BigFix

Session Relevance for the practical BigFix Admin

Mike Paishon
BigFix Architect

HCL SOFTWARE

A primer

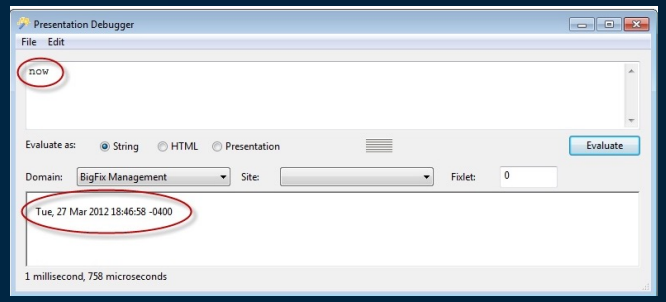
- Session Relevance is a BigFix proprietary language that is common to the console and web reports which allows for interactions on a read only basis.
- There are several exposed facilities to interact with the product through session relevance
- This session will focus on the activities and techniques that leverage session relevance that can assist in the day to day activities of a BigFix admin…

Outline / Agenda

- Primer
- Tools of the trade
  - Presentation Debugger
  - Web Reports /QNA
  - Custom Handler around relevance evaluation.
- Getting Acquainted
  - Know what to ask \ how to ask
- Tips and Tricks
  - Sort of Values
  - Aggregation
  - Combination of like types
- Concepts
  - Google with Session Relevance
  - Present a link
  - The concept of time \ alerting
  - Relevance HTML
- Take Homes \ JS templates

Reports & Queries Referenced \ including this provided w/ no warranty or support…

Tools of the Trade

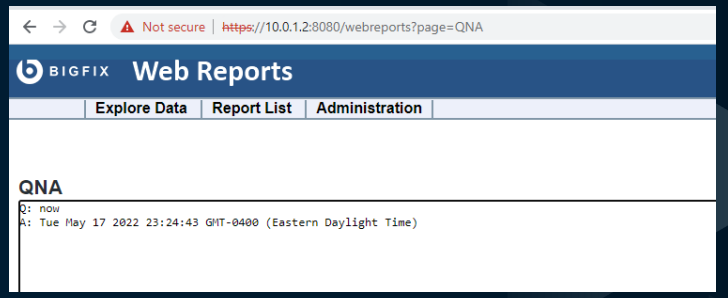


- Presentation Debugger
- https://developer.bigfix.com/tools/presentation_debugger.html

While the BigFix Console is running, press Ctrl-Shift-Alt-D to display the Debug window.

Click the check box next to Show Debug Menu at the top of the window. This installs a new menu in the Console called Debug that contains several handy debugging tools.

