux 6 or better 64 bit

02 - WebUI - Configuration

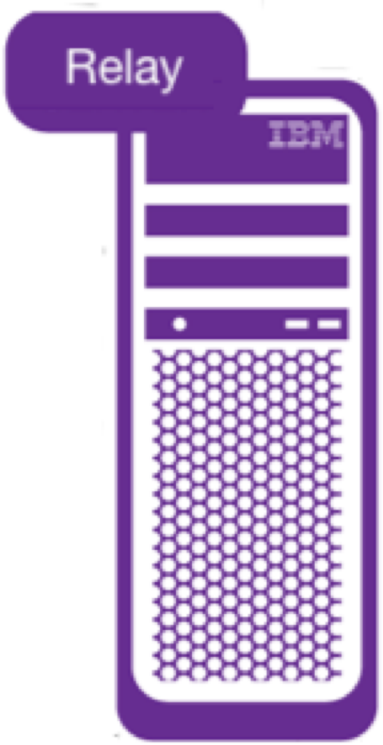
The server is very configurable so some settings to be aware of to make it perform the best in the environment you have are below
Most of these are set during the deployment of the WebUI via Fixlet

Client Settings

Base WebUI Directory: `_WebUIAppEnv_WebUI_DIR`
Sites WebUI Directory: `_WebUIAppEnv_WORK_DIR`



