HP OpenView Internet Services 6.10 and HP OpenView Operations Agent 8.x: Co-existence and Certificate Management

Version 1.1
5th October 2005

hp invent

Abstract

When planning to install both an OVO 8.x agent and OVIS 6.10 measurement server or probe station on the same system, there are additional certificate-related considerations during the installation. This white paper describes the recommended order of installation, how to install when the recommended order is not an option and detailed steps to configure HTTPS communications for TIPs.

Introduction

With OVO 8.0 onwards, there are two main communication methods between agent and server: DCE/NCS and HTTPS. This white paper is concerned with HTTPS communications only: i.e., the OVO 8.x agent, which establishes an SSL connection with the management server via node certificates which are issued by the OVO management server.

OVIS 6.0 introduced Troubleshooting Insight Packages (TIPs) which execute troubleshooting commands either on the OVIS server or on remote probe stations and return the output to the OVIS Dashboard. The OVIS internal components are referred to as the TIPs Server which runs on the OVIS measurement server and the TIPs Runner which runs on the local and remote probe stations. By default, the communications between TIPs Server and TIPs Runner is via HTTP. Where a more secure protocol is required to provide encryption and authentication, this can be changed to HTTPS. To achieve this, the OVIS measurement server is capable of issuing self-signed certificates to the probe stations.

Both the OVIS 6.10 measurement server and OVO 8.x management server are equipped to run their own certificate servers using the same common OV components and each is capable of issuing self-signed certificates. Nodes belonging to the OVO certificate server do not trust nodes belonging to the OVIS certificate server and vice versa.

Where this becomes important is when you want to have both OVIS 6.10 and an OVO 8.x agent installed on the same system. In this case, the node must be able to trust both the OVO management server and the OVIS measurement server. Additional configuration is required which is described in the remainder of this white paper.

The procedures documented here were tested with OVIS 6.10 and the OVO 8.12 agent on Windows Server 2003 Standard Edition for both the measurement server and remote probe station platforms.

Implementation Considerations

The two main considerations when deploying the OVO 8.x agent and OVIS 6.10 are:

- Order of installation.
- If HTTPS communications is required between the TIPs Server and TIPs Runners.

Order of installation

Install OVO 8.x agent before OVIS 6.10 (Recommended)

This is the recommended order of installation. It applies to both the OVIS 6.10 measurement server and OVIS 6.10 remote probe station. This is the quickest and easiest method, particularly if HTTPS is not required for TIPs communications.

Follow the OVO 8.x HTTPS Agent Concepts manual for installing the agent. By installing the OVO 8.x agent before installing the OVIS 6.10 measurement server, the node will request and install a certificate from the OVO 8.x management server.

Install OVO agent A.08.12 or higher, which includes the fix for a known co-existence problem (QXCR1000214514).

The only other consideration now is whether you want to configure HTTPS communications between the TIPs Server and TIPs Runners in OVIS 6.10. If this is not required, then no further certificate related configuration is required. If HTTPS communications between TIPs Server and TIPs Runners is required, then refer to "Remote Probe Stations" on page 9.

Install OVIS 6.10 before the OVO 8.x agent

Sometimes the OVIS 6.10 measurement server is installed before you are ready to install the OVO 8.x agent. If this happens, then:

- Because OVIS 6.10 (measurement server and probe station) includes some newer shared components than are provided in the OVO 8.x agent, the OVO agent install will require manual intervention to click through the warnings about newer component versions being already installed.
- On the OVIS 6.10 measurement server, a self-signed certificate is installed automatically. When you try to install the OVO 8.x agent, it will fail because the certificate authority that signed the certificate (i.e., the OVIS measurement server) is not trusted by the OVO management server. There are two methods to configure certificate handling in this situation:
  - Merge Process
  - Shared CA

The Merge Process is used to merge environments with separate Certificate Authorities. Both Certificate Authorities can issue certificates to the clients in their respective management domains. Where the management domains overlap such as when one server is running both an OVO agent and OVIS, we must establish a trust between the management domains.

It is also possible to work with only one Certificate Authority. In the Shared CA scenario, the OVIS Certificate Authority is removed and the OVO management server Certificate Authority issues certificates for both the OVIS and OVO environments, irrespective of whether or not a given OVIS probe station is also an OVO managed node.

