HP Insight Management Agents for OpenVMS
Installation Guide
Version 3.4

This document contains information required for installing and using Version 3.4 of the Management Agents for OpenVMS.

The document contains the following sections:

- Section 1, Installing HP TCP/IP and Enabling SNMP
- Section 2, Prior to Installing the Management Agents Software
- Section 3, Installing the Management Agents for OpenVMS Software
- Section 4, Working with MultiNet
- Section 5, Working with TCPware
- Section 6, Smart Array Agent Configuration
- Section 7, Notes
- Section 8, Appendix
- Section 9, Trademarks

1 Installing HP TCP/IP and Enabling SNMP

Before you install the Management Agents for OpenVMS software on your Alpha or I64 system with HP TCPIP stack, follow these steps:

1. Install TCP/IP

   For TCP/IP installation instructions, refer to *TCP/IP Services for OpenVMS – Management.*

2. Enable SNMP

   If SNMP is not enabled on your system, follow these steps:

   a. Execute the following command procedure:

      ```
      $ @SYS$MANAGER:TCPIP$CONFIG
      ```

   b. On the list of displayed options, select:

      ```
      Option 3 - Server components
      ```

   c. On the next list of displayed options, select:

      ```
      Option 17 - SNMP (for Version 5.1-ECO 4)
      Option 18 - SNMP (for Version 5.3 or later)
      ```

   d. On the next list of displayed options, select:

      ```
      Option 3 - Enable & Start service on this node
      ```

   e. Exit from the configuration utility.

3. Enter the following command after the DCL prompt:

   ```
   $ TCPIP SHOW CONFIGURATION -
   _$ SNMP/FULL
   ```

   The resulting display must be similar to the following:

   ```
   SNMP Configuration
   .
   .
   .
   Community   Type   Address_list
   public      Read   0.0.0.0
   ```

a. If the "public" Community does not appear in the display, enter the following command:

```
$ TCPIP SET CONFIG -
_$ SNMP/COMMUNITY="public"/ -
_$ type=read
```

b. Enter the following command again after the DCL prompt to display the "public" Community:

```
$ TCPIP SHOW CONFIGURATION -
_$ SNMP/FULL
```

4. To enable Sets (setting disk/CPU/memory threshold) and SNMP Traps on Management agents, refer to the User Guide, “Enabling Set and SNMP Traps” Section.
5. Restart the SNMP Server, after making any SNMP configuration changes

a. If you are running SNMP, you must stop and restart ESNMP. In SYS$MANAGER, run the following:

```
$ @TCPIP$SNMP_SHUTDOWN.COM
$ @TCPIP$SNMP_STARTUP.COM
```

b. If you are not running SNMP, you must start ESNMP. In SYS$MANAGER, run the following:

```
$ @TCPIP$SNMP_STARTUP.COM
```

6. Use the DCL command SHOW SYSTEM to ensure that SNMP is enabled on the system. The system must display the TCP/IP processes, as shown below:

```
TCPIP$SNMP_1
TCPIP$OS_MIBS
TCPIP$HR_MIB
```

If you do not see all of these processes, review your TCP/IP setup and repeat Section 1, if necessary.

Note

If you use MultiNet and TCPware from Process Software, refer to Sections 4 and 5 of this document for information on setting up the products to operate with the Management Agents.

2 Prior to Installing the Management Agents Software

Before you install the Management Agents for OpenVMS Version 3.4 kit, you must stop all Management Agent processes and processes from other products like the Smart Array Configuration Utility (ACU-XE) that are dependent on the Management Agents.

1. Enter the following DCL command:

```
$ SHOW SYSTEM
```

2. If any of the following processes are running, you must stop them before installing the kit:

Version 1	Version 2 and later	HP Array Configuration Utility for Smart Array Controllers
ELM/GINKGO	WBEM$SERVER	CPQ$ACUXE
CPQHOST_MIB	WBEM$CPQHOST	
CPQSCSI_MIB	WBEM$CPQSTORE	
CPQSYSINFO_MIB	WBEM$CPQSYSINFO	
CPQSTDEQUIPMIB	WBEM$CPQSTDEQUIP	
CPQHEALTH_MIB	WBEM$CPQHEALTH	
CPQTHRESH_MIB	WBEM$CPQTHRESH	
CPQNIC_MIB	WBEM$CPQNIC	
	WBEM$DCLSHOW	
	WBEM$SVRCLU	
	WBEM$CPQIDA	

