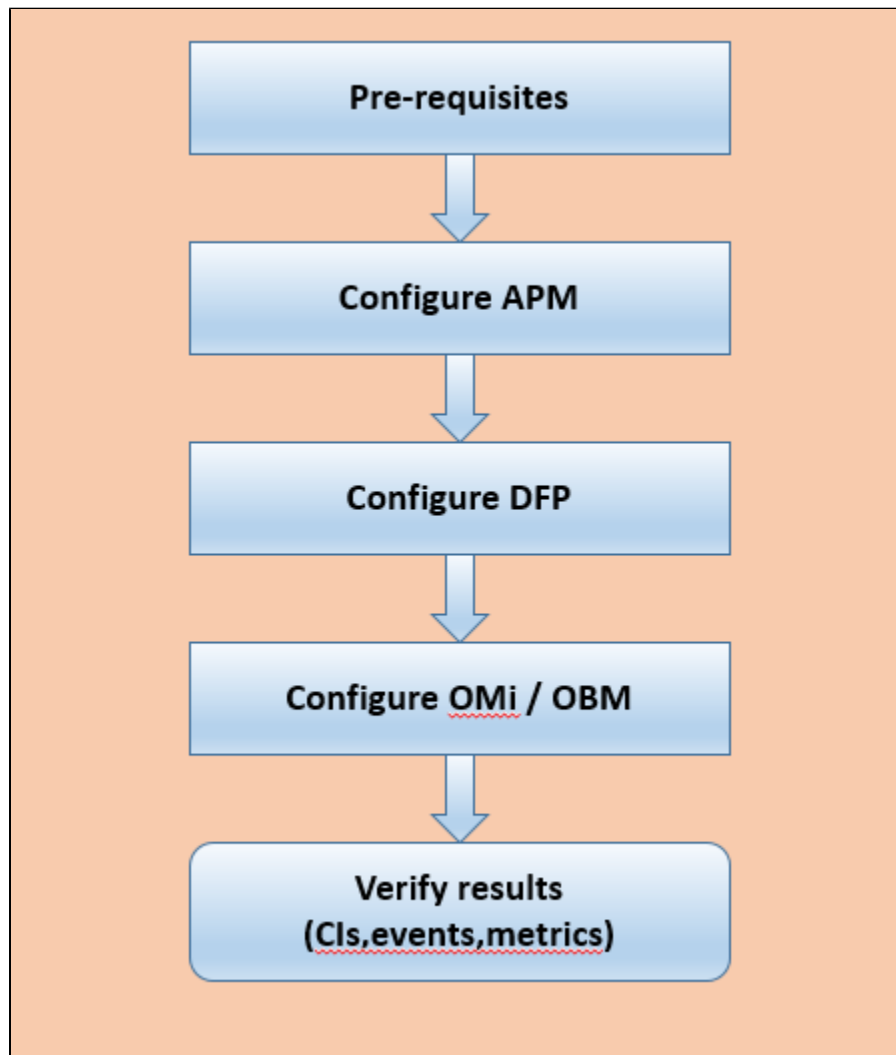


Tips for APM integration with OMi / OBM / OBM container

- Integration of APM in OMi/OBM workflow
- Pre-requisites
- APM Configuration
- DFP Configuration
- Verify the CIs synced from APM to OMi / OBM
- Troubleshooting

Integration of APM in OMi/OBM workflow



Pre-requisites

1. 1. Round trip

Its mandatory for both APM and OMi should have 0ms round trip. If they are remotely located the integration will fail . e.g.

```

C:\Users\Administrator>ping 16.60.160.64

Pinging 16.60.160.64 with 32 bytes of data:
Reply from 16.60.160.64: bytes=32 time=164ms TTL=116
Reply from 16.60.160.64: bytes=32 time=164ms TTL=116
Reply from 16.60.160.64: bytes=32 time=165ms TTL=116
Reply from 16.60.160.64: bytes=32 time=165ms TTL=116

Ping statistics for 16.60.160.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 164ms, Maximum = 165ms, Average = 164ms

C:\Users\Administrator>ping iwfv07056.hpeswlab.net

Pinging iwfv07056.hpeswlab.net [16.166.98.7] with 32 bytes of data:
Reply from 16.166.98.7: bytes=32 time<1ms TTL=127
Reply from 16.166.98.7: bytes=32 time<1ms TTL=127
Reply from 16.166.98.7: bytes=32 time=1ms TTL=127
Reply from 16.166.98.7: bytes=32 time=2ms TTL=127

Ping statistics for 16.166.98.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

```

1. 2. Import the certificates

It is mandatory to exchange the CA certificates between the APM and OBM for successful connection.

APM --> We need to import the OBM's CA certificate or Server certificate (if it is self-signed) to APM's JRE and JRE64 truststore and restart APM services for both GW, DPS.

OBM --> We need to import the APM's CA certificate or Server certificate (if it is self-signed) to OBM's JRE truststore and restart OBM services for both GW, DPS.

Note --> the trust store is located under <APM/OBM install dir >/JRE/lib/security/cacerts

Note --> we can use any third party tools like "keyStore Explorer" , "portecle-1.7" to import the certs

Container Certificate export and import --> the commands to export and import certs to OBM container are below

On Master Node

a. `kubectl exec -ti omi-0 -n opsbridge1 -c omi bash`

b. `/opt/OV/bin/ovcert -list`

c. `/opt/OV/bin/ovcert -exporttrusted -file <location of file> -alias <trusted certificate name>`

For example:

`/opt/OV/bin/ovcert -exporttrusted -file /tmp/trust.pem -alias CA_c37b8bd5-5b9b-4626-be18-c78ef76040e5_2048`

d. `exit`

e. `kubectl cp opsbridge1/omi-0:/tmp/newCA.pem /tmp -c omi`

APM Configuration

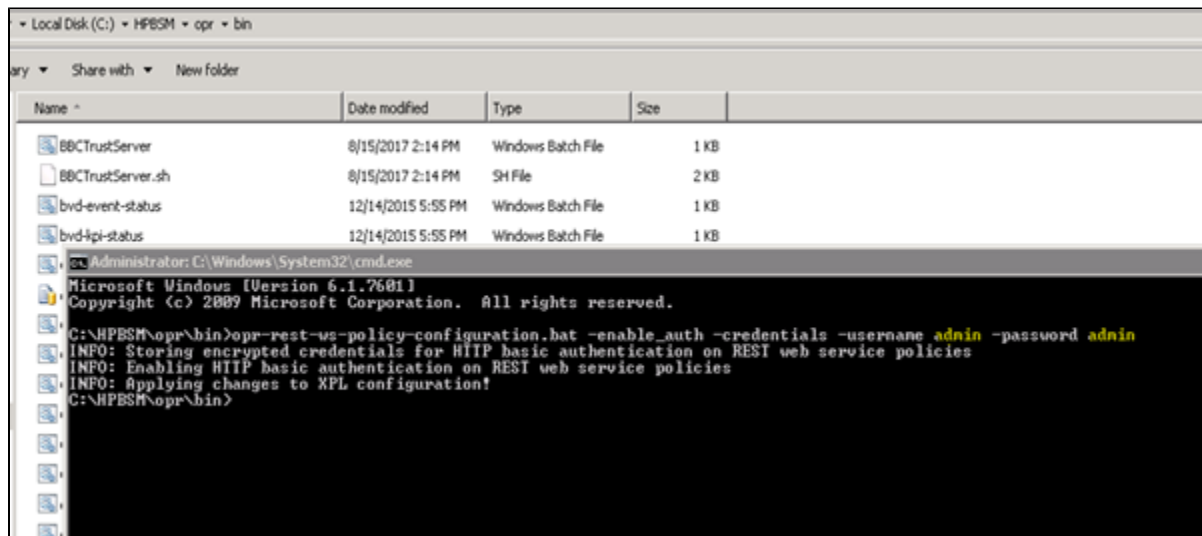
1. 1. Update the integration user in APM infra settings

