HP Operations Manager Agent

HTTPS Agent Configuration and Troubleshooting Guide

December 2007

This document describes how to install, configure and troubleshoot the HP Operations Manager HTTPS Agent.

Operating System:	OpenVMS Alpha Versions 7.3-2, 8.2 and 8.3
	OpenVMS Integrity servers Versions 8.2-1, 8.3 and 8.3-1H1
Software Version:	HP Operations Manager HTTPS Agent Version 8.0-1

Hewlett-Packard Company
Palo Alto, California

This document was prepared using DECdocument, Version 3.3-1B.

Contents

B Tracing OVO

Preface

This document provides information about installing, configuring, and troubleshooting the HP Operations Manager HTTPS Agent.

Intended Audience

This document is intended for system administrators and operators.

Structure of this Document

This document is organized is as follows:

- Chapter 1 provides an overview.
- Chapter 2 describes the concepts of managing HTTPS nodes.
- Chapter 3 describes the installation procedure.
- Appendix A provides troubleshooting guidelines for HTTPS-based communication.
- Appendix B provides problem tracing.

Related Documents

This document supplements the following:

– *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*

This document can be located at the following web address:
`http://h20230.www2.hp.com/selfsolve/manuals`

– *HP SSL for OpenVMS Installation Guide and Release Notes*

This document can be located at the following web address:
`http://h71000.www7.hp.com/openvms/products/ssl/ssl_doc.html`

Reader's Comments

HP welcomes your comments on this document. Please send comments to either of the following addresses:

Internet	**openvmsdoc@hp.com**
Postal Mail	Hewlett-Packard Company OpenVMS Documentation, ZKO3-4/Y02 110 Spit Brook Rd. Nashua, NH 03062-2698

Conventions

The following conventions are used in this document:

Convention	Meaning
( )	In command format descriptions, parentheses indicate that you must enclose multiple choices in parentheses.
[ ]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.
{}	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
`Example`	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies URLs, UNIX commands and pathnames, PC-based commands and folders, and certain elements of the C programming language.
italic type	Italic type indicates important information, complete titles of manuals or variables. Variables include information that varies in system output (for example, Internal error *number*), in command lines (/PRODUCER=*name*), and in command parameters in text (where *dd* represents the predefined code for the device type).
UPPERCASE TYPE	Uppercase indicates the name of a command, routine, file, file protection code, or the abbreviation of a system privilege.
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.

1

Operations Manager HTTPS Agent Overview

1.1 Introduction

HTTPS agent software provides highly secure communication between Operations Manager UNIX 8.x and their managed nodes. HTTPS agents are generally used and administered in the same way as DCE-based agents. Applications are launched in the same way. All functionality that is available with DCE-based agents is also available with HTTPS agents unless explicitly stated otherwise. Policies for HTTPS agents are created, assigned and deployed in a similar way as templates for DCE-based agents. For example, heartbeat polling of nodes results in the same type of status messages and are displayed in a very similar way in the message browser.

HTTPS-based communication provides you with the following major advantages:

- Simple management through firewalls with configurable, single-port, secure communication using, open, HTTPS-based communication techniques. Restrict outside access to dedicated HTTP proxies and reduce port usage by multiplexing over HTTP proxies.
- Out-of-the-box Internet Secure Communication using SSL/PKI encryption with server and client certificates for authentication.
- Communication is based on standard Web technologies (HTTP, SOAP, Proxies, SSL,), available in every environment today, and familiar to every IT administrator.
- Message format based on XML and SOAP used for message security from the Operations Manager HTTPS Agent to the Operations Manager Server.
- IP independence/dynamic IP (DHCP). Managed nodes can be identified by their unique `OvCoreID` and not necessarily by their IP addresses.

1.2 Organization of HTTPS Managed Nodes

The files associated with the HTTPS agent are found in the following directory structures:

Generic Directory Structure on Managed Nodes

- **<OVInstallDir>**

  `ovo$posix_root:[opt.OV]`

  This directory contains static files that are installed and never change, for example, executables.

- **<OVDataDir>**

  `ovo$posix_root:[var.opt.OV]`

This directory contains configuration and runtime data files that are used only on the local system. The most important directory contains the instrumentation files such as actions, commands and monitors:

```
ovo$posix_root:[var.opt.OV.bin.instrumentation]
```

1.3 HTTPS Communication Administration Commands

HTTPS Communication can be controlled using the following commands.

On the Operations Manager Server and Managed Nodes:

- `ovcoreid` (OpenView Unique System Identifier)

  The `ovcoreid` command is used to display existing `OvCoreId` value and, in addition, create and set new `OvCoreId` values on the local system.

  For details of how to use this tool, use `ovcoreid -h`.

- `ovc` (OpenView Process Control)

  ovc controls starting and stopping, event notification, and status reporting of all components registered with the OpenView Control service, ovcd.

  For details of how to use this tool, use `ovc -h`.

- `bbcutil`

  The `bbcutil` command is used to control the OV Communication Broker.

- `ovconfget`

  Installed OpenView components have associated configuration settings files that contain one or more namespaces. A namespace is a group of configuration settings that belong to a component. All configurations specified in the settings files are duplicated in the settings.dat configuration database. For each specified namespace, ovconfget returns the specified attribute or attributes and writes them to stdout. Used without arguments, ovconfget writes all attributes in all namespaces to stdout.

  For details of how to use this tool, use `ovconfget -h`.

- `ovconfchg`

  Installed OpenView components have associated configuration settings files that contain one or more namespaces. A namespace is a group of configuration settings that belong to a component. ovconfchg manipulates the settings in the configuration file, updates the configuration database, and triggers notification scripts.

  For details of how to use this tool, use `ovconfchg -h`.

- `ovpolicy`

  ovpolicy manages local policies and templates. A policy or template is a set of one or more specifications, rules and other information that help automate network, system, service, and process management. Policies and templates can be deployed to managed systems, providing consistent, automated administration across the network. Policies and templates can be grouped into categories. Each category can have one or more policies. Each category can also have one or more attributes, an attribute being a name value pair. You use ovpolicy to install, remove, enable, and disable local policies and templates.