3. While logged in to the same node from which you started the agents, enter the appropriate command for the process to be terminated:

Management Agents Prior to Version 2.1	`$ @SYS$SPECIFIC:[WBEM]STOP_WEBAGENTS`
Management Agents Version 2.1 and later	`$ @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN`
Array Configuration Utility for Smart Array Controllers	`$ @SYS$SPECIFIC:[WBEM.ACUXE]CPQ$ACUXE-stop`

4. Remove the existing version of the Management Agents from your system by entering the following DCL command:

```
$ PRODUCT REMOVE MGMTAGENTS
          or
$ PRODUCT REMOVE V83_MGMTAGENTS
          or
$ PRODUCT REMOVE V82_MGMTAGENTS
          or
$ PRODUCT REMOVE V73_MGMTAGENTS
```

5. Download and install the HP Secure Sockets Layer (SSL) for OpenVMS kit from this web site:

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

   Note

   Starting with OpenVMS V8.3, SSL is integrated with the operating system and need not be downloaded and installed separately.

6. If you have Smart Array controller hardware present in your system environment you may need to update the HP Array Configuration Utility for Smart Array controllers (ACU-XE) to a version compatible with this Management Agent kit. The updated ACU-XE utility and supporting documentation may be obtained from the HP Array Configuration Utility home page located at:

```
http://h71000.www7.hp.com/openvms/products/acuxe/
```

7. If upgrading from a previous version of Management Agent kit installation, administrators are advised to record all WBEM$ADMIN rights identifier assignments in the system UAF prior to installing the Insight Management Agents for OpenVMS software. Installation of the kit will revoke these rights identifiers unconditionally as part of the upgrade. The recorded assignments can be used to re-enable access privileges to the state prior to the Management Agent kit upgrade. Within the AUTHORIZE utility, enter the following command to identify holders of the WBEM$ADMIN rights identifier:

   ```
   UAF> SHOW /IDENTIFIER/FULL WBEM$ADMIN
   ```

8. Users upgrading from a prior version Management Agent kit are advised to backup any customizations made to the WEBAGENT.INI file since this file will be unconditionally replaced as part of the Management Agent upgrade process. The complete file specification is:

   ```
   SYS$SPECIFIC:[WBEM.WEB.IM.WEBAGENT]WEBAGENT.INI
   ```

9. Before installing the Management Kit please review the following configuration scenarios to determine which best applies to your system software environment

   - Standalone or Shared Media Cluster System Installation – You are installing the Management Agents onto a standalone or a shared storage OpenVMS cluster system environment. This is the most common installation type, encompassing first-time installation, upgrade, and re-installation of the Management Agents. Kit installation for this case follows the sequence detailed in Section 3 without modification.
   - Non-shared Cluster System Disk Installation – You are installing the Management Agents into a cluster configuration where two or more member nodes are configured with system volumes resident on non-shared physical media. If your system environment falls into this category note that you need to repeat the installation sequence detailed in Section 3 once for each non-shared system volume while logged into its resident OpenVMS environment.
   - Installation of a New Cluster Member– You are installing the Management Agents to a shared storage resident cluster member node that was not present at the time the Management Agents were installed on other nodes of the cluster. The installation procedure follows that described in Section 3 with the added requirement that the installation of the Management Agents be conducted from one of the nodes on which the Agents are already installed.

3 Installing the Management Agents for OpenVMS Software

The installation procedure of the Management Agents for OpenVMS software will vary depending on which installation scenario was identified in Section 2. It is important to choose the appropriate installation procedure in order to ensure a trouble free kit installation.

On an OpenVMS cluster sharing a common system disk, the agents need not be installed separately on each node of the cluster. You must however install the agents separately on all the nodes in which the system root is not residing on a shared common system disk. For more information, refer to Section 8, Appendix.