From the Debug menu, click **Presentation Debugger**



- Web Reports QNA
- https://developer.bigfix.com/tools/qna_wr.html

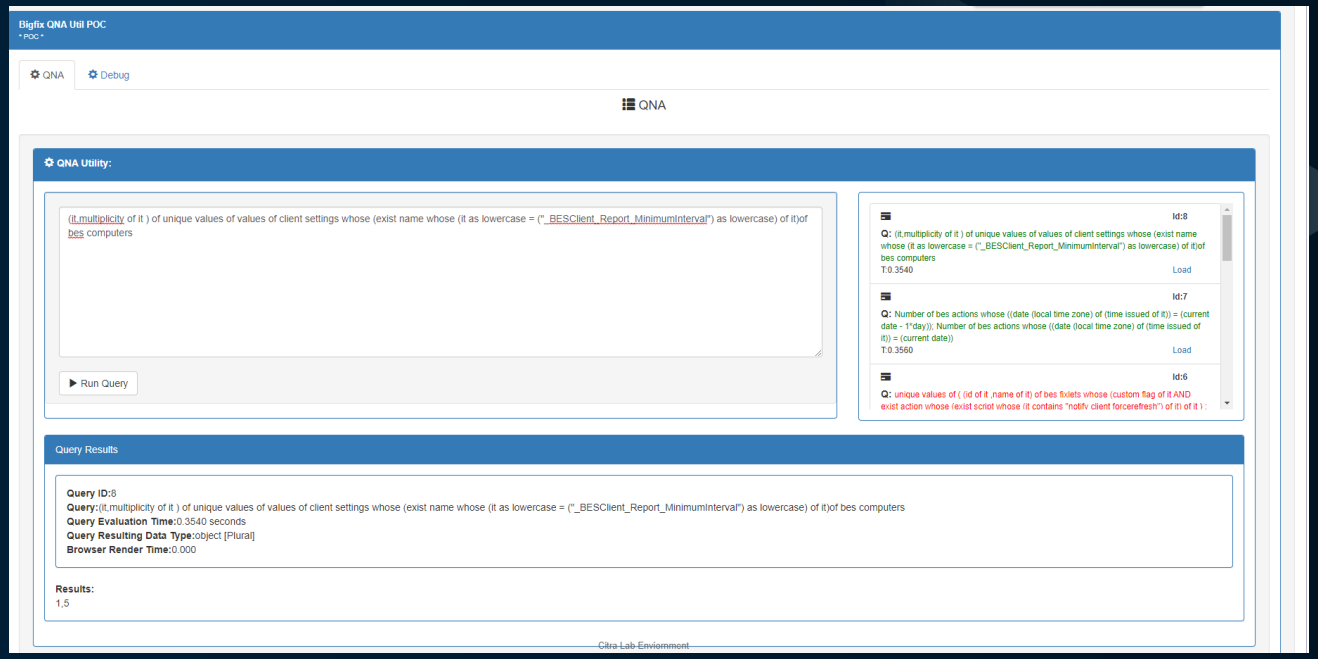
Within webreports navigate to /webreports?page=QNA

Tools of the Trade cont…

Wrapper Around built in relevance…

```
function js_async_relevance_qna( query, callback, tmpobj ){

                    Relevance( query, {
                     success: function ( result ) {
                                    callback( result, tmpobj );
                     },
                     failure: function ( error ) {
                              /*
                              Do some special error handling
                              */
                    },tmpobj)
}
```



Simple QNA Tester

- Allows multiline
- Stores prior query results (with result recall)
- Tracks Time \ Responsiveness
- Tracks returning type

https://github.com/bigfix/content/blob/master/reports/WRExample-Webreport-QNA-util.txt

Session Relevance is also exposed through both the REST and SOAP Interfaces..

All Reports & Queries Referenced will be provided w/ no warranty or support…

Getting Acquainted

BigFix

* Some Basic Skills
\\ There are Types and there are properties
Q: Types

\\Inspect the properties of a given type
Q: properties of type "bes computer“

\\We can query what properties are associated to a given type...
Q: (properties of it, it) of types

\\We can also leverage session relevance to locate any property associated to a given type
Q: (properties of it, it) of types whose (property of it as string contains "time")

Tips and Tricks

Use Case	Technique
Sorting Values	Unique Values
Aggregation	(it, multiplicity of it)
Combination of types	Use of Sets (;)
Reporting by Groups	Size of intersections

Sorting

Technique - The use of Unique Values will sort on base types (as long as the types are the same) for example

Q: unique values of names of bes computers
Q: unique values of last report times of bes computers
Q: unique values of ip addresses of bes computers

Aggregation

Technique - The use of (it,multiplicity of it) of unique values can return the aggregate counts of a value

Use Case: I want to see all configured values for a given client setting.
Q:(it,multiplicity of it) of unique values of values of client settings whose (exist name whose (it as lowercase = ("_BESClient_Report_MinimumInterval") as lowercase) of it)of bes computers

Use Case: I want to see how many machines are reporting to a given relay...
Q:(it, multiplicity of it) of unique values of relay servers of bes computers whose (exist relay server of it)

