Certificate Handling for OMi in Service Provider Environments

Table of Contents:

Table of Figures:

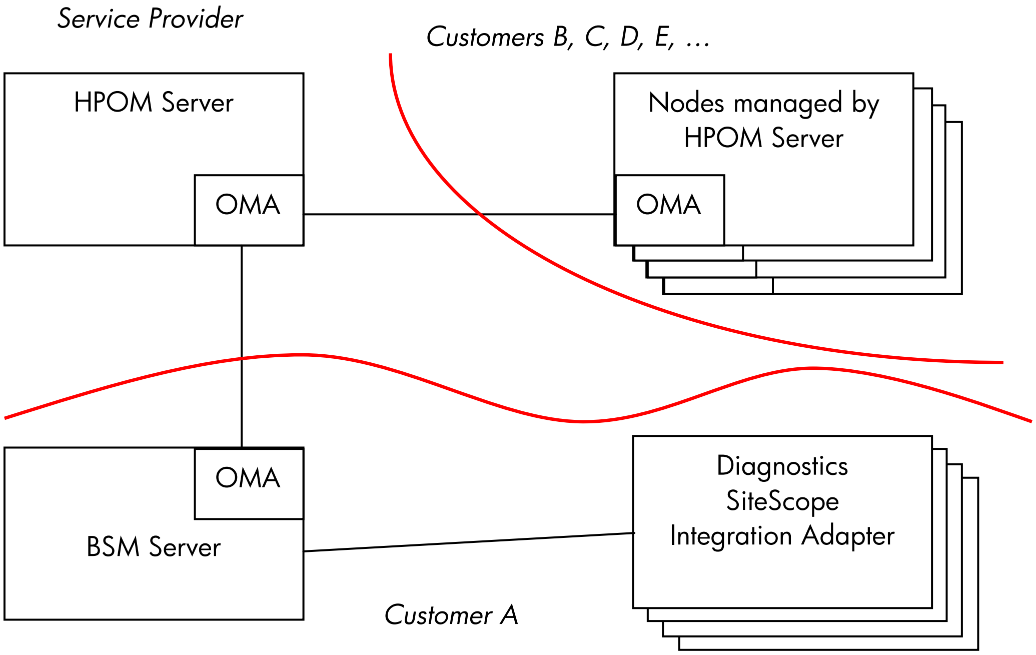
Problem Description

When operating BSM/OMi in a service provider setup together with HPOM (OMW/OML/OMU), special care is required for certificate handling. It is important not to distribute certificate trusts into the wrong organization.

The service provider operates HPOM and manages nodes for several customers. Operations Agent (OMA) is installed on all managed nodes. Customers want to install BSM on the servers managed by the service provider. These servers also have with an OMA installed.

Certificate handling as described in the BSM manual does not include this special case, but only the case where messages/events are exchanged between your BSM and HPOM instances. Using the certificate handling described in the BSM manuals, the certificate trust to the BSM system is also distributed to all other customer's (Customer B, D, E, …). This is not appropriate, and the certificate setup must be done differently to prevent the distribution of the certificate-based trust via the BSM Server to all the other customers' systems.

Figure 1: Service Provider setup



Certificates After BSM Installation

After installing BSM, the certificates on the Data Processing Server (DPS) and the Gateway Servers (GW) are issued by the BSM Certification Authority (CA) that is running on the DPS. The certificates previously issued by the monitoring HPOM server are deleted. As a result the HPOM server no longer has connection to the BSM servers. It is no longer possible to synchronize messages, execute tool or actions, or deploy policies.

If the certificates are now exchanged as described in the BSM Deployment Guide, the trusts to the BSM systems are distributed across the Service Provider's managed nodes (Customer B, C, D, E, …) when the certificates are updated on the managed nodes of HPOM (e. g. ovcert –updatetrusted) or if new certificates are created (installation of additional nodes managed by HPOM).

In addition, the trust to the HPOM systems is distributed across all Diagnostics Servers, SiteScope Servers, Integration Agents, and HPOM servers attached to the BSM servers.