To install the Management Agents for OpenVMS software, follow these steps:

1. Log in to the OpenVMS system using the SYSTEM account. If you need to use another privileged account, it must have the SETPRV privilege or all the following privileges:

   ```
   AUDIT, CMKRNL, DETACH, DIAGNOSE, LOG_IO, PHY_IO,
   NETMBX, OPER, PRMMBX, TMPMBX, SECURITY, SHARE,
   SYSLCK, SYSNAM, SYSPRV, WORLD
   ```

2. Copy the HP Insight management agents kit and the manifest file (For Kit validation on OpenVMS V8.3 and above) to SYS$UPDATE:

   ```
   HP-I64VMS-MGMTAGENTS-V0304-1-1.PCSI$COMPRESSED
   (Kit on I64)

   HP-I64VMS-MGMTAGENTS-V0304-1-1.PCSI$COMPRESSED_ESW
   (Manifest file on I64)

   or

   HP-AXPVMS-MGMTAGENTS-V0304-1-1.PCSI$COMPRESSED
   (Kit on Alpha)

   HP-AXPVMS-MGMTAGENTS-V0304-1-1.PCSI$COMPRESSED_ESW
   (Manifest file on Alpha)
   ```

   IMPORTANT

   It is required to perform step #3 below prior to initiating the PRODUCT INSTALL operation on the Management Agent kit. Failure to adhere to this instruction could result in installation errors and incomplete kit component file delivery.

3. Ensure that all Management Agent processes and other processes that are dependent on the Management Agents (such as ACU-XE) have been stopped. The Management Agents processes can be shutdown by executing the following command. You may ignore any ‘file not found’ or non-existent process messages resulting from executing this command.

   ```
   $ MC SYSMAN SET ENVIRONMENT/CLUSTER

   SYSMAN > DO @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN

   SYSMAN > EXIT
   ```

   To shutdown other processes dependent on the Management Agents, refer to the respective product documentation. As an example, to shut down the ACU-XE processes, execute the following DCL command

   ```
   $ MC SYSMAN SET ENVIRONMENT/CLUSTER

   SYSMAN > DO @SYS$SPECIFIC:[WBEM.ACUXE]CPQ$ACUXE –
   stop

   SYSMAN > EXIT
   ```

4. To install the appropriate PCSI kit, enter the following DCL command:

   ```
   $ PRODUCT INSTALL MGMTAGENTS
   ```

5. The file SYS$MANAGER:WBEM$LOGICALS.COM defines the logical names used by the Management Agents for OpenVMS. This file lists all the logical names supported by the agents, but the lines are commented out by default. Using a text editor, open this file, uncomment the lines containing the logical names you require, and edit the parameters if required. The file includes comments that explain the significance of each logical name.

   - To use the DCL SHOW command application, define the following logical name:

     ```
     $ DEFINE/SYSTEM/EXEC WBEM$DCL TRUE
     ```

   - To make your cluster name known to the cluster subagent, define the following logical name:

     ```
     $ DEFINE/SYSTEM/EXEC WBEM$CLUSTER_NODE clustername
     ```

     The cluster name must correspond to a valid TCP/IP cluster alias.

   - To specify a warning temperature for your system, define the following logical name:

     ```
     $ DEFINE/SYSTEM/EXEC WBEM$WARNING_TEMP warningtemperature
     ```

     The warning temperature corresponds to an integer value.

     A default value which is about 5° C below the shutdown temperature defined for the system will be taken for DS20, DS25, ES40, ES45 and GS Alpha systems.

     Similarly, for an I64 system (OpenVMS Version 8.2-1 and above), the maximum operational temperature on the system will be used as the default value.

     For all other hardware, you need to specify a value relevant to your system by defining this logical name. If you do not specify this value, the temperature threshold will display as 0^{o} C, and SNMP traps will not be generated. Refer to the documentation that came with your system for the appropriate temperature threshold value.

   - To view environmental details (like temperature, fan, power sensor information) on DS25, ES45, GS and later Alpha systems, define the following logical name:

     ```
     $ DEFINE/SYSTEM/EXEC WBEM$PRIVATEER TRUE
     ```

     On an Alpha system, to view environmental details (like temperature, fan, power sensor information) on DS25, ES45 and later systems, you must have the following:

     - OpenVMS Version 7.3 or later
     - Firmware revision Version 6.2 or later

     To view environmental details on GS80 and later systems, you need to have the following on your system:

     - OpenVMS Version 7.3-1 or later
     - Firmware revision Version 6.2 or later

     To view environmental details on Next Generation AlphaServers such as GS1280, ES47 and ES80, you must be running OpenVMS V7.3-2 or later.

     If your system meets or exceeds these requirements, you can enable the display of the environmental details by defining the above logical name.

