HP OpenVMS Operations Manager HTTPS Agents Version 8.6 Administrator's Guide

Table of Contents

1 Introduction....5
1.1 Verifying the Prerequisites on an OpenVMS System....5
1.2 Installing HPOM Software on the Managed Node....6
1.2.1 Management server is Operations Manager for (OMU 8.3x)....6
1.2.1.1 Configuration on the Management Server....6
1.2.1.2 Remote Installation....8
1.2.1.3 Manual Installation....10
1.2.2 Management Server is Operations Manager for Windows (OMW 8.x)....10
1.2.2.1 Configuration on the Management Server....10
1.2.2.2 Remote Installation....14
1.2.2.3 Manual Installation....14
1.2.3 Management Server is Operations Manager for UNIX (OMU 9.x and OML 9.x)....18
1.2.3.1 Configuration on the Management Server....18
1.2.3.2 Remote Installation....22
1.2.3.3 Manual Installation....25
1.2.3.4 Manually Requesting the Certificate from the Managed Node....26
1.3 Uninstalling HPOM Software from the Managed Node....28
1.3.1 Management server is Operations Manager for UNIX (OMU 8.3x)....28
1.3.2 Management Server is Operations Manager for Windows (OMW 8.x)....29
1.3.3 Management Server is Operations Manager for UNIX (OMU 9.x or OML 9.x)....29
1.4 Agent Processes on HTTPS Managed Nodes....31
1.5 APIs and Libraries....32
1.6 HP Encourages Your Comments....35

1 Introduction

This guide describes the procedures to install and uninstall the HP OpenVMS HTTPS Operations Manager Agents software. It also describes how to compile and link application program using Operations Agent Message and Monitor APIs.

1.1 Verifying the Prerequisites on an OpenVMS System

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

HP Operations Manager HTTPS Agents and Smart Plug-In (SPI) software is now available on OpenVMS Alpha Version 7.3-2, 8.2, 8.3, and OpenVMS Integrity servers Version 8.2-1, 8.3, and 8.3-1H1. Ensure that 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 V5.0 or later`
- OpenVMS Integrity servers Version 8.3
  - `VMS83I_UPDATE V1.0 or later`
  - `VMS83I_SYS V1.0 or later`
  - `HP I64VMS VMS83I_ICXXL V5.0 or later`
- OpenVMS Integrity servers Version 8.3-1H1
  - `HP I64VMS VMS831H1I_ICXXL V2.0 or later`

The patches are available at the HP ITRC web address:

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

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

NOTE:

- Process Software's MultiNet and TCPWare are currently NOT supported by the HTTPS Operations Manager Agents for OpenVMS.
- Remote installation of Agents fail if previous kits of Operations Manager Agents exist in the SYS$UPDATE directory.
- If install or uninstall fails due to some reason, a cleanup operation has to be done as follows on the OpenVMS node before starting remote installation again:
  - Execute the command `@sys$update:opc_inst -c`
  - Stop any Agent or VMSSPI processes
  - Delete node specific directory `(OVO$<NodeName>)` and common directory (`OVO$COMMON_ALPHA` or `VO$COMMON_IA64`)
  - Delete the lock file `SYS$SYSTEM:LOCK.LCK`, if it exists.
- While doing remote installation or uninstallation on nodes especially in homogenous clusters, the Management Server console may appear to be hanging at times. This is a normal behavior.
- If you want to upgrade to OpenVMS HTTPS Operations Manager Agents V8.6 from previous version, the kit will be installed in the same disk, where the previous kit was installed irrespective of the disk name provided at the time of installation. Also, the policies are to be redeployed from the management server as new certificates are deployed during upgrade.
- If Management Server is configured not to grant certificates automatically, remote installation of Agents will result in a pending certificate request. You need to grant manually from the certificate request window on the Management Server and Agents must be restarted on the managed node subsequently.
- If installation or upgradation results in a failure message on the Management Server console, it is required to check the PCSI database on the OpenVMS node for confirmation. Sometimes it shows a failure message even if the Agents are installed successfully.

Make sure you have REXEC, RSH, and FTP services enabled on the remote agent (HTTPS-based) before you start the HPOM agent installation. Otherwise the agent installation will fail. Make sure that the SNMP agent is running before adding a managed node to the HPOM database.

1.2 Installing HPOM Software on the Managed Node

1.2.1 Management server is Operations Manager for (OMU 8.3x)

1.2.1.1 Configuration on the Management Server

1. Download `OpenVMS-OA-8.6.030C.tar` from the web to a directory (say /temp) on the Management Server and untar it by logging into the management server as 'root' user.

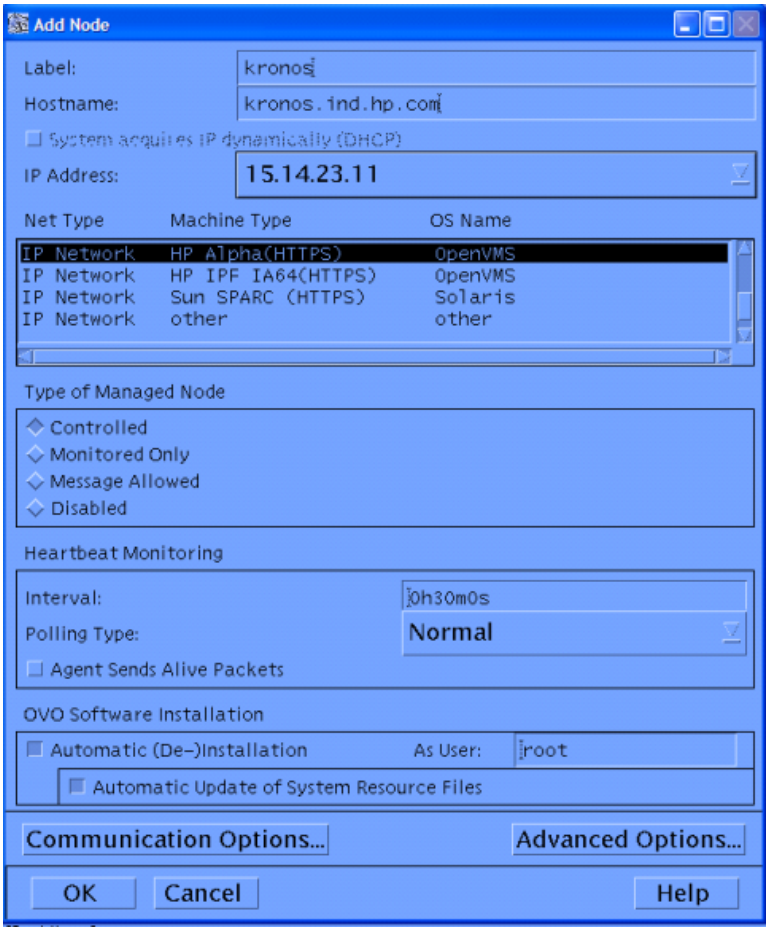
   ```
   # cd /temp
   # tar –xvf OpenVMS-OA-8.6.030C.tar
   ```

2. Execute the following script. This script performs the required validations on the management server.

   ```
   # cd /temp/OVMS8.60
   # ./OA-setup.sh
   ```

   You can use '-h' option with 'OA-setup.sh' for help.