Use Case: I want to know all the client settings on my relays and I want to know how many relays machines have them
Q:(it, multiplicity of it) of unique values of names of client settings of bes computers whose (exist client settings of it and relay server flag of it)

Use Case I want to see all settings w/ values as an aggregate
Q:(it, multiplicity of it) of unique values of (name of it & "=" & value of it) of client settings whose (1=1) of bes computers whose (exist client settings of it)

Use Case I want to see all relay settings w/ values as an aggregate
Q:(it, multiplicity of it) of unique values of (name of it & "=" & value of it) of client settings whose (name of it contains "_Relay") of bes computers whose (exist client settings of it)

Sets \ Combination of like types

Technique - The use of sets to return data of like types can be used to go to the well once for more interesting data...

Using Sets we can return multiple queries as long as they return the same type
Good ex: 1;2;3;4
Bad ex: 1;2;3;4;"y"

We can to this with arrays too
"a","b",1,2;
"c","d",3,4

Sets \ Combination of like types continued…

Use case: I want to see how many Multi action groups I have with over 100,150,and 200
number of bes actions whose ((multiple flag of it) and (number of member actions of it > 50) and (state of it = "Open")) ;
number of bes actions whose ((multiple flag of it) and (number of member actions of it > 100) and (state of it = "Open")) ;
number of bes actions whose ((multiple flag of it) and (number of member actions of it > 200) and (state of it = "Open"))

(name of it, name of issuer of it) of bes actions whose ((multiple flag of it) and (number of member actions of it > 50) and (state of it = "Open")) ;
(name of it, name of issuer of it) of bes actions whose ((multiple flag of it) and (number of member actions of it > 100) and (state of it = "Open")) ;
(name of it, name of issuer of it) of bes actions whose ((multiple flag of it) and (number of member actions of it > 200) and (state of it = "Open"))

Size of Intersection \ Group Reporting

```
(((
(name of it) as string)
, ((id of it) as string)
, ((display name of site of it) as string)) of it
, (size of (intersection of (applicable computer set of it;member sets of bes computer groups
whose ((id of it) as string = "13189" AND name of it = "Mod 1 Group")))) as string
, (size of (intersection of (applicable computer set of it;member sets of bes computer groups
whose ((id of it) as string = "13190" AND name of it = "Mod 2 Group")))) as string
, (size of (intersection of (applicable computer set of it;member sets of bes computer groups
whose ((id of it) as string = "13474" AND name of it = "Mod Group 1")))) as string
, (size of (intersection of (applicable computer set of it;member sets of bes computer groups
whose ((id of it) as string = "13475" AND name of it = "Mod Group 2")))) as string
)

of bes fixlets
whose (applicable computer count of it > 0
and source of it as lowercase contains "microsoft"
and name of it as lowercase does not contain "corrupt patch"
and not exist mime field "x-fixlet-superseded" of it and analysis flag of it = False
and display name of site of it contains "Patches for Windows"
and exist source release date whose (it as string ends with "2022") of it
)
```

Concepts

- Google with Session Relevance
- Present a link
- Present a Command
- Relevance and HTML
- The concept of time \ alerting

Google with Session Relevance

BigFix

//Technique - Lets use session relevance as a search engine... "Google with Session Relevance"

On a fixlet

(id of it, name of it) of bes fixlets whose (custom flag of it AND exist action whose (exist script whose (it contains "notify client forcerefresh") of it) of it)

On a action

(id of it, name of it) of bes actions whose (((exist action script of it and (action script of it as lowercase contains "notify client forcerefresh"))))

Now lets join it up using what we learned about sets...

("Fixlet",id of it, name of it) of bes fixlets whose (custom flag of it AND exist action whose (exist script whose (it contains "notify client forcerefresh") of it) of it)
;
("Action", id of it,name of it) of bes actions whose (((exist action script of it and (action script of it as lowercase contains "notify client forcerefresh"))))

Present a link

Building on the prior use case...
Technique - We can integrate html as a return in session relevance, in pres debugger this is relatively useful

Use Case: I want to see all actionsripts that reference a particular string
Using session rel to look for signature in action
Leveraging html as link & br

(link of it) of bes fixlets whose (custom flag of it AND exist action whose (exist script whose (it contains "notify client forcerefresh") of it) of it)
;
(link of it) of bes actions whose (((exist action script of it and (action script of it as lowercase contains "notify client forcerefresh"))))

Present a command

Building on the prior use case...

