IBM Security

A little bit of Rest Magic

IBM BIGFIX

Jgo - John Golembiewski
jgo@us.ibm.com
Kenye rest
BigFix Technical Pre-sales

11/18/2016

IBM

magic (*usually uncountable*, *plural* **magics**)

The use of rituals or actions, especially based on supernatural or occult knowledge, to manipulate or obtain information about the natural world, especially when seen as falling outside the realm of religion; also the forces allegedly drawn on for such practices. [from 14th c.] [quotations ▼]

A specific ritual or procedure associated with supernatural magic or with mysticism; a spell. [from 14th c.]

Something producing remarkable results, especially when not fully understood; an enchanting quality; exceptional skill. [from 17th c.] [quotations ▼]

A conjuring trick or illusion performed to give the appearance of supernatural phenomena or powers. [from 19th c.]

A specific kind of special power or ability.

magic (*usually uncountable*, *plural* **magics**)

Something producing remarkable results, especially when not fully understood; an enchanting quality; exceptional skill. [from 17th c.]

Agenda

- Survey of what is possible
  - Client Side API
  - Server Side API
- Troubleshooting Rest API
- Examples
  - Query Tester Tool
  - CVE Dashboard
  - Automatic Patch Tool

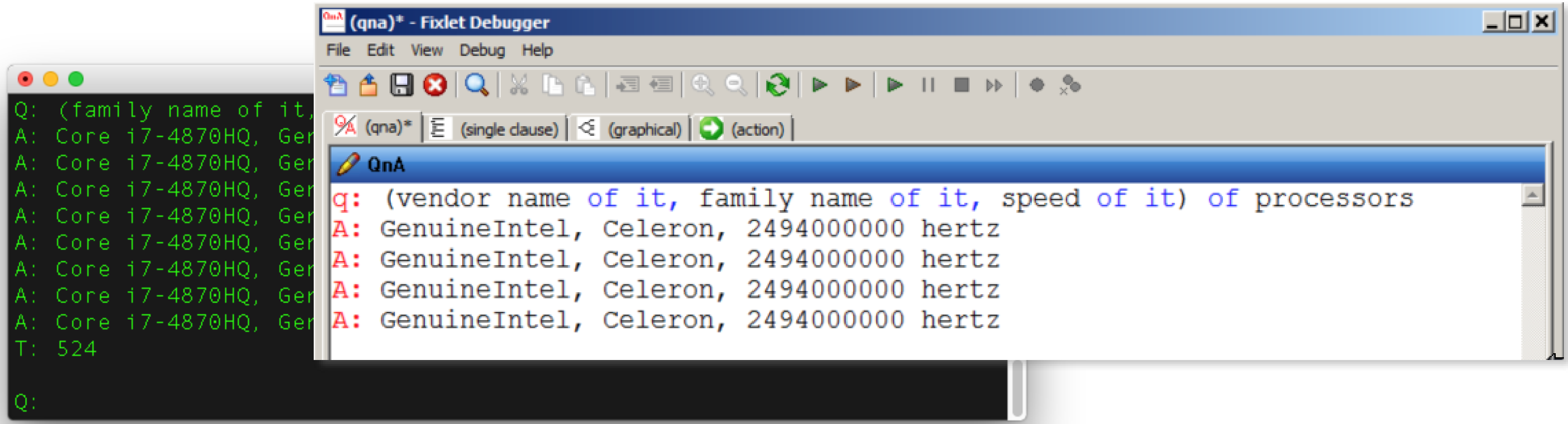
HOW DOES ONE PERFORM REST API MAGIC?

What Is possible with BigFix Magic?

An augmented using BigFix REST API producing remarkable results, especially when not fully understood by the end user

BigFix Relevance & ActionScript Language

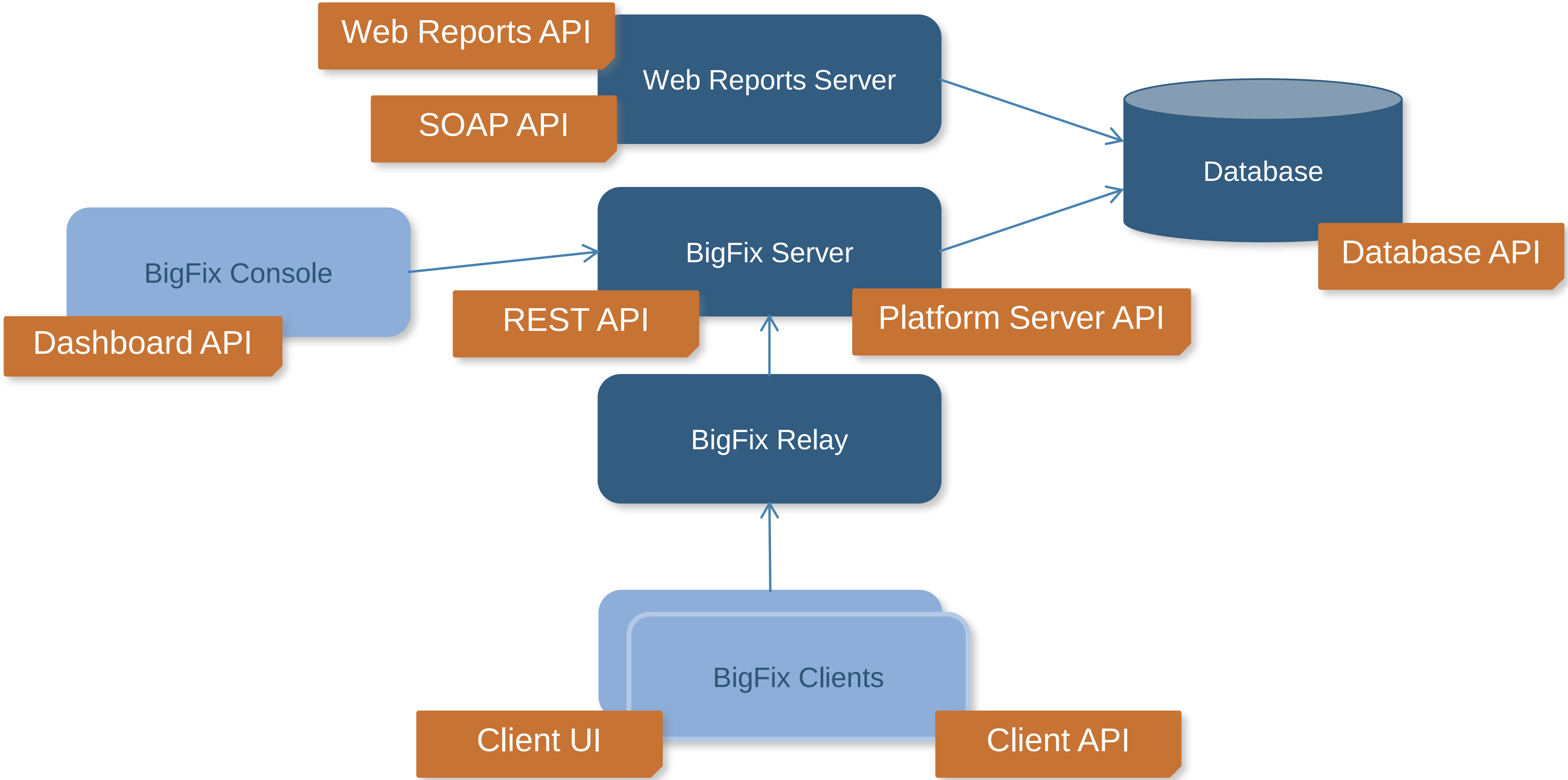
- Foundational scripting language used for all
  - Fixlets, Tasks, Analyses, Baselines, Properties
  - Same language construct across all components
- High level non-procedural 4GL
- Cross platform for Windows, UNIX, Linux, and Mac OS X