Note

- You do not have to make these entries for older Alpha hardware.
- Environmental details might not get displayed on older Alpha hardware.
- If you define this logical name on OpenVMS Version 7.3 systems with older firmware revisions, the system might crash.

For OpenVMS I64 system, the logical, is not required to be defined. The environmental details (temperature, fan, and power sensor information), are supported from OpenVMS I64 V8.2-1 onwards.

Note

There is delay of 4-5 minutes in the display of environmental details after starting Management Agents on I64 systems.

6. To run the Management Agents, enter the following commands:

```
$ SET DEFAULT SYS$SPECIFIC:[WBEM]
$ @WBEM$STARTUP
```

   Ensure that the Management agents are started using the SYSTEM account or any account having the privileges mentioned in Step #1.

7. To verify that the Management Agents are running, enter the DCL command

```
$ SHOW SYSTEM/PROCESS=WBEM*
```

   The system should display the following processes:

Process	Definition
WBEM$CPQNIC	This process implements the Compaq NIC MIB[1] and provides Network Interface Card information.
WBEM$CPQTHRESH	This process implements the Compaq Threshold MIB[1]. It is used to set thresholds (like Disk, CPU, Memory) and raises SNMP Traps when the threshold is exceeded.
WBEM$CPQHEALTH	This process implements the Compaq Health MIB[1] and provides the Environmental details (See Step #5, defining WBEM$PRIVATEER logical) and power on messages.
WBEM$CPQSTORE	This process implements the COMPAQ SCSI SUPPORT SNMP MIB[1], COMPAQ FIBRE CHANNEL ARRAY SNMP MIB[1] and Compaq Manageable IDE Drive MIB[1]. It provides details on SCSI controllers/Fiber Channel (FC) Controller/IDE devices installed on your system (The Adapter is connected to the system). It does not provide details on Smart Array controller SA5300A, SA6400A, SA6402, SA6404, P400 connected to the system as the WBEM$CPQIDA process is used to provide the details of these controllers.

[1] To get more details on the MIB variables supported by Insight Management Agents on OpenVMS, refer to the User Guide, Appendix Section. The MIB files are located in SYS$SPECIFIC:[WBEM.AGENTS] directory, after installation.

WBEM$CPQSYSINFO	This process implements the COMPAQ SYSTEM INFORMATION SNMP MIB[1]. This process provides details like the architecture, System serial number.
WBEM$CPQSTDEQUIP	This process implements the Standard PC equipment configuration MIB[1]. It provides details on standard equipment (Like CPU, PCI, serial/parallel ports etc)
WBEM$CPQHOST	This process implements the COMPAQ HOST OS RELATED INFORMATION SNMP MIB[1]. It provides Host specific details like, Host name, Type, Disks and CPU utilization etc.
WBEM$CPQIDA	This process implements the DRIVE ARRAY SNMP MIB[1] and STORAGE SYSTEMS SNMP MIB[1]. It provides details on Smart Array SA5300A, SA6400A, SA6402 (I64) and SA6404 (I64), P400 (I64) controllers and attached storage. This process would terminate, if no relevant Smart Array controllers is detected.
WBEM$SVRCLU	This process implements the COMPAQ Common Cluster Management MIB[1]. It provides the details of the nodes in the cluster. This process runs only on a clustered system. You need to define the logical WBEM$CLUSTER_NODE (See Step#5), for the process to work.
WBEM$SERVER	This process provides the display and navigation to Insight Management Agents Homepage and the related pages under - Configuration, Mass Storage, NIC, Utilization, Recovery sections.
WBEM$DCLSHOW	This process provides display and navigation to OpenVMS DCL Show Commands. The Logical WBEM$DCL should be defined to “TRUE” (See Step #5) for the process to run.
WBEM$GSVIEW	This process provides display and navigation to See GSView system in the local subnet. This process runs only on GS-Series Alpha Server.

8. To ensure that the Management Agents survive a reboot, edit the SYSTARTUP_VMS.COM file. Insert the following line in SYS$STARTUP:SYSTARTUP_VMS.COM, following the entries required to start the TCP/IP and SSL processes:

   ```
   $ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP
   ```

9. You are now ready to view your OpenVMS system or systems using a web browser or Systems Insight Manager. Use either of the following instructions:

   - From a web browser, enter the following URL, which will allow you to communicate with the management agent of the system you want to manage:

     ```
     https://node_address:2381
     ```

     For *node_address*, substitute the TCP/IP node name or address of the system you want to monitor.