On Managed Nodes:

- `ovcert` The ovcert command is used to manage certificates on an HTTPS node through the Certificate Client. You can execute tasks such as adding managed node certificates and importing the private keys, adding certificates to the trusted root certificates, and checking the certificate status.

  For details of how to use this tool, use `ovcert -h`.

On the Operations Manager Server:

- `opccsacm` (Certificate Server Adapter Control Manager)

  The opccsacm command is used to issue new node certificates and installation keys manually on the HP OpenView server. It also modifies the database to reflect the changes made by certificate management actions.

  For details of how to use this tool, use `opccsacm(1m)`.

2

Concepts of Managing HTTPS Nodes

2.1 Controlling HTTPS Nodes

The Operations Manager Server can perform the following functions on HTTPS nodes:

- Remote control of HTTPS agents.
- Manual installation of HTTPS agents.
- Remote and manual configuration deployment.
- Heartbeat polling.
- Security management of HTTPS nodes.
- Support of HTTPS nodes through the Operations Manager Server APIs and utilities.

2.2 Configuration Deployment to HTTPS Nodes

Configuration deployment to HTTPS agents differs slightly from that of DCE-based nodes:

- Policies are used by HTTPS agents in place of Templates.
- Instrumentation is the single term used by HTTPS agents for Actions, Commands, and Monitors.
- A configuration parameter schema with a name-value pair policy type for HTTPS agents replaces nodeinfo and opcinfo files.

The following sections explain the new configuration management concepts introduced with the HTTPS agents.

2.2.1 Policy Management

A policy is a template in XML format, with the strict separation of data and meta information. The header contains attributes such as name, type, version, and state. Five operations are possible on policies: install, remove, enable, disable and list. Template files contain all individual templates of a certain source type in one file, a policy file contains only the content of one template and this information is referred to as the policy data.

It is possible to manually install and remove policies using the ovpolicy tool, provided that you adhere to some guidelines.

Existing templates can also be used with HTTPS agents as these are converted into policies at distribution time by the opcbbcdist process. In addition to the unique policy id, the header contains the policy name, policy type name, policy version, policy type version, and status. These attributes are generated by opcbbcdist as the data is being deployed.

Only one version of a policy can be installed on a node. A policy is identified by its id, but also the name plus policy type must be unique.

All policies that are deployed from the Operations Manager Server are allocated the version number 1 as Operations Manager on UNIX does not support policy versioning.

The status of a policy deployed for the first time is set to enabled. If the policy is already present on the system, a newly deployed policy assumes the status of the policy it replaces.

There is a utility called opctemplate for HTTPS nodes, which is wrapper for ovpolicy.

2.2.2 Instrumentation Management

On HTTPS nodes, the actions-, commands-, and monitor directories are replaced with:

```
ovo$posix_root:[var.opt.OV.bin.instrumentation]
```

which can have one level of sub directories. All instrumentation programs are installed at this location.

Note

The directory for executables on the Operations Manager Server is located under:

```
/var/opt/OV/share/databases
```

No instrumentation directory is created and the directories actions, commands, and monitors are used. Typically, action, command, and monitor executables are referenced in templates. As long as these executables are not referred with their full path in policies, this change is transparent, because the new locations of the binaries is also added to the path variables of utilities like the action agent, monitor agent and logfile encapsulator.

2.2.3 Heartbeat Polling of HTTPS Nodes

Heartbeat polling of managed nodes checks for following things:

- Does the managed node respond to ping.
- Is ovbbccb (HTTPS) reachable.
- Is ovcd (HTTPS) reachable.
- Is the message agent (opcmsga) reachable.

Note

Other agent processes, such as opcmona, opcle, and opcacta, are not checked by the heartbeat polling but are monitored by the agent's health check. If any of these processes dies and is not disabled, ovcd issues a message and automatically re-start the process.

Heartbeat polling of HTTPS nodes and DCE-based nodes is very similar. Heartbeat polling of managed nodes is driven by the request sender process ovoareqsdr and is divided into three phases:

- The request sender ovoareqsdr sends ping packages to check whether the node is reachable.
- The HTTPS agent communication broker is polled.
- OV Control RPC server is requested.

Note

You can use the RPC_only mode, where the ping phase is omitted, to get through firewalls which have the ICMP filter enabled. In RPC_only mode, less checks are executed. Should a problem arise, the detail available from the error messages is reduced. You can set different polling intervals per node.

3
Installation of HTTPS Managed Nodes

To manage an OpenVMS system from an Operations Manager Server, complete the following tasks on both the Operations Manager Server system and on the OpenVMS systems before you install the software:

- Verifying the Prerequisites on an OpenVMS System
- Configuring the Operations Manager Server

3.1 Verifying the prerequisites on an OpenVMS System

To verify the prerequisites on an OpenVMS system, follow these steps:

HP Operations Manager HTTPS Agent and Smart Plug-In (SPI) software is now available on OpenVMS Alpha Version 7.3-2 or later and OpenVMS Integrity servers Version 8.2-1 or later. Ensure the following OpenVMS patches have been applied.

For OpenVMS Alpha:

- OpenVMS Alpha Version 7.3-2
  - VMS732_SYS V8.0 or later
  - VMS732_PTHREAD V3.0 or later
  - VMS732_UPDATE V5.0 or later
  - VMS732_RPC V4.0 or later
- OpenVMS Alpha Version 8.2
  - VMS82A_UPDATE V7.0 or later
  - VMS82A_SYS V7.0 or later
- OpenVMS Alpha Version 8.3
  - VMS83A_UPDATE V3.0 or later

For OpenVMS Integrity servers:

- OpenVMS Integrity servers Version 8.2-1
  - VMS821I_UPDATE V5.0 or later
  - HP I64VMS VMS821I_ICXXL V2.0 or later
- OpenVMS Integrity servers Version 8.3
  - VMS83I_UPDATE V1.0 or later
  - VMS83I_SYS V1.0 or later
  - HP I64VMS VMS83I_ICXXL V2.0 or later

The patches are available at the HP ITRC web address:

```
http://www2.itrc.hp.com/service/patch/mainPage.do
```

- SSL for OpenVMS

  You must have SSL Version 1.2 or later installed and running on your OpenVMS system. The SSL kits are available at the following web address:

  ```
  http://h71000.www7.hp.com/openvms/products/ssl/ssl.html
  ```

- You need to install the HP Operations Manager HTTPS Agent and SPI software on ODS-5 disk.