03 - Relays - Basics

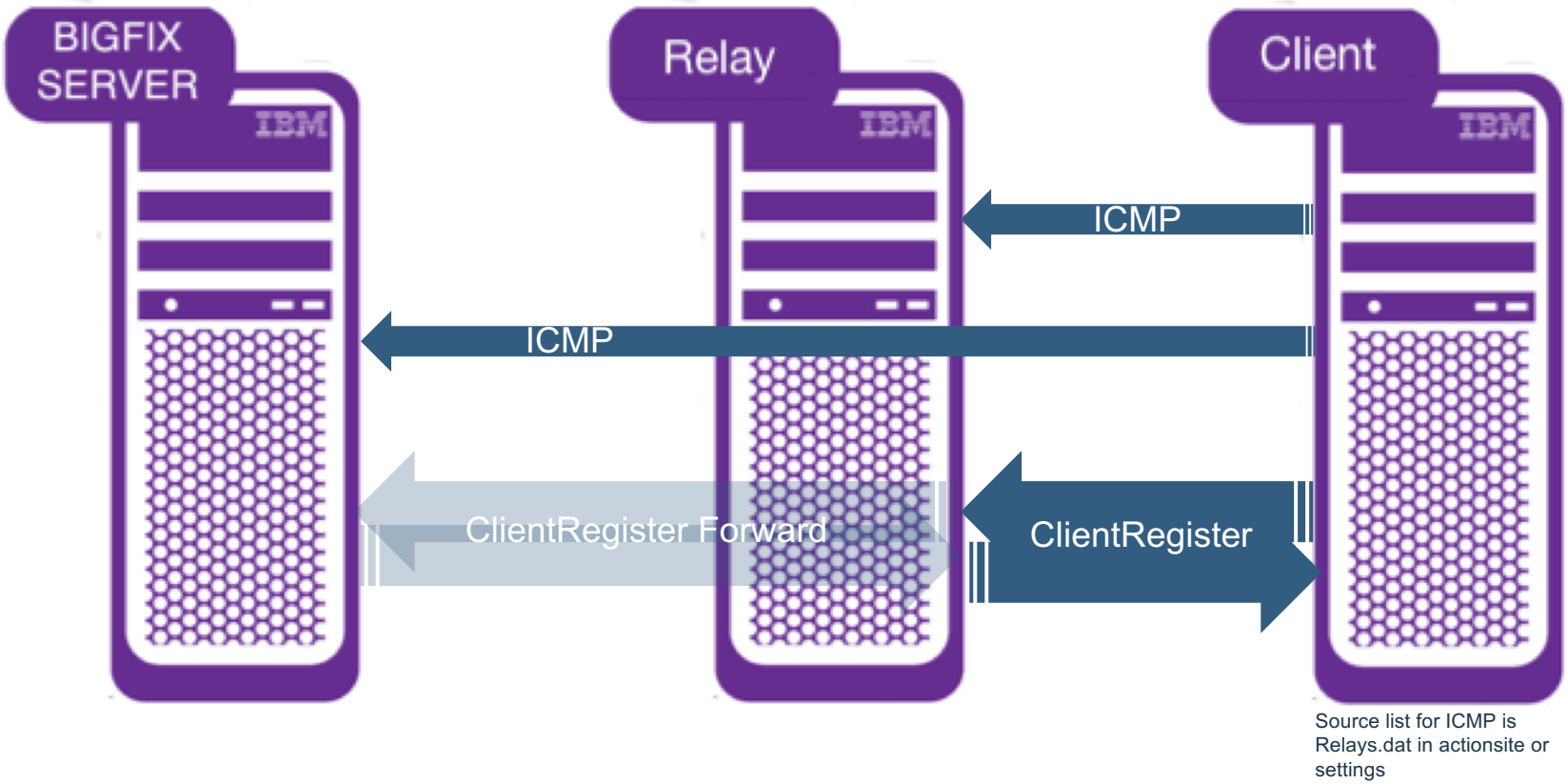


Infrastructure Communication
HTTP/HTTPS TLS 1.2 TCP Port 52311

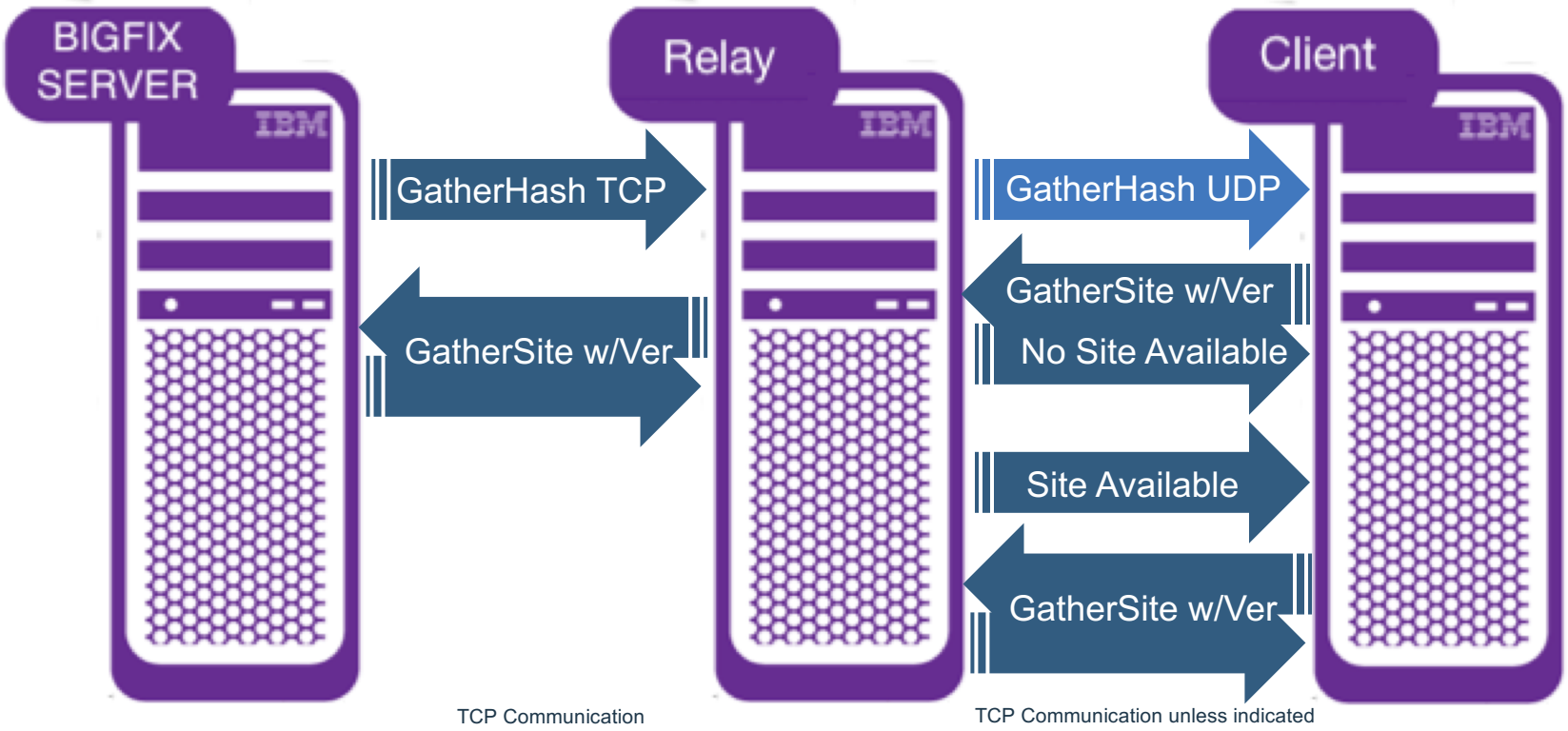
Client Communication
HTTP/HTTPS TLS 1.0/1.2 TCP/UDP Port 52311

