HP OpenVMS Operations Manager HTTPS Agents Version 8.6 Configuration Guide

Table of Contents

1 Introduction

HTTPS agent software provides highly secure communication between HP Operations Manager 8.x management servers and their managed nodes. HTTPS agents are generally used and administered in the similar 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 policies for DCE-based agents.

This document has references to HP Operations Manager (HPOM) and HP OpenView Operations (HP OVO). Note that all these product names refer to the same product. For information about HP Operations HTTPS Agent architecture, see HTTPS Agent Concepts and Configuration Guide Version: 8.51.

Organization of HTTPS Managed Nodes

Generic Directory Structure on a Managed Node

By default, the files associated with the HTTPS agent are found in the following directories and its sub directories:

- `OVINSTALLDIR` logical name refers to `OVO$POSIX_ROOT:[OPT.OV]`

  This directory contains static files that are installed from the product and never change. For example, executable.

- `OVDATADIR` logical name refers to `OVO$POSIX_ROOT:[VAR.OPT.OV]`

  This directory contains configuration and runtime data files that are used only on the local system.

- `OVDATADIR:[BIN.INSTRUMENTATION]`

  The most important directory contains the instrumentation files such as actions, commands and monitors.

- The `OVINSTALLDIR:[NEWCONFIG.INVENTORY]*.xml` files contain a list of all the directories and files that are created and installed with the agent software.

HPOM Agent User Accounts

By default, the HPOM agent runs from SYSTEM account on OpenVMS. The current release does not support running HPOM agents by alternative users.

HTTPS agent libraries

On OpenVMS operating system, applications must link with the shared libraries, located at:

For OpenVMS Integrity servers:

`SYS$SHARE:OVO$LIBOPC_R.EXE`

For OpenVMS Alpha:

`SYS$SHARE:OVO$LIBOPC_R.EXE`

Include Files

On supported managed node platforms, use the appropriate include file, such as, `OVO$POSIX_ROOT:[OPT.OV.INCLUDE]opcapi.h`

HTTPS Communication Administration Commands

HTTPS Communication can be controlled using commands such as `ovcoreid, ovc, bbcutil, ovconfget, ovconfchg, ovpolicy, and ovcert`. For more information about HTTPS communication administration commands, see chapter *HP Operations HTTPS Agent Overview* of the HTTPS Agent Concepts and Configuration Guide Version: 8.51.

HTTPS Communication

For information about HTTPS communication concepts, see chapter *Concepts of HTTPS Communication* of the HTTPS Agent Concepts and Configuration Guide Version: 8.51.

Security

For information about the following security concepts, see chapter *Security Concepts* of the HTTPS Agent Concepts and Configuration Guide Version: 8.51:

- HTTPS Based Security Components
- Security in Manager of Manager (MoM) Environments
- Related HPOM commands that differs in syntax on OpenVMS
  - `ovcert -remove "<alias>"`
  - `ovconfchg -ns sec.cm.client -set “CERTIFICATE_SERVER”`
  - `"<management server B hostname>"`
  - `ovconfchg -ns sec.core.auth -set “MANAGER”`
  - `ovconfchg -ns sec.core.auth -set “MANAGER_ID” "<management server B OvCoreId>"`

Working with Certificates

For information about Working with Certificates, see chapter *Working with Certificates* of the HTTPS Agent Concepts and Configuration Guide Version: 8.51.

Following are the HPOM related commands that differ in syntax on OpenVMS:

- `opc_inst -configure <profile> is not supported`
- `ovcoreid -set <id> -force`
- `ovconfchg -nssec.cm.client -set “CERTIFICATE_DEPLOYMENT_TYPE” “MANUAL”`
- `ovcert -importcert -file <filename>`
- `ovcert -certreq -instkey <filename>`

Manager of Manager (MoM) Environments

For information about MoM Environments, see HTTPS Agent Concepts and Configuration Guide Version: 8.51 .

Logging and Tracing

This section describes the various methods available for error logging and tracing.