In order to decide which method to use, consider the following:

Use the Merge Process when:

- You have an existing environment with two certificate authorities. To covert to the shared CA scenario would require you to replace all certificate that have been granted by one of the CAs.
- You do not want to be dependent on one Certificate Authority for the entire OVO and OVIS combined management environment.
- You want to be able to issue certificates from the OVIS server for the OVIS probe stations (only required if you want to configure HTTPS communications between TIPs Server and TIPs Runner, as explained in the HP OpenView Internet Services User's Reference Guide).

Use the Shared CA process when:

- You do not plan to use HTTPS communications between TIPs Server and TIPs Runners.
- You want to manage the combined OVO and OVIS environment from a single CA. For example, OVO is already established and you are now introducing OVIS.
- OVO is already established and you are now installing OVIS 6.10 in an environment where all or the majority of probe stations are also OVO managed nodes.

Merge Process

The Merge Process involves exchanging the root certificates between the two management servers (OVO and OVIS) and then updating the list of trusted root certificates on the nodes.

These instructions apply if you have already installed OVIS 6.10 measurement server and now want to install an OVO 8.x agent on the same system.

Prerequisites

- OVIS 6.10 measurement server is installed.
- Install the latest patches for the OVO 8.x agent on the OVO management server. As a minimum, install the OVO A.08.12 agent patch.

Install OVO 8.x agent

1. Prepare for the OVO agent installation as follows:

   Add node to OVO Node Bank.

   Get the ovcoreid from the OVIS node:

   ```
   ovcoreid
   ```

   On the OVO management server, run the opcnode command to update the node with the ovcoreid of the OVIS node:

   ```
   /opt/OV/bin/OpC/utils/opcnode -chg_id id=xxx node_name=<OVIS_node.FQDN>
   ```

2. Exchange root certificates and update trusts on the nodes:

   This step is required because the OVIS node has a certificate issued by the OVIS server automatically when it is installed. To exchange root certificates and update trusts:

   On the OVIS measurement server, run:

   ```
   ovcert -exporttrusted -file <filename1> -ovrg server
   ```

   FTP <filename1> to the OVO management server.

   On the OVO management server, run:

   ```
   ovcert -exporttrusted -file <filename2> -ovrg server
   ```

   FTP <filename2> to the OVIS node.

   ```
   ovcert -importtrusted -file <filename1> -ovrg server
   ```

   On the OVIS measurement server, run:

   ```
   ovcert -importtrusted -file <filename2> -ovrg server
   ```

   Update the nodes as follows:

   On the OVO management server, run:

   ```
   ovcert -updatetrusted
   ```

   You may need to re-run this command if the certificate does not appear as shown below. Refer to http://openview.hp.com/ecare/getsupportdoc?docid=QXCR1000216372 for details.

You should now see something similar to the following on the OVO management server:

```
# ovcert -list
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
|     b730cfc6-f736-750c-025f-85a06c74e724 (*)          |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|     CA_b730cfc6-f736-750c-025f-85a06c74e724           |
|     CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8           |
+-------------------------------------------------------+

+-------------------------------------------------------+
| Keystore Content (OVRG: server)                       |
+-------------------------------------------------------+
| Certificates:                                         |
|     b730cfc6-f736-750c-025f-85a06c74e724 (*)          |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|     CA_b730cfc6-f736-750c-025f-85a06c74e724 (*)       |
|     CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8           |
+-------------------------------------------------------+
```

Observe that the root certificate of the OVIS measurement server (CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8 in this example) is installed as a trusted certificate for the node and as a trusted certificate for the server.

On the OVIS measurement server, run:

```
ovcert -updatetrusted
```

If it fails with an error like this:

```
WARNING: Trusted certificate update was not successful.
```

run this command instead:

```
ovcert -importtrusted -file <filename2>
```

where <filename2> is the one that was copied across from the OVO management server in the previous step.

Refer to QXCR1000222525 for details of this known problem.