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)

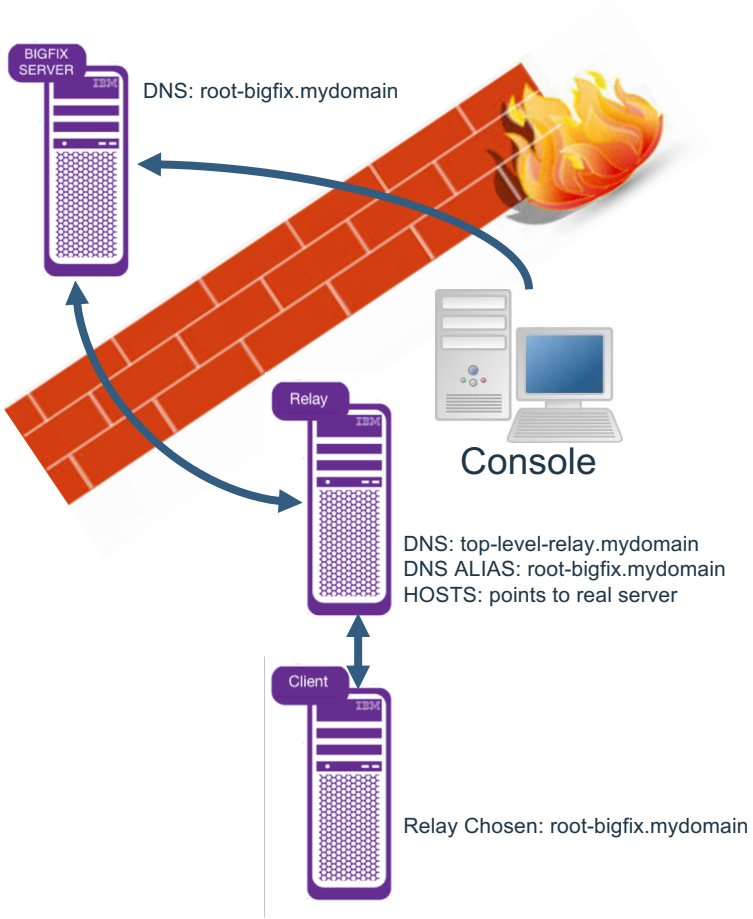
03 - Relays – Relay Select and Registration