Create the integration in omi through command line utility **opr-rest-ws-policy-configuration.bat [sh]**

e.g. we can use any name for the user

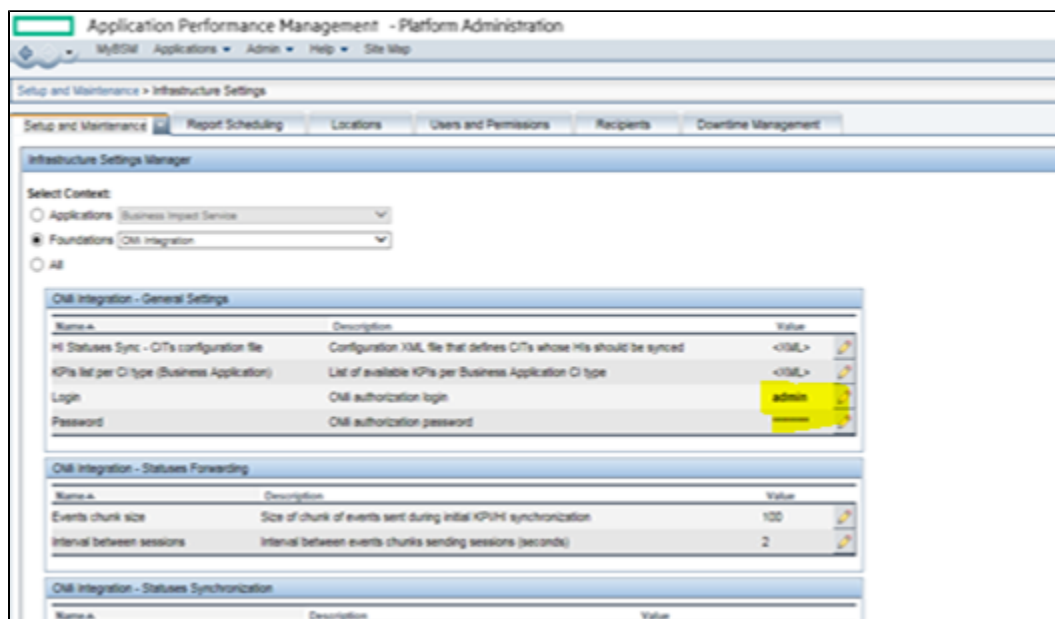
C:\HPBSM\opr\bin>

opr-rest-ws-policy-configuration.bat -enable_auth -credentials -username intuser -password intuser



The same user and password should be updated to the APM's infrastructure settings à

APM -> Admin -> Platform -> Infrastructure Settings -> Foundations select "OMi Integration"

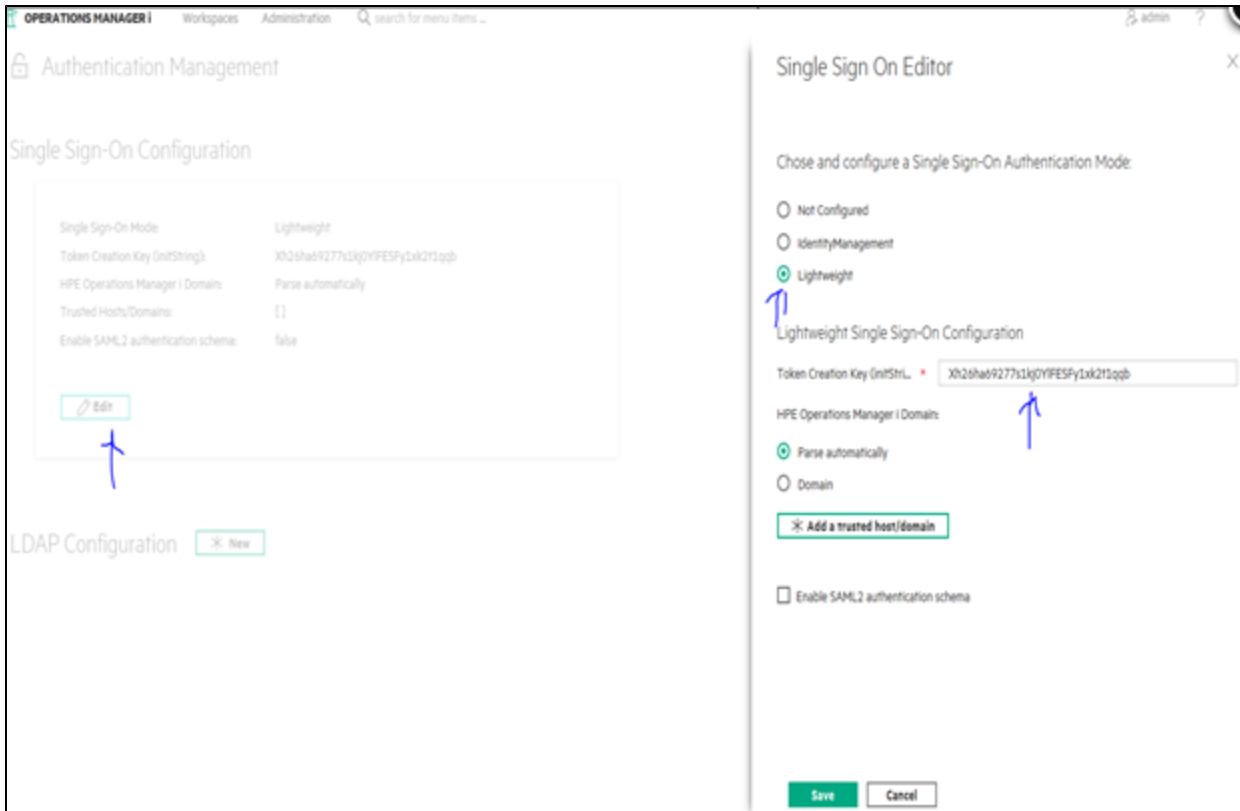


1. 2. Update the LWSSO from OMi to APM

Copy LW SSO from Omi and paste it APM LW SSO through jmx .