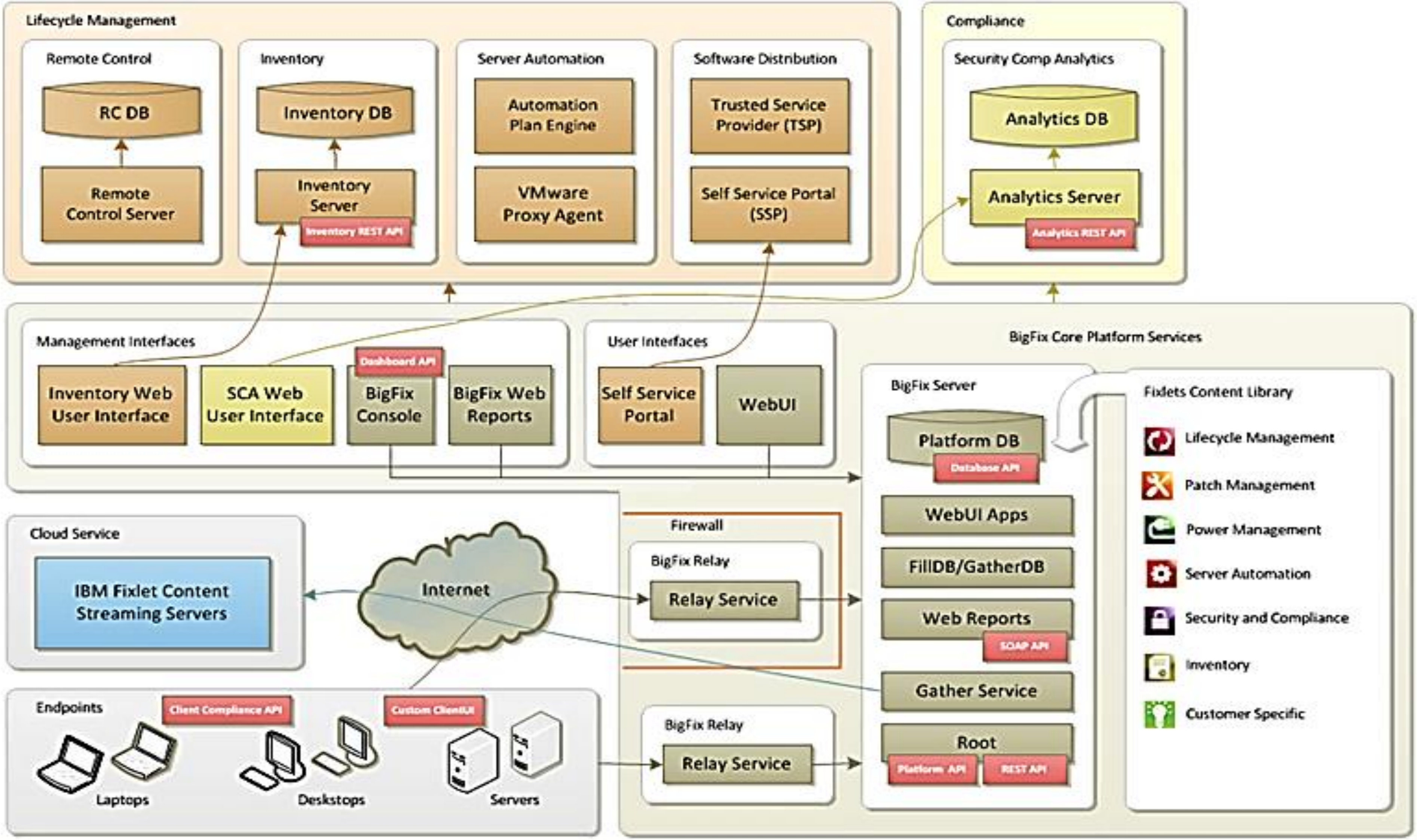
```
Q: (family name of it,
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
A: Core i7-4870HQ, Ger
T: 524

Q:
```

```
q: (vendor name of it, family name of it, speed of it) of processors
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
```

BigFix APIs


Web Reports API
Web Reports Server
SOAP API
Database
BigFix Console
BigFix Server
Database API
Dashboard API
REST API
Platform Server API
BigFix Relay
BigFix Clients
Client UI
Client API

BigFix Architecture Components



Client Side API’s

BigFix Client APIs

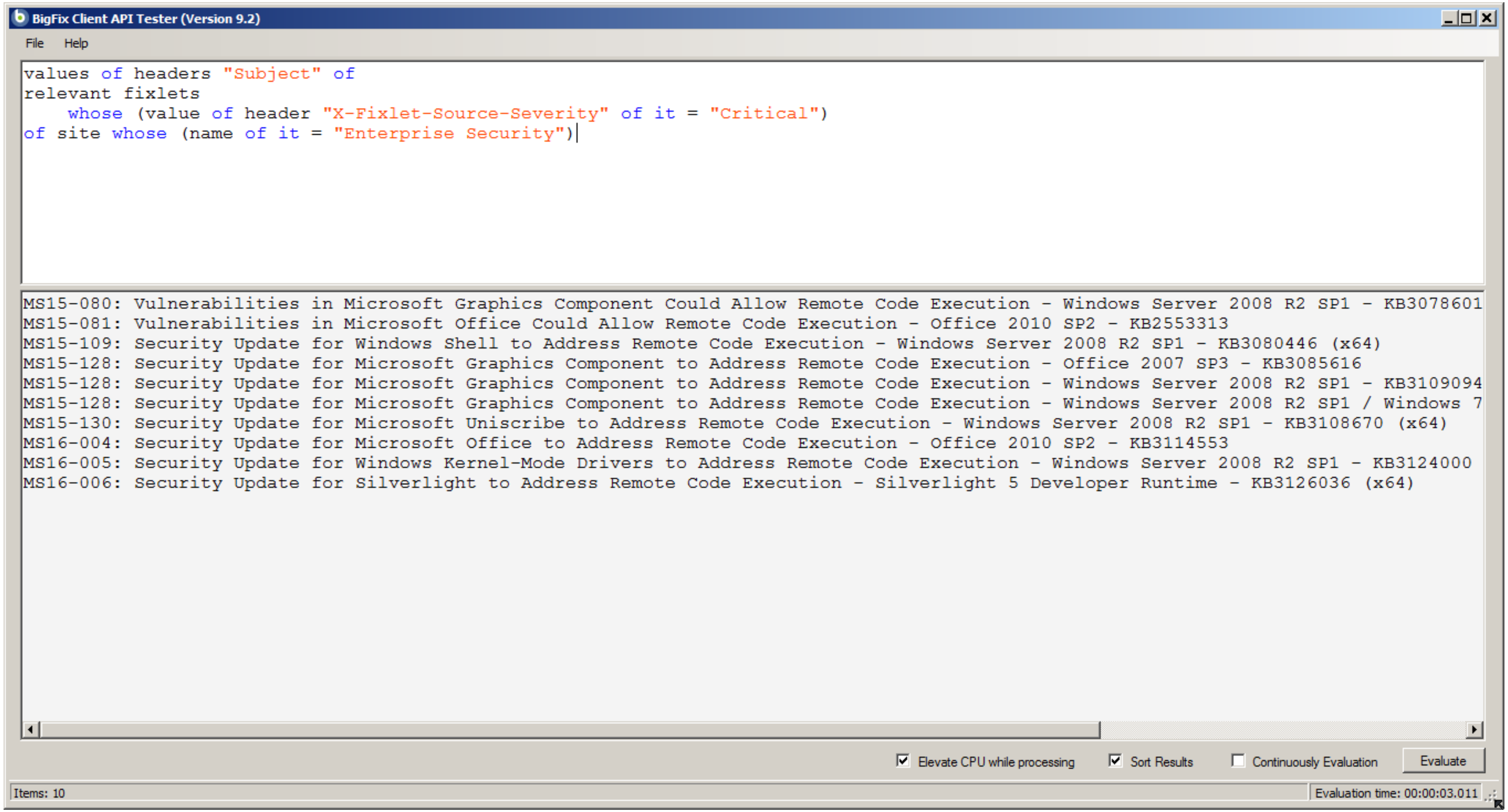
API	Execute Against	Language / Interface	Read or Write	Popularity (10 – high, 1 – low)	Demo / Uploaded
Client API	BigFix Client	Client Relevance / MS COM	Read	2	Yes / Yes
Client UI	BigFix Client	HTML, Client Relevance / -	Read	2	Yes / No