Error Logging for HTTPS Agents

The errors for HTTPS Agents are automatically logged in the “system.txt” error log file. This error log file is located at:

```
OVDATADIR:[LOG]System.txt
```

VMSSPI Logging

To debug VMSSPI issues, logging for VMSSPI must be enabled. The log files will take the form of the following:

```
VMSSPI$PERFORMANCE_nodename.LOG
```

```
VMSSPI$SECURITY_nodename.LOG
```

```
VMSSPI$SYSTEM_nodename.LOG
```

To turn on logging, define the logical that controls the log file location. The log file must be set to a VALID disk and a VALID qualified directory. If you enter a disk that is not mounted to the machine where the VMSSPI is running or if you enter a directory that does not exist, the VMSSPI will not run. After logging is turned on complete the following steps:

1. Shut down the VMSSPI and HTTPS agents by executing the following commands:

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

2. Define the log file logical as follows:

   ```
   $ define/sys ovo$logdir SYS$SYSDEVICE:[OVO]
   ```

   All the log files for the VMSSPI will now be written to the specified disk.

3. Restart the VMSSPI and HTTPS Agents:

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

Tracing Overview

To activate normal tracing, complete the following steps:

1. Stop all agent processes including VMSSPI by executing the following commands:

   ```
   $ @sys$startup:ovo8$define
   $ @sys$startup:vmsspi$shutdown ovc -stop
   ```

2. Activate the trace facility for the HTTPS agent processes by executing the following:

   ```
   $ ovconfchg -ns eaagt -set “OPC_TRACE” “TRUE”
   $ ovconfchg -ns eaagt -set “OPC_TRACE_AREA” “ALL”
   $ ovconfchg -ns eaagt -set “OPC_TRC_PROCS” “<process1>,
   <process2>,...”
   ```

3. Start all agent processes including VMSSPI by executing the following commands:

   ```
   $ @sys$startup:ovo8$define
   $ @sys$startup:ovo8$startup
   $ @sys$startup:vmsspi$startup
   ```

To activate debug tracing, complete the following steps:

1. Stop all agent processes including VMSSPI.

   ```
   $ @sys$startup:ovo8$define
   $ @sys$startup:vmsspi$shutdown
   ovc –stop
   ```

2. Activate the trace facility for the HTTPS agent processes by executing the following:

   ```
   $ ovconfchg -ns eaagt -set “OPC_TRACE” “TRUE”
   $ ovconfchg -ns eaagt -set “OPC_TRACE_AREA” “ALL,DEBUG”
   $ ovconfchg -ns eaagt -set “OPC_TRC_PROCS” “<process1>,
   <process2>,...”
   ```

```
$ ovconfchg -ns eaagt -set “OPC_DBG_PROCS” “<process1>,
<process2>,...”
```

3. Start all agent processes including VMSSPI by executing the following commands:

   ```
   $ @sys$startup:ovo8$define
   $ @sys$startup:ovo8$startup
   $ @sys$startup:vmsspi$startup
   ```

To deactivate normal or debug tracing, execute the following commands:

```
$ @sys$startup:ovo8$define
$ @sys$startup:vmsspi$shutdown
$ ovc –stop
$ ovconfchg -ns eaagt -clear OPC_TRACE
```

or

```
$ ovconfchg -ns eaagt -set OPC_TRACE FALSE
$ ovconfchg -ns "eaagt" -clear "OPC_TRACE_AREA"
$ ovconfchg -ns "eaagt" -clear "OPC_TRACE"
$ ovconfchg -ns "eaagt" -clear "OPC_TRC_PROCS"
$ ovconfchg -ns "eaagt" -clear "OPC_DBG_PROCS"
```

The trace file is created at `OVO$POSIX_ROOT:[VAR.OPT.OV.TMP.OPC]trace`.

HP Encourages Your Comments

HP welcomes your comments on this document.

Send comments to the following address:

openvmsdoc@hp.com