To get the LWSSO init string from OMi / OBM

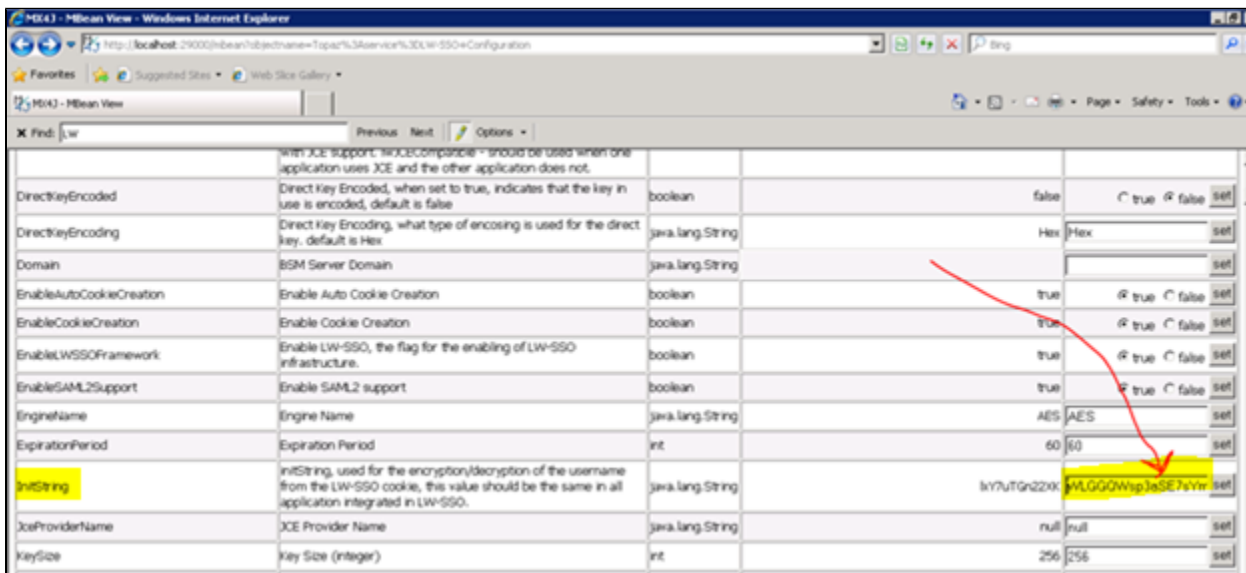
OMi -> Administration -> Users -> Authentication Management



To copy the LWSSO init string in APM

Login into the JMX using any web browser in the Gateway machine using <http://localhost:29000/>

Search for "LW-SSO configuration" and then search for "InitString" and paste it there



Note :- The LW-SSO won't work if APM and OBM are not using same protocol (http or https).

DFP Configuration

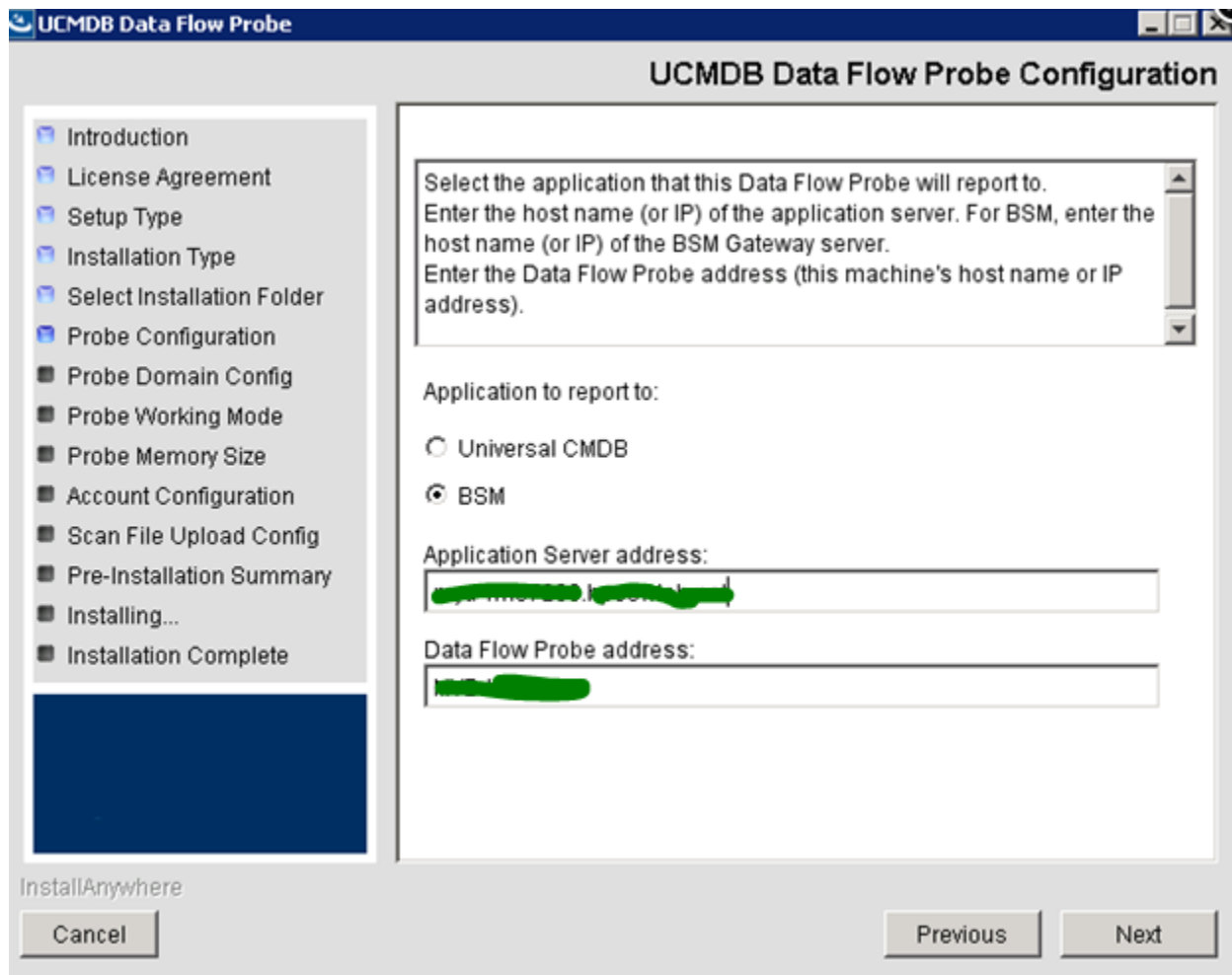
Pre-check:

1. Make sure the Data flow probe version and OBM RTSM version are same, else the integration will fail.
1. *Only if TLS is enabled in OBM* à If OBM is configured to use HTTPS, enable TLS in the Data Flow Probe as well:
 - 2.1 Open the file <Data Flow Probe install folder>/conf/DataFlowProbe.properties.
 - 2.2 Change the property appilog.agent.probe.protocol from HTTP to HTTPS.
 - 2.3 Change the property serverPortHttps from 8443 to 443. (only for containerized Omi)

Installation:

Click on Next >>Next until we get this screen:

Select BSM (i.e this is an option before APM-Omi split)



Provide the **Omi** FQDN in Application server address:

Click on next and make sure the test connection not thrown any error:

Proceed with next steps, when it asks for password, try the password which you can remember

If the system didn't accept your customized password, do not waste time just use: **Password_123** (p uppercase), (Make a note in notepad and save it in desktop for reference) and continue with installation.