You should now see something similar to the following on the OVIS measurement server:

```
C:\>ovcert -list
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
|     f1d6c142-e8f4-750e-168a-d6d3aa556fb8 (*)          |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|     CA_b730cfc6-f736-750c-025f-85a06c74e724           |
|     CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8           |
+-------------------------------------------------------+

+-------------------------------------------------------+
| Keystore Content (OVRG: server)                       |
+-------------------------------------------------------+
| Certificates:                                         |
|     f1d6c142-e8f4-750e-168a-d6d3aa556fb8 (*)          |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|     CA_b730cfc6-f736-750c-025f-85a06c74e724           |
|     CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8 (*)       |
+-------------------------------------------------------+
```

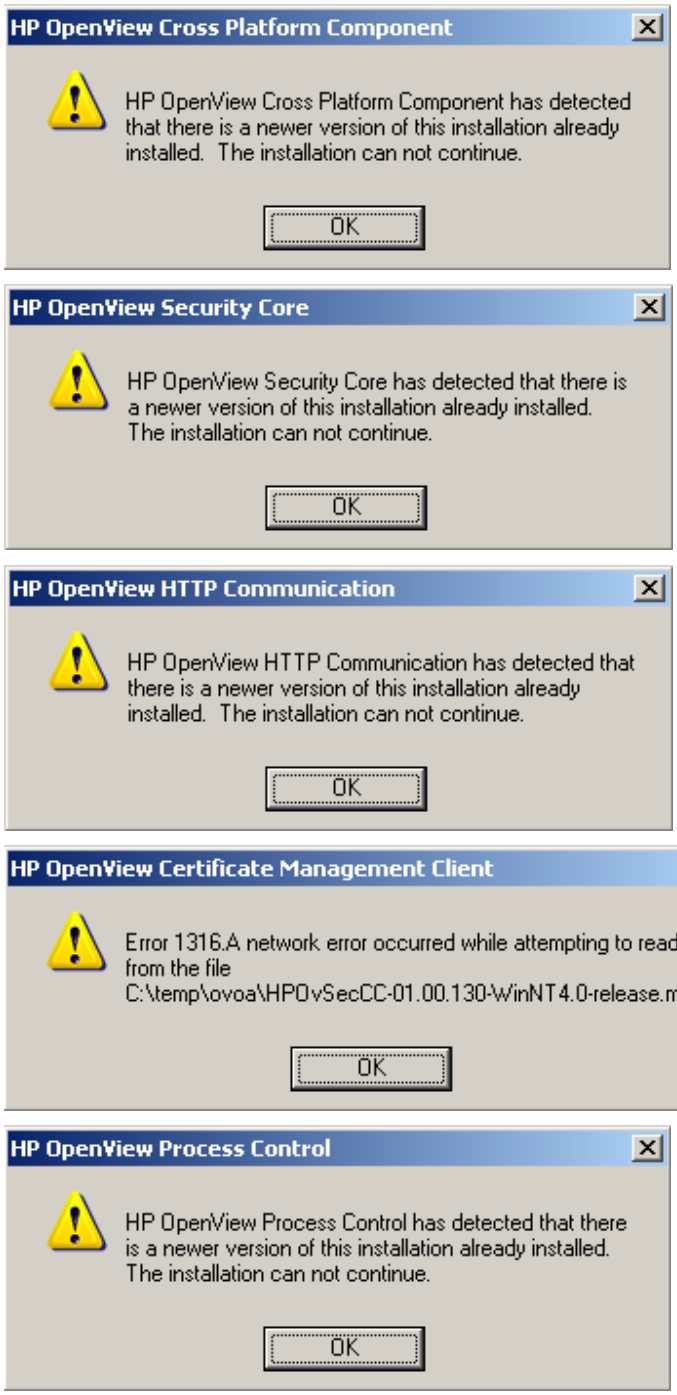
Observe that the root certificate of the OVO management server (CA_b730cfc6-f736-750c-025f-85a06c74e724 in this example) is installed as a trusted certificate for the node and as a trusted certificate for the server.

3. Install the OVO agent as you would normally. For example, install the agent software from the OVO GUI or FTP the agent software to the OVIS node from the management server.

Note: When you run the command:

```
cscript opc_inst.vbs
```

the following popup windows will appear. In each case, click the "OK" button and ignore the errors. The installation will still work.



Shared CA Process

In this process, we remove the OVIS certificate server. All certificates for the OVIS environment are issued by the OVO management server.