After installation of BSM, the following certificates are installed on the various servers:

- **Data Processing Server Host System**

Figure 2: Certificates on DPS - Initial State

```
C:\Temp>ovcert -list
+---------------------------------------------------------+
| Keystore Content                                        |
+---------------------------------------------------------+
| Certificates:                                           |
|     d2404302-1866-755a-0d67-8bc1402a495a (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170             |
+---------------------------------------------------------+

+---------------------------------------------------------+
| Keystore Content (OVRG: server)                         |
+---------------------------------------------------------+
| Certificates:                                           |
|     7f9e9c42-19f7-755a-027c-eb7583af7170 (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170 (*)         |
+---------------------------------------------------------+
```

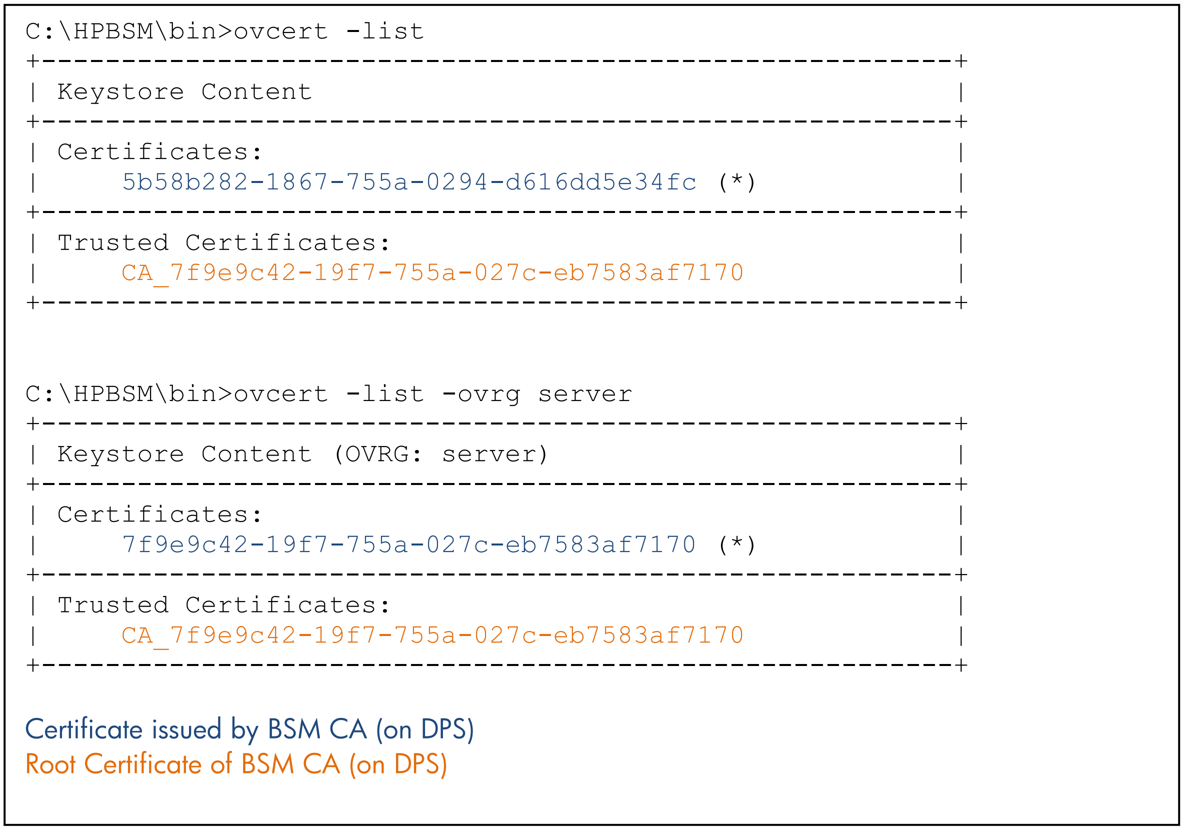
Certificate issued by BSM CA
Root Certificate of BSM CA