Import OMi Certificate info Probe: (these steps are from OBM server)

Classic Omi deployment:

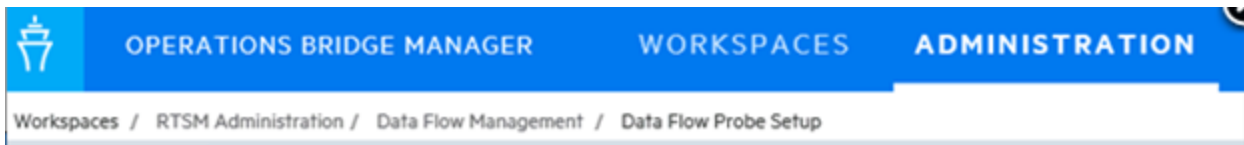
1. Access the Omi page then download the certificate.
2. Place it in DFP server
3. In DFP server launch cmd prompt and run the below command, by updating the <> values.
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\security\cacerts -file <certificate relative/full path> -alias <aliasname>.cer
4. If it asks for password, then provide our keystore password i.e **changeit**
5. Navigate to C:\ProgramData\Microsoft\Windows\Start Menu\Programs\UCMDB
6. Start the service in console mode
7. Open WrapperProbeGw log and verify that no error occurred (c:\hp\UCMDB\DataFlowProbe\runtime\log\WrapperProbeGw)
8. Type yes, to make this certificate as trusted. Then we should get the text as **"Certificate was added to keystore"**

Containerized Omi Deployment:

1. Run this command: openssl s_client -showcerts -servername <FQDN_Omi server> -connect <FQDN_Omi server>:443 </dev/null
2. From the command output, copy the content beginning with -----BEGIN CERTIFICATE until END CERTIFICATE----- and copy it into a file. Save the file with the name certificate.pem
3. Convert the file into the .der format: openssl x509 -outform der -in certificate.pem -out certificate.der
4. From DFP machine >> Import the certificate into JRE's trust store: <Data Flow Probe install folder>/bin/jre/bin/keytool -import -trustcacerts -file certificate.der -alias <FQDN_Omi server> -keystore <Data Flow Probe install folder>/bin/jre/lib/security/cacerts
5. If it asks for password, type **changeit**
6. Type yes, to make this certificate as trusted. Then we should get the text as **"Certificate was added to keystore"**
7. Navigate to C:\ProgramData\Microsoft\Windows\Start Menu\Programs\UCMDB
8. start the service in console mode
9. open WrapperProbeGw log and verify that no error occurred (c:\hp\UCMDB\DataFlowProbe\runtime\log\WrapperProbeGw)

Verify the probe in Omi:

Navigate to DFP setup page

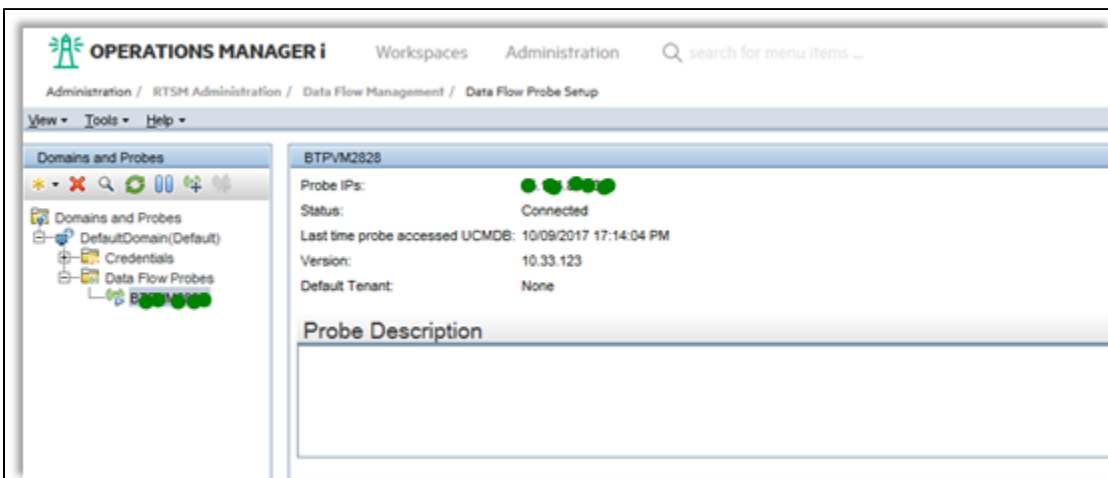


Verify that, DefaultDomain(Default) should get displayed and the DFP Host & IP should read under domains and probes table

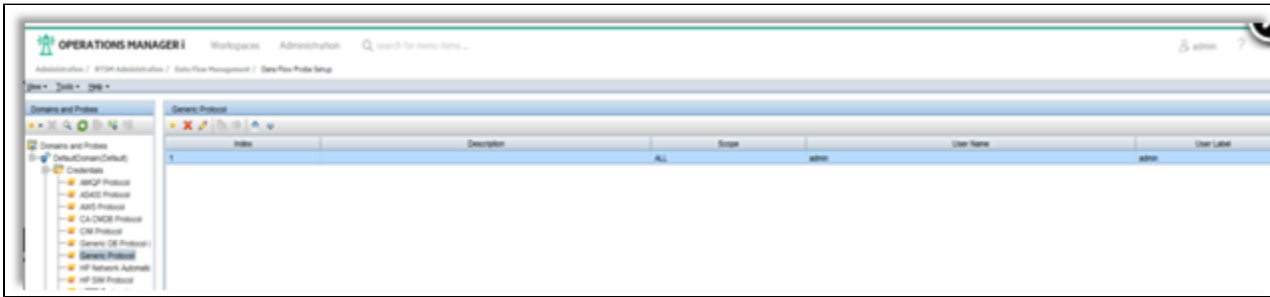
The final output should look like the below and the DFP should show as "Connected" status like below

The screenshot shows a table titled 'Data Flow Probes' under the 'Domains and Probes' section. The table has four columns: 'Probe Name', 'IP', 'Status', and 'Last Access time'. A single row is visible with the following data:

Probe Name	IP	Status	Last Access time
MYD-VM07773	16.59.62.19	Connected	02/14/2018 21:28:15 PM



Under credentials -> generic protocol -> create new credential with user “admin “ and password “admin”