3.1.1 Configuring the Operations Manager Server on UNIX

For a Operations Manager Server on UNIX the release kits for HTTPS agents are supplied in a UNIX tar file.

To configure on Operations Manager Server on UNIX, follow these steps:

1. Log in to your Operations Manager Server.

   Note

   You need to apply the following patches to the Operations Manager Server on UNIX if you have not applied the patches earlier:

   - HP-UX PA-RISC Server: PHSS_36119
   - HP-UX IA-64 Server: PHSS_36118
   - Solaris Server: ITOSOL_00576

2. Copy the OVO8A_V0800_AGENT.TAR (for Alpha) or OVO8I_V0800_AGENT.TAR (for Integrity servers) tar file to Operations Manager Server on UNIX into a temporary directory such as /tmp.
3. To make the required updates to the Operations Manager Server on UNIX, follow these steps:

   Note

   Perform the following steps in this section ONLY ONCE, even if you add the nodes later or update the Operations Manager Server on UNIX.

   a. To distribute the files on the Operations Manager Server on UNIX, set your directory to the root directory and untar the file by entering the following commands:

      For OpenVMS Alpha:

      ```
      # cd /
      # tar -xvf <your-temp-directory>/OVO8A_V0800_AGENT.tar
      ```

      For OpenVMS Integrity servers:

      ```
      # cd /
      # tar -xvf <your-temp-directory>/OVO8I_V0800_AGENT.tar
      ```

      This command will extract the installation file for the OpenVMS managed node and configuration files for Operations Manager Server on UNIX.

b. Load the Agent Platform file into the OpenView database by entering the following command:

   For OpenVMS Alpha:

   ```
   # opcagtdbcfg -p hp/alpha/ovms -d -f
   ```

   For OpenVMS Integrity servers:

   ```
   # opcagtdbcfg -p hp/ipf64/ovms -d -f
   ```

c. On the Operations Manager Server on UNIX, if you have modified any of the existing policies save them with a different name before uploading the new policies to the Operations Manager Server on UNIX.

d. Upload the templates so that they can be distributed later to the agent nodes by entering the following commands:

   ```
   # opccfgupld -replace VMSAgent
   # opccfgupld -replace VMSSPI
   ```

Note

If you are uploading the template for the first time to the Operations Manager Server on UNIX, use the -add command instead of -replace.

e. Add the OpenVMS nodes using the Graphical User Interface (GUI) that you want to monitor. If the specific OpenVMS node is already added to the Operations Manager Server on UNIX as a DCE agent node, then remove the specific node entry and add it again as HTTPS agent node.

f. Add the OpenVMS message group to the responsibilities matrix for the users who will monitor the messages from SPIs.

3.2 Installing the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS System

To install the HP Operations Manager HTTPS Agent and SPI software, follow these steps:

1. Log in to the SYSTEM account on the OpenVMS managed node.
2. Uninstall OpenVMS DCE agents and OSSPI on the OpenVMS managed node if you have installed the software previously by entering the following commands:

   ```
   $ @SYS$STARTUP:VMSSPI$SHUTDOWN
   $ @SYS$STARTUP:OVO$SHUTDOWN
   $ PRODUCT REMOVE OVOAGENTS
   $ PRODUCT REMOVE VMSSPI
   ```

3. Create a temporary directory on an ODS-5 disk to copy the installation files.

   For example,

   ```
   $ CREATE/DIRECTORY DISK$:[TEMP]
   ```

4. FTP the OVO8-V0800-x-AXP.EXE or OVO8-V0800-x-I64.EXE installation file from Operations Manager Server on UNIX to the temporary directory.

   For example,

On OpenVMS Alpha:

```
$ SET DEF DISK$:[TEMP]
$ FTP <OMU server>
ftp>cd /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/
alpha/ovms/ A.08.10.160
ftp> bin
ftp> get OVO8-V0800-x-AXP.EXE
ftp> bye
```

On OpenVMS Integrity servers:

```
$ SET DEF DISK$:[TEMP]
$ FTP <OMU server>
ftp>cd /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/
ipf64/ovms/ A.08.10.160
ftp> bin
ftp> get OVO8-V0800-x-I64.EXE
ftp> bye
```

5. To extract the installation files, run OVO8-V0800-x-AXP.EXE (for Alpha) or OVO8-V0800-x-I64.EXE (for Integrity servers) by entering the following command:

   For OpenVMS Alpha:

   ```
   $ RUN OVO8-V0800-x-AXP.EXE

     HP-AXPVMS-OVBBC-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVCONF-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVCTRL-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVDEPL-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVEAAGT-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVSECCC-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVSECCO-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-OVXPL-V0800-1-1.PCSI$COMPRESSED;1
     HP-AXPVMS-VMSSPI-V0800-1-1.PCSI$COMPRESSED;1
     OPC_INST.COM
     OPCACTIVATE.COM
     OPC_CLU_NODE_CONF.COM
     OPC_UNINST.COM
     README_HTTPS_OVMS_OPSMANAGER_AGENT.TXT
     RELNOTES_HTTPS_OVMS_OPSMANAGER_AGENT.TXT
   ```

   For OpenVMS Integrity servers:

   ```
   $ RUN OVO8-V0800-x-I64.EXE

     HP-I64VMS-OVBBC-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVCONF-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVCTRL-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVDEPL-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVEAAGT-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVSECCC-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVSECCO-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-OVXPL-V0800-1-1.PCSI$COMPRESSED;1
     HP-I64VMS-VMSSPI-V0800-1-1.PCSI$COMPRESSED;1
     OPC_INST.COM
     OPCACTIVATE.COM
     OPC_CLU_NODE_CONF.COM
     OPC_UNINST.COM
     README_HTTPS_OVMS_OPSMANAGER_AGENT.TXT
     RELNOTES_HTTPS_OVMS_OPSMANAGER_AGENT.TXT
   ```