3. To add a node, click **Actions** and select **Node** in the `Node Group` window.
4. Click **Add**. The **ADD Node** window is displayed. Enter the label and hostname as shown in the following figure and click **OK**.



5. If OpenVMS OS policies are not available on the management server, then download `ovmspolicies_u.tar` for OMU from the web to a directory on the management server. Execute the following steps as 'root' user for uploading the OpenVMS policies to OMU 8.3x Management Servers:
   a. Take a backup of previously existing OpenVMS policies, if any, on the management server as follows:
      1) In the **OVO Node Bank** window, go to **Window Menu** -> **Message source templates**.
      2) Select the **Template Group**, which has to be backed up.
      3) Click **Modify**.
      4) Change the **Template Group Name** in the **Modify Template Group** window.
   b. FTP `ovmspolicies_u.tar` to the OMU Management Server in binary mode.
   c. On the OMU Management Server, change directory to the location where `ovmspolicies_u.tar` file exists.
   d. RUN `tar -xvf ./ovmspolicies_u.tar`.
   e. RUN `./ovmspol-setup.sh`. This uploads the policies to the OMU management server.

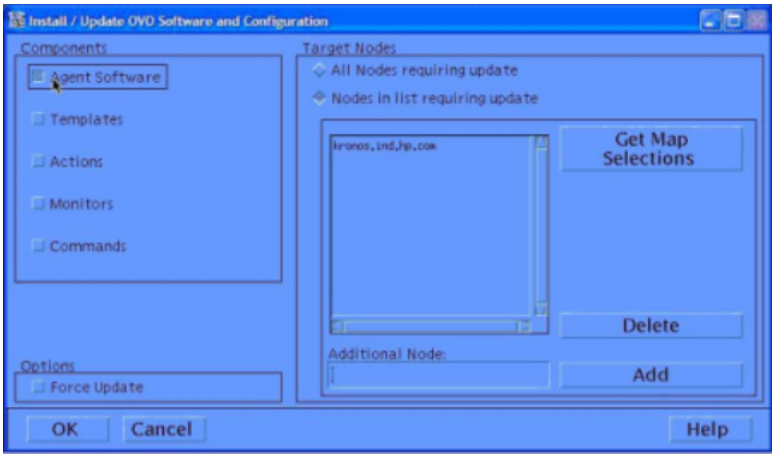
1.2.1.2 Remote Installation

Execute the following steps on the Management Server after logging in as 'root' user.

1. To install or update the software and configuration, click **Actions** and select **Agents** in the **Node Group** window.

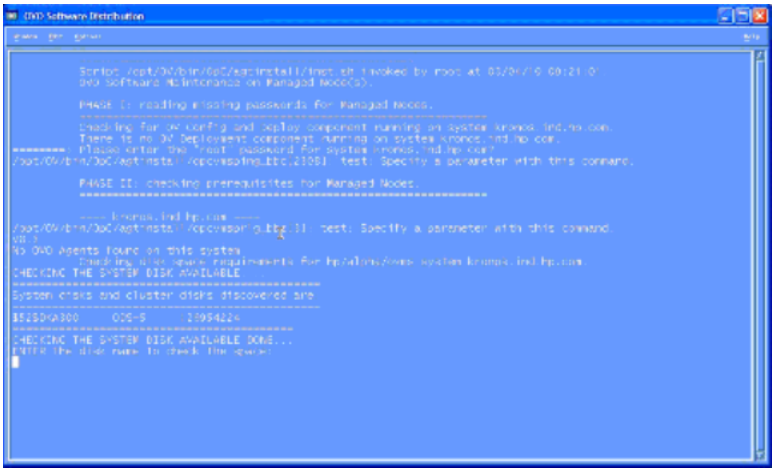
   If it is a new node, add the managed node to the Management Server.

2. Click **Agent/Install SW & Config**. The **Install/Update OVO Software and Configuration** screen appears.

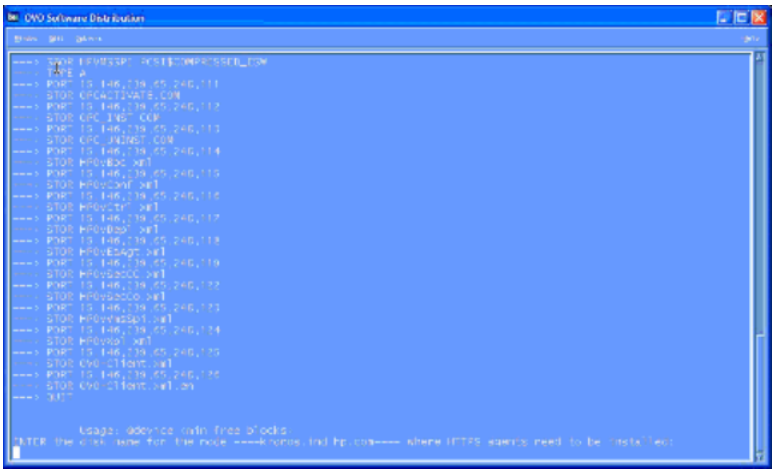


3. Select **Agent Software** and click **OK**.
4. Enter the system password of the managed node to continue the installation.

5. Enter one of the ODS-5 disks listed on the screen when prompted.

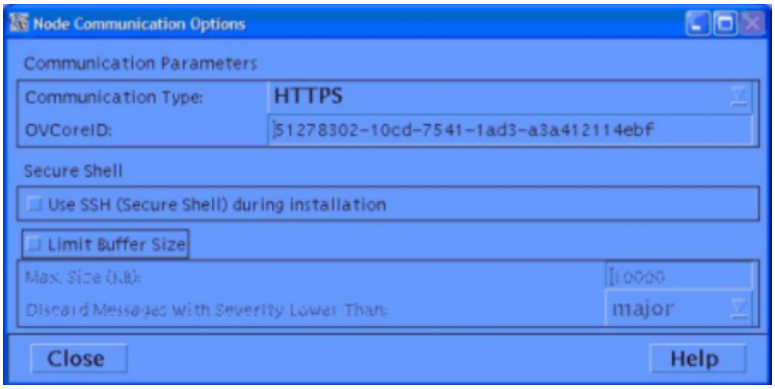


6. After you provide the disk name, it downloads the packages to the node and it prompts you to enter the ODS-5 disk name where the Openview agents will be installed.



7. After entering the disk name again, the installation starts. After the installation is complete, successful installation screen is displayed.

8. After the installation completes, check whether `ovcoreid` of the node is registered in the management server.



9. Login into the OpenVMS agent and check whether all the process are running.

```
$ ovc
ovcd    OV Control                    CORE         (1135)     Running
ovbbccb  OV Communication Broker       CORE           (1136)    Running
opcacta  OVO Action Agent              AGENT,EA       (1138)    Running
opcle   OVO Logfile Encapsulator      AGENT,EA      (1140)    Running
opcmona  OVO Monitor Agent             AGENT,EA       (1141)    Running
opcmsga  OVO Message Agent             AGENT,EA       (1137)    Running
opcmsgi  OVO Message Interceptor       AGENT,EA       (1142)    Running
ovconfd  OV Config and Deploy          COREXT         (1139)    Running
$
```

1.2.1.3 Manual Installation

See the Manual Installation section for "Management Server is Operations Manager for Windows (OMW 8.x)" (page 10).