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

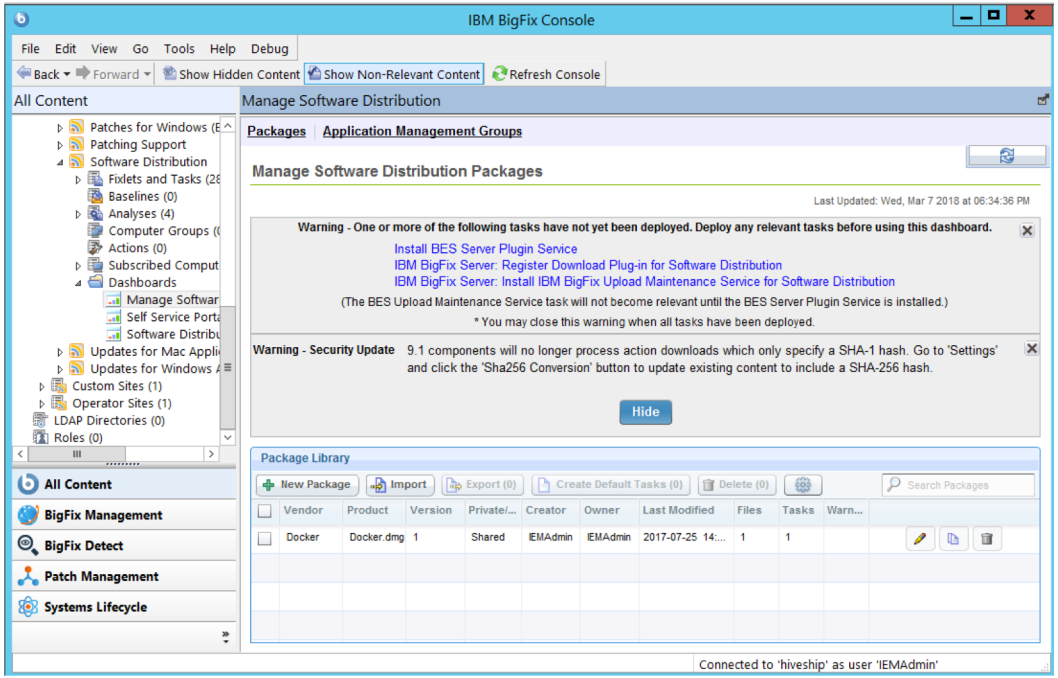
02 WEBUI

03 INTEGRATION

HCL

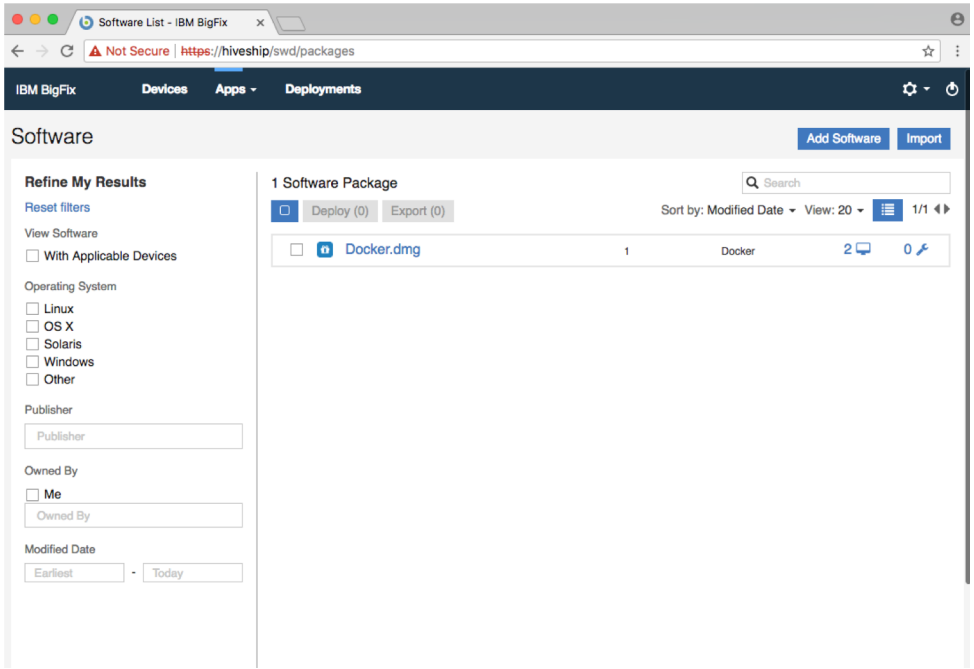
01 – Legacy Application Example (SWD)