6. Start the installation by entering the following command:

   ```
   $ @opc_inst -srv <management-server-name> -cert_srv <certificate-server-name>
   ```

7. Add the following line to the LOGIN.COM script:

   ```
   $ @SYS$STARTUP:OVO8$DEFINE.COM
   ```

8. To install the certificates manually, follow these steps:

   a. Set the installation type to MANUAL by entering the following command:

      ```
      $ ovconfchg -ns sec.cm.client  -set "CERTIFICATE_DEPLOYMENT_TYPE" "MANUAL"
      ```

   b. Check if `ovcoreid` is set by entering the following command:

      ```
      $ ovcoreid -show
      ```

      If `ovcoreid` is not set, the following message will be displayed:

      ```
      INFO: No OvCoreId is set.
      ```

   c. If `ovcoreid` is not set, create the `ovcoreid` by entering the following command:

      ```
      $ ovcoreid -create
      ```

      An error message "ERROR: No input stream" will be displayed that can be ignored.

   d. To check whether the settings are correct, run ovconfget certificate.

      For example,

      ```
      [sec.cm.client]
      CERTIFICATE_DEPLOYMENT_TYPE=MANUAL

      [sec.core]
      CORE_ID=fc200278-8f86-751f-0e73-cbd79be7b384

      [sec.core.auth]
      MANAGER=my.mgmt.srvr.com
      MANAGER_ID=970qedsd-4212-7564-1234-qwn6kuu2d07
      ```

   e. Log in to the Operations Manager Server on UNIX as a root user and add the "coreid" of OpenVMS managed node manually to the Operations Manager Server by entering the following command:

      ```
      #/opt/OV/bin/OpC/utils/opcnode -chg_id node_name=
      <OpenVMS_managed_node>   id=<coreid_of_the_managed_node>
      ```

      For example,

      ```
      #/opt/OV/bin/OpC/utils/opcnode -chg_id node_name=
      test.in.hp.com  id= fc200278-8f899-701f-0e73-cbd79be7b384
      ```

      To obtain the coreid enter the following command on the OpenVMS managed node:

      ```
      $ ovcoreid -show
      ```

   f. Create a signed certificate and the corresponding private key for a specific managed node manually using the opccsacm command line tool. You must provide a password to encrypt the created data.

Note

Password length must be 8 characters only.

```
#/opt/OV/bin/OpC/opccsacm -issue -file <cert_file_name>
-name <managed_node_name>  -coreid <coreid_of_managed_node>
```

For example,

```
#/opt/OV/bin/OpC/opccsacm -issue -file /tmp/cert_sample.p12
-name test.in.hp.com   -coreid fc200278-8f899-701f-0e73-cbd79be7b384
```

g. Transfer the certificate file in a secure mode that is created to the OpenVMS managed node.

h. On the OpenVMS managed node, import the certificate using the ovcert command line tool. Specify the same password used in step e when requested.

To import the certificate, enter the following command:

```
$ ovcert -importcert -file cert_mgd_node
```

i. Run ovconfchg by entering the following command:

```
$ OVCONFCHG
```

j. After installation, delete the certificate file from the managed node and the Operations Manager Server on UNIX.

3.3 Installing the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS Cluster

Installing on Cluster Nodes with their Own System Disk:

If you are installing HP Operations Manager HTTPS Agent and SPI software on nodes in a cluster that does not have a common system disk, you must install HP Operations Manager HTTPS Agent and SPI software on each node separately and configure each node separately. For more information on installing, see Section 1.3, Installing the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS System.

Installing on Cluster Nodes with Common System Disk:

To install the HP Operations Manager HTTPS Agent and SPI software on cluster nodes with common system disk, follow these steps:

1. Install the HP Operations Manager HTTPS Agent and SPI software on a shared disk, on any one of the cluster nodes as described in Section 1.3, Installing the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS System.
2. Uninstall OpenVMS DCE agents and OSSPI on other cluster nodes if you have installed the software previously by entering the following commands:

```
$ @SYS$STARTUP:VMSSPI$SHUTDOWN
$ @SYS$STARTUP:OVO$SHUTDOWN
$ PRODUCT REMOVE OVOAGENTS
$ PRODUCT REMOVE VMSSPI
```

3. Run the OPC_CLU_NODE_CONF.COM on each of the other cluster nodes in the cluster.

```
$ @sys$manager:opc_clu_node_conf -srv <MgmtSrvName> -cert_srv <CertSrvName>
```

4. To install the certificates manually on each of these cluster nodes, follow step 7 and step 8 as described in section 1.3, Installing the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS System.

3.4 Using the HP Operations Manager HTTPS Agent and SPI software

1. Start the HP Operations Manager HTTPS Agent by entering the following commands:

   ```
   $ @SYS$STARTUP:OVO8$STARTUP
   ```

2. Use the Operations Manager Server to deploy the policies that you want to use on your OpenVMS node. The policies that are provided with the HP Operations Manager HTTPS Agent and SPI are available in these policy groups:

   ```
   OpenVMS
   SPI for OpenVMS
   ```

3. Start the OSSPI by entering the following command:

   ```
   $ @SYS$STARTUP:VMSSPI$STARTUP
   ```

   To customize the SPI configuration files, refer to the manual "HP OpenView Smart Plug-In (SPI) for OpenVMS User's Guide." You can locate this manual at OVO$POSIX_ROOT: [000000]VMSSPI_USER_GUIDE.PDF

4. Stop the Operations Manager Agent and OSSPI by entering the following commands:

   ```
   $ @SYS$STARTUP:VMSSPI$SHUTDOWN
   $ @SYS$STARTUP:OVO8$SHUTDOWN
   ```

3.5 Uninstalling the HP Operations Manager HTTPS Agent and SPI Software on OpenVMS System

To uninstall HP Operations Manager HTTPS Agent and SPI software on nodes in a cluster that do not have a common system disk, enter the following command on each node separately:

```
$ @SYS$MANAGER:OPC_UNINST.COM
```

Note

Run @SYS$MANAGER:OPC_UNINST.COM on any one of the cluster nodes sharing a common system disk to uninstall the HP Operations Manager HTTPS Agent and SPI software.