1. Add the OVIS node to the OVO Node Bank.

2. On the OVIS node, remove all the certificates:

   Run "ovcert -list" to list the certificates. Then remove each one:

   ```
   ovcert -remove <cert_id>
   ovcert -remove <cert_id> -ovrg server
   ovcert -remove CA_<cert_id>
   ovcert -remove CA_<cert_id> -ovrg server
   ```

   Run "ovcert -list" again to verify that all certificates have been removed:

   ```
   C:\>ovcert -list
   +-------------------------------------------------------+
   | Keystore Content                                      |
   +-------------------------------------------------------+
   | Certificates:                                         |
   +-------------------------------------------------------+
   | Trusted Certificates:                                 |
   +-------------------------------------------------------+

   +-------------------------------------------------------+
   | Keystore Content (OVRG: server)                       |
   +-------------------------------------------------------+
   | Certificates:                                         |
   +-------------------------------------------------------+
   | Trusted Certificates:                                 |
   +-------------------------------------------------------+
   ```

3. Unregister the Certificate Server (ovcs) component from OVIS system using the command:

   ```
   ovcreg -del ovcs
   ```

4. Install the OVO agent as described in steps 3 and 4 of the Merge Process. Note that, because we removed the local certificate in step 1, the OVO agent installation will automatically request a certificate from the OVO management server. If this was a manual agent installation, remember to grant the certificate request on the OVO management server either in the OVO GUI or via the command line:

   ```
   ovcm –listpending –l
   ovcm –grant <request-id>
   ```

Remote Probe Stations

If the remote probe station will also be an OVO 8.x managed node, it is recommended that you install the OVO 8.x agent before the probe station to avoid the 5 popup errors already described.

Consider if the remote probe station needs to be configured for secure HTTPS communications. By default, the TIPs Server communicates with local and remote probe systems and TIPs Runners using HTTP. You can configure HTTPS communications if secure communications is required.

If you choose to use secure communication, the TIPs Server and all the TIPs Runners communicating with that TIPs Server must run in secure mode.

If an OVO agent is installed on the remote probe station, then the required certificates will be installed via the OVO agent installation.

If the remote probe station does not have an OVO agent installed on it, then you need to request and install a client certificate. If you are using the Shared CA method, then this certificate is issued by the OVO management server. If you are using the Merge Process, the certificate is issued by the OVIS measurement server.

Installing Certificate to Remote TIPs Runner Systems using the Merge Process

On each TIPs Runner system, request a certificate. There are two ways to do this.

Issue the certificate request and grant the certificate across the network

1. On the TIPs Server system, start the OV certificate server:

   ```
   ovc -start ovcs
   ```

2. On each TIPs Runner system, request a certificate:

   ```
   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <host name of TIPs Server>

   ovcert -certreq
   ```

3. On the TIPs Server system, list the pending certificates:

   ```
   ovcm -listpending -l
   ```

   This command displays the request identifier for each TIPs Runner system that is requesting a certificate.

4. On the TIPs Server system, grant the TIPs Runner certificate:

   ```
   ovcm -grant <request_id>
   ```

5. Verify that the certificate is installed. On the TIPs Runner system:

   ```
   C:\>ovcert -list
   +-------------------------------------------------------+
   | Keystore Content                                      |
   +-------------------------------------------------------+
   | Certificates:                                         |
   |     ae69e5c2-fef9-750e-1e0d-a47f1fe99bca (*)          |
   +-------------------------------------------------------+
   | Trusted Certificates:                                 |
   |     CA_b730cfc6-f736-750c-025f-85a06c74e724           |
   |     CA_f1d6c142-e8f4-750e-168a-d6d3aa556fb8           |
   +-------------------------------------------------------+
   ```

Issue the certificate on the TIPs Server and copy to the TIPs Runner

This method is used where you do not want certificate related information to be transmitted across the network.

1. On the TIPs Server system:

   ```
   ovcm -issue -name <hostname of TIPs Runner> -file <filename> -coreid <coreid
   of TIPs Runner> -pass <passphrase>
   ```

2. On the remote TIPs Runner system:

   ```
   ovcert -importcert -file <filename> -pass <passphrase>
   ```

3. Repeat steps 1 and 2 for each remote TIPs Runner.

Installing Certificate to Remote TIPs Runner Systems using Shared CA

On each TIPs Runner system, request a certificate. There are two ways to do this.