1.2.2 Management Server is Operations Manager for Windows (OMW 8.x)

1.2.2.1 Configuration on the Management Server

1. Download `OpenVMS-OA-8.6.030C.tar` from the web to a directory (say c:\temp) on the Management Server and unzip the tar file using WINZIP by logging into the management server as 'Administrator'.
2. Execute the following batch file. This performs the required validations on the management server and copies the agent packages.

   ```
   cd c:\temp
   c:\temp\OVMS8.60\OA-setup.bat
   ```

   The agent packages for OpenVMS are copied to the following directories.

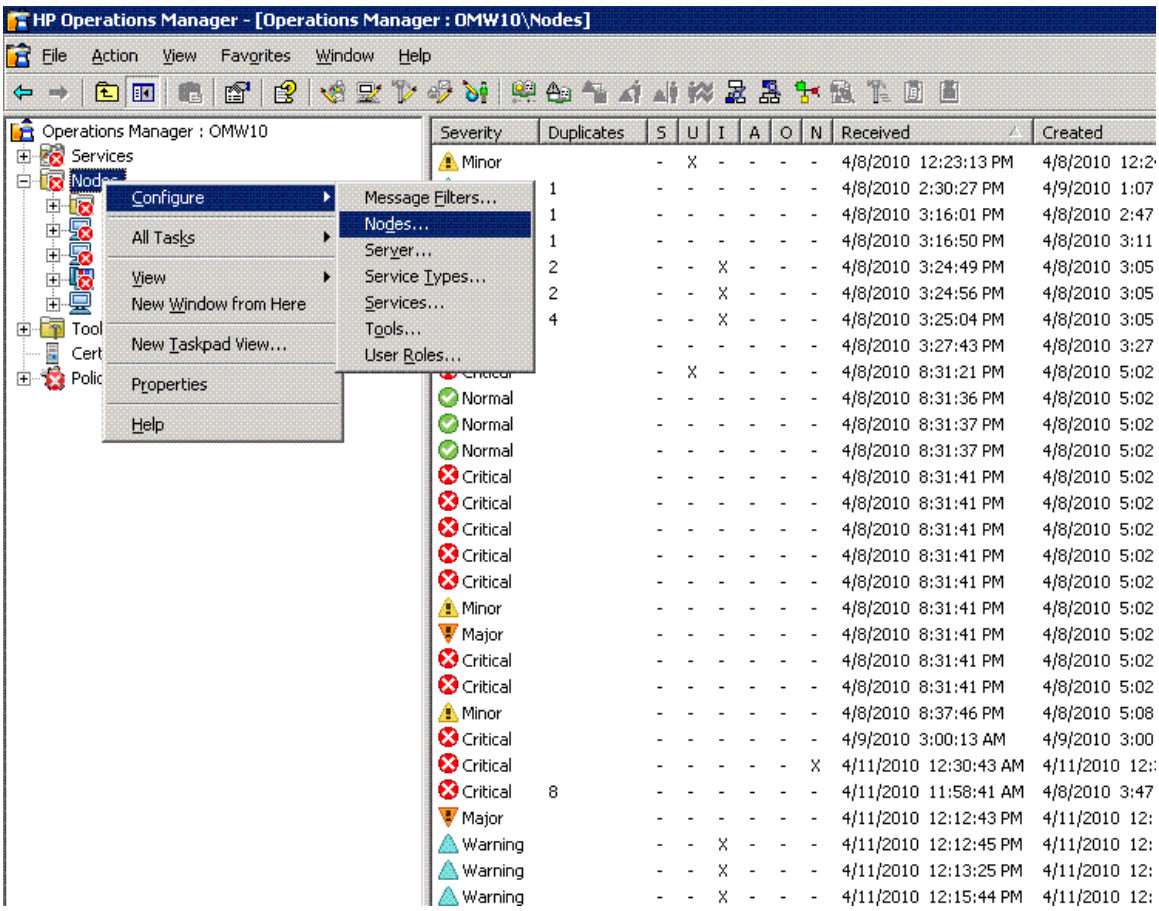
   For OpenVMS on Alpha:

   ```
   %OvShareDir%Packages\HTTPS\openvms\hp\7.3.2 8.2.0
   8.3.0\alpha\Operations-agent\08.60.030C\64\https
   ```

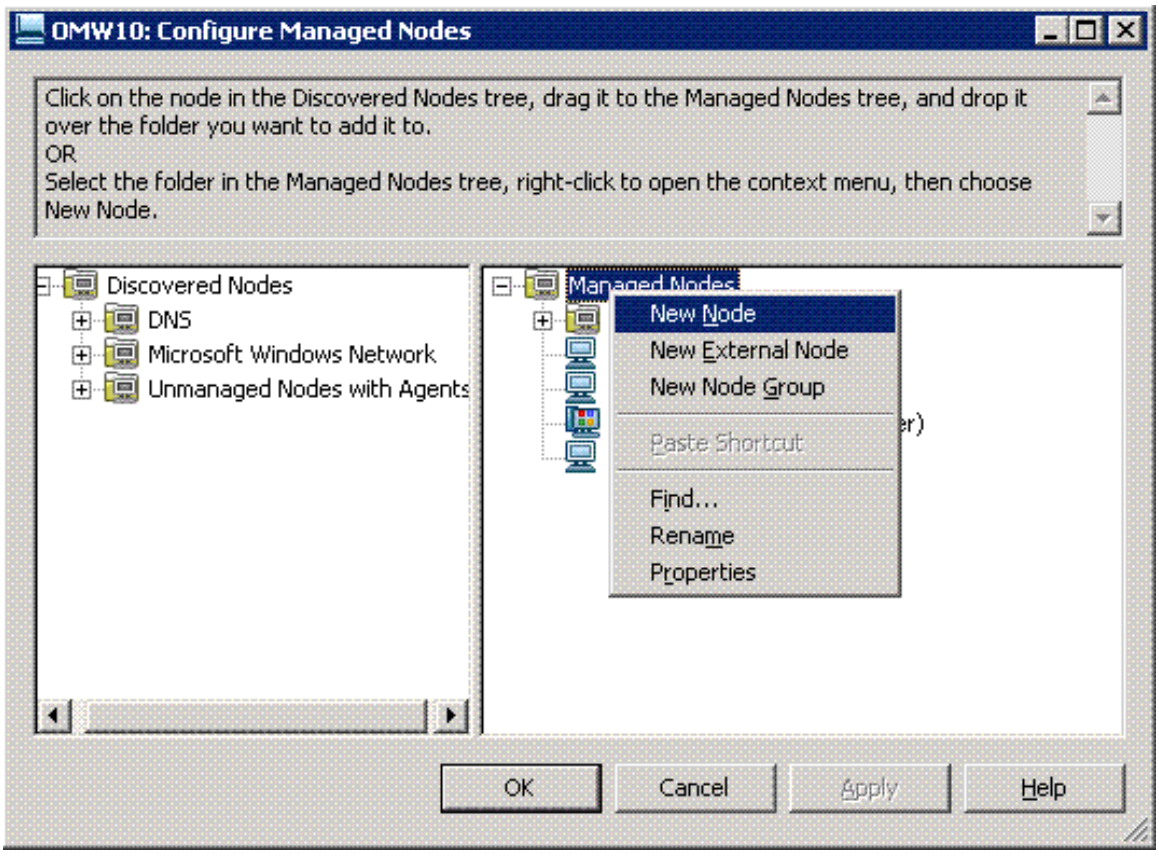
   For OpenVMS on Integrity servers:

   ```
   %OvShareDir%Packages\HTTPS\openvms\hp\8.2.1 8.3.0
   8.3.1\ipf64\Operations-agent\08.060.030C\64\https
   ```

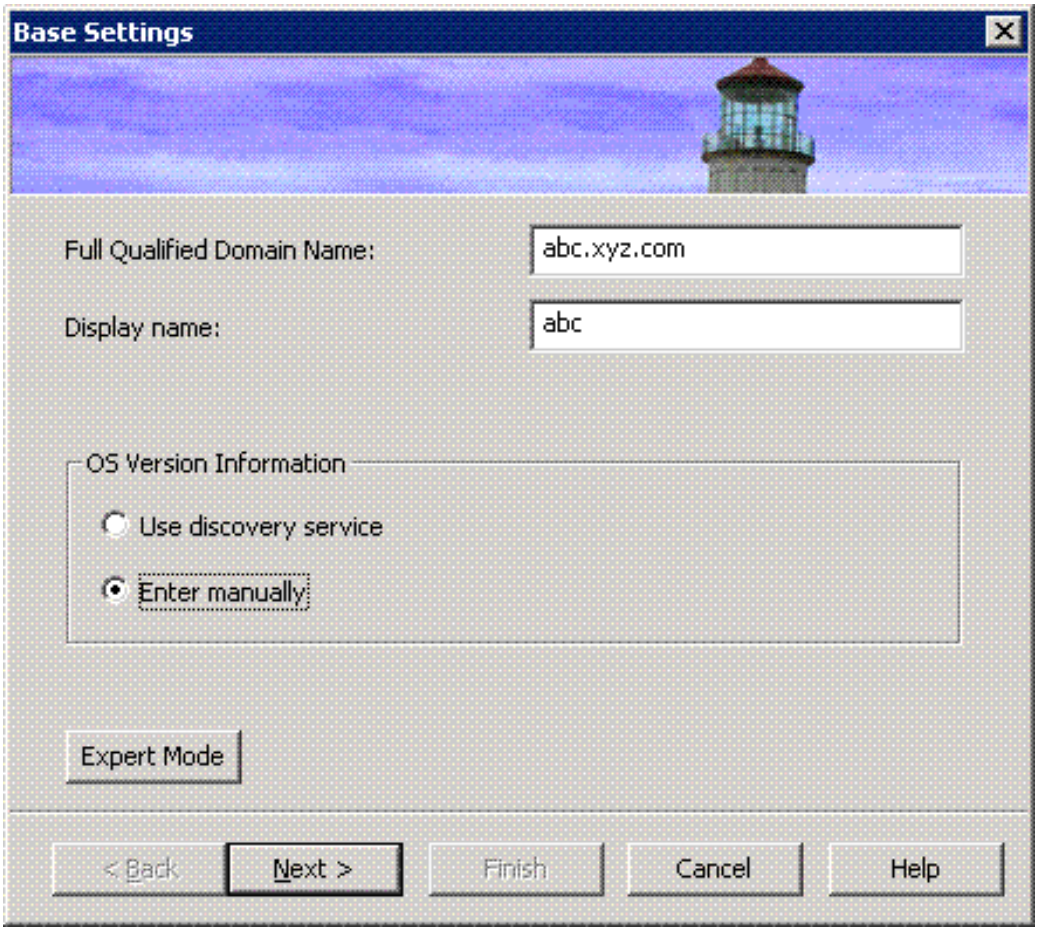
3. To add a node, right-click on **Nodes** on the left pane of HP Operations Manager console and select **Configure** -> **Nodes...**.



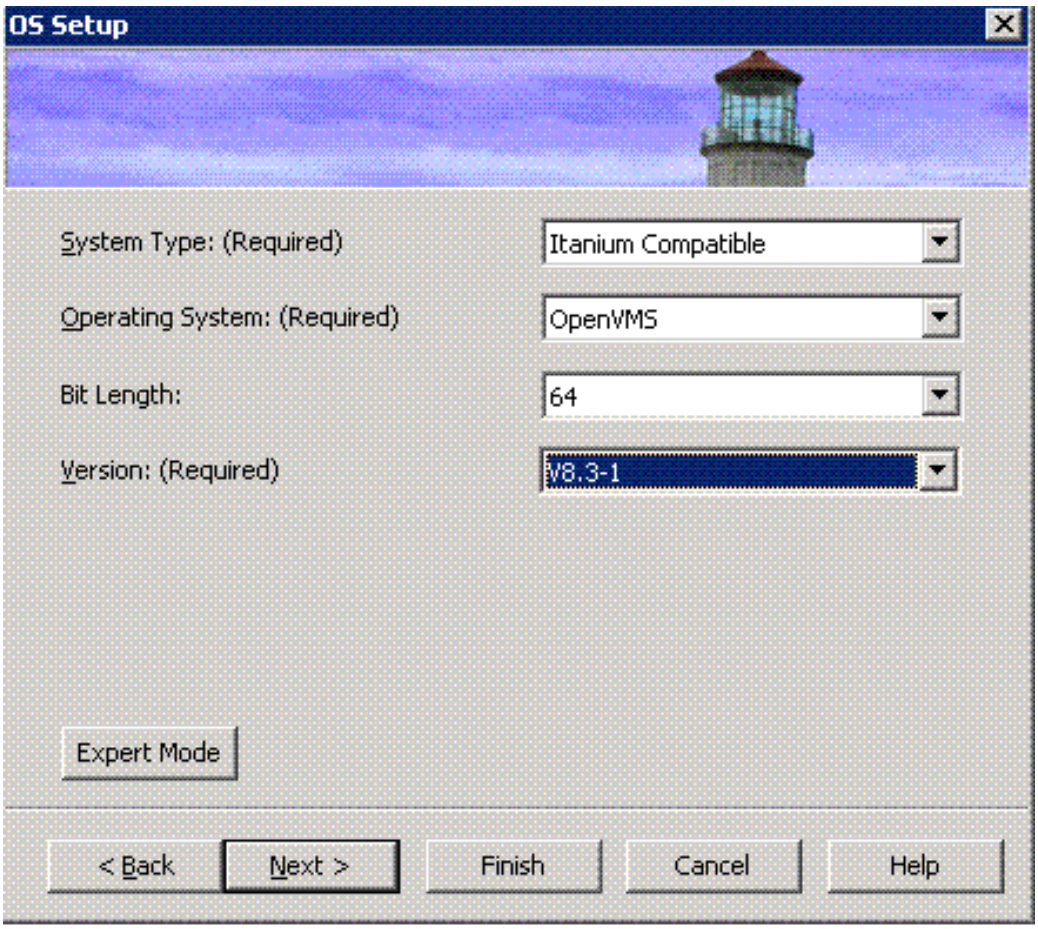
4. In the **Configure Managed Nodes** window, right-click on **Managed Nodes** and select **New Node**.



