IBM Security

BigFix Query Unleashed!

Lee Wei
leewei@us.ibm.com

October, 2016

BigFix Query Requirements

- 9.5 Patch 2 (9.5.2.56 or greater) required for all components
  - This means no support for
    - Windows XP
    - Windows Server 2003
    - Mac OS X 10.7 Lion
    - RHEL 4

- Agents need to be able to receive UDP notifications
  - Does not work with agents behind firewall, NATed, etc.

Important Restriction – Agent Context / Automatic Group

- Agent invokes QNA to process queries

- Query does not work with Inspectors requiring agent context
  - Examples:
    - `number of relevant fixlets whose (value of header "X-Fixlet-Source-Severity" of it = "Critical") of site whose (name of it = "Enterprise Security")`
    - `expiration date of client license`
    - `now of registration server`

Settings – Long Running Queries

- By default, queries are timed out after the following amount of elapse time to avoid bad queries that overwhelm the endpoints

- _BESClient_Query_MOMaxQueryTime
  - Seconds – default 60

- _BESClient_Query_NMOMaxQueryTime
  - Seconds – default 10

Settings – CPU Utilization

- By default, queries are throttled to use around 2% of the CPU

- _BESClient_Query_WorkTime
  - Milliseconds – default 10

- _BESClient_Query_SleepTime
  - Milliseconds – default 480

Settings – How Long to Keep the Requests and Responses

- BESAdmin settings
  - queryHoursToLive
    - Hours – default 1440 (60 days)
  - queryResultsHoursToLive
    - Hours – default 4 hours

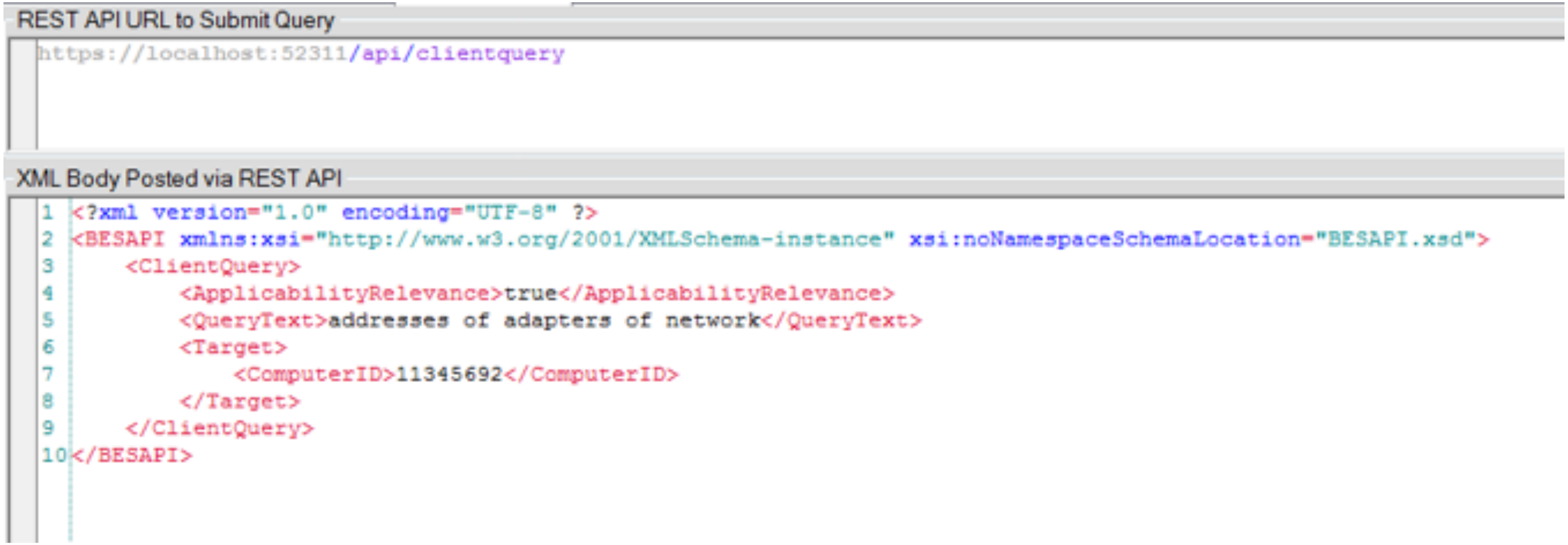
REST API

- Simple to implement
  - One URL to submit queries
  - One URL to retrieve results, with the paging capability