- 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



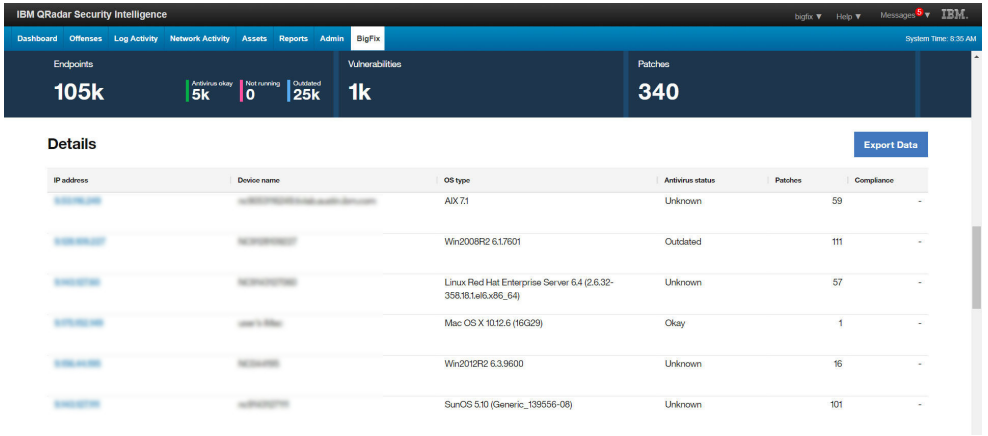
02 – WebUI Application Example (SWD)