   - If you are using Systems Insight Manager, add the TCP/IP addresses of your OpenVMS nodes to the device discovery section, perform a device discovery, and select your OpenVMS node.

4 Working with MultiNet

This section describes how to use the Management Agents for OpenVMS with MultiNet TCP/IP Version 4.3 for OpenVMS or later from Process Software. You must install some components of the Compaq or HP TCP/IP product along with MultiNet to ensure that all features of the Management Agents work correctly.

For more information about MultiNet, refer to the MultiNet User documentation.

Follow these instructions to set up MultiNet to work with the Management Agents for OpenVMS:

1. Install MultiNet TCP/IP Version 4.3 for OpenVMS or later, with required patches.
2. Add the following line to the file MULTINET:SNMPD.CONF

```
AGENTX_PEER 127.0.0.1
AGENTX_PEER <IP address 1>
AGENTX_PEER <IP address 2>
...
AGENTX_PEER <IP address n>
```

   Where "IP address 1", "IP address 2", **. . ., "**IP address n" is the IP address configured on the OpenVMS system on each of the NIC interface.

3. Comment out any SMUX_PEER from the file MULTINET:SNMPD.CONF.

```
! SMUX_PEER <IP Address>
```

4. Add the following community strings to MULTINET:SNMPD.CONF

```
community public 127.0.0.1 READ
community public <ip address 1> READ
community public <ip address 2> READ
...
community public <ip address n> READ
```

Where "IP address 1", "IP address 2", . . ., "IP address n" is the IP address configured on the OpenVMS system on each of the NIC interface.

5. Extract TCPIP$ACCESS_SHR.EXE and TCPIP$ESNMP_SHR.EXE from the Compaq TCP/IP Services V5.1 or later kit and place them in SYS$SHARE:

```
$ PRODUCT EXTRACT FILE/SELECT=<filename>
```

Note

Make sure all files extracted from the TCP/IP Services kit have WORLD:RE protection.

6. Copy TCPIP$ESNMP_SHR.EXE to SYS$SHARE:UCX$ESNMP_SHR.EXE.
7. Extract TCPIP$HR_MIB.EXE from the TCP/IP Services kit and place it in the SYS$SYSTEM directory. Define the following logical names:

```
$ DEFINE/SYSTEM/EXECUTIVE MULTINET_SNMP_AGENTX 1
$ DEFINE/SYSTEM TCPIP$AGENTX_INET_PORT 705
$ DEFINE/SYSTEM TCPIP$AGENTX_LOCAL_PORT 705
```

8. Create the file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_CONF.DAT and add the following line to the file:

```
community public 127.0.0.1 read
```

9. Create the file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$VMS_SNMP_CONF.DAT on the target system

   Sample contents of the file TCPIP$VMS_SNMP_CONF.DAT:

```
#
# TCPIP$VMS_SNMP_CONF.dat - Sample config file for
  SNMP
# configuration extensions.
#
# Note about general format, tab vs. spaces.
# Note about # as comment.
#
# Keyword "config" precededs any options which
  will  be assigned to process
# usermode logical.  "TCPIP$" is prepended to each
  logical, so for example
# SNMP_TRACE becomes logical name
TCPIP$SNMP_TRACE.
# Some default, some no need value.
# Examples:
# config SNMP_TRACE
#
# if want process visible, first #config is:
# config SNMP_SYSTEM_LOGICALS
# Keyword "accept" controls for remote subagents.
#
# Other keywords as in UNIX snmpd.conf.  Note
  about sysname
# sysname Moxie909
# config snmp_allow_inet_transport
  config    trap    v1      elmginkgo 127.0.0.1
```

10. To enable Sets (setting disk/CPU/memory threshold) and SNMP Traps on Management agents, refer to the User Guide, “Enabling Set and SNMP Traps” Section.
11. Enable the SNMP Service and Start/Restart the Multinet SNMP services as described in the Multinet Install and Admin Guide (Configuring Multinet SNMP Services section).
12. Start the HR_MIB if it is not already started::

```
$ RUN/PROCESS=HR_MIB SYS$SYSTEM:TCPIP$HR_MIB
```

    The Host Resources MIB (RFC 1514) supplied with TCP/IP Services will now work with MultiNet.