- Does not require the WebUI framework

- Best documentation for Query REST API
  - Link

REST API Query Example



REST API URL to Submit Query

```
https://localhost:52311/api/clientquery
```

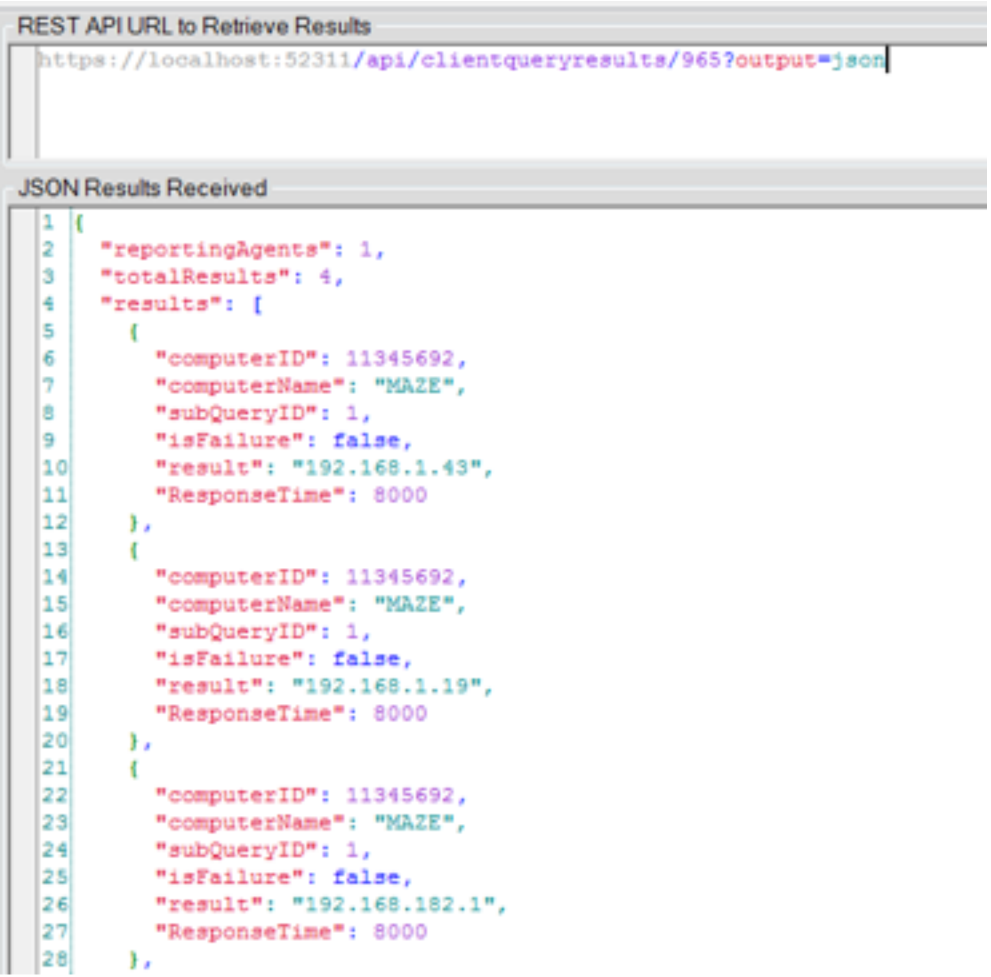
XML Body Posted via REST API

```
<?xml version="1.0" encoding="UTF-8" ?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
    <ClientQuery>
        <ApplicabilityRelevance>true</ApplicabilityRelevance>
        <QueryText>addresses of adapters of network</QueryText>
        <Target>
            <ComputerID>11345692</ComputerID>
        </Target>
    </ClientQuery>
</BESAPI>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BESAPI.xsd">
<ClientQuery>
    <ApplicabilityRelevance>true</ApplicabilityRelevance>
    <QueryText>addresses of adapters of network</QueryText>
    <Target></Target>
</ClientQuery>
</BESAPI>
```