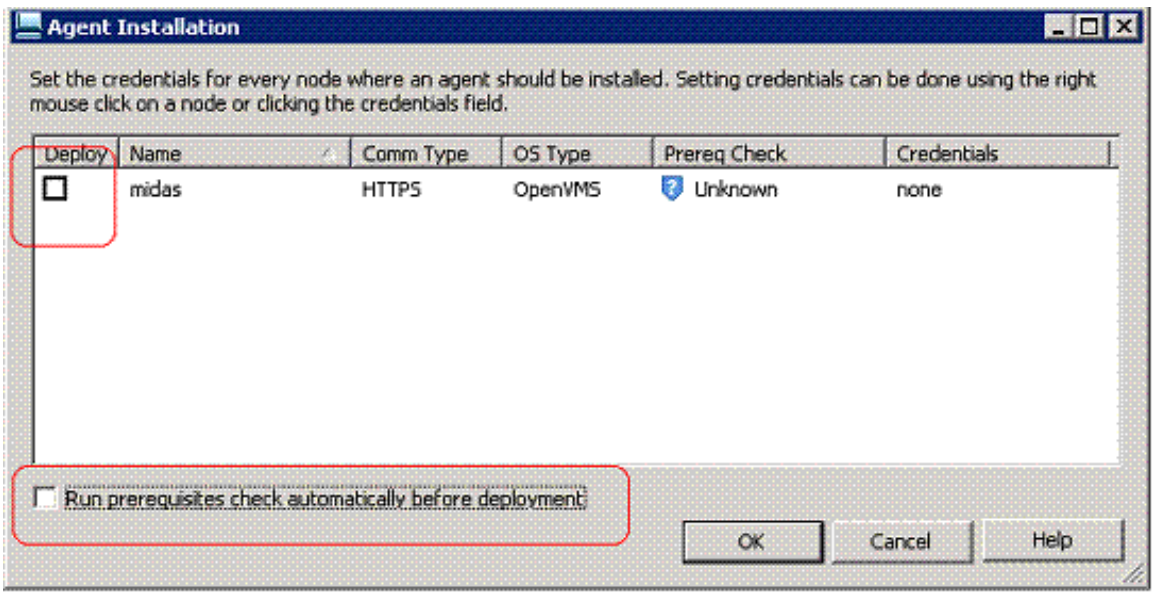
5. In the **Base Settings** window, provide OpenVMS node name and select the option **Enter Manually** under **OS Version Information**.



6. Provide the OpenVMS system details and click **Finish**.



7. Uncheck all the check-boxes on the **Agent Installation** window and click **OK**.



8. If OpenVMS OS policies are not available on the management server, then download `ovmspolicies_w.tar` for OMW from the web to a directory on the management server. Execute the following steps as 'Administrator' for uploading the OpenVMS policies to OMW 8.x Management Servers:

a. Download `ovmspolicies_w.tar` to the OMW Management Server.

b. On the OMW Management Server, change directory to the location where `ovmspolicies_w.tar` file exists.

c. Unzip `ovmspolicies_w.tar` using winzip.

d. In the management console, under **Policy management** ->**Policy groups**, rename OpenVMS_policies and OpenVMS_SPI_policies groups. Uploading new policies overwrites the modified policies, if any.

e. Execute `ovmspol-setup.bat`. This takes a backup of existing OpenVMS policies and uploads the new policies to the OMW management server.

1.2.2.2 Remote Installation

Remote installation is not supported when the management server is Operations Manager for Windows (OMW 8.x).

1.2.2.3 Manual Installation

1. Download `OpenVMS-OA-8.6.030C.tar` from the web to a temporary directory on the OpenVMS Managed Node and untar it by logging into managed node as 'SYSTEM'. If tar utility is not available on the OpenVMS node, then download VMSTAR.ALPHA_EXE (for Alpha) or VMSTAR.IA64_EXE (for Integrity server) from the web.

Execute the following commands to untar:

```
$ set proc/par=ext
$ tar :==$[<temporary directory>]:VMSTAR.IA64_EXE (For Integrity servers)
```

Or

```
$ tar :==$[<temporary directory>]:VMSTAR.ALPHA_EXE (For Alpha)
$ tar -xvf OpenVMS-OA-8^.6^.030C.tar
```

This untars the files in the OVMS8_60 directory under the temporary directory.

2. Change directory to OVMS8_60 and execute the script `OA_SETUP.COM` as 'SYSTEM':

```
$ @OA-SETUP.COM -i -srv <<management server>> -cert_srv <<certificate server>>
```

For example,

```
 $ @OA-SETUP.COM -i -srv abc.def.hp.com -cert_srv ghi.jkl.hp.com
```

3. Provide the ODS-5 disk details when prompted for installation disk. The installation of agents starts.

4. To check if the agents are installed successfully, execute the following commands:

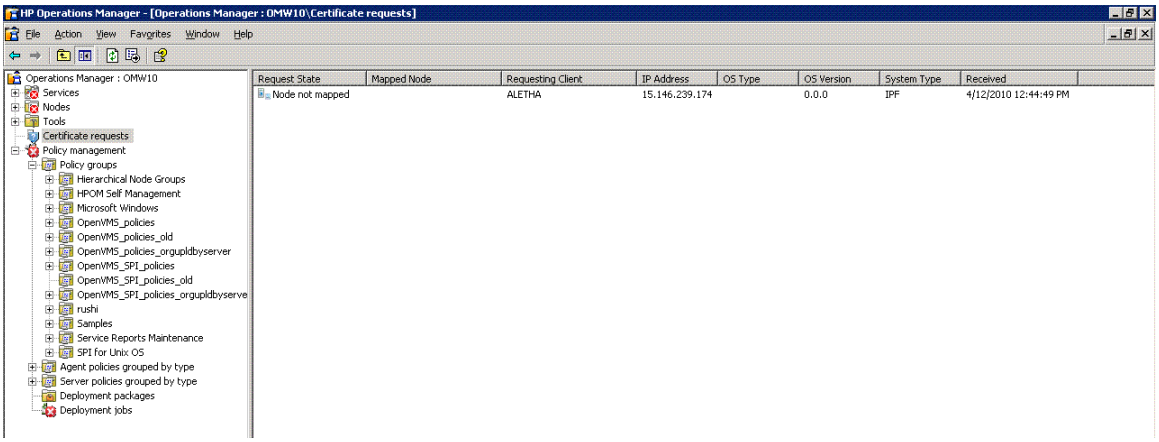
```
$PRODUCT SHOW PRODUCT OV*,VMSSPI
$ovc –status
$ovcert –list
```