Client API

- Microsoft COM based API
- Used to query BigFix Client for endpoint information
- Commonly used to interface with other endpoint agents (e.g. NAC), or custom end-user applications
- Allows BigFix partners and integrators to expose the results of an endpoint inspection conducted by the BigFix Client to their own logic embedded in 3rd-party clients executing on the client machine
- Potential use cases
  - Detect if security products (anti-virus, firewall) are installed or running
  - Detect that wireless networks are disabled
  - Patch status on the endpoint

Added Content – Not Presented.

Client API – Example Client API Tester



```
values of headers "Subject" of
relevant fixlets
    whose (value of header "X-Fixlet-Source-Severity" of it = "Critical")
of site whose (name of it = "Enterprise Security")
```

```
MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Server 2008 R2 SP1 - KB3078601
MS15-081: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office 2010 SP2 - KB2553313
MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3080446 (x64)
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Office 2007 SP3 - KB3085616
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3109094
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7
MS15-130: Security Update for Microsoft Uniscribe to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3108670 (x64)
MS16-004: Security Update for Microsoft Office to Address Remote Code Execution - Office 2010 SP2 - KB3114553
MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3124000
MS16-006: Security Update for Silverlight to Address Remote Code Execution - Silverlight 5 Developer Runtime - KB3126036 (x64)
```

☑ Elevate CPU while processing ☑ Sort Results □ Continuously Evaluation

Items: 10

Evaluation time: 00:00:03.011

Added Content – Not Presented.

Server Side API’s

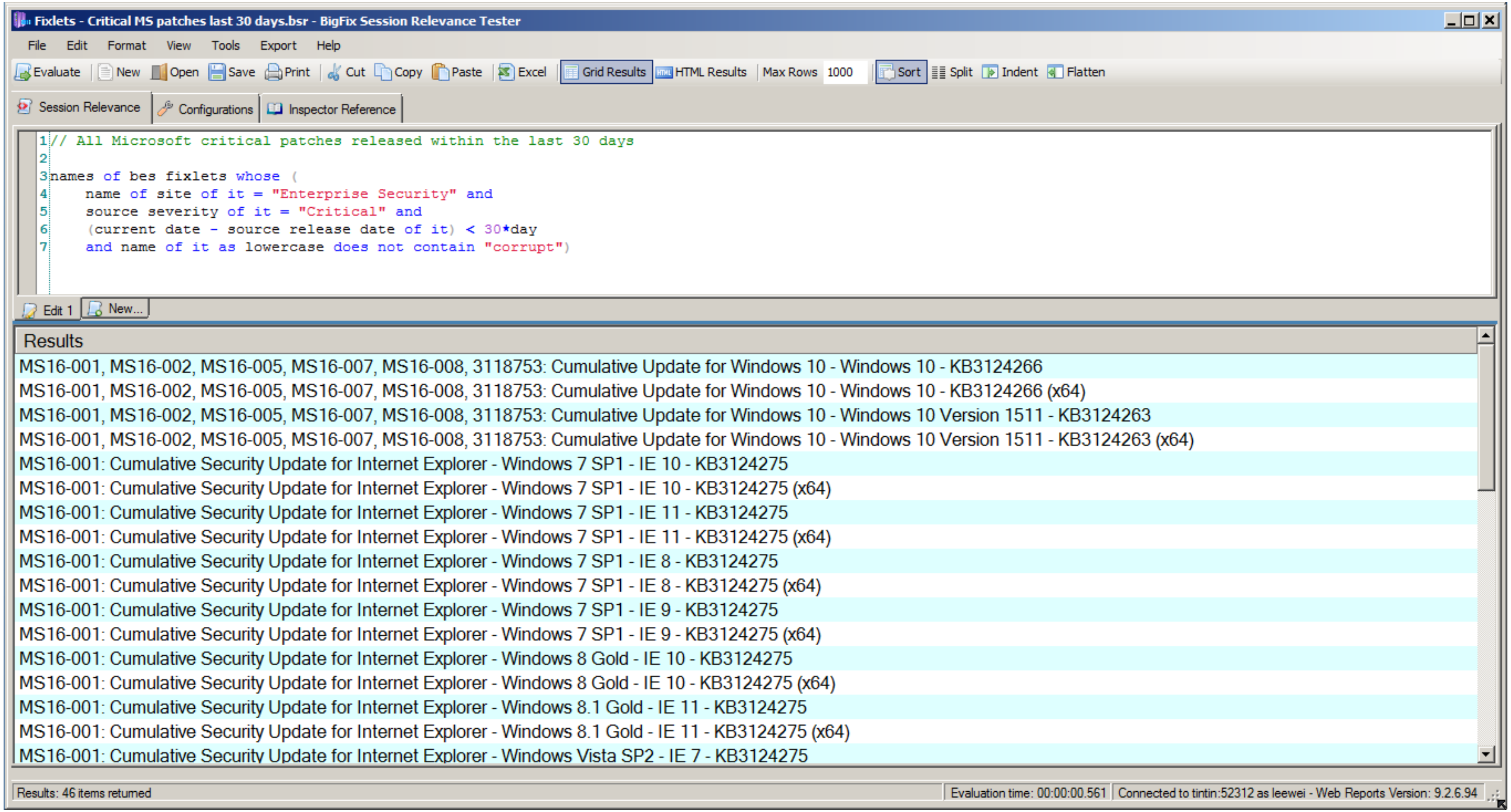
BigFix Server APIs

API	Execute Against	Language / Interface	Read or Write	Popularity (10 – high, 1 – low)	Demo / Uploaded
REST API (Platform)	BigFix Server	Any Language / HTTPS	Read / Write	10	Yes / No
REST API (Inventory)	Inventory Server	Any Language / HTTPS	Read / Write	3	No / No
REST API (SCA)	Security Compliance Analytics Server	Any Language / HTTPS	Read / Write	3	No / No
Platform Server API	BigFix Server	Any Language / MS COM	Write	4	Yes / Yes
Database API	BigFix Database	SQL / (ODBC, ADO, JDBC)	Read	3	Yes / Yes
SOAP API	Web Reports	Session Relevance / SOAP	Read	5	Yes / Yes
Dashboard API	BigFix Console	Session Relevance / -	Read / Write	2	Yes / No

SOAP API

- XML based SOAP API for querying objects in the BES Web Reports
- Results returned as XML documents
- Used only for reading

SOAP API – Example Session Relevance Tester



```
// All Microsoft critical patches released within the last 30 days

names of bes fixlets whose (
    name of site of it = "Enterprise Security" and
    source severity of it = "Critical" and
    (current date - source release date of it) < 30*day
    and name of it as lowercase does not contain "corrupt")
```