REST API Results

- Results are returned in:
  - XML
  - JSON



REST API URL to Retrieve Results

```
https://localhost:52311/api/clientqueryresults/965?output=json
```

JSON Results Received

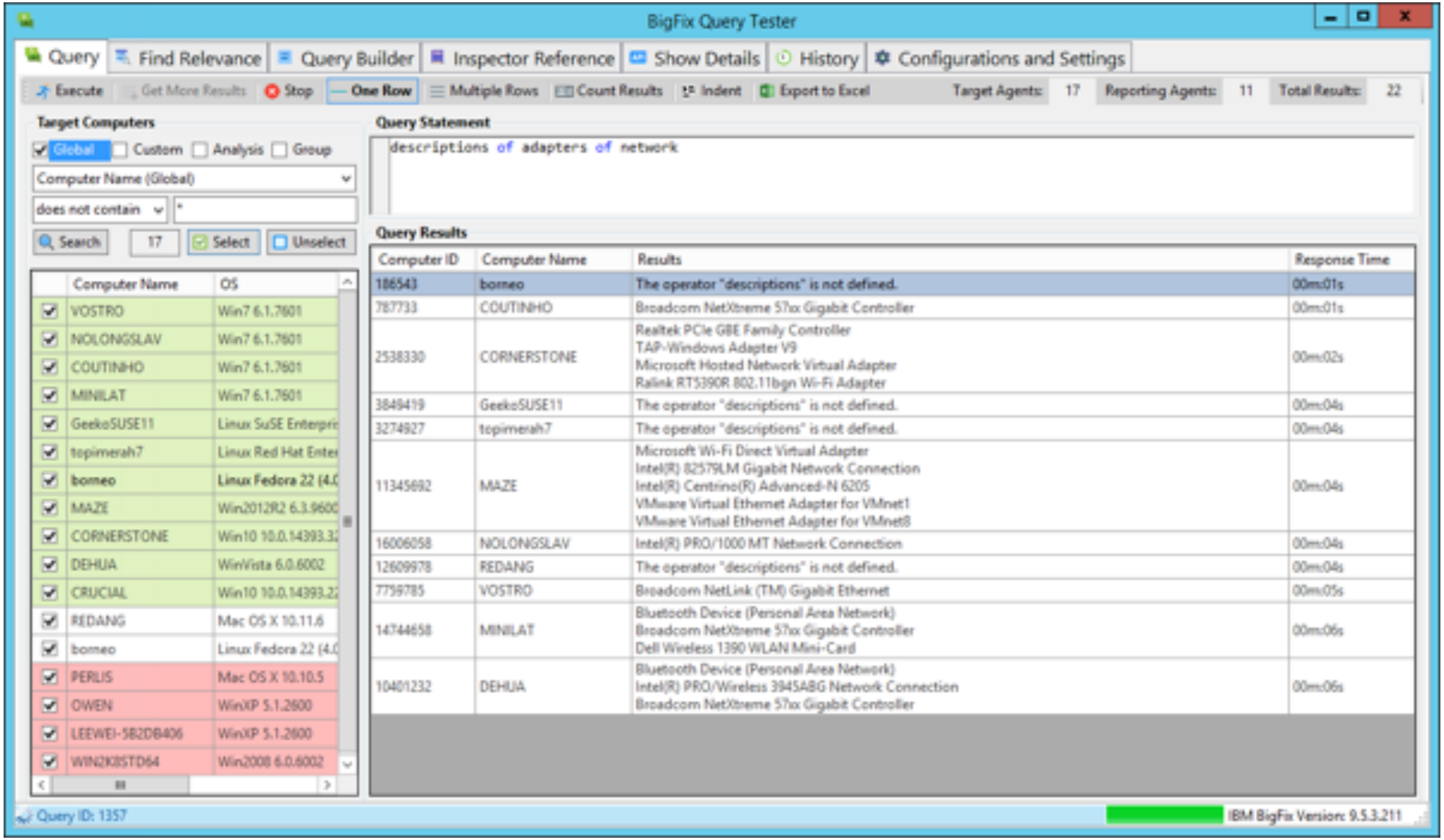
```
{
  "reportingAgents": 1,
  "totalResults": 4,
  "results": [
    {
      "computerID": 11345692,
      "computerName": "MAZE",
      "subQueryID": 1,
      "isFailure": false,
      "result": "192.168.1.43",
      "ResponseTime": 8000
    },
    {
      "computerID": 11345692,
      "computerName": "MAZE",
      "subQueryID": 1,
      "isFailure": false,
      "result": "192.168.1.19",
      "ResponseTime": 8000
    },
    {
      "computerID": 11345692,
      "computerName": "MAZE",
      "subQueryID": 1,
      "isFailure": false,
      "result": "192.168.182.1",
      "ResponseTime": 8000
    },
```