13. Start the Management Agents for OpenVMS using the following command:

```
$ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP.COM
```

5 Working with TCPware

This section describes how to use the Management Agents for OpenVMS with TCPware TCP/IP Version 5.5 for OpenVMS or later from Process Software. You must install some components of the Compaq or HP TCP/IP product along with TCPware to ensure that all features of the Management Agents work correctly.

For more information about TCPware, refer to the TCPware User documentation.

Follow these instructions to set up TCPware to work with the Management Agents for OpenVMS:

1. Install TCPware TCP/IP Version 5.5 for OpenVMS or later, with required patches. Ensure that the Loopback address (127.0.0.1) is configured properly on TCPWARE.
2. Add the following line to the file TCPWARE:SNMPD.CONF

```
AGENTX_PEER 127.0.0.1
AGENTX_PEER <IP address 1>
AGENTX_PEER <IP address 2>
...
AGENTX_PEER <IP address n>
```

Where "IP address 1", "IP address 2", . . ., "IP address n" is the IP address configured on the OpenVMS system on each of the NIC interface.

3. Comment out any SMUX_PEER from the file TCPWARE:SNMPD.CONF.

```
! SMUX_PEER <IP Address>
```

4. Add the following community strings to TCPWARE: SNMPD.CONF

```
community public 127.0.0.1 READ-ONLY
community public <ip address 1> READ-ONLY
community public <ip address 2> READ-ONLY
...
community public <ip address n> READ-ONLY
```

Where "IP address 1", "IP address 2", . . ., "IP address n" is the IP address configured on the OpenVMS system on each of the NIC interface.

5. Ensure that the SNMP agent and AGENT X service are enabled during the configuration of SNMP on TCPware.
6. Extract TCPIP$ACCESS_SHR.EXE and TCPIP$ESNMP_SHR.EXE from the Compaq TCP/IP Services V5.1 or later kit and place them in SYS$SHARE:

```
$ PRODUCT EXTRACT FILE/SELECT=<filename>
```

Note

Make sure all files extracted from the TCP/IP Services kit have WORLD:RE protection.

7. Copy TCPIP$ESNMP_SHR.EXE to SYS$SHARE:UCX$ESNMP_SHR.EXE.
8. Extract TCPIP$HR_MIB.EXE from the TCP/IP Services kit and place it in the SYS$SYSTEM directory. Define the following logical names:

```
$ DEFINE/SYSTEM TCPIP$AGENTX_INET_PORT 705

$ DEFINE/SYSTEM TCPIP$AGENTX_LOCAL_PORT 705
```

9. Create the file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_CONF.DAT and add following line to the file

```
community public 127.0.0.1 read
```

10. Create the file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$VMS_SNMP_CONF.DAT on the target system

Sample contents of the file TCPIP$VMS_SNMP_CONF.DAT:

```
#
# TCPIP$VMS_SNMP_CONF.dat - Sample config file
  for SNMP
# configuration extensions.
#
# Note about general format, tab vs. spaces.
# Note about # as comment.
#
# Keyword "config" precededs any options which
will   be assigned to process
# usermode logical.  "TCPIP$" is prepended to each
logical, so for example
# SNMP_TRACE becomes logical name
TCPIP$SNMP_TRACE.
# Some default, some no need value.
# Examples:
# config SNMP_TRACE
#
# if want process visible, first #config is:
# config SNMP_SYSTEM_LOGICALS
# Keyord "accept" controls for remote subagents.
#
# Other keywords as in UNIX snmpd.conf.  Note
about   sysname
# sysname Moxie909
# config snmp_allow_inet_transport
config    trap    v1      elmginkgo 127.0.0.1
```

11. To enable Sets (setting disk/CPU/memory threshold) and SNMP Traps on Management agents, refer to the User Guide, “Enabling Set and SNMP Traps” Section.
12. Enable the SNMP service and Start/Restart the TCPWare SNMP services as described in the TCPWare Installation and Configuration Guide (Configure SNMP Services section).
13. Start the HR_MIB if it is not already started:

    ```
    $ RUN/PROCESS=HR_MIB SYS$SYSTEM:TCPIP$HR_MIB
    ```

    The Host Resources MIB (RFC 1514) supplied with TCP/IP Services will now work with TCPware.
14. Start the Management Agents for OpenVMS using the following command:

    ```
    $ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP.COM
    ```

6 Smart Array Agent Configuration

The Smart Array (CPQIDA) SNMP agent can be configured to provide the following functionality:

- Physical Drive Location – A physical drive attached to a Smart Array controller under inspection from the Management Agent’s Device Home Page can be made to flash its LEDs via the “Identify Drive” function on the drive’s property page.
- Smart Array event notification via SNMP traps – The Smart Array agent will generate SNMP traps on detection of certain events occurring in the storage array environment provided by the controller.