Certificates and trusts issued by

	Store	
	Client	Server
Certificate	BSM CA	BSM CA
Trusts	BSM CA	BSM CA
	HPOM (if installed according to manual)	HPOM (if installed according to manual)

- **Gateway Server Host Systems**

Figure 3: Certificates on Gateway Servers - Initial State



```
C:\HPBSM\bin>ovcert -list
+----------------------------------------------------------+
| Keystore Content                                         |
+----------------------------------------------------------+
| Certificates:                                            |
|     5b58b282-1867-755a-0294-d616dd5e34fc (*)             |
+----------------------------------------------------------+
| Trusted Certificates:                                    |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170              |
+----------------------------------------------------------+


C:\HPBSM\bin>ovcert -list -ovrg server
+----------------------------------------------------------+
| Keystore Content (OVRG: server)                          |
+----------------------------------------------------------+
| Certificates:                                            |
|     7f9e9c42-19f7-755a-027c-eb7583af7170 (*)             |
+----------------------------------------------------------+
| Trusted Certificates:                                    |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170              |
+----------------------------------------------------------+
```

Certificate issued by BSM CA (on DPS)

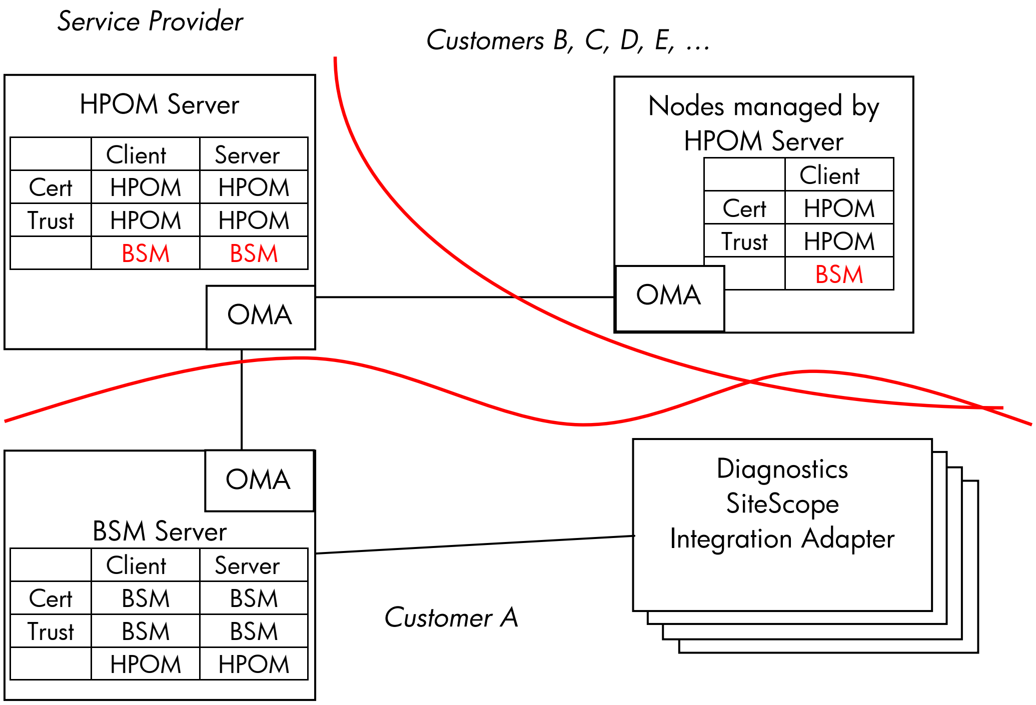
Root Certificate of BSM CA (on DPS)

Certificates and trusts issued by

	Store	
	Client	Server
Certificate	BSM CA	BSM CA
Trusts	BSM CA	BSM CA
	HPOM (if installed according to manual)	

If the configuration is done as described in the BSM Deployment Guide, the distribution of certificates is as illustrated in **Figure 4**. The red trusts are the problematic ones:

Figure 4: Certificate Setup as Described in the BSM Deployment Guide



Change Certificates

The certificate arrangement now needs to be changed so that the certificates are issued by the HPOM system and the trust to HPOM is added. Several steps are required:

- Remove certificates on the DPS and the GW from the node key stores
- Get the CoreID on the DPS and the GW
- Issue certificates on the HPOM server for the GW and the DPS
- Install issued certificates on the DPS and the GW
- Add root certificates of HPOM to the DPS and the GW

Remove Certificates from the DPS and the GW

To remove the certificates from the BSM servers, get the ID of the certificate as follows:

- On the BSM servers (DPS and GW) enter the command

  ```
  ovcert -list
  ```

- Enter the command

  ```
  ovcert -remove <ID>
  ```

  where ID is the GUID of the GUID below “Certificates” in the “Keystore Content” section (`d2404302-1866-755a-0d67-8bc1402a495a` and `5b58b282-1867-755a-0294-d616dd5e34fc` in the above example)

Get CoreID of the DPS and the GW

From command line on the DPS and GW server enter the command:

```
ovcoreid
```

The output on stdout is the coreID of the systems. These are different on the DPS and the GW.

Issue Certificates on the HPOM Server for the GW and the DPS

Issue certificates on the HPOM server for the BSM DPS & GW servers.

To issue the certificate for the DPS enter the command:

```
ovcm –issue -file DPS.cer -name <FQDN of DPS> -coreid <coreid of DPS>
```

<coreid of DPS> is the coreID received in the last step on the DPS. Provide a password. You will need the password in the next step to import the certificate on DPS server.

Copy the file DPS.cer from the HPOM server to the DPS server.

Follow the same procedure for the GW. Name the file GW.cer and use the coreID received in the last step on the GW server.

Install Issued Certificates on the DPS and the GW

To install the certificate on the BSM servers

- On the DPS enter the command:

  ```
  ovcert –importcert –file DPS.cer
  ```

  Provide the password you chose in previous step.
- On the GW enter the command:

  ```
  ovcert –importcert –file GW.cer
  ```

  Provide the password you chose in previous step.

Add the Root Certificates of HPOM to the DPS and the GW

Add the root certificates of the HPOM server to the DPS and the GW host systems as follows:

- Export root certificate on the HPOM server: `ovcert –exporttrusted –alias CA_<ovcoreid> –file HPOM.cer`
- CopytheHPOM.cer file to the DPS and the GW host systems
- On the DPS and the GW host systems, import the HPOM root certificate onto the node and the resource group “server” key store as follows:

  ```
  Ovcert –importtrusted –file HPOM.cer
  ```

  ```
  Ovcert –importtrusted –file HPOM.cer –ovrg server
  ```

Add Missing Certificates on GW Server

If the certificates on the GW server have not been installed according to the BSM documentation prior to executing the procedure described above, the certificates and trusts on the GW server as well as the client certificate in the resource group server are missing on the GW. To install these certificates, complete the following steps:

- On the DPS enter the command:

  ```
  ovcert –exporttrusted –file DPS-trust.cer
  ```

  Provide a password. You will need the password in the next step to import the certificate on GW server.
- Copy the file to the GW and enter the command:

  ```
  ovcert –importtrusted –file DPS-trust.cer
  ```

  ```
  ovcert –importtrusted –file DPS-trust.cer –ovrg server
  ```

  Ignore the warning messages during import. As the export action exported the trusts to the HPOM system as well, and these already existed on the GW, the warning notifies these already exist.

- On the GW enter the command:

  ```
  Ovcoreid
  ```

  The output on stdout is the coreID of the system.

- On the DPS enter the command:

  ```
  ovcm -issue -file GW-server.cer -name <FQDN of GW> -coreid <coreid of
  GW>
  ```

  Provide a password. You will need the password in the next step to import the certificate on GW server.
- Copy the file to the GW and enter the command:

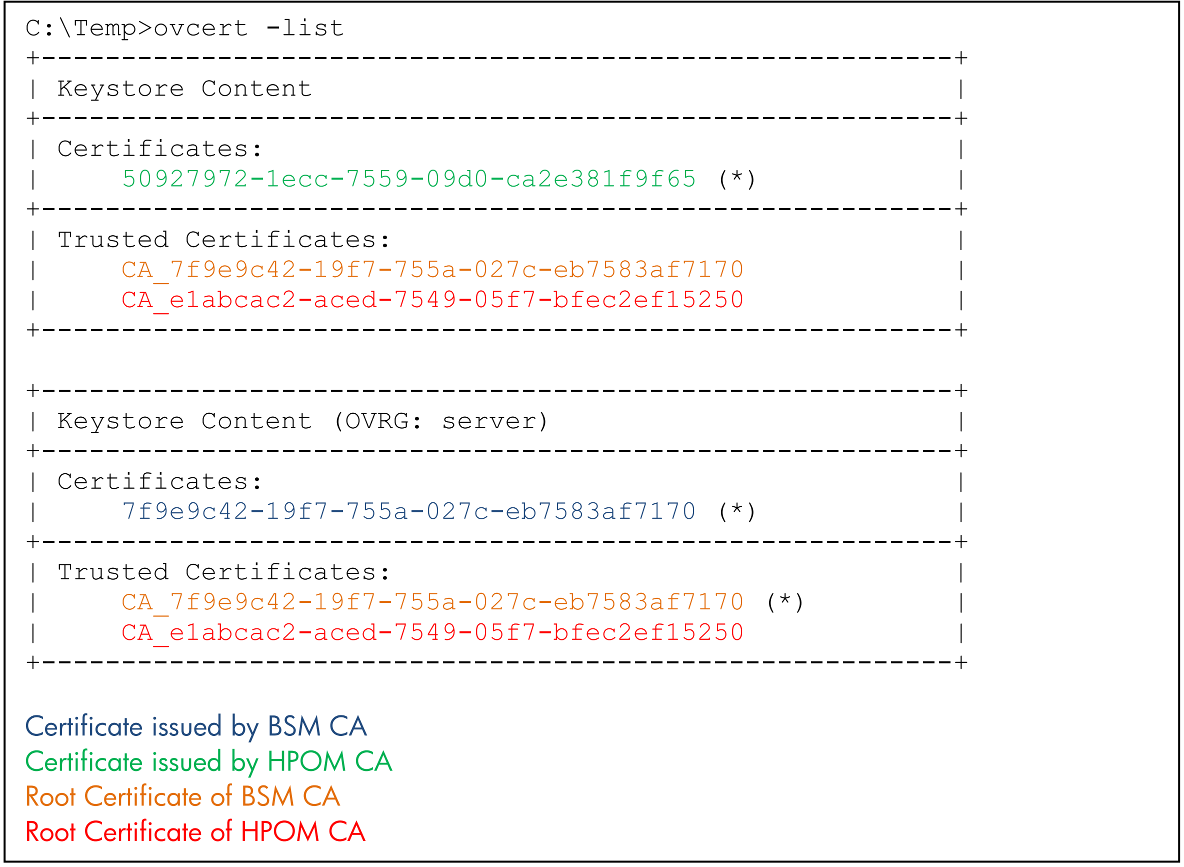
  ```
  ovcert –importcert –file GW-server.cer –ovrg server
  ```

Final State

Finally, the certificates on the BSM servers should look like this:

- **Data Processing Server Host System**

Figure 5: Certificates on DPS - Final State



```
C:\Temp>ovcert -list
+---------------------------------------------------------+
| Keystore Content                                        |
+---------------------------------------------------------+
| Certificates:                                           |
|     50927972-1ecc-7559-09d0-ca2e381f9f65 (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170             |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250             |
+---------------------------------------------------------+

+---------------------------------------------------------+
| Keystore Content (OVRG: server)                         |
+---------------------------------------------------------+
| Certificates:                                           |
|     7f9e9c42-19f7-755a-027c-eb7583af7170 (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170 (*)         |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250             |
+---------------------------------------------------------+
```

Certificate issued by BSM CA

Certificate issued by HPOM CA

Root Certificate of BSM CA

Root Certificate of HPOM CA

Certificates and trusts issued by

	Store	
	Client	Server
Certificate	HPOM CA	BSM CA
Trusts	BSM CA	BSM CA
	HPOM (if installed according to the manual)	HPOM (if installed according to the manual)