A

Troubleshooting HTTPS-based Communication

If communication between an Operations Manager Server and an HTTPS agent appears to be interrupted, for example, messages do not arrive at the Message Browser, or software or instrumentation is not distributed, execute the appropriate troubleshooting steps as described in the following sections.

Before you continue with the described actions, you should be familiar with the new HTTPS agent and the underlying communication concepts such as certificates.

This guideline describes possible actions to identify and solve HTTPS communication problems between Operations Manager Servers, Certificate Authority Servers and managed node agents.

It is assumed, that the HTTPS agent software is installed, but there is a problem in the communication between managed nodes and Operations Manager Servers in one or both directions.

In most installations, the Operations Manager Server and Certificate Authority servers are installed on the same system.

A.1 Troubleshooting Tools

Ping an HTTPS-Based Application

HTTPS-based applications can be pinged to test if the application is active and responding. A ping may be executed against an application whether or not it has SSL enabled.

The `bbcutil` utility supports a -ping command line parameter that can be used to ping an HP OpenView HTTPS-based application. Use the following command to ping a specified HTTPS-based application:

On HTTPS managed node:

```
bbcutil -ping [<hostname_or_ip_addr>] [count]
```

On Operations Manager Server:

```
bbcutil -ovrg server -ping [<hostname_or_ip_addr>] [count]
```

For example,

```
HTTP   bbcutil -ovrg server -ping http://...
HTTPS bbcutil -ovrg server -ping https://...
```

Checks whether the communication service on the managed node specified by <hostname_or_ip_addr> is alive. If the hostname or IP address is omitted, localhost is assumed. An optional loop count can be specified after the hostname or IP address which causes the ping command to be repeated by the number of times specified.

In general, all bbcutil calls from an Operations Manager Server to a managed node should include the -ovrg server parameter. for example:

```
bbcutil -ovrg server -ping https://...
```

Display All Applications Registered to a Communication Broker

The Communication Broker at a specified location can be requested to display all applications that are registered to it.

Use the following command to list all applications that are registered to the specified Communication Broker:

```
bbcutil -registrations|-reg <hostname_or_ip_addr>
```

Queries a Communication Broker on the managed node specified by <hostname_ or_ip_addr> and displays a list of all registered applications. If the hostname or IP is omitted, localhost is assumed.

Display the Current Status of an HTTPS-Based Application

An HTTPS-based application at a specified location can be requested to display its current status.

Use the following command to query a specified application:

```
bbcutil -status <hostname_or_ip_addr:port>
```

Queries the communication server located at the hostname and port specified by <hostname_or_ip_addr:port> for details about the current state of the server.

Standard TCP/IP Tools

If SSL is not enabled, standard TCP/IP tools such as telnet can be used to contact HP OpenView HTTPS-based application. To use telnet to ping an HTTPS-based application execute the following commands:

Two carriage returns are required after the PING input line to telnet.

To end the telnet session, enter control+] and type Quit and Return:

```
telnet <host> <port>
PING /Hewlett-Packard/OpenView/BBC/ping HTTP/1.1
```

The output takes the following form:

```
HTTP/1.1 200 OK
content-length: 0
content-type: text/html
date: Thu, 08 Aug 2002 08:20:24 GMT
senderid: fd7dc9c4-4626-74ff-9e5a09bffbae
server: BBC X.05.00.01.00; ovbbccb 05.00.100
telnet> quit
Connection closed.
```

HTTP status 200 OK indicates the HTTPS-based application has recognized the request and successfully responded. Other status may indicate a failure in the request or other error.

RPC Calls Take Too Long

If an RPC call takes longer than the default timeout of 5 minutes, the following error messages may be displayed, for example, for a policy installation:

```
ERROR: General I/O exception while connecting to host '<hostname>'.
(xpl-117) Timeout occurred while waiting for data.
or

ERROR: The Configuration server is not running on host '<hostname>'.
Check
if the Configuration server is in state running.
(bbc-71) There is no server process active for address:
https://<hostname>/com.hp.ov.conf.core/bbcrpcserver
```

This may happen if 1000 policies are installed using the PolicyPackage interface from OvConf or if the connection or target-machine is slow.

To prevent this the communication timeout (response timeout) can be changed using the following commands with the required time out value:

On the target system:

```
ovconfchg -ns bbc.cb -set RESPONSE_TIMEOUT <seconds>
```

On the Operations Manager Server:

```
ovconfchg -ovrg server -ns bbc.http.ext.conf -set \
RESPONSE_TIMEOUT <seconds>
```

Note

The RESPONSE_TIMEOUT parameter must be set on both managed nodes.

A similar situation can arise when running any command that takes over 5 minutes to complete. The timeouts should be extended as follows. On the HTTPS managed node enter the commands:

Note

The unit is milliseconds in the second case.

```
ovconfchg -ns bbc.cb -set RESPONSE_TIMEOUT <seconds>
ovconfchg -ns depl -set CMD_TIMEOUT <milliseconds>
```

On the Operations Manager Server, enter the command:

```
ovconfchg -ovrg server -ns bbc.http.ext.depl -set \
RESPONSE_TIMEOUT <seconds>
```

A.2 Communication Problems between Management Server and HTTPS Agents

The most likely areas where communication problems may be experienced are divided into the following sections:

- Network Troubleshooting Basics
- HTTP Communication Troubleshooting Basics
- Authentication and Certificates Troubleshooting for HTTP
- Communication Troubleshooting

A.2.1 Network Troubleshooting Basics

Basic network troubleshooting uses the following commands:

```
Ucx ping
tcpip show host
telnet
```

Note

The actions described below may not work if communication between an Operations Manager Server or Certificate Authority server and managed node has to pass:

- Firewalls
- NATs
- HTTP Proxies

Contact your Network Administrator for more information.