Example Query Tester Application

- 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



Target Agents: 17 Reporting Agents: 11 Total Results: 22

Target Computers

☑ Global ☐ Custom ☐ Analysis ☐ Group

Computer Name (Global)

does not contain: *

17

	Computer Name	OS
☑	VOSTRO	Win7 6.1.7601
☑	NOLONGSLAV	Win7 6.1.7601
☑	COUTINHO	Win7 6.1.7601
☑	MINILAT	Win7 6.1.7601
☑	GeekoSUSE11	Linux SuSE Enterpri
☑	topimerah7	Linux Red Hat Enter
☑	borneo	Linux Fedora 22 (4.0
☑	MAZE	Win2012R2 6.3.9600
☑	CORNERSTONE	Win10 10.0.14393.32
☑	DEHUA	WinVista 6.0.6002
☑	CRUCIAL	Win10 10.0.14393.22
☑	REDANG	Mac OS X 10.11.6
☑	borneo	Linux Fedora 22 (4.0
☑	PERLIS	Mac OS X 10.10.5
☑	OWEN	WinXP 5.1.2600
☑	LEEWEI-5B2DB406	WinXP 5.1.2600
☑	WIN2K8STD64	Win2008 6.0.6002

Query Statement

```
descriptions of adapters of network
```

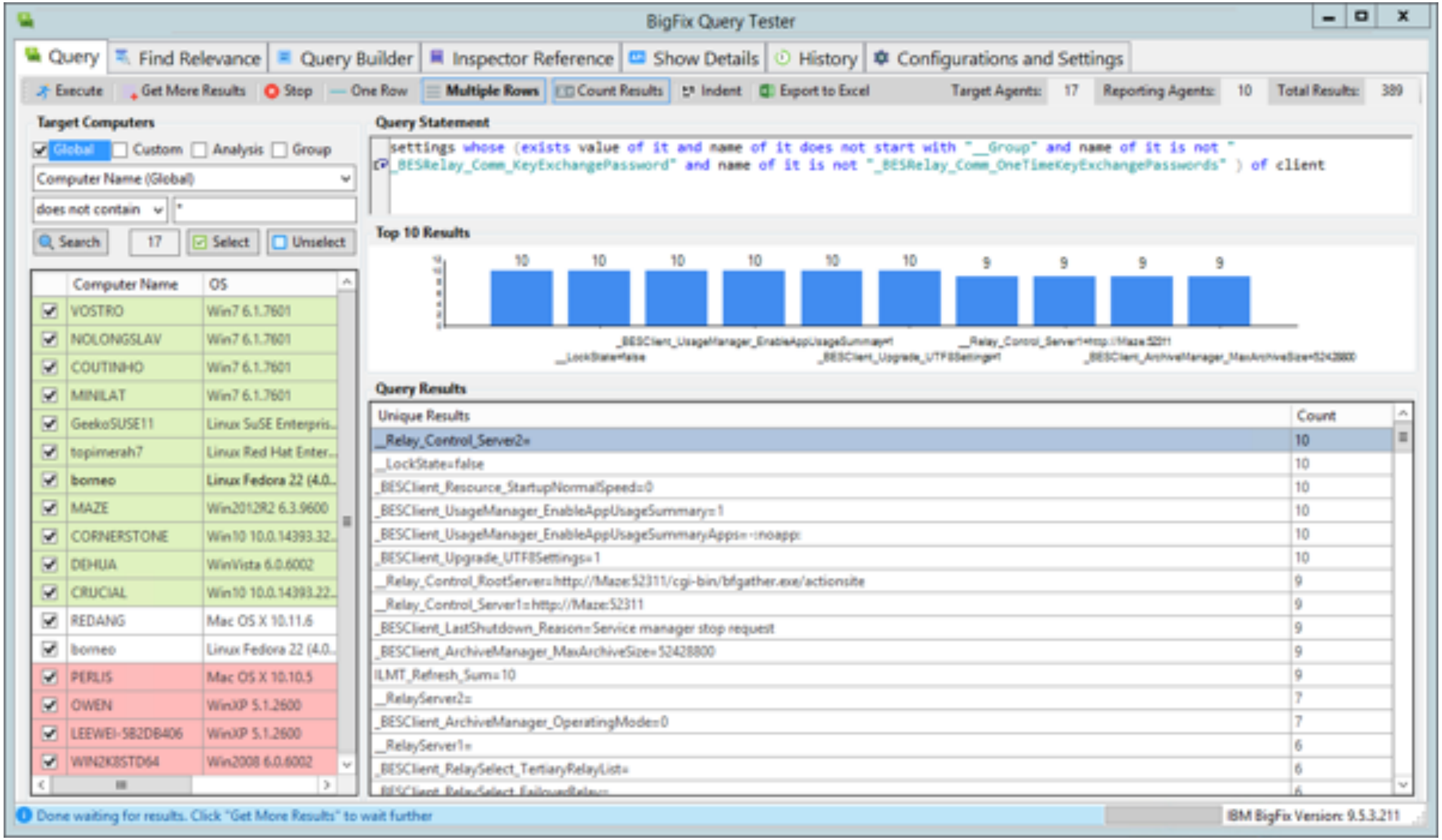
Query Results

Computer ID	Computer Name	Results	Response Time
186543	borneo	The operator "descriptions" is not defined.	00m:01s
787733	COUTINHO	Broadcom NetXtreme 57xx Gigabit Controller	00m:01s