- **Gateway Server Host Systems**

Figure 6: Certificates on Gateway Servers - Final State

```
C:\HPBSM\bin>ovcert -list
+---------------------------------------------------------+
| Keystore Content                                        |
+---------------------------------------------------------+
| Certificates:                                           |
|     89688212-8b84-7554-1786-e0f606dcc6b8 (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170             |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250             |
+---------------------------------------------------------+


C:\HPBSM\bin>ovcert -list -ovrg server
+---------------------------------------------------------+
| Keystore Content (OVRG: server)                         |
+---------------------------------------------------------+
| Certificates:                                           |
|     7f9e9c42-19f7-755a-027c-eb7583af7170 (*)            |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_7f9e9c42-19f7-755a-027c-eb7583af7170             |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250             |
+---------------------------------------------------------+
```

Certificate issued by BSM CA
Certificate issued by HPOM CA
Root Certificate of BSM CA
Root Certificate of HPOM CA

Certificates and trusts issued by

	Store	
	Client	Server
Certificate	HPOM CA	BSM CA
Trusts	BSM CA	BSM CA
	HPOM (if installed according to the manual)	HPOM (if installed according to the manual)

The details of the certificates can be checked by entering the following command:

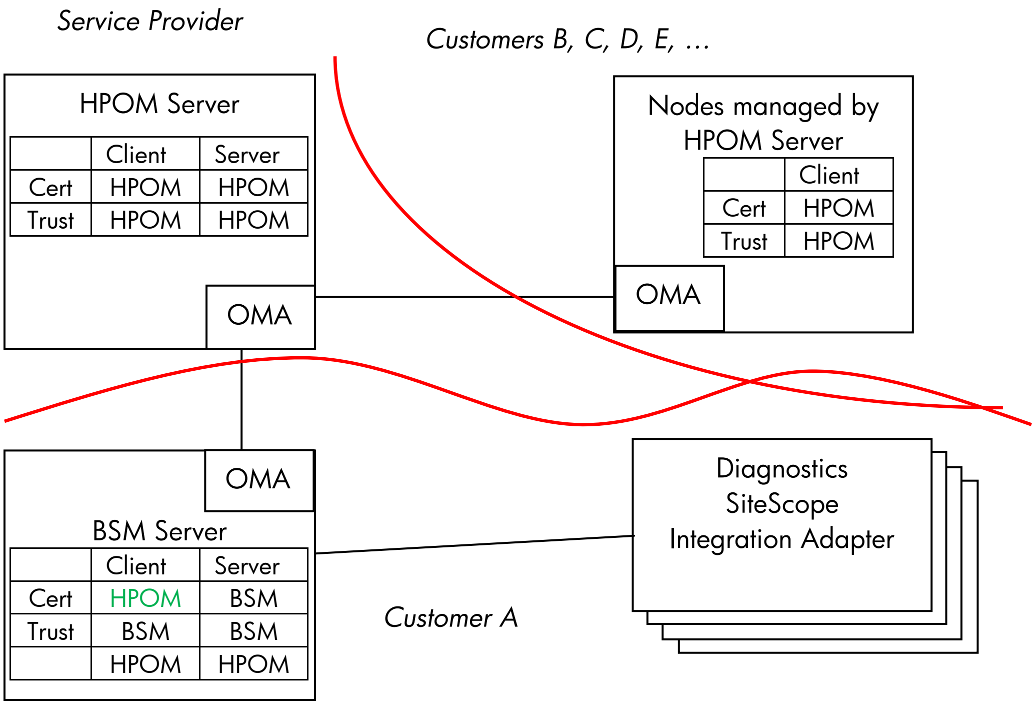
`ovcert -certinfo <Certificate_ID>`

Add the parameter "`-ovrg server`" to the above command if the certificate is in the resource group `server`.
To display the list of certificates available on the node, enter the following command:

`ovcert -list` or `ovcert -list -ovrg server`

The distribution of certificates is now as illustrated in **Figure 7**. The problematic ones (red in previous picture) are gone, and the major changes are depicted in green:

Figure 7: Required Certificate Setup



HPOM Server

	Client	Server
Cert	HPOM	HPOM
Trust	HPOM	HPOM

Nodes managed by HPOM Server

	Client
Cert	HPOM
Trust	HPOM

BSM Server

	Client	Server
Cert	HPOM	BSM
Trust	BSM	BSM
	HPOM	HPOM

Configuration of Integration Adapter, SiteScope (event integration) and Diagnostics

If Integration Adapter (IA), SiteScope (SiS, using event integration) or Diagnostics (Diag) are to be connected to BSM, there are 2 different scenarios that need to be taken into account:

1. IA, SiS, Diag are NOT monitored by a Service Provider and send all data only to BSM.
2. IA, SiS, Diag are also monitored by the Service Provider, but send some of the data to BSM.

The main difference between these two scenarios is from which server these nodes get their certificates. In the 2nd case also additional configuration is required so the agent sends selective messages to the BSM server (all messages created by IA, SiS or Diag) whereas all node related messages are sent to the monitoring HPOM Server.

Certificate Configuration

IA, SiS, Diag Connected to BSM Only

In this case, the certificate for these nodes must be issued by the BSM DPS server. Connection and configuration of these nodes must be done according to the manuals.

IA, SiS, Diag Monitored by HPOM and also Connected to BSM

In this case, the certificates on the systems must be issued by the HPOM server. The BSM server also trusts (due to configuration described above) the CA that issued the certificate for the IA, SiS or Diag server which also allows communication to the BSM server.

Message Forwarding Configuration

If IA, SiS and Diag nodes are connected only to BSM, no special configuration is required.

If IA, SiS and Diag nodes are monitored by HPOM and also connected to BSM, additional configuration is required to ensure the messages generated by IA, SiS and Diag are sent to the BSM server whereas the agent, monitoring the remainder of the system, sends its messages to the managing HP OM Server.

NOTE: This is a local configuration that must be done directly on the node; these policies cannot be distributed from the HPOM server. This also means that executing “purge” operations to distribute policies from the HPOM server to the nodes will overwrite customized policies deleting the additional configuration. To change the configuration command line tools are used, so it is possible to configure a cron job/scheduled task to reload the configuration on a frequent basis.

Integration Adapter

Configure a flexible management policy on the IA node based on the description in the “Using HP BSM Integration Adapter” guide in section “Managing HP BSM Integration Adapter with HPOM”.

Diagnostics

On the diagnostics server follow the instructions as described in the “Diagnostics Install Guide” in chapter “Diagnostics 9.X and OM Agent Co-existence”.

SiteScope

On the SiS server copy the content of below’s figure into file `%OvDataDir%\datafiles\policies\mgrconf\3F9A8F04-B5E3-43C3-999A-7A9492C35014_data` (data section).

Figure 8: Data Section of a Flexible Management Policy

```
RESPMGRCONFIGS
      RESPMGRCONFIG
      DESCRIPTION "Enable HPOM and BSM"
            SECONDARYMANAGERS
              SECONDARYMANAGER
                    NODE IP 0.0.0.0 "${OM_MGR_SRV}" ID
"${OM_MGR_SRV_ID}"
                    DESCRIPTION "HPOM management server"
              SECONDARYMANAGER
                    NODE IP 0.0.0.0 "${OMi_MGR_SRV}" ID
"${OMi_MGR_SRV_ID}"
                    DESCRIPTION "HP BSM gateway server"
    ACTIONALLOWMANAGERS
      ACTIONALLOWMANAGER
        NODE IP 0.0.0.0 "${OM_MGR_SRV}" ID "${OM_MGR_SRV_ID}"
        DESCRIPTION "HPOM management server"
      ACTIONALLOWMANAGER
        NODE IP 0.0.0.0 "${OMi_MGR_SRV}" ID "${OMi_MGR_SRV_ID}"
        DESCRIPTION "HP BSM gateway server"
    MSGTARGETRULES
      MSGTARGETRULE
        DESCRIPTION "BSM events"
        MSGTARGETRULECONDS
          MSGTARGETRULECOND
            DESCRIPTION "BSM events"
            APPLICATION "SiteScope"
        MSGTARGETMANAGERS
          MSGTARGETMANAGER
            TIMETEMPLATE "$OPC_ALWAYS"
            OPCMGR IP 0.0.0.0 "${OMi_MGR_SRV}" ID "${OMi_MGR_SRV_ID}"
      MSGTARGETRULE
        DESCRIPTION "Send remaining events to HPOM"
        MSGTARGETRULECONDS
        MSGTARGETMANAGERS
          MSGTARGETMANAGER
            TIMETEMPLATE "$OPC_ALWAYS"
            OPCMGR IP 0.0.0.0 "${OM_MGR_SRV}" ID "${OM_MGR_SRV_ID}"
```