OMi / OBM Configuration

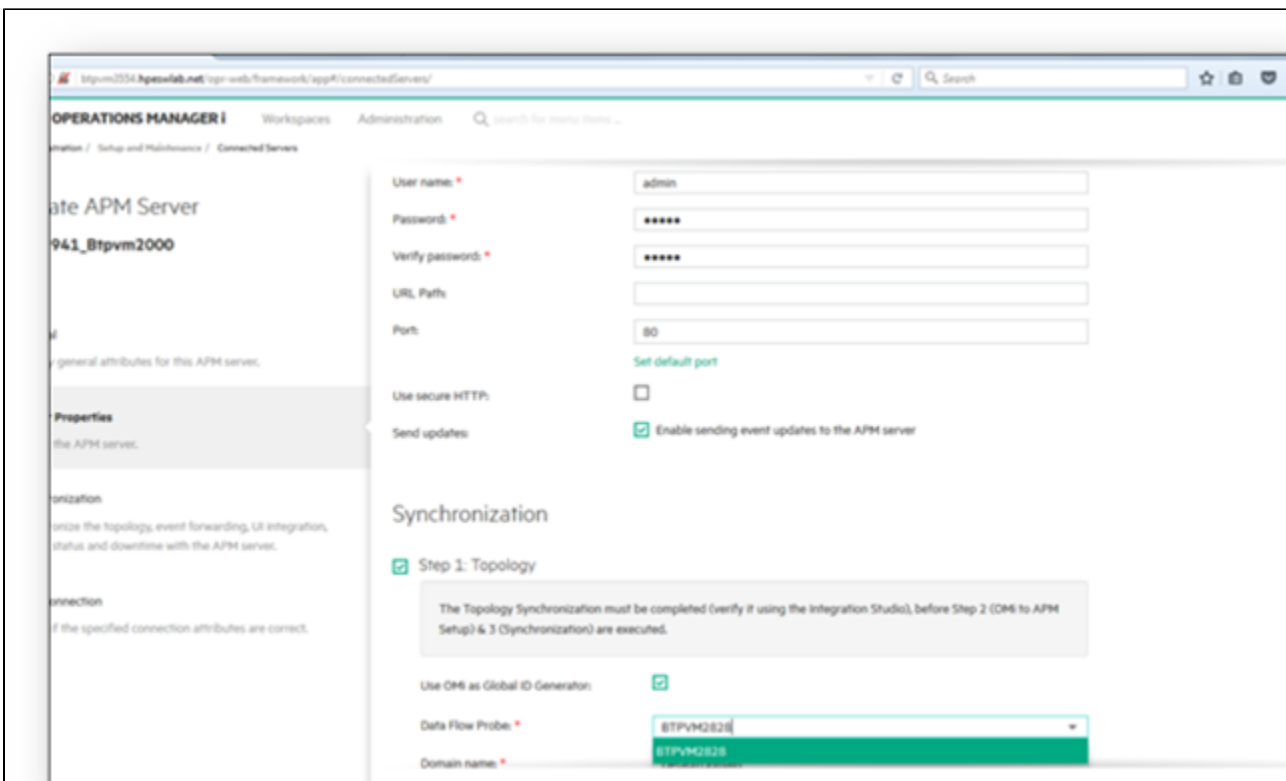
Follow the 3 steps and do it one by one and then deploy “OprEvent” policy on OBM

- Check topology first
- OMi to APM Setup
- Synchronization

Note -> the test connection button does not work and we have open defect for it and we can proceed without using it .the button is redundant and we will remove it soon.

Note -> ensure all the prerequisites are taken care that are mentioned above before adding the APM

Select the DFP that was configured in previous step . Select “Use OMi as Global ID generator” based on your use case.



Below are success messages for each step . Please ensure it is done one by one only.

OPERATIONS MANAGER i

WorkspacesAdministration

search for menu items ...

Administration / Setup and Maintenance / Connected Servers

Connected Servers

All

Operations Manager i

Operations Manager for UNIX

Operations Manager for Windows

External Event Processing

Operations Connector

ArcSight

SiteScope

APM

Business Value Dashboard

Alias

APM941_Btpvm2000

Raghu Test

Trouble Ticket System

Incomplete

Status: succeeded

Message: Topology synchronization is succeeded.

Type: APM

ID: 46b9befe-536c-4509-8b09-91158da13429

Active: ✓

Send updates: Yes

Name: APM941_Btpvm2000

Fully qualified domain name: btpvm2000.hpeswlab.net

Description: Raghu Test

Edit

OPERATIONS MANAGER i

WorkspacesAdministration

search for menu items ...

Administration / Setup and Maintenance / Connected Servers

Connected Servers

All

Operations Manager i

Operations Manager for UNIX

Operations Manager for Windows

External Event Processing

Operations Connector

ArcSight

SiteScope

APM

Business Value Dashboard

Alias

APM941_Btpvm2000

Raghu Test

Trouble Ticket System

Incomplete

Status: succeeded

Message: The Deployment of the enrichment rule succeeded.Download of APM UI components succeeded.