2538330	CORNERSTONE	Realtek PCIe GBE Family Controller TAP-Windows Adapter V9 Microsoft Hosted Network Virtual Adapter Ralink RT5390R 802.11bgn Wi-Fi Adapter	00m:02s
3849419	GeekoSUSE11	The operator "descriptions" is not defined.	00m:04s
3274927	topimerah7	The operator "descriptions" is not defined.	00m:04s
11345692	MAZE	Microsoft Wi-Fi Direct Virtual Adapter Intel(R) 82579LM Gigabit Network Connection Intel(R) Centrino(R) Advanced-N 6205 VMware Virtual Ethernet Adapter for VMnet1 VMware Virtual Ethernet Adapter for VMnet8	00m:04s
16006058	NOLONGSLAV	Intel(R) PRO/1000 MT Network Connection	00m:04s
12609978	REDANG	The operator "descriptions" is not defined.	00m:04s
7759785	VOSTRO	Broadcom NetLink (TM) Gigabit Ethernet	00m:05s
14744658	MINILAT	Bluetooth Device (Personal Area Network) Broadcom NetXtreme 57xx Gigabit Controller Dell Wireless 1390 WLAN Mini-Card	00m:06s
10401232	DEHUA	Bluetooth Device (Personal Area Network) Intel(R) PRO/Wireless 3945ABG Network Connection Broadcom NetXtreme 57xx Gigabit Controller	00m:06s