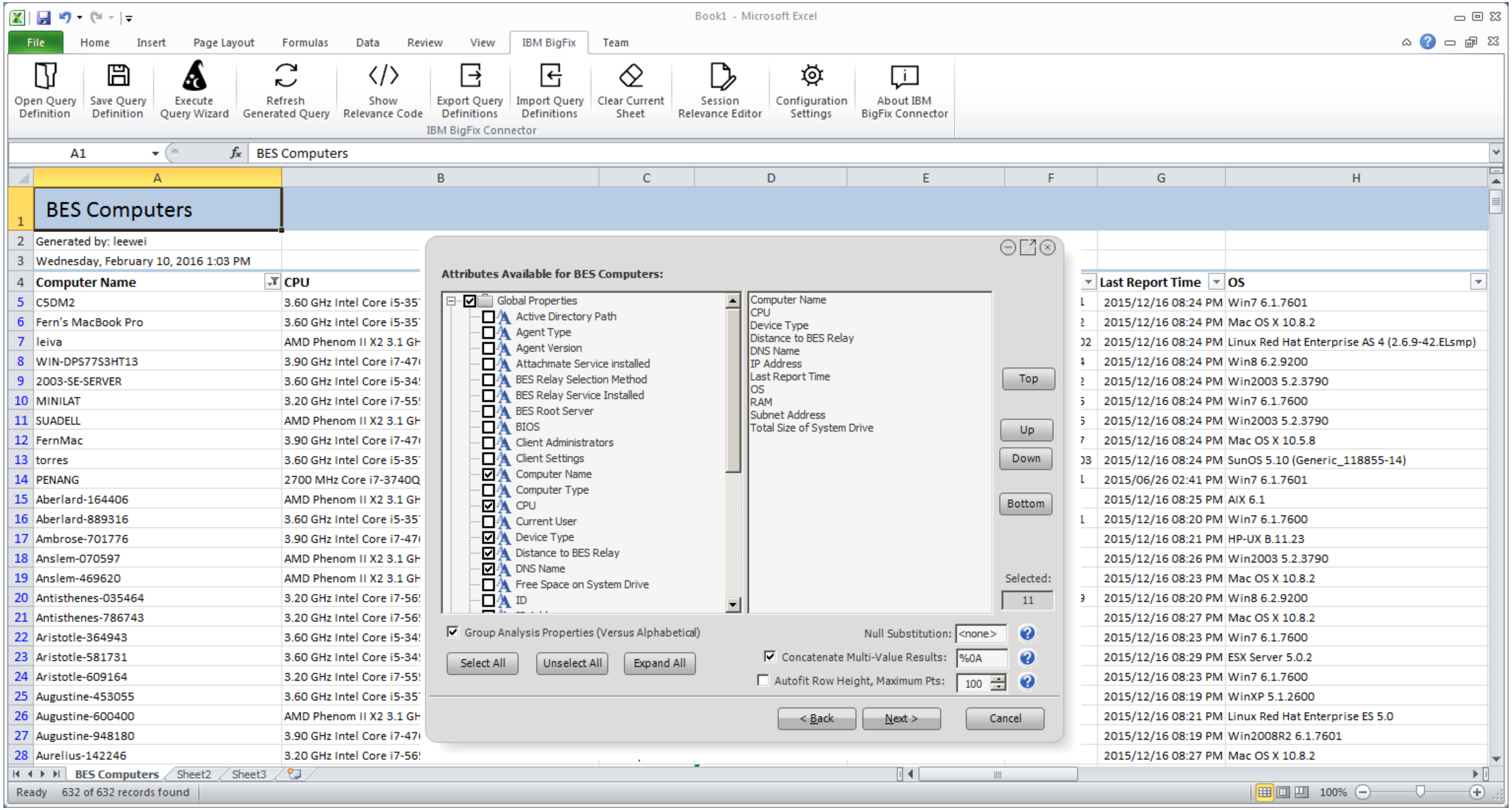
```
Results
MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 - KB3124266
MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 - KB3124266 (x64)
MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 Version 1511 - KB3124263
MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 Version 1511 - KB3124263 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 10 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 10 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 8 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 8 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 9 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 9 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 8 Gold - IE 10 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 8 Gold - IE 10 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3124275
MS16-001: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3124275 (x64)
MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 7 - KB3124275
```

```
Results: 46 items returned | Evaluation time: 00:00:00.561 | Connected to tintin:52312 as leewei - Web Reports Version: 9.2.6.94
```

REST API

- Perform the majority of tasks present in the console via a standardized and operating system independent method
- Communicates over HTTPS
- Results in either XML or JSON
- The only API that allows performing
  - Visibility / read functions, e.g. get info
  - Control / write functions, e.g. take actions

REST API example



A1 *fx* BES Computers

BES Computers

Generated by: leewei

Wednesday, February 10, 2016 1:03 PM

Computer Name	CPU		Last Report Time	OS
C5DM2	3.60 GHz Intel Core i5-35	1	2015/12/16 08:24 PM	Win7 6.1.7601
Fern's MacBook Pro	3.60 GHz Intel Core i5-35	2	2015/12/16 08:24 PM	Mac OS X 10.8.2
leiva	AMD Phenom II X2 3.1 GH	02	2015/12/16 08:24 PM	Linux Red Hat Enterprise AS 4 (2.6.9-42.ELsmp)
WIN-DPS77S3HT13	3.90 GHz Intel Core i7-47	4	2015/12/16 08:24 PM	Win8 6.2.9200
2003-SE-SERVER	3.60 GHz Intel Core i5-34	2	2015/12/16 08:24 PM	Win2003 5.2.3790
MINILAT	3.20 GHz Intel Core i7-55	5	2015/12/16 08:24 PM	Win7 6.1.7600
SUADELL	AMD Phenom II X2 3.1 GH	5	2015/12/16 08:24 PM	Win2003 5.2.3790
FernMac	3.90 GHz Intel Core i7-47	7	2015/12/16 08:24 PM	Mac OS X 10.5.8
torres	3.60 GHz Intel Core i5-35	03	2015/12/16 08:24 PM	SunOS 5.10 (Generic_118855-14)
PENANG	2700 MHz Core i7-3740Q	1	2015/06/26 02:41 PM	Win7 6.1.7601
Aberlard-164406	AMD Phenom II X2 3.1 GH		2015/12/16 08:25 PM	AIX 6.1
Aberlard-889316	3.60 GHz Intel Core i5-35	1	2015/12/16 08:20 PM	Win7 6.1.7600
Ambrose-701776	3.90 GHz Intel Core i7-47		2015/12/16 08:21 PM	HP-UX B.11.23
Anslem-070597	AMD Phenom II X2 3.1 GH		2015/12/16 08:26 PM	Win2003 5.2.3790
Anslem-469620	AMD Phenom II X2 3.1 GH		2015/12/16 08:23 PM	Mac OS X 10.8.2
Antisthenes-035464	3.20 GHz Intel Core i7-56	9	2015/12/16 08:20 PM	Win8 6.2.9200
Antisthenes-786743	3.20 GHz Intel Core i7-56		2015/12/16 08:27 PM	Mac OS X 10.8.2
Aristotle-364943	3.60 GHz Intel Core i5-34		2015/12/16 08:23 PM	Win7 6.1.7600
Aristotle-581731	3.60 GHz Intel Core i5-34		2015/12/16 08:29 PM	ESX Server 5.0.2
Aristotle-609164	3.20 GHz Intel Core i7-55		2015/12/16 08:23 PM	Win7 6.1.7600
Augustine-453055	3.60 GHz Intel Core i5-35		2015/12/16 08:19 PM	WinXP 5.1.2600
Augustine-600400	AMD Phenom II X2 3.1 GH		2015/12/16 08:21 PM	Linux Red Hat Enterprise ES 5.0
Augustine-948180	3.90 GHz Intel Core i7-47		2015/12/16 08:19 PM	Win2008R2 6.1.7601
Aurelius-142246	3.20 GHz Intel Core i7-56		2015/12/16 08:27 PM	Mac OS X 10.8.2