Type: APM

ID: 46b9befe-536c-4509-8b09-91158da13429

Active: ✓

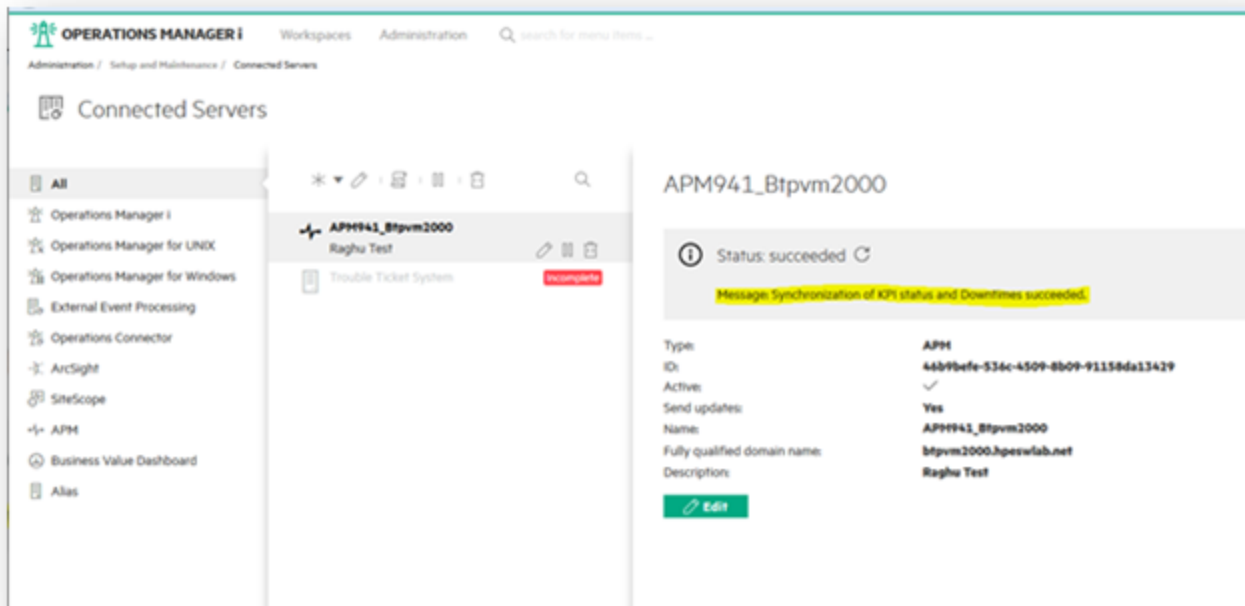
Send updates: Yes

Name: APM941_Btpvm2000

Fully qualified domain name: btpvm2000.hpeswlab.net

Description: Raghu Test

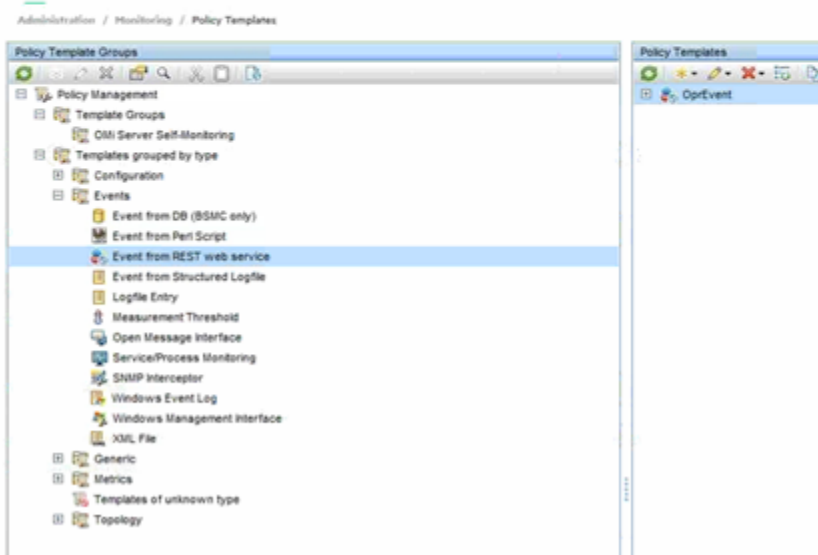
Edit



Deploy the "OprEvent" policy from OBM / OMi

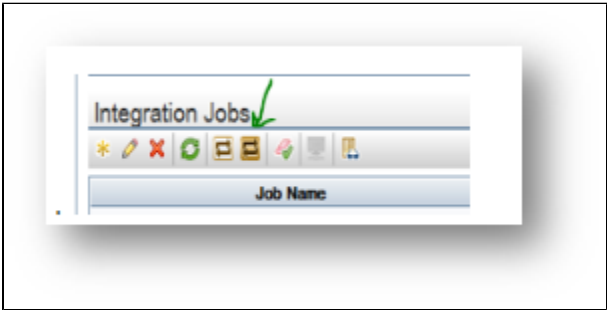
Deploy the "OprEvent" policy

Omi10 > Administration > Monitoring > Policy templates



Verify the CIs synced from APM to OMi / OBM

go to RTSM -> integration studio (by default the automation sync frequency is 15 mins , in case you want to see the CIs synched asap then click on the "Synchronize" button .



OPERATIONS MANAGER i Workspaces Administration search for menu items ... admin

Administration / RTSM Administration / Data Flow Management / Integration Studio

Integration Point

APM2COM APM541_Bpm2000 Population jobs update the local CMDB with CI Types and attributes from an external data repository

Integration Jobs

Job Name	Status	Start Time	Finish Time
sync_continuous	Did not run		
sync_init	Completed successfully	Mon Oct 9 2017 08:38 PM IST	Mon Oct 9 2017 08:38 PM IST

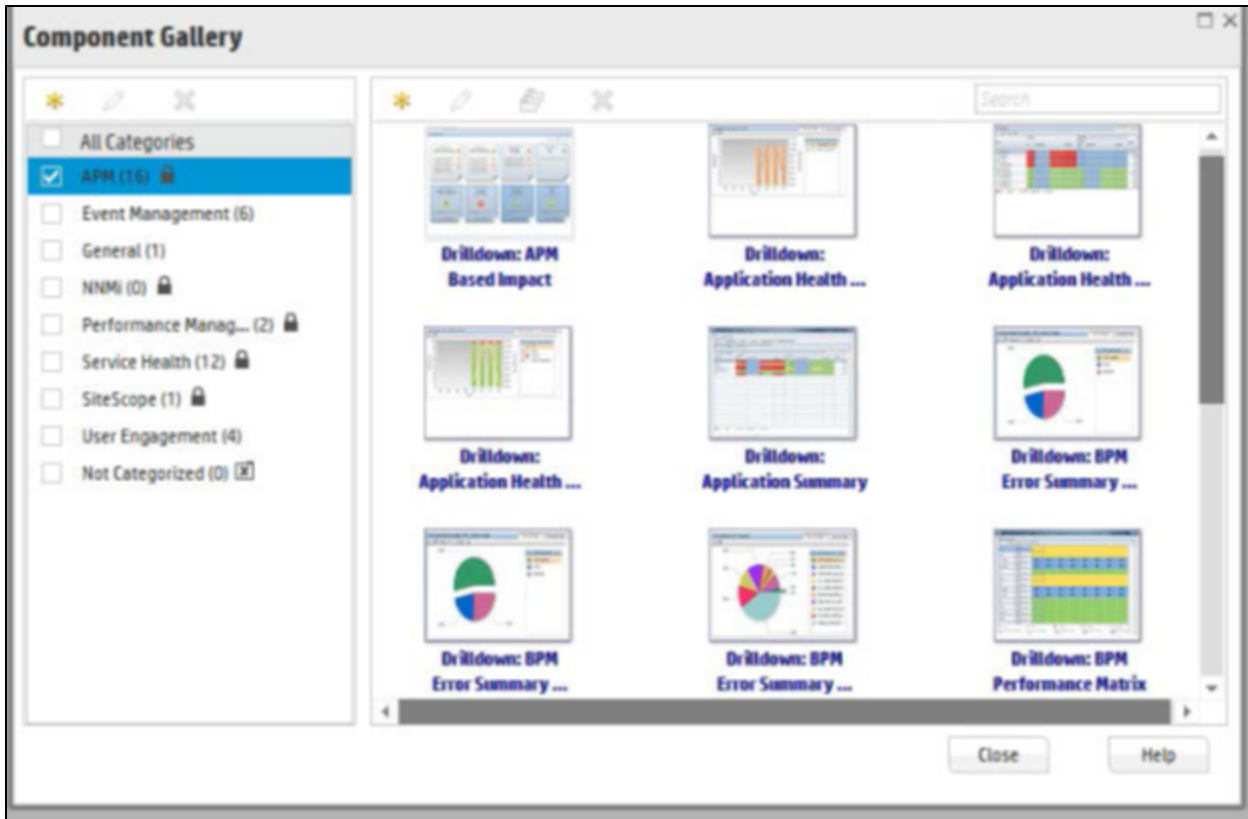
Statistics Query Status

Filter: Time Range[All]

CI Type	Created	Updated	Deleted	Failed
Business-Application	4	0	0	0
Collection	4	0	0	0
Containment	4	0	0	0
Ownership	2	0	0	0
SiteScope Group	5	0	0	0
SiteScope Measurement Group	2	0	0	0
SiteScope Profile	2	0	0	0
Unix	1	0	0	0
Windows	0	1	0	0
Total	24	1	0	0

Last Updated: 10/09/2017 20:28:49 PM (Valid to: 10/09/2017 20:38:50 PM)

Create some APM reports in OMi workspace gallery and check for APM reports in OMi /OBM