Query ID: 1357

IBM BigFix Version: 9.5.3.211

BigFix Query Tester



Target Agents: 17 Reporting Agents: 10 Total Results: 389

Target Computers

☑ Global ☐ Custom ☐ Analysis ☐ Group

Computer Name (Global)

does not contain *

17

	Computer Name	OS
☑	VOSTRO	Win7 6.1.7601
☑	NOLONGSLAV	Win7 6.1.7601
☑	COUTINHO	Win7 6.1.7601
☑	MINILAT	Win7 6.1.7601
☑	GeekoSUSE11	Linux SuSE Enterpris...
☑	topimerah7	Linux Red Hat Enter...
☑	**borneo**	**Linux Fedora 22 (4.0...**
☑	MAZE	Win2012R2 6.3.9600
☑	CORNERSTONE	Win10 10.0.14393.32...
☑	DEHUA	WinVista 6.0.6002
☑	CRUCIAL	Win10 10.0.14393.22...
☑	REDANG	Mac OS X 10.11.6
☑	borneo	Linux Fedora 22 (4.0...
☑	PERLIS	Mac OS X 10.10.5
☑	OWEN	WinXP 5.1.2600
☑	LEEWEI-5B2DB406	WinXP 5.1.2600
☑	WIN2K8STD64	Win2008 6.0.6002

Query Statement

```
settings whose (exists value of it and name of it does not start with "__Group" and name of it is not "
_BESRelay_Comm_KeyExchangePassword" and name of it is not "_BESRelay_Comm_OneTimeKeyExchangePasswords" ) of client
```