632 of 632 records found

Attributes Available for BES Computers:

☑ Global Properties
- ☐ Active Directory Path
- ☐ Agent Type
- ☐ Agent Version
- ☐ Attachmate Service installed
- ☐ BES Relay Selection Method
- ☐ BES Relay Service Installed
- ☐ BES Root Server
- ☐ BIOS
- ☐ Client Administrators
- ☐ Client Settings
- ☑ Computer Name
- ☐ Computer Type
- ☑ CPU
- ☐ Current User
- ☑ Device Type
- ☑ Distance to BES Relay
- ☑ DNS Name
- ☐ Free Space on System Drive
- ☐ ID

Computer Name
CPU
Device Type
Distance to BES Relay
DNS Name
IP Address
Last Report Time
OS
RAM
Subnet Address
Total Size of System Drive

Selected: 11

☑ Group Analysis Properties (Versus Alphabetical)

Null Substitution: <none>

☑ Concatenate Multi-Value Results: %0A

☐ Autofit Row Height, Maximum Pts: 100

REST Troubleshooting : How To Demonstration

Rest API

- Simple to implement
  - One URL to submit queries
  - One URL to retrieve results, with the paging capability
- Best documentation for Query REST API

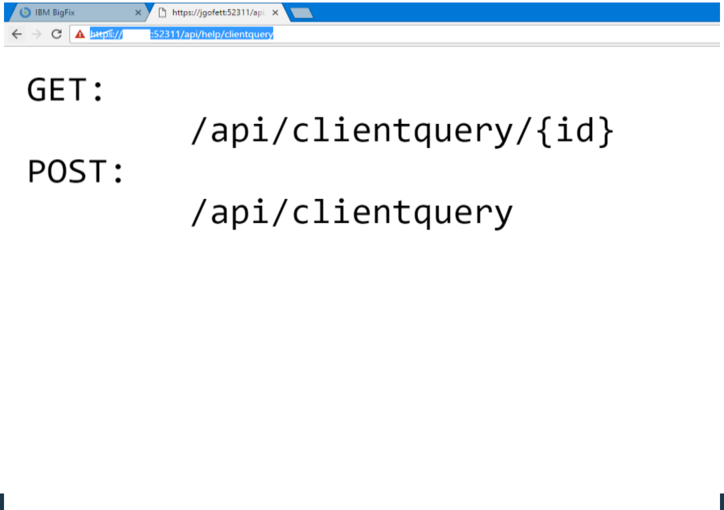
Link or Developer.BigFix.com

More Help!

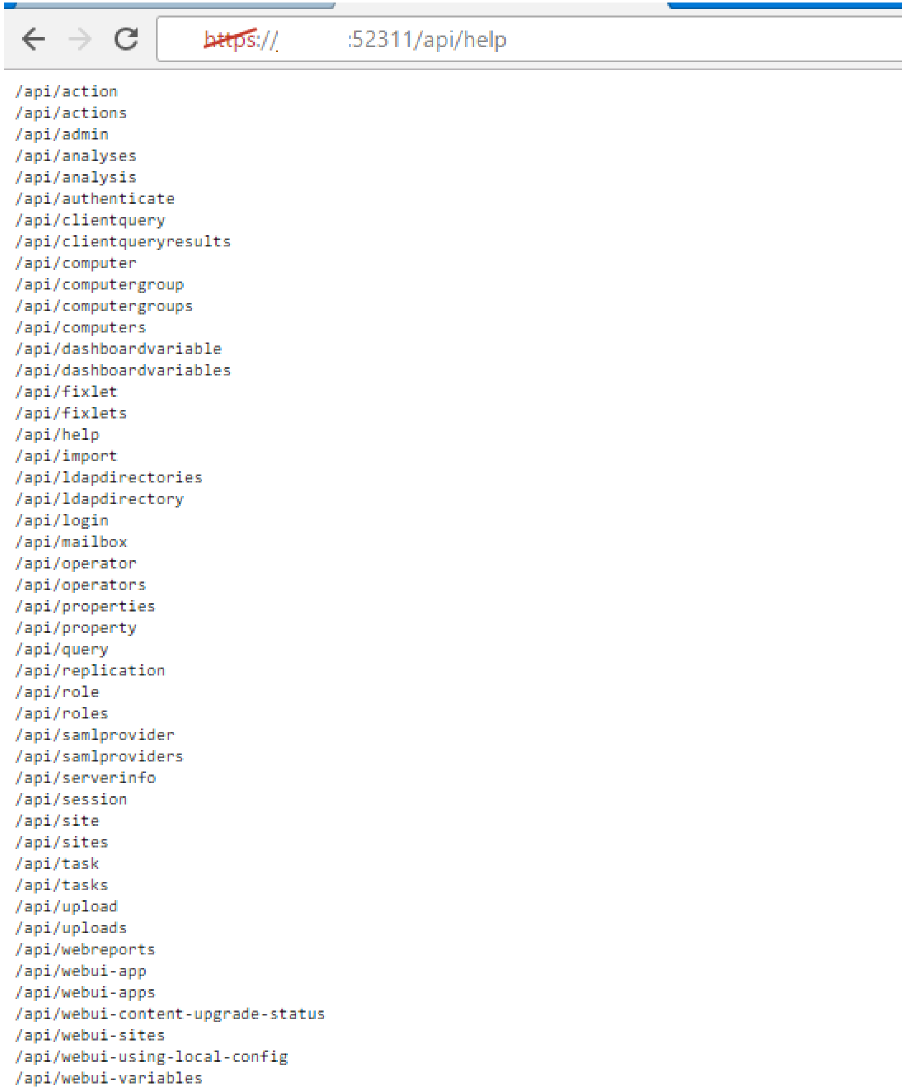
- https://localhost:52311/api/help

More Help?

- https://localhost:52311/api/help/object
  - https://localhost:52311/api/help/clientquery
  - https://localhost:52311/api/help/action
  - https://localhost:52311/api/help/action/{i}


IBM BigFix
https://jgofett:52311/api
~~https~~:// :52311/api/help/clientquery

```
GET:
        /api/clientquery/{id}
POST:
        /api/clientquery
```



```
/api/action
/api/actions
/api/admin
/api/analyses
/api/analysis
/api/authenticate
/api/clientquery
/api/clientqueryresults
/api/computer
/api/computergroup
/api/computergroups
/api/computers
/api/dashboardvariable
/api/dashboardvariables
/api/fixlet
/api/fixlets
/api/help
/api/import
/api/ldapdirectories
/api/ldapdirectory
/api/login
/api/mailbox
/api/operator
/api/operators
/api/properties
/api/property
/api/query
/api/replication
/api/role
/api/roles
/api/samlprovider
/api/samlproviders
/api/serverinfo
/api/session
/api/site
/api/sites
/api/task
/api/tasks
/api/upload
/api/uploads
/api/webreports
/api/webui-app
/api/webui-apps
/api/webui-content-upgrade-status
/api/webui-sites
/api/webui-using-local-config
/api/webui-variables
```