To check for basic network problems, complete the following steps:

1. Check if the name resolution for the Operations Manager Server, Certificate Authority server and HTTPS managed node is consistent on all affected systems.

   Use ping, and `bbcutil -gettarget` (on Solaris: `ovgethostbyname`) with the Fully Qualified Domain Name (FQDN) on all systems with all systems as targets.

   ```
   bbcutil -gettarget <nodename>
   ```

2. Check if all systems (Operations Manager Server, Certificate Authority server and HTTPS managed node) are accessible.

   Use one of the following commands:

   ```
   bbcutil -ping <FQDN>
   telnet <FQDN>
   ```

3. Check if HTTP communication is working by using a Web browser to connect to the Communication Broker. The Communication Broker, ovbbccb, must be running for this check.

   To retrieve the assigned `<AGENT-BBC-PORT>` value, enter the command:

   ```
   bbcutil -getcbport <agenthostname>
   ```

   For example, if you enter the command:

   ```
   bbcutil -getcbport mysystem.mycom.com
   ```

   Output of the following form is displayed:

   ```
   mysystem.mycom.com:8008
   ```

   Open a Web browser and enter the following URL:

   ```
   http://<OVO managed node>:<AGENT-BBC-PORT>/ \Hewlett-Packard/OpenView/BBC/
   ```

   The default port number for `<AGENT-BBC-PORT>` is 383.

Repeat this step on Operations Manager Server:

```
http://<OVO management server>:<AGENT-BBC-PORT>/ \
Hewlett-Packard/OpenView/BBC/
```

The HP OpenView BBC Information Modules page should appear and allow you to check ping and status or list registered services and OV resource groups (ovrg).

A.2.2 HTTP Communication Troubleshooting Basics

Basic HTTP communication troubleshooting uses the following commands:

```
ovc
ovconfget
ovbbccb
```

Note

Even if the communication between Operations Manager Server or Certificate Authority server and HTTPS managed node has to pass:

- Firewalls
- NATs
- HTTP Proxies

the following actions must work! If they do not, contact your Network Administrator for more information.

To check for HTTP communication problems, complete the following steps:

1. On all systems, the Operations Manager Server, Certificate Authority server and HTTPS managed node, check if:

   The OV Communication Broker ovbbccb is running with the following commands:

   ```
   ovc -status
   ```

   The `ovbbccb` process must be listed as running. The output takes the following form:

   ```
   ovcd        OV Control                          CORE         (731907515) Running
   opcacta     OVO Action Agent                    AGENT,EA     (731907518) Running
   opcle       OVO Logfile Encapsulator            AGENT,EA     (731907520) Running
   opcmona     OVO Monitor Agent                   AGENT,EA     (731907521) Running
   opcmsga     OVO Message Agent                   AGENT,EA     (731907517) Running
   opcmsgi     OVO Message Interceptor             AGENT,EA     (731907522) Running
   ovbbccb     OV Communication Broker             CORE         (731907516) Running
   ovconfd     OV Config and Deploy                COREXT       (731907519) Running
   show system/proc="ovbbccb"
   ovbbccb must be listed.
   ```

   ```
   bbcutil -status
   ```

   Status of ovbbccb must be ok.

Note

Make a note of the ports listed using the command:

```
bbcutil -getcbport <hostname>
```

- on HTTPS managed node as <AGENT-PORT>
- on Operations Manager Server as <MGMT-SRV-PORT>
- on Certificate Authority server as <CA-SRV-PORT>

Alternatively, you can use the command:

```
ovconfget bbc.cb.ports PORT
```

You can start the Communication Broker with the command:

```
ovc -start ovbbccb
```

No error messages should be displayed.

2. Check the configuration of the Communication Broker port settings with the following commands:

   a. Lists all Communication Broker ports:

   ```
   bbcutil -getcbport <hostname>
   ```

   b. Check if the default DOMAIN parameter is correctly set for the managed nodes using the command:

   ```
   ovconfget bbc.http DOMAIN
   ```

   This should be set to the default domain, for example, myco.com.

   c. Check if a process has the Communication Broker port open and is listening for connections using the command:

   ```
   pipe tcpip netstat -an |search sys$pipe 383

   You should see something similar to (varies on each platform):
   tcp        0      0  *.383                    *.*                      LISTEN
   ```

   LISTEN verifies that a process is listening on the specified port. If this is displayed and the Communication Broker is not running, another process is using the port and the Communication Broker will not startup.

3. Check the HTTP Communication capabilities by entering the following commands.

   On the Operations Manager Server and the Certificate Authority server:

   ```
   <OvInstallDir>/bin/bbcutil -ovrg server -ping \
   http://<OVO managed node>[:<AGENT-PORT>]/
   ```

   On the HTTPS managed node:

   ```
   bbcutil ping http://OVO management server[:<MGMT-SRV-PORT>]/
   ```

   On the Certificate Server:

   ```
   <OvInstallDir>/bin/bbcutil -ping http://Certificate Authority server[:<CA-SRV-PORT>]/
   ```

   If no port is specified in these command, the default port 383 is used.

Each call should report:

```
status=eServiceOK
```

A.2.3 Authentication and Certificates Troubleshooting for HTTP Communication

Troubleshooting Basic HTTP communication uses the following commands:

```
ovc
ovconfget
ovconfchg
ovcoreid
ovcert
bbcutil
```

To check for authorization and certificate related HTTP communication problems, complete the following steps:

1. Check the `OvCoreID` of each system. On the Operations Manager Server or the Certificate Authority server, enter the command:

   ```
   ovcoreid
   ```

   On HTTPS managed node, enter the command:

   ```
   ovcoreid
   ```

   Make a note of each of the displayed `OvCoreID` values:

   - <MGMT-SRV-COREID>
   - <CA-SRV-COREID>
   - <AGENT-COREID>

2. Check the certificates on the Operations Manager Server or Certificate Authority server and on HTTPS managed node using the following command:

   ```
   ovcert -list
   ```

   On each system there must be at least following Certificates.