- 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



BigFix Details

01 SECURITY MODEL

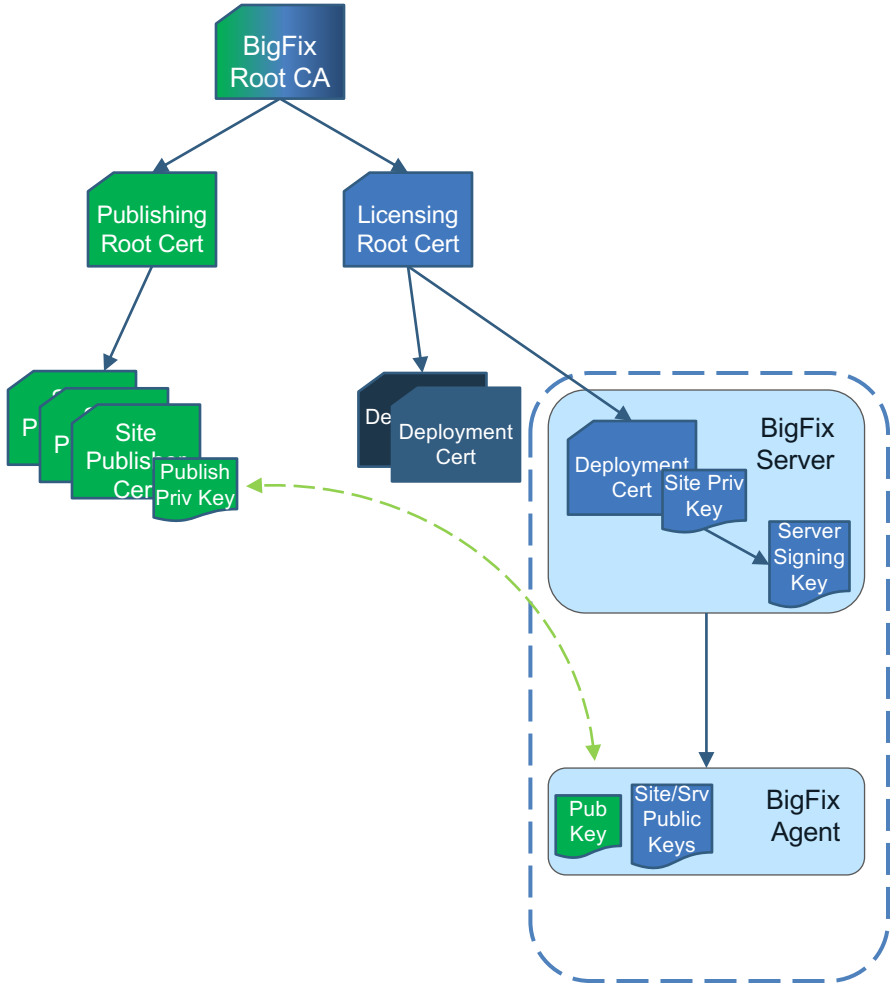
02 SETTINGS MANAGEMENT

03 CLIENTS

HCL

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

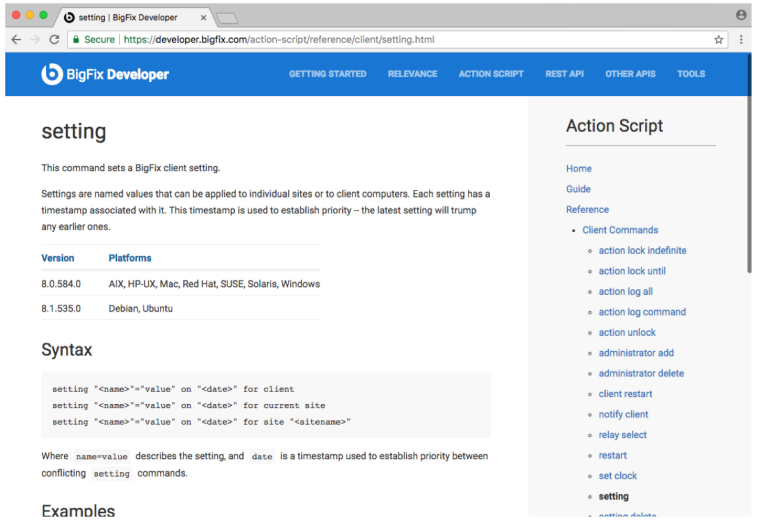


02 – Settings Management

ActionScript usually performs settings changes to endpoints
https://developer.bigfix.com

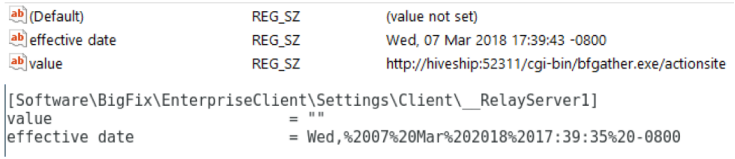
setting "<name>"="value" on "<date>" for client

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}"



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



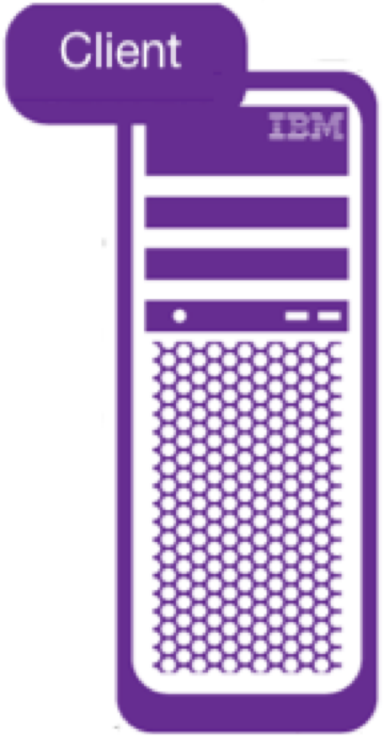
Some useful settings

- 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)