The output of the commands must be as follows:

```
$PRODUCT SHOW PRODUCT OV*, VMSSPI
------------------------------------ ----------- ---------
PRODUCT                              KIT TYPE    STATE
------------------------------------ ----------- ---------
HP I64VMS OVBBC V8.6-1               Full LP     Installed
HP I64VMS OVCONF V8.6-1              Full LP     Installed
HP I64VMS OVCTRL V8.6-1              Full LP     Installed
HP I64VMS OVDEPL V8.6-1              Full LP     Installed
HP I64VMS OVEAAGT V8.6-1             Full LP     Installed
HP I64VMS OVSECCC V8.6-1             Full LP     Installed
HP I64VMS OVSECCO V8.6-1             Full LP     Installed
HP I64VMS OVXPL V8.6-1               Full LP     Installed
HP I64VMS VMSSPI V8.6-1              Full LP     Installed
------------------------------------ ----------- ---------
9 items found
$ovc -status
ovcd        OV Control                          CORE         (95D)    Running
```

```
opcacta     OVO Action Agent                    AGENT,EA     (960)    Running
opcle       OVO Logfile Encapsulator            AGENT,EA     (963)    Running
opcmona     OVO Monitor Agent                   AGENT,EA     (964)    Running
opcmsga     OVO Message Agent                   AGENT,EA     (95F)    Running
opcmsgi     OVO Message Interceptor             AGENT,EA     (965)    Running
ovbbccb     OV Communication Broker             CORE         (95E)    Running
ovconfd     OV Config and Deploy                COREXT       (961)    Running

$ovcert -list
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
+-------------------------------------------------------+
```

5. Login to the Windows Management Server to check whether a certificate request has been received for the OpenVMS node. Note that this certificate request is automatically initiated as part of installation.

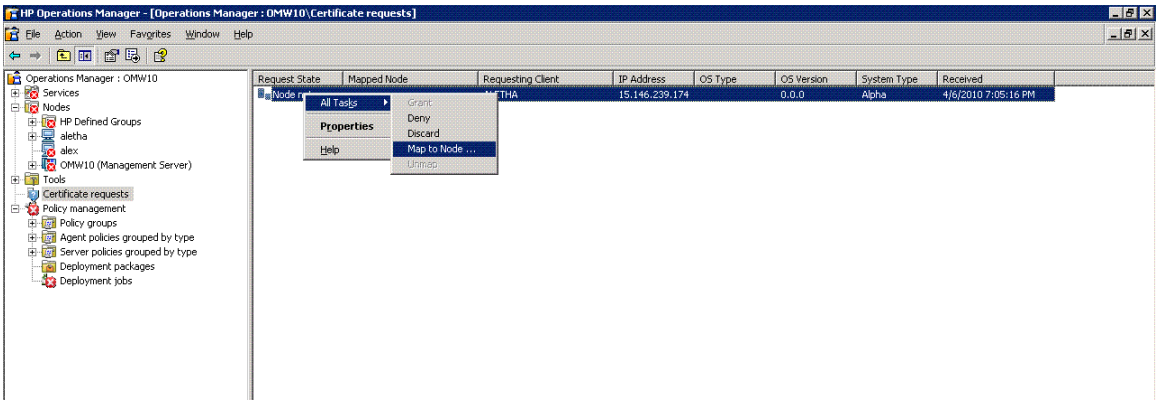


If the certificate request for the OpenVMS node is not listed, login to the OpenVMS node as SYSTEM and execute the following commands to initiate a certificate request:

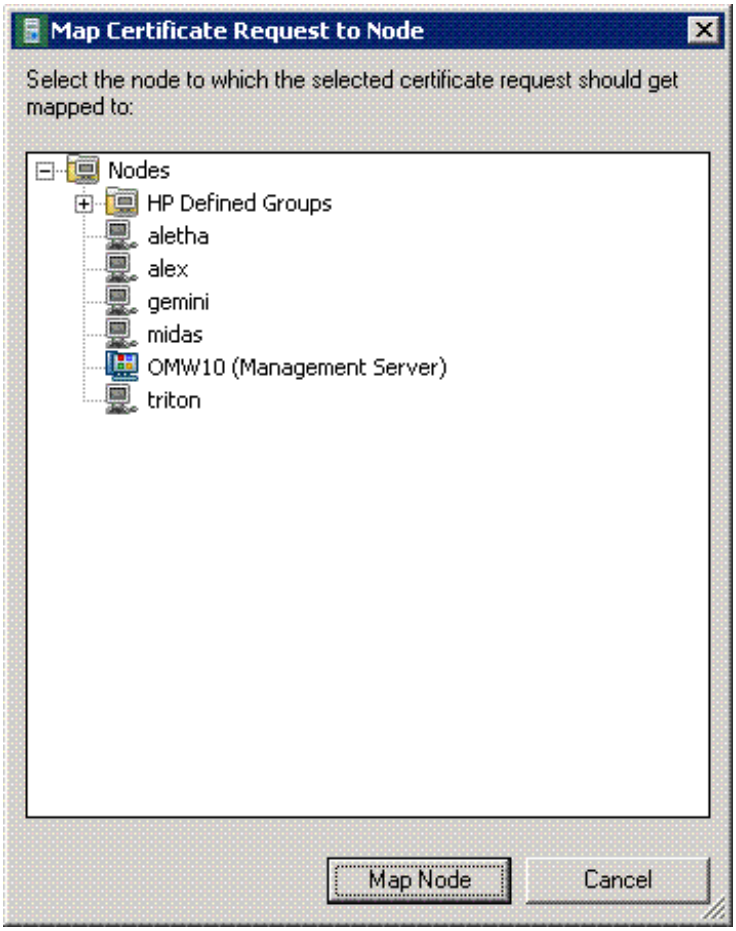
```
$@SYS$STARTUP:OVO8$DEFINE
$ovcert -certreq
```

6. Map the certificate request to the OpenVMS node on the Windows Management Server. Open the **Certificate request** window.

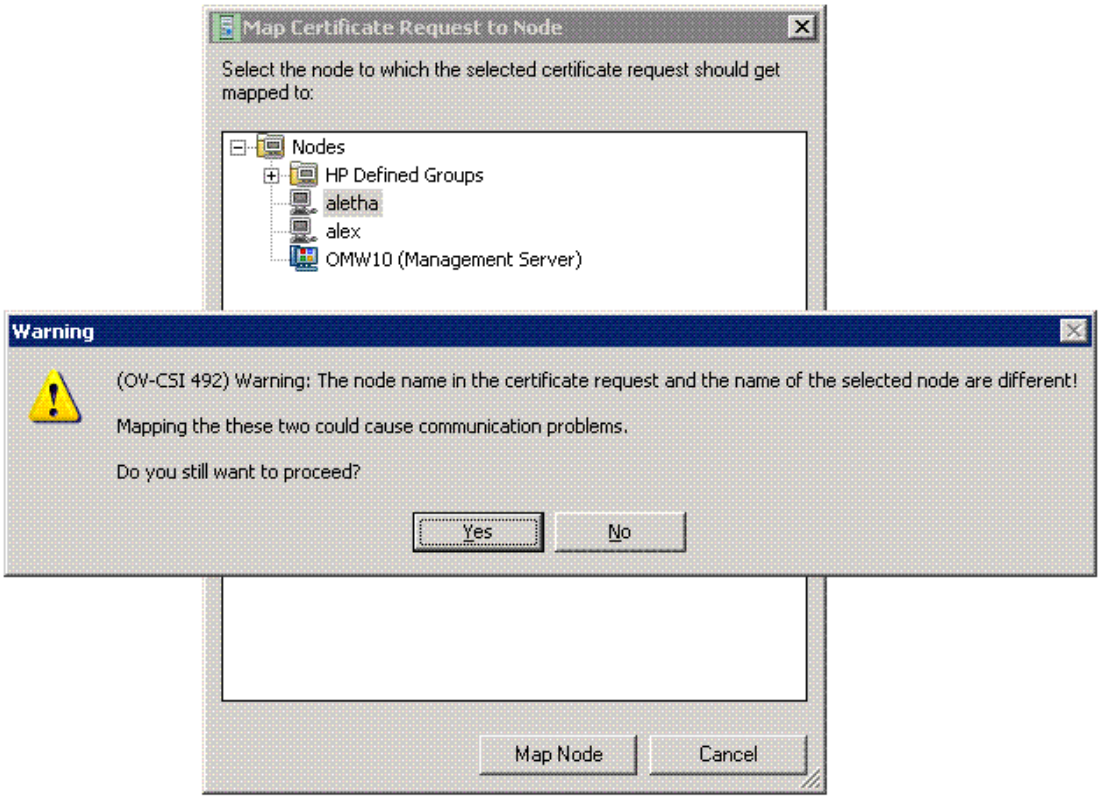
   To map the certificate request, right-click on the certificate request, select **All Tasks** -> **Map to Node...**.