Issue the certificate request and grant the certificate across the network

This requires the TIPs Runner system and the OVO management server to have network connectivity and that they each can resolve the other's full qualify hostname.

1. On each TIPs Runner system, request a certificate:

   ```
   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <host name of OVO Server>

   ovcert -certreq
   ```

2. On the OVO management server, list the pending certificates:

   ```
   ovcm -listpending -l
   ```

   This command displays the request identifier for each TIPs Runner system that is requesting a certificate.

3. On the OVO management server, grant the TIPs Runner certificate:

   ```
   ovcm -grant <request_id>
   ```

4. Verify that the certificate is installed. On the TIPs Runner system:

   ```
   C:\>ovcert -list
   +-------------------------------------------------------+
   | Keystore Content                                      |
   +-------------------------------------------------------+
   | Certificates:                                         |
   |     ae69e5c2-fef9-750e-1e0d-a47f1fe99bca (*)          |
   +-------------------------------------------------------+
   | Trusted Certificates:                                 |
   |     CA_b730cfc6-f736-750c-025f-85a06c74e724           |
   +-------------------------------------------------------+
   ```

Issue the certificate on the OVO Management Server and copy to the TIPs Runner

This method is used if the probe station and OVO management server do not have network connectivity or you do not want certificate related information sent across the network.

1. On the OVO management server:

   ```
   ovcm -issue -name <hostname of TIPs Runner> -file <filename> -coreid <coreid
   of TIPs Runner> -pass <passphrase>
   ```

2. On the remote TIPs Runner system:

   ```
   ovcert -importcert -file <filename> -pass <passphrase>
   ```

3. Repeat steps 1 and 2 for each remote TIPs Runner.

Configure secure communications between TIPs Server and TIPs Runners

When certificates are installed on all the TIPs Runner systems, you can enable secure HTTPS communications. This is documented in the TIPs online help. A concise version of the steps to enable HTTPS communications is shown here for completeness.

1. Configure and Restart the TIPs Server in Secure Mode

```
ovc -stop ovtomcatA
OvTIPsServer.bat -secure true
ovc -start ovtomcatA
```

2. Configure and Restart the TIPs Runners in Secure Mode

   On the TIPs Server system:

```
ovc -stop ovtiprn
ovtiprn -secure true
ovc -start ovtiprn
```

   On each remote TIPs Runner system:

```
ovc -stop ovtiprn
ovtiprn -secure true
ovc -start ovtiprn
```

3. Verify that secure mode is being used for both the TIPs Server and TIPs Runners.

   On the Remote TIPs Runner system:

   View the OVTIPsRunner.log.txt file and look for the entry when ovtiprn starts:

```
0: INF: Wed Jun 22 08:15:58 2005: TIPsRunner (480/444): Note: TID{444}
Communication between the server warren.rose.hp.com 192.168.221.135 and this
agent bunny.rose.hp.com 192.168.221.134 will be secure.
```

   On the TIPs Server system:

   Verify the local TIPs Runner is using secure mode:

```
C:\>ovtiprn -retrieve secure
secure: true
```

   Verify the TIPs Server is using secure mode:

```
C:\temp\ovoa>ovtipsserver -retrieve secure
java version "1.4.2_02"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_02-b03)
Java HotSpot(TM) Client VM (build 1.4.2_02-b03, mixed mode)

22/06/2005 19:56:23 com.hp.ov.tips.util.XPLTracer doLogMessage
INFO: UTILS: Operation: OVCommonProcesses->recordInitialLogMessage():
************************** ><XPL Logger/Tracer Started Or Restarted By
OVCommonProcesses **************************
secure: true
```

References and Further Reading

HP OpenView Internet Services User's Reference Guide, March 2005

HP OpenView Operations HTTPS Agent Concepts and Configuration Guide, A.08.10, Edition 4

HP OpenView Troubleshooting Insight Packages

TIPs Configuration Program online help, HP OpenView Internet Services, A.06.10

XXXX-XXXXEN, 07/2003