We presented a link last time, now lets present a command…

Use Case: I want to Export \ Backup content within a site named X

("iem.exe get fixlet/custom/" & name of site of it & "/" & ((id of it) as string) & " >" & ((id of it) as string) & ".bes") of fixlets of bes custom sites whose (name of it = "CS_Testing_and_dev")

Return HTML

```
//Building on the prior use case...
I want to get more information data in a table view

table of concatenation of ((
trs of
(
td of (link of it )
& td of ((id of it) as string)
& td of ((name of issuer of it) as string)
)
 of bes fixlets whose
 (custom flag of it AND exist action whose (exist script whose (it contains "notify client forcerefresh") of it) of it )
))
```

Reports & Queries Referenced \ including this will be provided
* w/ no warranty or support…

The concept of time \ alerting

New External Content within last 48 hours
https://raw.githubusercontent.com/bigfix/content/master/reports/Scheduled%20Notification%20-%20External%20Content%20Published%20within%20last%2048%20hours.txt

Action Taken within Force Refresh
https://raw.githubusercontent.com/bigfix/content/master/reports/Scheduled%20Notification%20-%20Warning%20Customer%20has%20taken%20actions%20containing%20notify%20client%20forcerefresh.txt

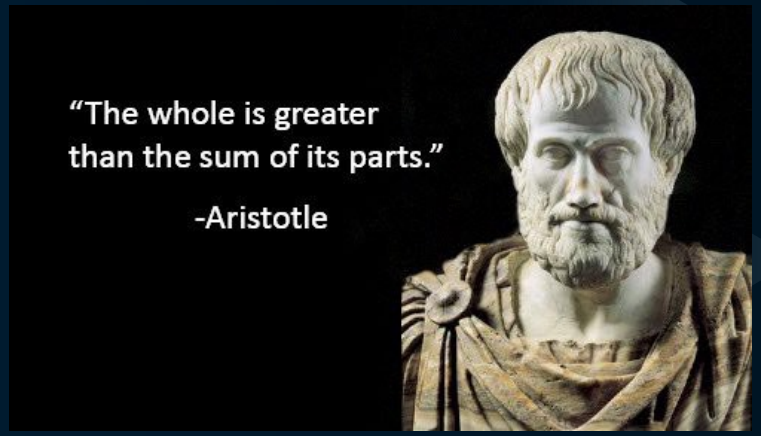
Monitor Alterations to Components of Action \ Relevance (Example SCM)
https://raw.githubusercontent.com/bigfix/content/master/reports/Scheduled%20Notification%20-%20SCM%20Content%20Inventory.txt

- Need to alter whose to 30 days for demonstration…

Custom Content Published Yesterday
https://raw.githubusercontent.com/bigfix/content/master/reports/Scheduled%20Notification%20-%20New%20Custom%20Content%20Published%20Yesterday.txt

* Need to alter whose to 1 day…

Taking it Further w/ JS



Recent Content Released in last 10 days
https://github.com/bigfix/content/blob/master/reports/WRExample-Content-Released-in-last-10days.txt

Content Search (search for action signature)
https://raw.githubusercontent.com/bigfix/content/master/reports/WRExample-Content-Search-Utility.txt

- notify client ForceRefresh
- _BESClient_Register_Affiliation_SeekList

Recent Internal Ask \ Conti Malware associated content.
https://raw.githubusercontent.com/bigfix/content/master/reports/WRExample-ContiMalware.txt

Reference Reports

https://github.com/bigfix/content/tree/master/reports

BigFix

QNA

HCL SOFTWARE