Use the following configuration checklists in conjunction with the procedures described elsewhere in the Management Agents and TCPIP documentation to enable additional Smart Array agent functionality. Unless otherwise specified, all host references in the checklists are to the system containing the Smart Array controller hardware. Drive location and SNMP trap delivery by the Smart Array agent can be jointly enabled by an appropriate combination of SNMP and Management Agents configuration operations, which meet the requirements, detailed below.

6.1 Configuration for Physical Drive Location

1. A SNMP community name must be configured on the host and defined with WRITE access. Keep in mind that SNMP community names are case sensitive.
2. The host SNMP configuration must include the SETS flag.
3. If the configured community name supporting Smart Array agent functionality is defined to be something other than the “public” community, the value of the IDS_SNMP_WRITE_COMMUNITY variable in the file SYS$SYSROOT:[WBEM.WEB.IM.WEBAGENT]WEBAGENT.INI must be changed to correspond to the configured SNMP community name.
4. The default address list for a newly defined SNMP community provides for unrestricted access by host IP address (i.e., 0.0.0.0). If the configured SNMP community address list is further restricted from the default, the host’s IP loopback address (127.0.0.1) must be included in the IP address list associated with the configured community name. Other IP addresses may be included in the address list as appropriate.
5. The Identify Drive function requires that a user login with account credentials that include the WBEM$ADMIN rights identifier.

   An example of a basic configuration permitting physical drive location which employs the “public” community and an unrestricted host IP access list can be established by executing the following two commands:

   ```
   $ TCPIP SET CONFIGURATION SNMP /FLAG=SETS
   ```

```
$ TCPIP SET CONFIGURATION SNMP /COMMUNITY="public" /TYPE=WRITE
```

After making these configuration changes, it is necessary to restart the SNMP service and Management Agents in the following order:

```
$ @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN

$ @SYS$MANAGER:TCPIP$SNMP_SHUTDOWN

$ @SYS$MANAGER:TCPIP$SNMP_STARTUP

$ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP
```

6.2 Smart Array SNMP Trap Configuration

The essential configuration steps to provide SNMP trap notification of Smart Array events are:

1. An SNMP community name must be configured on the host containing the Smart Array controller hardware, which has been defined for TRAP delivery. Keep in mind that SNMP community names are case sensitive when configuring your network monitoring station.
2. The SNMP community configured for trap delivery must have the host's IP loopback address (127.0.0.1) configured as part of its defined IP address list and ip_address where you want the trap message to be delivered (Network Monitoring Station like IM7); for example, 16.0.0.23.

   An example configuration for permitting of SNMP trap events generated by the Smart Array agent to the "elmginkgo" community with a network monitoring station address 16.0.0.23 can be established by executing the following SNMP configuration commands:

   ```
   $ TCPIP SET CONFIGURATION SNMP /COMMUNITY="elmginkgo" /TYPE=TRAP

   $ TCPIP SET CONFIGURATION SNMP /COMMUNITY="elmginkgo" -
   _$/ADDRESS=(127.0.0.1, 16.0.0.23)
   ```

   After making these configuration changes, it is necessary to restart the SNMP service and Management Agents in the following order:

   ```
   $ @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN

   $ @SYS$MANAGER:TCPIP$SNMP_SHUTDOWN

   $ @SYS$MANAGER:TCPIP$SNMP_STARTUP

   $ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP
   ```

7 Notes

1. The following default file locations are used as the launch points for the Availability Manager and the OpenVMS Management Station:

Application	Location
Availability Manager on Windows 2000 or XP	C:\Documents and Settings\All Users\Start Menu\Programs\Availability Manager\dataan~1.lnk
OpenVMS Management Station on Windows	C:\WINNT\Profiles\All Users\Start Menu\Programs\OpenVMS Management Station\openvm~1.lnk
OpenVMS Management Station on Windows 95	C:\Windows\Start Menu\Programs\OpenVMS Management Station\openvm~1.lnk

   If you are unable to launch one of these products, the products were probably not installed at the default locations.