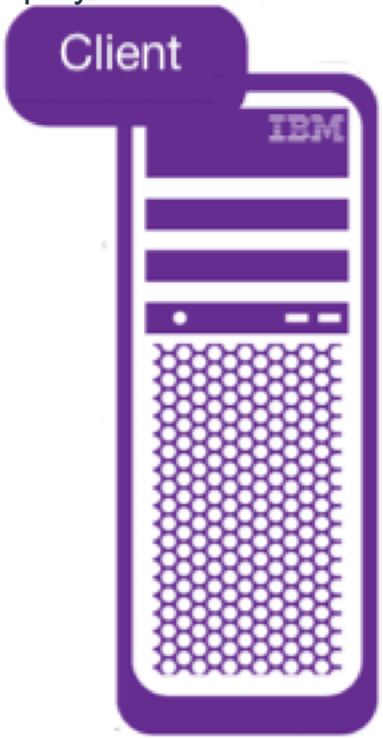
AIX 6.1
AIX 7.1
AIX 7.2
CentOS 5 i686
CentOS 5 x86_64
CentOS 6 i686
CentOS 6 x86_64
CentOS x86_64
Debian 6 i386
Debian 6 amd64
Debian 7 i386
Debian 7 amd64
Debian 8 i386
Debian 8 amd64
Debian 9 i386
Debian 9 amd64
ESX 4
HPUX 11.11
HPUX 11.23
HPUX 11.31
OEL 6 i686
OEL 6 x86_64
OEL 7 x86_64
OSX 10.7
OSX 10.8
OSX 10.9
OSX 10.10
OSX 10.11
OSX 10.12
OSX 10.13
Power KVM
RHEL 5 i686
RHEL 5 x86_64
RHEL 5 s390x
RHEL 5 PPC64BE
RHEL 6 i686
RHEL 6 x86_64
RHEL 6 s390x
RHEL 6 PPC64BE
RHEL 7 x86_64
RHEL 7 s390x
RHEL 7 PPC64BE
RHEL 7 PPC64LE

Solaris 9 SPARC
Solaris 10 i86
Solaris 10 SPARC
Solaris 11 i86
Solaris 11 SPARC
SuSE 10 i686
SuSE 10 x86_64
SuSE 10 s390x
SuSE 10 PPC64BE
SuSE 11 i686
SuSE 11 x86_64
SuSE 11 s390x
SuSE 11 PPC64BE
SuSE 12 x86_64
SuSE 12 s390x
SuSE 12 PPC64LE
Ubuntu 10 LTS i386
Ubuntu 10 LTS amd64
Ubuntu 12 LTS i386
Ubuntu 12 LTS amd64
Ubuntu 14 LTS i386
Ubuntu 14 LTS amd64
Ubuntu 14 LTS PPC64LE
Ubuntu 16 LTS i386
Ubuntu 16 LTS amd64
Ubuntu 16 LTS PPC64LE
Windows XP
Windows XPe
Windows XP-2003
Windows 2003
Windows Vista
Windows 2008
Windows 7
Windows 7 embedded
Windows 2008 R2
Windows 8
Windows 2012
Windows 8.1
Windows 2012 R2
Windows 10
Windows 10 Anniversary and later
Windows 2016

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: 480
   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=RegisterMe60&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 '__TempUpdateF
   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
- forum.bigfix.com
- developer.bigfix.com
- www.hcltech.com/products-and-platforms

HCL