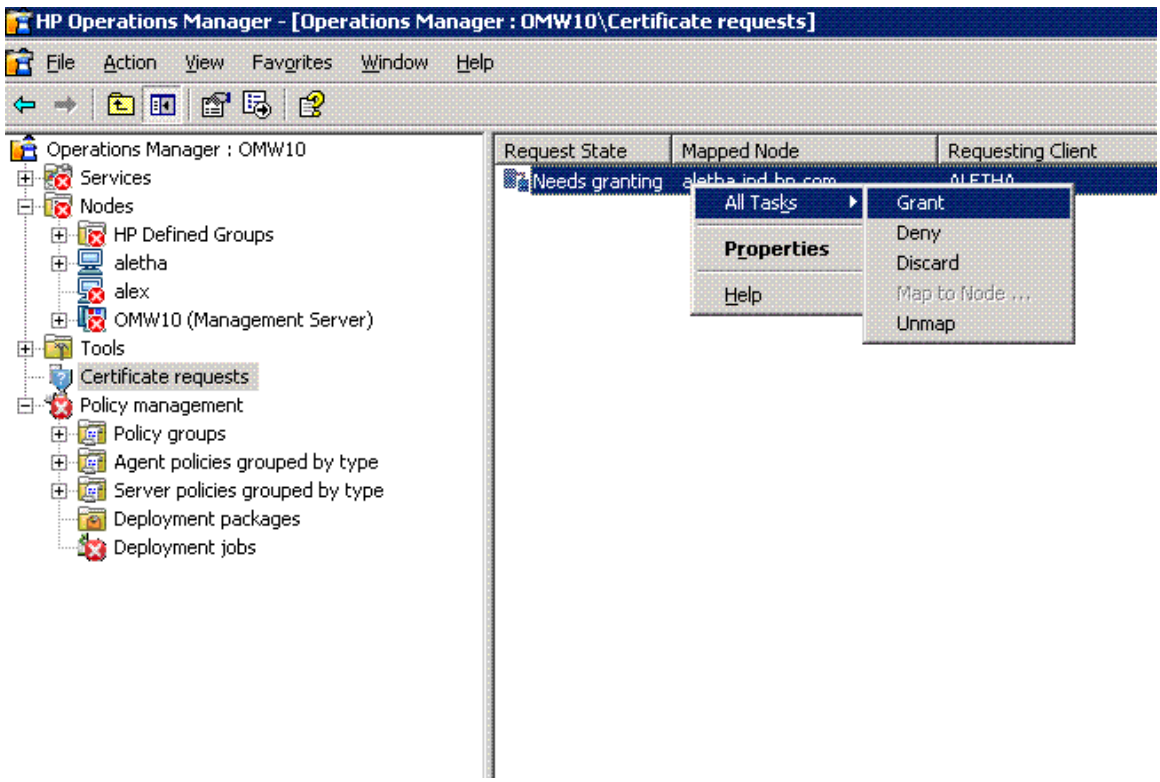
7. In the **Map Certificate Request to Node** window, select the OpenVMS node and click the **Map Node** button.



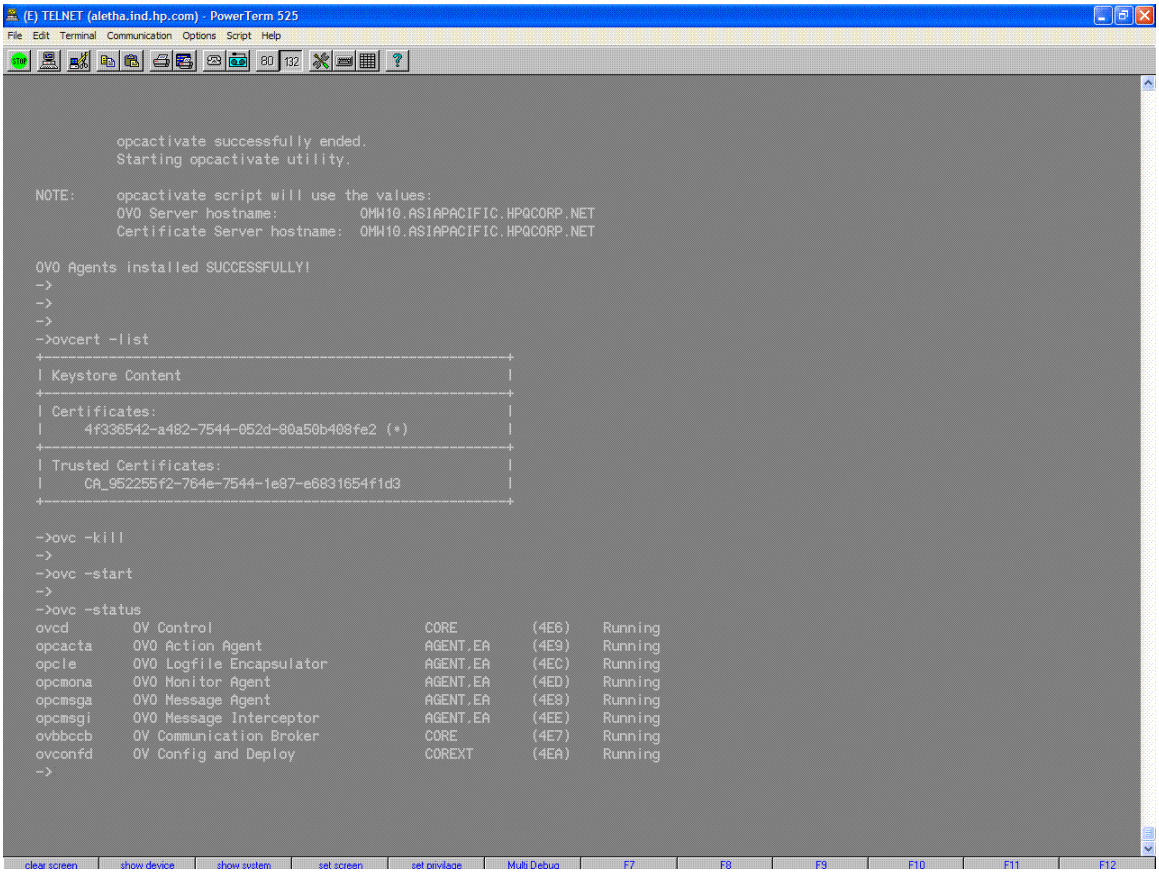
Following warning message pops up. Click **Yes** to proceed.