Troubleshooting

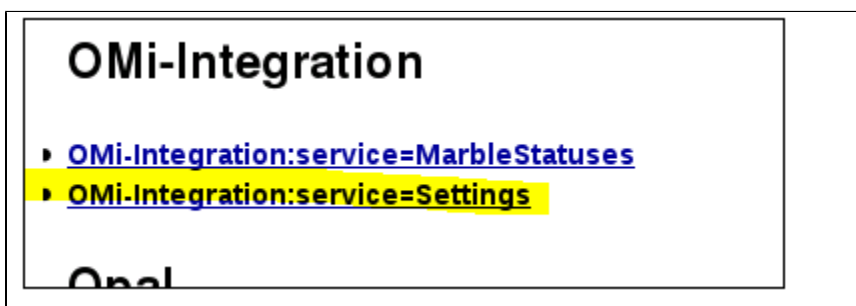
1. APM is on HTTP and OBM on HTTPS and events are not created in OBM -->

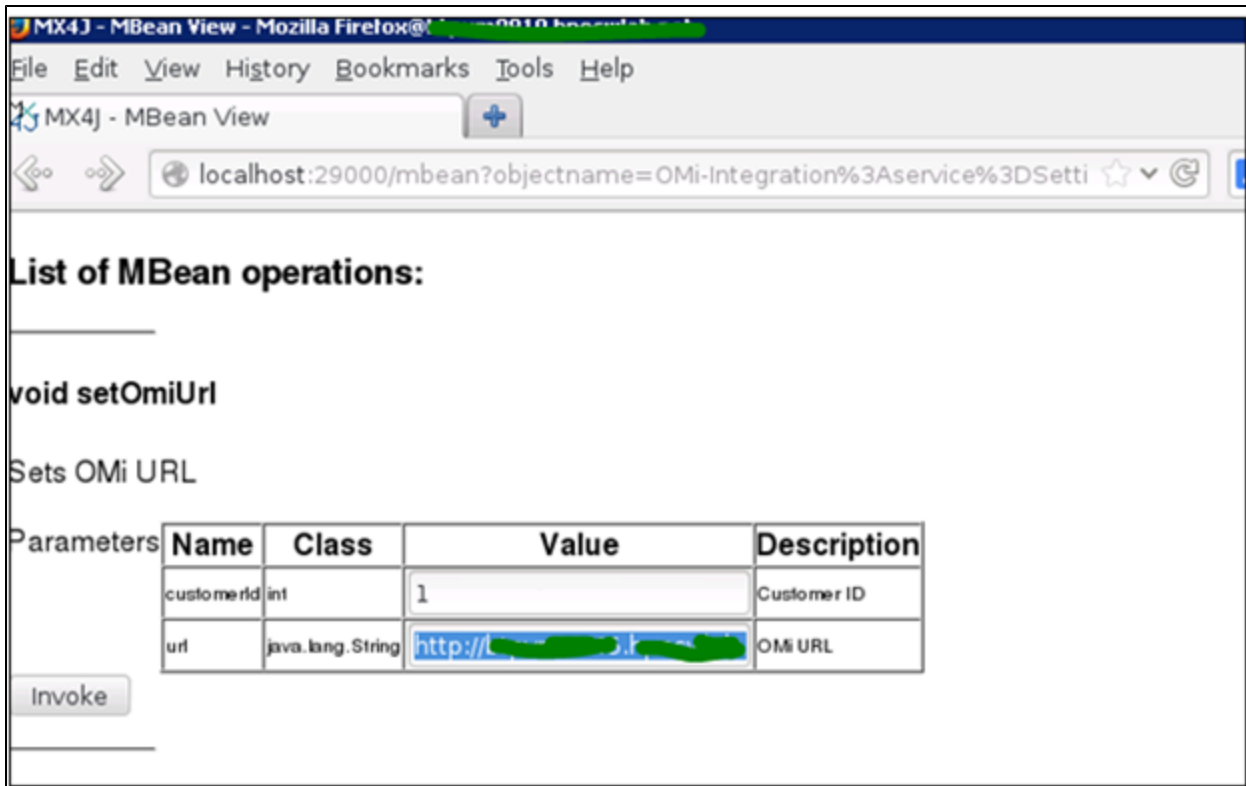
- check if the REST API on the OMi server is working fine using URL [http\(s\)://<OMi / OBM :30005/bsmc/rest/events/OprEvent](http(s)://<OMi / OBM :30005/bsmc/rest/events/OprEvent)
- By default the OMi event channel is https, we need to make it http by changing in the below JMX in the gateway of APM under OMi Integra

setOmiURL

Customer id -> 1

OMi URL à <http://<omiHostname>.hpeswlab.net:30005>





To confirm if it is set properly or not . check

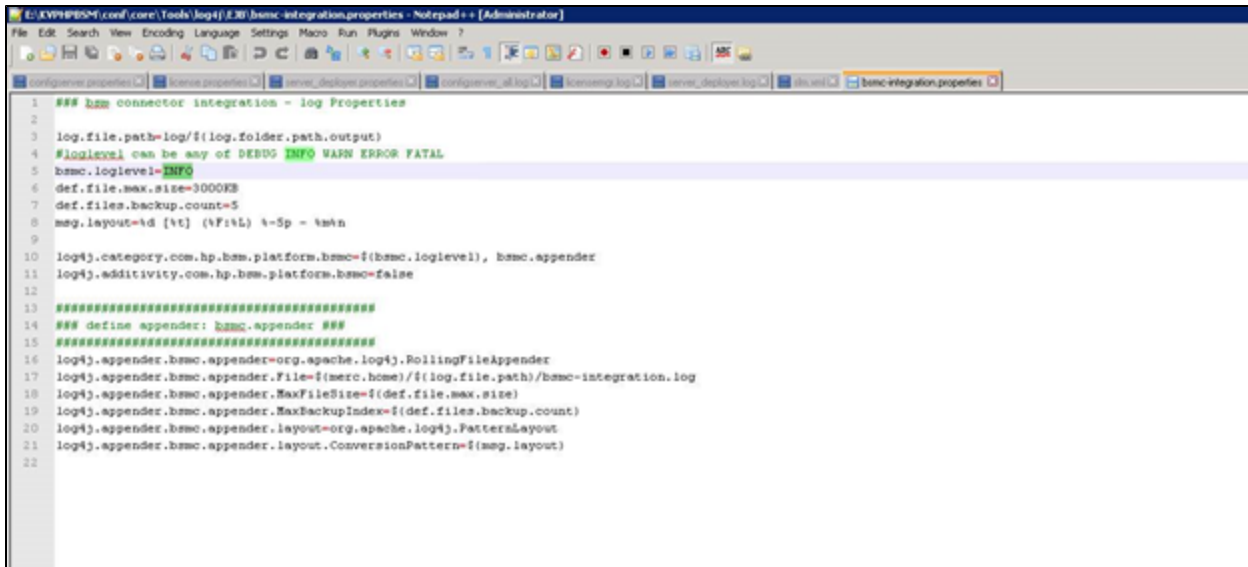
java.lang.String getOmiUrl



2. Logs ==>

APM side

For details logs first make the bsmc-integration.log to DEBUG using below



```
1 ### bsmc connector integration - log Properties
2
3 log.file.path=log/${log.folder.path.output}
4 #log.level can be any of DEBUG INFO WARN ERROR FATAL
5 bsmc.log.level=INFO
6 def.file.max.size=3000KB
7 def.files.backup.count=5
8 msg.layout=%d [%t] (%F:%L) %-5p - %m%n
9
10 log4j.category.com.hp.bsmc.platform.bsmc=${bsmc.log.level}, bsmc.appender
11 log4j.additivity.com.hp.bsmc.platform.bsmc=false
12
13 #####
14 ### define appender: bsmc, appender ###
15 #####
16 log4j.appender.bsmc.appender=org.apache.log4j.RollingFileAppender
17 log4j.appender.bsmc.appender.File=${merc.bmc}/${log.file.path}/bsmc-integration.log
18 log4j.appender.bsmc.appender.MaxFileSize=${def.file.max.size}
19 log4j.appender.bsmc.appender.MaxBackupIndex=${def.files.backup.count}
20 log4j.appender.bsmc.appender.layout=org.apache.log4j.PatternLayout
21 log4j.appender.bsmc.appender.layout.ConversionPattern=${msg.layout}
22
```

then you can observe the <apm>/log/marble_worker_x/bsmc-integration.log file

OMi Side -->

Check for errors in log file (<HPOMI>/log/jboss/opr-webapp.log)