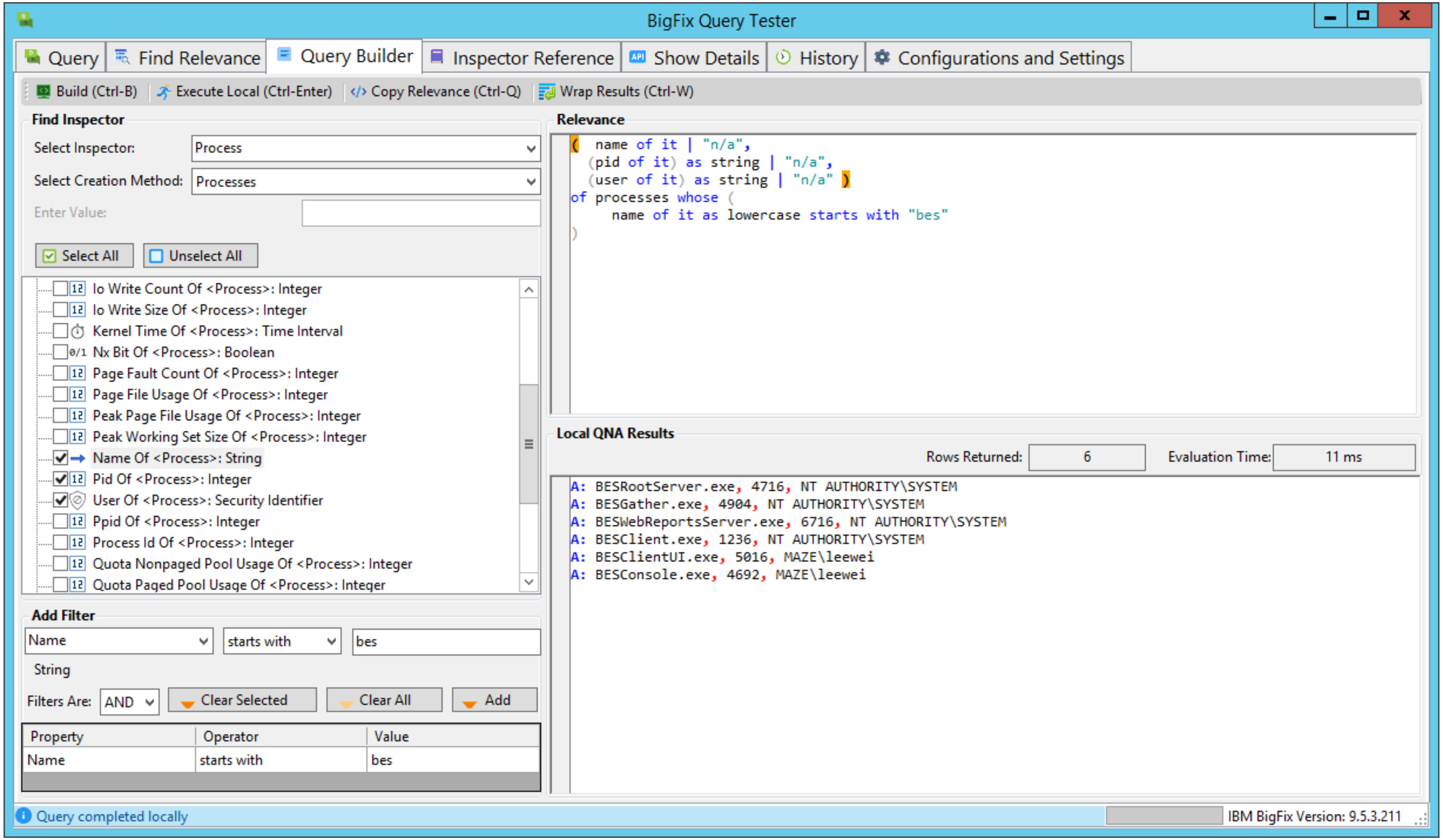
Example Applications made with REST

BigFix Query Tester

- Syntax highlighted Relevance statements
- Return multiple row results as one unit
- Count unique occurrences of the results
- Use any Relevance statements from properties, analyses, and Fixlets
- Query history
- Experimental Query Builder

- http://leewei.com/bigfix/prod/query/BigFixQueryTesterV2.0.zip

BigFix Query Tester



Find Inspector

Select Inspector: Process

Select Creation Method: Processes

Enter Value:

- □ Io Write Count Of <Process>: Integer
- □ Io Write Size Of <Process>: Integer
- □ Kernel Time Of <Process>: Time Interval
- □ Nx Bit Of <Process>: Boolean
- □ Page Fault Count Of <Process>: Integer
- □ Page File Usage Of <Process>: Integer
- □ Peak Page File Usage Of <Process>: Integer
- □ Peak Working Set Size Of <Process>: Integer
- ☑ Name Of <Process>: String
- ☑ Pid Of <Process>: Integer
- ☑ User Of <Process>: Security Identifier
- □ Ppid Of <Process>: Integer
- □ Process Id Of <Process>: Integer
- □ Quota Nonpaged Pool Usage Of <Process>: Integer
- □ Quota Paged Pool Usage Of <Process>: Integer

Add Filter

Name | starts with | bes

String

Filters Are: AND

Property	Operator	Value
Name	starts with	bes

Relevance

```
( name of it | "n/a",
  (pid of it) as string | "n/a",
  (user of it) as string | "n/a" )
of processes whose (
    name of it as lowercase starts with "bes"
)
```

Local QNA Results

Rows Returned: 6 Evaluation Time: 11 ms

```
A: BESRootServer.exe, 4716, NT AUTHORITY\SYSTEM
A: BESGather.exe, 4904, NT AUTHORITY\SYSTEM
A: BESWebReportsServer.exe, 6716, NT AUTHORITY\SYSTEM
A: BESClient.exe, 1236, NT AUTHORITY\SYSTEM
A: BESClientUI.exe, 5016, MAZE\leewei
A: BESConsole.exe, 4692, MAZE\leewei
```