   On HTTPS managed node:

   ```
   | Certificates: |
   | <AGENT-COREID> (*) |
   ```

   On the Operations Manager Server or the Certificate Authority server:

   ```
   | Certificates: |
   | <MGMT-SRV-COREID>|<CA-SRV-COREID> (*) |
   ```

   On all systems:

   ```
   | Trusted Certificates: |
   | <CA-SRV-COREID> |
   ```

   Note

   The (*) signifies that the private key for the certificate is available.

   To get more detailed information about the installed certificates, use the following commands:

On HTTPS managed node:

```
ovcert -check
```

On the Operations Manager Server:

```
ovcert -check
```

An example of the output is shown below:

```
OvCoreId set : OK
Private key installed : OK
Certificate installed : OK
Certificate valid : OK
Trusted certificates installed : OK
Check succeeded.
```

To check that the installed certificates are valid, use the following command and make sure that the current date is between the valid from and valid to dates of the installed certificates:

```
ovcert -certinfo <CertificateID>
```

Note

The CertificateID of a trusted certificates is the `OvCoreID` of the certificate server prefixed with a CA_.

An example of the output is shown below:

```
# ovcert -certinfo 071ba862-3e0d-74ff-0be4-b6e57d0058f2
Type : X509Certificate
Subject CN : 071ba862-3e0d-74ff-0be4-b6e57d0058f2
Subject DN : L: alien2.ext.bbn.com
O: Hewlett-Packard
OU: OpenView
CN: 071ba862-3e0d-74ff-0be4-b6e57d0058f2
Issuer CN : CA_99300c4e-f399-74fd-0b3d-8938de9900e4
Issuer DN : L: tcbbn054.bbn.hp.com
O: Hewlett-Packard
OU: OpenView
CN: CA_99300c4e-f399-74fd-0b3d-8938de9900e4
Serial no. : 04
Valid from : 01/27/04 12:32:48 GMT
Valid to : 01/22/24 14:32:48 GMT
Hash (SHA1): 60:72:29:E6:B8:11:7B:6B:9C:82:20:5E:AF:DB:D0: ...
```

3. Check the HTTPS communication capabilities using the following commands:

   On an Operations Manager Server or Certificate Authority server:

   ```
   bbcutil -ovrg server -ping https://<OVO managed node name>[:<AGENT-PORT>]/
   ```

   On HTTPS managed node:

   ```
   bbcutil -ping https://<OVO management server name>[:<MGMT-SRV-PORT>]/
   bbcutil -ping \
   https://Certificate Authority server[:<CA-SRV-PORT>]/
   ```

   Each call should report:

   ```
   status=eServiceOK
   The reported OvCoreID must match with the OvCoreIDs that you
   noted in the first step:
   coreID=<COREID>
   ```

A.2.4 Communication Troubleshooting

Troubleshooting communication uses the following commands:

```
Ovc
Ovconfget
Ovconfchg
Ovcoreid
Ovpolicy
Opcnode
opc /usr/bin/OpC/opc
```

To check for communication problems, complete the following steps:

1. HTTPS managed nodes must be in the Node Bank.
2. The Fully Qualified Domain Name (FQDN) of the managed node must match.
3. The communication type of the managed node must be HTTPS.
4. The `OvCoreID` of the managed node must match.

   In server, check the value of the managed node `OvCoreID` stored in the database using the command:

   ```
   opcnode -list_id node_list=<OVO managed node>
   ```

   It must match the <AGENT-COREID>.

   To check, on the managed node call the command:

   ```
   ovcoreid
   ```

   You can change the managed node `OvCoreID` from the Operations Manager Server using the command:

   ```
   opcnode -chg_id node_name=<OVO managed node> id=<AGENT-COREID>
   ```

   You can change the `OvCoreID` on the managed node using the command:

   ```
   ovcoreid -set <NEW-AGENT-COREID>
   ```

   Note

   Changing the `OvCoreId` of a system is an operation that must be done with great care because it changes the identity of a managed node. All managed node-related data, such as messages, are linked by the `OvCoreId` of a managed node. Changing the value of the `OvCoreID` should only be executed by experienced users who know exactly what they want to do and what is being affected by attempting this change, especially on the Operations Manager Server.

5. Check, that all Operations Manager Server processes are running using the commands:

   ```
   opcsv -status
   ```

   All registered processes must be in the state running.

   ```
   ovc -status
   ```

   All registered core processes must be in state running.

6. Make sure that the operator is responsible for the:
   - HTTPS managed node and its node group
   - Message group

   Reload the Message Browser.
7. If there are no managed node messages in the Message Browser on managed node, execute the following checks:
   - Check if all processes are running:

     ```
     ovc -status
     ```

     All registered processes must be running.
   - Check if the expected policies are deployed:

     ```
     ovpolicy -list
     ```
   - Check the MANAGER, MANAGER_ID, and CERTIFICATE_SERVER settings:

     ```
     ovconfget sec.cm.client "CERTIFICATE_SERVER"
     ```

     This must match the Certificate Authority server.

     ```
     ovconfget sec.core.auth "MANAGER"
     ```

     This must match the Operations Manager Server.

     ```
     ovconfget sec.core.auth "MANAGER_ID"
     ```

     This must match the `OvCoreID` of the Operations Manager Server.

     To check the `OvCoreId` of the management server, on the management server enter the command:

     ```
     ovcoreid
     ovconfget eaagt OPC_PRIMARY_MGR
     ```

     This setting is optional, but when set, it must match the Operations Manager Server.