Probe side --->

- C:\UCMDB\DataFlowProbe\runtime\log\ probe-error.log
- C:\UCMDB\DataFlowProbe\runtime\log\ WrapperProbeGw.log

Issue ==> If Events are not sent from APM to OMi (APM . OMi both on HTTPS)

Message

- 2018-08-09 10:47:44,745 [pool-20-thread-1] (OprEventSubmitter.java:51) **ERROR - The event has not been sent to OMI, status: 0**
- 2018-08-09 10:47:48,787 [pool-20-thread-1] (OprEventSubmitter.java:51) **ERROR - The event has not been sent to OMI, status: 0**
- 2018-08-09 10:47:48,818 [pool-20-thread-1] (OprEventSubmitter.java:51) **ERROR - The event has not been sent to OMI, status: 401**

1. In order to push events from APM to OMI 1, REST Api needs to be open. I forgot to add to troubleshooting section this morning. Many customer are facing this issue.

- 1. Port 30005 not open
- 2. Check two things make sure Oprevent Policy is deployed.

Run Ovpolicy -list

```
C:\HPBSM\opr\support>ovpolicy -list
* List installed policies for host 'localhost'.
```

Type	Name	Status	Version
le	"OMi Event Receiver Logfile"	enabled	0002.0010
le	"OMi Monitoring Automation Logfile"	enabled	0003.0000
le	"OMi Nanny Logfile"	enabled	0002.0010
le	"OMi Scripting Host Logfile"	enabled	0002.0011
letmpl	"OMi Event Receiver Logfile"	enabled	0002.0010
letmpl	"OMi Monitoring Automation Logfile"	enabled	0003.0000
letmpl	"OMi Nanny Logfile"	enabled	0002.0010
letmpl	"OMi Scripting Host Logfile"	enabled	0002.0011
monitor	"OMi Server Processes <Windows>"	enabled	0001.0000
monitor	"OMi CertMonitor"	enabled	0002.0011
monitortmpl	"OMi Server Processes <Windows>"	enabled	0001.0000
monitortmpl	"OMi CertMonitor"	enabled	0002.0011
xml-ws	"OprEvent"	enabled	0001.0000

2. Verify port is open after restarting agent

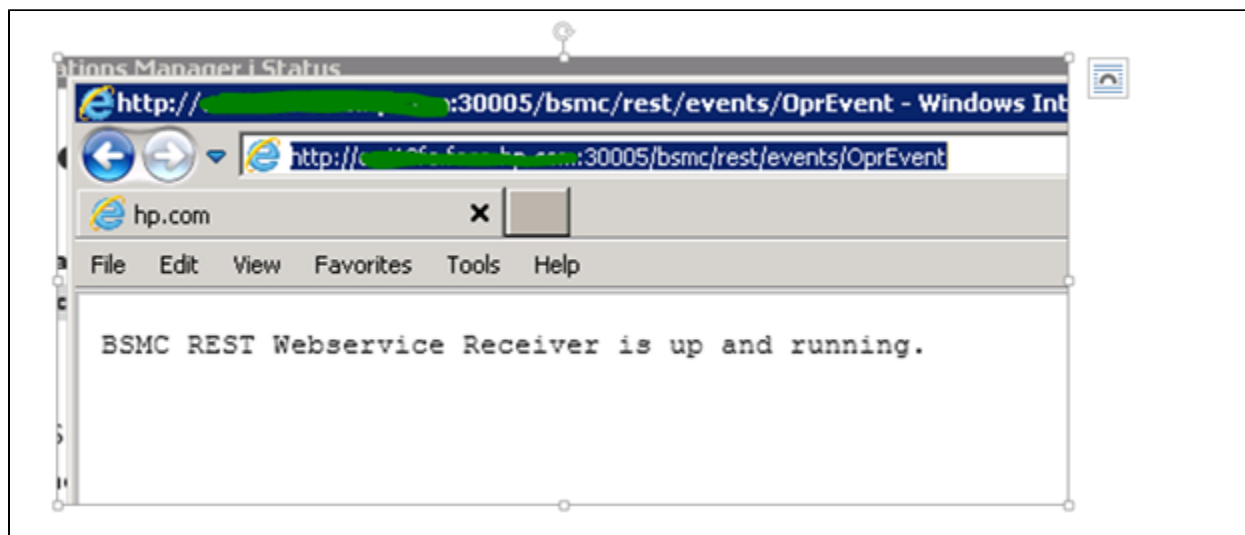
Restart Agent

opcagt -restart

>netstat -na | findstr "30005"

3. Test Your you pulled from jmx

https://omiHostname_fqdn:30005/bsmc/rest/events/OprEvent



4. if this does not come up to test

If you need disable authentication to OMI 10.70xx

C:\HPBSM\opr\bin>opr-rest-ws-policy-configuration.bat -disable_auth

opr-rest-ws-policy-configuration.bat -disable_auth

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\HPBSM\opr\bin>opr-rest-ws-policy-configuration.bat -disable_auth
INFO: Disabling HTTP basic authentication on REST web service policies
INFO: Applying changes to XPL configuration!
C:\HPBSM\opr\bin>_
```

and try again. This is just a workaround and not recommended

5. Once this works you can work on cert issue as mentioned in the pre-requisites .

Check if the issue you are facing are among the open defects (these will be fixed in Future releases of APM)

QCCR11131614 (for 9.50) Events not sent to OMi for alerts that are generated on the APM when APM , OMi are on HTTPS

QCCR11131619 (for 9.50) APM 9.50 -> Downtimes' recipients assignments are getting deleted when integrate with OBM

QCCR11131620 (for 9.50) APM9.50 ==> "removedRecipient" , "removedUser" is not appearing when recipient and users are deleted respectively

QCCR11131457 (for 9.50) APM == OMi Integration -BPM Alerts don't use the Global ID

QCCR11131362 (for 9.50) Application Health component isn't sensitive to CI Change wiring in MyBSM or OMi Workspace

QCCR11130836 (9.40) AppHealth component in OMi workspace doesn't work with wiring

QCCR11131370 (9.40) apphealth page not loading in OBM when the APM is on NON HTTPS

QCCR11131239 (9.50) Party CI not showing in EUM view in OBM