Make sure you change the following values in the template

- ${OM_MGR_SRV}: hostname of the HPOM system, (e. g. hpom1.mycompany.com)
- ${OM_MGR_SRV_ID}: CoreID of the HPOM system (on a command shell enter the command `Ovcoreid` and use the output)
- ${OMi_MGR_SRV}: hostname of the BSM Gateway server (or Load Balancer or Reverse Proxy), (e. g. bsm_gw.mycompany.com)
- ${OMi_MGR_SRV_ID}: Core ID of the BSM DPS server (on a command shell enter the command `ovcoreid -ovrg server` and use the output)

On the SiS server copy the content of below's figure into file `%OvDataDir%\datafiles\policies\mgrconf\3F9A8F04-B5E3-43C3-999A-7A9492C35014_header.xml` (header section).

Figure 9: Header Section of a Flexible Management Policy

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<header xmlns="http://openview.hp.com/xmlns/conf/2003/04">
  <policy>
   <ids>
    <container_id>3F9A8F04-B5E3-43C3-999A-7A9492C35014</container_id>
    <version_id>3F9A8F04-B5E3-43C3-999A-7A9492C35014</version_id>
   </ids>
   <name>BSM/OMi Integration</name>
   <version>0001.0001</version>
   <description>Enable HPOM and BSM</description>
   <status>enabled</status>
   <owner>HPOprSiS</owner>
   <files>
    <data>
     <file_name>3F9A8F04-B5E3-43C3-999A-7A9492C35014_data</file_name>
     <encoding>text/plain</encoding>
     <checksum/>
     <signature/>
    </data>
   </files>
   <categories/>
   <attributes>
    <attribute>
     <name>creation_user</name>
     <value>HPOprSiS</value>
    </attribute>
    <attribute>
     <name>creation_date</name>
     <value>${NOW}</value>
    </attribute>
    <attribute>
     <name>checksum_header</name>
     <value/>
    </attribute>
    <attribute>
     <name>product_id</name>
     <value/>
    </attribute>
    <attribute>
     <name>version_info</name>
     <value/>
    </attribute>
   </attributes>
  </policy>
  <policytype>
   <container_id>7d33071a-1824-4a1b-a667-54170430ab72</container_id>
   <version>0001</version>
   <name>mgrconf</name>
  </policytype>
  <certificate/>
</header>
```

To sign the newly created policy, go to directory `%OvDataDir%\datafiles\policies\mgrconf` and enter the command:

```
"C:\Program Files (x86)\Java\jre6\bin\java" -
Djava.library.path=C:\SiteScope\tools\OMIntegration -cp
"C:\SiteScope\integrations\om\lib\*"
com.hp.opr.policymanagement.PolicyActivation sign 3F9A8F04-B5E3-43C3-
999A-7A9492C35014_header.xml
```

To activate the newly created policy, go to directory `%OvDataDir%\datafiles\policies` and enter the command:

```
ovpolicy -install -dir mgrconf
```

The SiteScope specific policies will now report to the BSM server and all of the other policies will report to the HPOM server.

For more information

http://support.openview.hp.com/selfsolve/manuals
HP Business Service Management: Deployment Guide
HP Diagnostics: Installation Guide
HP Integration Adapter: Installation Guide
HP SiteScope: Installation Guide

November2012

Version 1.0