A.2.5 Change the Management Server Responsible for a Managed Node

It is sometimes necessary to change the management server which manages a managed node. In the following steps, we concentrate on the changes required on the managed node. With DCE agents, you basically just had to change the OPC_MGMT_SERVER entry in the opcinfo file. With HTTPS agents, it is more complicated and the following topics must be taken into consideration:

1. Policy Cleanup on the Managed Node

   If the new server has a different certificate authority than the old one, the agent needs a new certificate. This also means that the policies on the agent become unreadable as soon as the agent gets a certificate from the new CA. Remove all policies, because they cannot be read anymore, using the command:

   ```
   ovpolicy -remove -all
   ```

If the CAs are the same, then the policies are basically readable, but the OvCoreId of the old server, which is contained in the certificates as part of the policy header files, must still be authorized. This is achieved by entering the name of the old management server in the mgrconf policy. The following file must exist and the old manager must be mentioned in it: <OvDataDir>/datafiles/policies/mgrconf/*data

If this is not the case, enter the command:

```
ovpolicy -remove all
```

2. Stop the Agent

   The agent should be stopped before doing further modifications:

   ```
   ovc -kill
   ```

3. Certificate Cleanup on the Agent

   If the new target server shares the same certificate authority as the old one, then the certificates can remain as they are. If not, then you must create new certificates.

   Remove the existing ones using the command:

   ```
   ovcert -remove <all_certs_listed_in_ovcert_-list_output>
   ```

4. Configuration Settings Cleanup

   Change some basic settings on the agent. The OvCoreId can remainunchanged:

   - If the certificate authority has changed, enter the following command to specify the new certificate authority:

     ```
     ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <new_CA>
     (typically the fully qualified hostname)
     ```

   - Set the new management server using the following command:

     ```
     ovconfchg -ns sec.core.auth -set MANAGER <new_mgmtsv>
     (typically the fully qualified hostname)
     ```

   - Obtain the management server OvCoreId value with the command:

     ```
     ovcoreid -ovrg server
     ```

   - Set the OvCoreId of the new management server on the agent:

     ```
     ovconfchg -ns sec.core.auth -set MANAGER_ID <new_manager_core_id>
     ```

5. Create New Certificates

   If the old certificates were removed, create a new certificate and perform manual certificate installation.

6. Prepare the Management Server

   On the new management server proceed in the same way as for adding a new managed node, certificate installation, assigning policies, and deploying configuration.

B

Tracing OVO

To help you investigate the cause of problems, OVO provides problem tracing. Trace logfiles can help you pinpoint when and where problems occur, for example, if processes or programs abort, performance is greatly reduced, or unexpected results appear.

B.1 OVO-Style Tracing Overview

All opcinfo trace settings used in OVO 7 can also be applied to the Operations Manager HTTPS agents. However, these are now configuration settings, which are set with the ovconfchg command.

You can activate the OVO trace facility for the HTTPS agent processes by entering the following ovconfchg command:

```
ovconfchg -ns eaagt -set OPC_TRACE TRUE
```

To de-activate tracing enter the following command:

```
ovconfchg -ns eaagt -clear OPC_TRACE
```

or

```
ovconfchg -ns eaagt -set OPC_TRACE FALSE
```

To trace an agent process enter the following command:

```
ovconfchg -ns eaagt -set OPC_TRACE TRUE -set OPC_TRC_PROCS <process>
```

where <process> refers to OVO process to be traced .

B.2 OpenView-Style Tracing Overview

Static Manual tracing using trace configuration files is currently supported on OpenVMS platform. manually create the trace configuration files specifying the components to be traced and log the trace output into a file.

Trace configuration file name should be exactly `OVTrace.tcf` (mixed case) since this is reserved in XPL.

'APP' line in `OVTrace.tcf` on OpenVMS should be in Capital letters with '.EXE' suffixed (ex: APP: "OVBBCCB.EXE")

'SINK' line in `OVTrace.tcf` specifies the name of the trace output file.

An example of OVTrace.tcf file to trace Communication broker:

```
TCF Version 3.2
APP: "OVBBCCB.EXE"
SINK: File "/var/opt/OV/tmp/tracebbc.trc" "force=2;maxfiles=10;maxsize=1500;"
TRACE: "xpl.log"             "Trace"      Info Developer
TRACE: "xpl.runtime"             "Trace"      Info Developer
TRACE: "xpl.thread.mutex"             "Trace"      Info Developer
TRACE: "xpl.config"            "Trace"      Info Developer
TRACE: "xpl.thread"            "Trace"      Info Developer
TRACE: "xpl.io"             "Trace"      Info Developer
TRACE: "bbc.cb"             "Trace"      Info Developer
TRACE: "xpl.cfgfile"             "Trace"      Info Developer
TRACE: "bbc.http"             "Proc"      Info Developer
TRACE: "bbc.http"             "Trace"      Info Developer
TRACE: "bbc.http.client"             "Trace"      Info Developer
TRACE: "bbc"             "Trace"      Info Developer
TRACE: "xpl.msg"             "Trace"      Info Developer
TRACE: "xpl.net"             "Trace"      Info Developer
TRACE: "bbc.messenger"             "Proc"      Info Developer
TRACE: "bbc.rpc"             "Proc"      Info Developer
TRACE: "bbc.rpc.server"             "Trace"      Info Developer
TRACE: "bbc.http.server"             "Trace"      Info Developer
TRACE: "bbc.http.dispatcher"             "Trace"      Info Developer
TRACE: "opcmsg"                    "Trace"      Info Developer
```

To enable static tracing copy OVTrace.tcf~ config file to the following location before starting agents:

```
OVO$POSIX_ROOT:[VAR.OPT.OV.CONF.OVXPLTRC]OVTrace.tcf
```

(or)

Define a logical "TRACE_CONFIG_FILE" to specify the name and location of the trace configuration file.

For example:

```
define/sys TRACE_CONFIG_FILE OVO$POSIX_ROOT:[VAR.OPT.OV.DATAFILES.XPL]OVTrace.tcf
```

Restart OVO Agents to start tracing.

The trace output file(SINK) file will be in binary format and can be converted to ascii using ovtrcmon utiility:

```
ovtrcmon -fromfile <Binary sink file name> -tofile <Destination file>
```

Shut down OVO Agents to stop tracing. Make sure that either OVTrace.tcf is deleted and "TRACE_CONFIG_FILE" is deassigned before agents are restarted for normal operation (without tracing).