Query completed locally

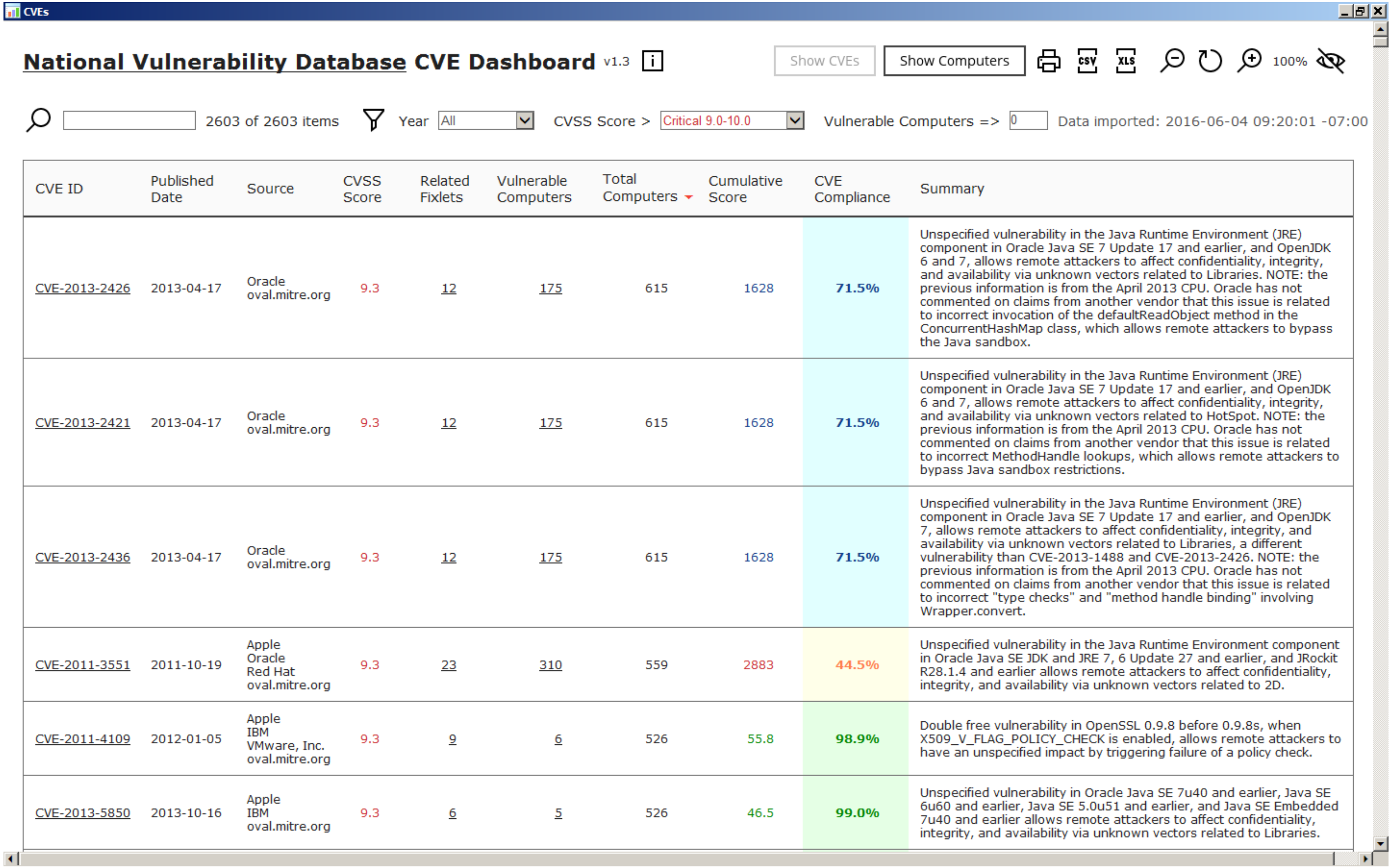
IBM BigFix Version: 9.5.3.211

REST API – CVE Dashboard

- In general this is how it works:
- There is a command line utility that is scheduled via a Fixlet. You can also run it manually.
- The utility downloads any CVEs from the National Vulnerability Database (NVD) if there are corresponding Fixlets.
- The Console Dashboard is then used to browse and search the data.

Link to the CVE Dashboar on IBM X-Force AppExchange

REST API – CVE Dashboard



National Vulnerability Database CVE Dashboard v1.3

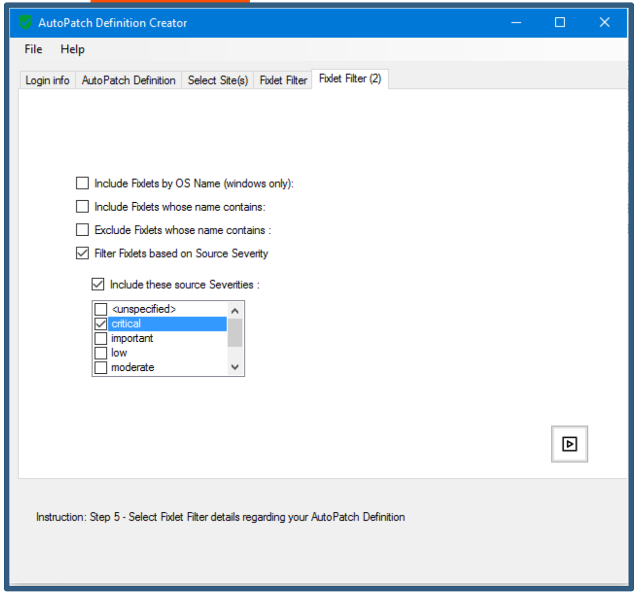
2603 of 2603 items Year All CVSS Score > Critical 9.0-10.0 Vulnerable Computers => 0 Data imported: 2016-06-04 09:20:01 -07:00

CVE ID	Published Date	Source	CVSS Score	Related Fixlets	Vulnerable Computers	Total Computers	Cumulative Score	CVE Compliance	Summary
CVE-2013-2426	2013-04-17	Oracle oval.mitre.org	9.3	12	175	615	1628	71.5%	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect invocation of the defaultReadObject method in the ConcurrentHashMap class, which allows remote attackers to bypass the Java sandbox.
CVE-2013-2421	2013-04-17	Oracle oval.mitre.org	9.3	12	175	615	1628	71.5%	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to HotSpot. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect MethodHandle lookups, which allows remote attackers to bypass Java sandbox restrictions.
CVE-2013-2436	2013-04-17	Oracle oval.mitre.org	9.3	12	175	615	1628	71.5%	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-1488 and CVE-2013-2426. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect "type checks" and "method handle binding" involving Wrapper.convert.
CVE-2011-3551	2011-10-19	Apple Oracle Red Hat oval.mitre.org	9.3	23	310	559	2883	44.5%	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2011-4109	2012-01-05	Apple IBM VMware, Inc. oval.mitre.org	9.3	9	6	526	55.8	98.9%	Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.
CVE-2013-5850	2013-10-16	Apple IBM oval.mitre.org	9.3	6	5	526	46.5	99.0%	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.

REST API – Auto Patch

- AutoPatch Definition Creates Baselines and Actions Automatically.
- 1 Definition can be run on a schedule to create Actions and Baselines

- Download Available:
  - Link here
  - Md5s /SHA’s / etc.- here



□ Include Fixlets by OS Name (windows only):

□ Include Fixlets whose name contains:

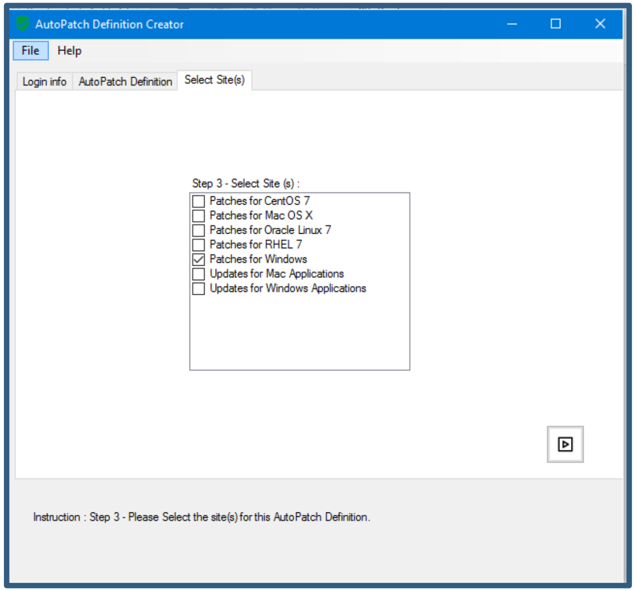
□ Exclude Fixlets whose name contains :

☑ Filter Fixlets based on Source Severity

☑ Include these source Severities :

- □ <unspecified>
- ☑ critical
- □ important
- □ low
- □ moderate

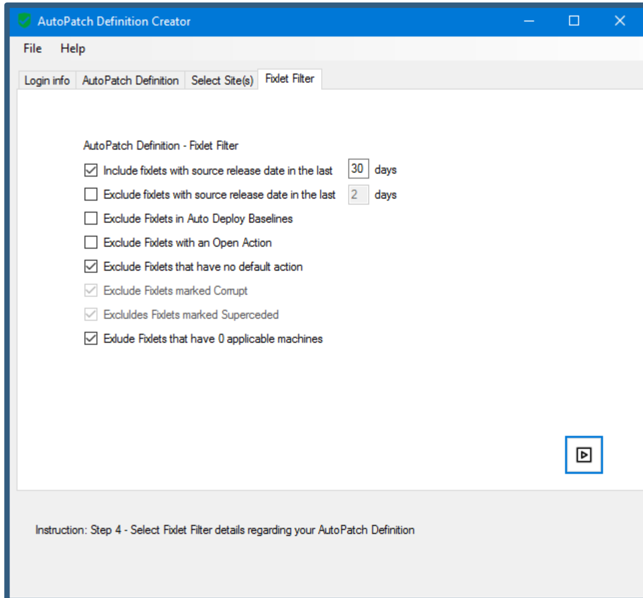
Instruction: Step 5 - Select Fixlet Filter details regarding your AutoPatch Definition



Step 3 - Select Site (s) :

- □ Patches for CentOS 7
- □ Patches for Mac OS X
- □ Patches for Oracle Linux 7
- □ Patches for RHEL 7
- ☑ Patches for Windows
- □ Updates for Mac Applications
- □ Updates for Windows Applications

Instruction : Step 3 - Please Select the site(s) for this AutoPatch Definition.