2. If you ever need to restart the Management Agents without rebooting, stop and then restart the Management Agents' processes using the following commands:

   ```
   $ @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN
   .
   ```

```
.
.
$ @SYS$SPECIFIC:[WBEM]WBEM$STARTUP
```

8 Appendix

This appendix contains a sample installation of OpenVMS Management Agents V3.4 on OpenVMS 7.3-2 system.

Ensure that all Management Agent processes and other processes that are dependent on the Management Agents (such as ACU-XE) have been stopped. If any of the following processes are running, you must stop them before installing the kit:

```
$ SHOW SYSTEM

WBEM$SERVER

WBEM$CPQHOST

WBEM$CPQSTORE

WBEM$CPQSYSINFO

WBEM$CPQSTDEQUIP

WBEM$CPQHEALTH

WBEM$CPQTHRESH

WBEM$CPQNIC

WBEM$DCLSHOW

WBEM$SVRCLU

WBEM$CPQIDA

CPQ$ACUXE
```

The Management Agents processes can be shutdown by executing the following command:

```
$ MC SYSMAN SET ENVIRONMENT/CLUSTER

SYSMAN > DO @SYS$SPECIFIC:[WBEM]WBEM$SHUTDOWN

SYSMAN > EXIT
```

To shutdown other processes dependent on the Management Agents, refer to the respective product documentation. As an example, to shut down the ACU-XE processes, execute the following DCL command:

```
$ MC SYSMAN SET ENVIRONMENT/CLUSTER

SYSMAN > DO  @SYS$SPECIFIC:[WBEM.ACUXE]CPQ$ACUXE –
stop

SYSMAN > EXIT
```

Remove the existing version of Management Agents from your system by entering the following DCL command:

```
$ PRODUCT REMOVE V73_MGMTAGENTS
```

The following product has been selected:

```
HP AXPVMS V73_MGMTAGENTS V3.3-1      Layered Product


Do you want to continue? [YES]
```

```
%PCSI-I-NOREF, product CPQ AXPVMS SSL V1.2 is no
longer referenced


-PCSI-I-NODEP, by another product as a software
dependency requirement

-PCSI-I-REMLP, you can remove product CPQ AXPVMS SSL
V1.2 at this time


Do you want to take this action? [NO]


Do you want to continue? [YES]


The following product will be removed from destination:


HP AXPVMS V73_MGMTAGENTS V3.3-1
DISK$ALPHA732:[VMS$COMMON.]

Portion done:
0%...10%...20%...30%...40%...50%...60%...70%...80%...
90%...100%

The following product has been removed:


HP AXPVMS V73_MGMTAGENTS V3.3-1      Layered Product
```

To install the PCSI kit, enter the following DCL command:

```
$ prod insta mgmtagents

The following product has been selected:

HP AXPVMS MGMTAGENTS V3.4-1           Layered Product

Do you want to continue? [YES]


Configuration phase starting ...


You will be asked to choose options, if any, for each
selected product and for any products that may be
installed to satisfy software dependency requirements.


HP AXPVMS MGMTAGENTS V3.4-1: HP Management Web Server


© 2006 Hewlett-Packard Development Company, L.P. All
rights reserved.


Hewlett Packard Company


Do you want the defaults for all options? [YES]


Do you want to review the options? [NO]


Execution phase starting ...
```

```
The following product will be installed to destination:

HP AXPVMS MGMTAGENTS V3.4-1 DISK$AXP731:[VMS$COMMON.]



Portion done:
0%...10%...20%...30%...40%...50%...60%...70%...80%...90
% ...100%

The following product has been installed:

HP AXPVMS MGMTAGENTS V3.4-1            Layered Product

HP AXPVMS MGMTAGENTS V3.4-1: HP Management Web Server

A current version of TCPIP was found. If you have not
enabled SNMP, please enable it now.
```

Note

Installation on OpenVMS Cluster may take several minutes or more after PCSI ...90 % complete status message is displayed before the installation progresses. The OpenVMS Management Agents uses this time to install the files on the other nodes in the cluster.

9 Trademarks

Hewlett-Packard and the HP logo are trademarks of Hewlett-Packard Development Company, L.P. in the U.S. and/or other countries.

MultiNet and TCPware are registered trademarks of Process Software.

All other trademarks and registered trademarks are the property of their respective holders.