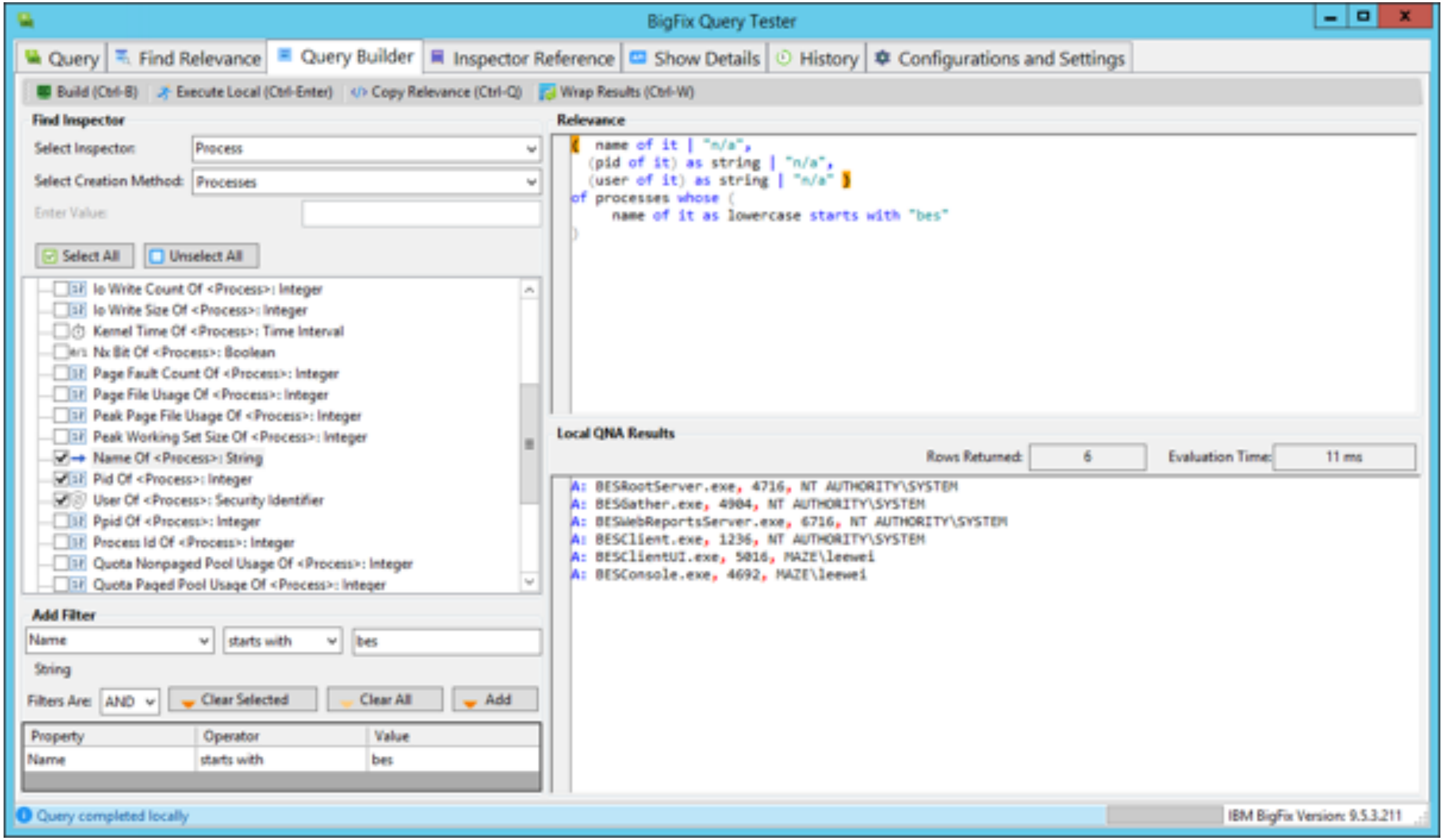
Query Results

Unique Results	Count
__Relay_Control_Server2=	10
__LockState=false	10
_BESClient_Resource_StartupNormalSpeed=0	10
_BESClient_UsageManager_EnableAppUsageSummary=1	10
_BESClient_UsageManager_EnableAppUsageSummaryApps=-:noapp:	10
_BESClient_Upgrade_UTF8Settings=1	10
__Relay_Control_RootServer=http://Maze:52311/cgi-bin/bfgather.exe/actionsite	9
__Relay_Control_Server1=http://Maze:52311	9
_BESClient_LastShutdown_Reason=Service manager stop request	9
_BESClient_ArchiveManager_MaxArchiveSize=52428800	9
ILMT_Refresh_Sum=10	9
__RelayServer2=	7
_BESClient_ArchiveManager_OperatingMode=0	7
__RelayServer1=	6
_BESClient_RelaySelect_TertiaryRelayList=	6
_BESClient_RelaySelect_FailoverRelay=	6

Done waiting for results. Click "Get More Results" to wait further

IBM BigFix Version: 9.5.3.211

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

Resource Links

- Very useful and detailed official documentation at Knowledge Center
  - Link
- Settings relating to Query
  - Link
- Engineering Blog with REST API information
  - Link
- Download BigFix Query Tester application
  - Link

Roadmap Features for R2

- Query Parameterization
  - Link
    - `versions of regapps "firefox.exe"`
    - `versions of regapps "{QUERY_PARAMETER{applicationName, "Enter the application executable name", "firefox.exe"}}"`
- Additional Out of the Box Queries
  - Link
- Query Authorization
    - Queries authorized by site, capabilities by user type (e.g. admin vs. operator)

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