AutoPatch Definition - Fixlet Filter

☑ Include fixlets with source release date in the last 30 days

□ Exclude fixlets with source release date in the last 2 days

□ Exclude Fixlets in Auto Deploy Baselines

□ Exclude Fixlets with an Open Action

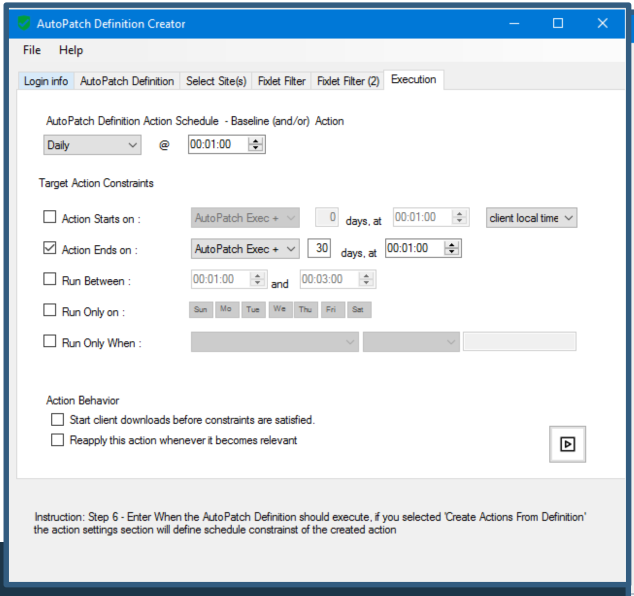
☑ Exclude Fixlets that have no default action

☑ Exclude Fixlets marked Corrupt

☑ Excludes Fixlets marked Superceded

☑ Exlude Fixlets that have 0 applicable machines

Instruction: Step 4 - Select Fixlet Filter details regarding your AutoPatch Definition



AutoPatch Definition Action Schedule - Baseline (and/or) Action

Daily @ 00:01:00

Target Action Constraints

□ Action Starts on : AutoPatch Exec + 0 days, at 00:01:00 client local time

☑ Action Ends on : AutoPatch Exec + 30 days, at 00:01:00

□ Run Between : 00:01:00 and 00:03:00

□ Run Only on : Sun Mo Tue We Thu Fri Sat

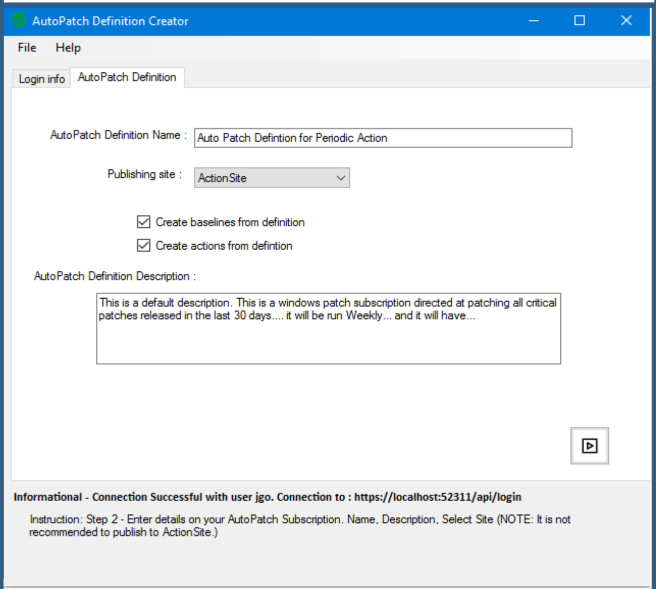
□ Run Only When :

Action Behavior

□ Start client downloads before constraints are satisfied.

□ Reapply this action whenever it becomes relevant

Instruction: Step 6 - Enter When the AutoPatch Definition should execute, if you selected 'Create Actions From Definition' the action settings section will define schedule constraint of the created action



AutoPatch Definition Name : Auto Patch Defintion for Periodic Action

Publishing site : ActionSite

☑ Create baselines from definition

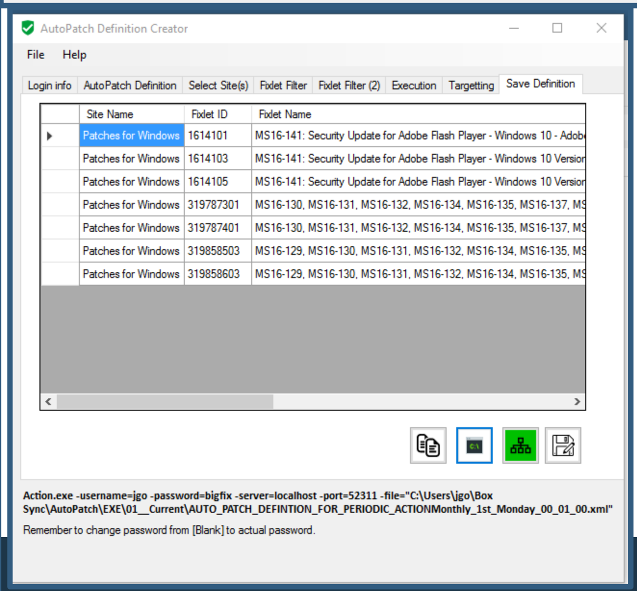
☑ Create actions from defintion

AutoPatch Definition Description :

This is a default description. This is a windows patch subscription directed at patching all critical patches released in the last 30 days.... it will be run Weekly... and it will have...

Informational - Connection Successful with user jgo. Connection to : https://localhost:52311/api/login

Instruction: Step 2 - Enter details on your AutoPatch Subscription. Name, Description, Select Site (NOTE: It is not recommended to publish to ActionSite.)



Site Name	Fixlet ID	Fixlet Name
Patches for Windows	1614101	MS16-141: Security Update for Adobe Flash Player - Windows 10 - Adob
Patches for Windows	1614103	MS16-141: Security Update for Adobe Flash Player - Windows 10 Versior
Patches for Windows	1614105	MS16-141: Security Update for Adobe Flash Player - Windows 10 Versior
Patches for Windows	319787301	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS
Patches for Windows	319787401	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS
Patches for Windows	319858503	MS16-129, MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS
Patches for Windows	319858603	MS16-129, MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS

Action.exe -username=jgo -password=bigfix -server=localhost -port=52311 -file="C:\Users\jgo\Box Sync\AutoPatch\EXE\01__Current\AUTO_PATCH_DEFINTION_FOR_PERIODIC_ACTIONMonthly_1st_Monday_00_01_00.xml"

Remember to change password from [Blank] to actual password.

Demonstrations

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®