8. The request state changes to **Needs granting**. Right-click on the certificate request. Then, select **All Tasks** -> **Grant** to grant certificate.



9. On the OpenVMS node, verify that certificate is granted and then restart agents.



1.2.3 Management Server is Operations Manager for UNIX (OMU 9.x and OML 9.x)

1.2.3.1 Configuration on the Management Server

1. Download `OpenVMS-OA-8.6.030C.tar` from the web to a directory (say /temp) on the Management Server and untar it by logging into the management server as 'root' user.

   ```
   # cd /temp
   # tar -xvf OpenVMS-OA-8.6.030C.tar
   ```

2. Execute the following script. This script performs the required validations on the management server.

   ```
   # cd /temp/OVMS8.60
   # ./OA-setup.sh
   ```

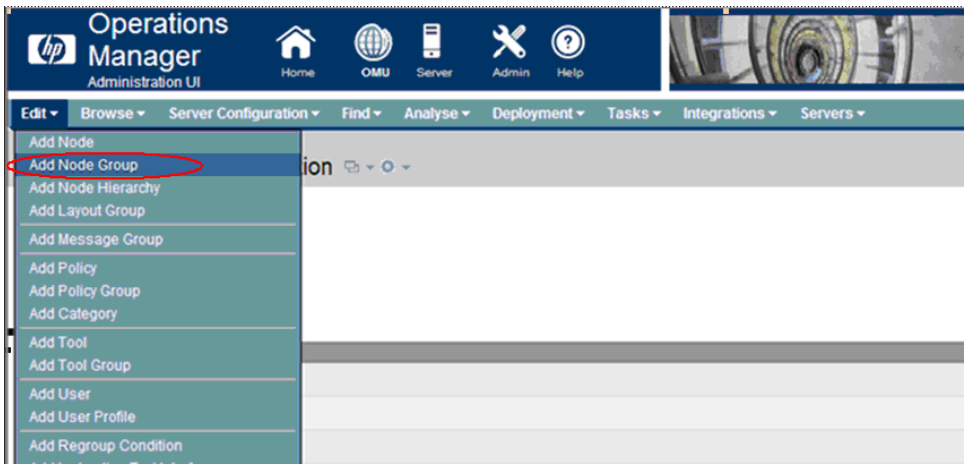
   You can use '-h' option with 'OA-setup.sh' for help.

3. If the Management Server is OML 9.x, execute the following command to register OpenVMS machine types:

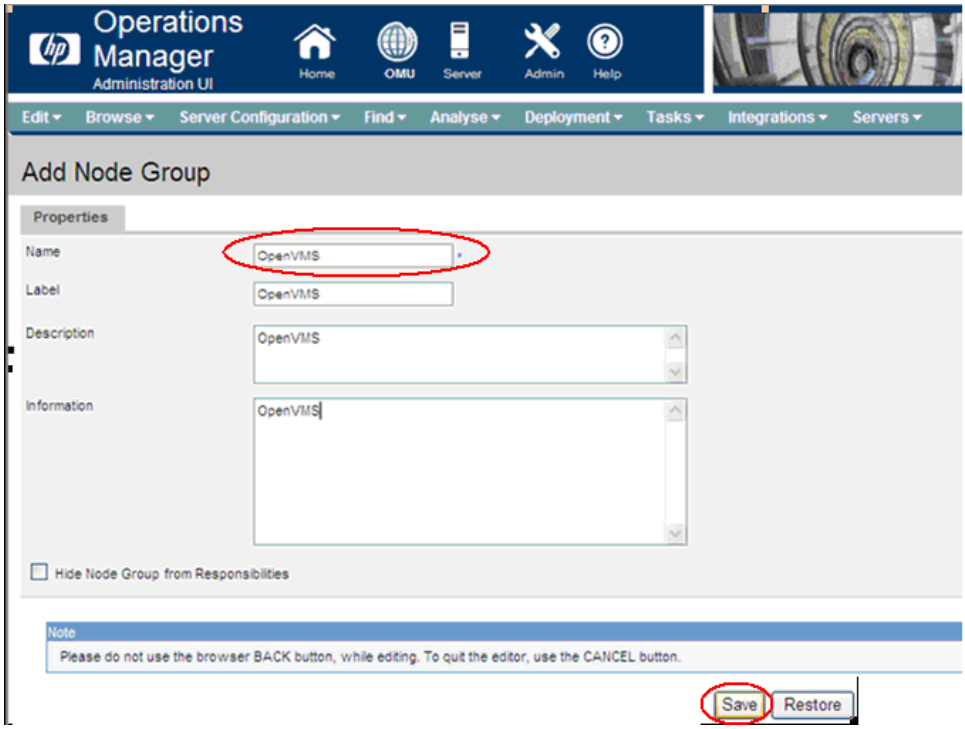
NOTE: This step is not applicable for OMU 9.x (HP-UX and Solaris).

```
# cd /opt/OV/OMU/adminUI
# ./adminui ant -f run.xml intern.init_ovomachtype
# ./adminui machtypes
# ./adminui clean
# ./adminui start
```

4. If OpenVMS OS policies are not available on the management server, then download `ovmspolicies_u9.tar` for OMU9 from the web to a directory on the management server. Execute the following steps as 'root' user for uploading the OpenVMS policies to OMU 9.x Management Servers:
   a. FTP `ovmspolicies_u9.tar` to the OMU 9.x Management Server in binary mode.
   b. On the OMU9 Management Server, change directory to the location where `ovmspolicies_u9.tar` file exists.
   c. Run `tar -xvf ./ovmspolicies_u9.tar`.
   d. If the Management Server is OMU 9.x, run `./ovmspol-setup.sh`. This uploads the policies to the OMU 9.x management server.
   e. If the Management Server is OML 9.x, run `chroot / ./ovmspol-setup.sh`. This uploads the policies to the OML 9.x management server.
5. To create OpenVMS node group, follow these steps:
   a. In the **Operations Manager Administration UI** window, go to **Edit** ->**Add Node Group**.



   b. The **Add Node Group** screen appears. Enter the Node group Name as OpenVMS and click **Save**.



6. To add the OpenVMS Managed Node to the Management Server, follow these steps:

   If the Management Server is OMU 9.x (HP-UX or Solaris):

   a. Add the Alpha managed node or Integrity servers managed node to the Management Server, execute the following commands from the command line.

      On Alpha managed node:

      ```
      /opt/OV/bin/OpC/utils/opcnode -add_node node_name=<node_name>
      node_label=<nodelabel> group_name=OpenVMS net_type=NETWORK_IP
      mach_type=MACH_BBC_VMS_ALPHA
      ```

      For example:

      ```
      /opt/OV/bin/OpC/utils/opcnode -add_node node_name=node1.xyz.com
      node_label=node1 group_name=OpenVMS net_type=NETWORK_IP
      mach_type=MACH_BBC_VMS_ALPHA
      ```

      On Integrity servers managed node:

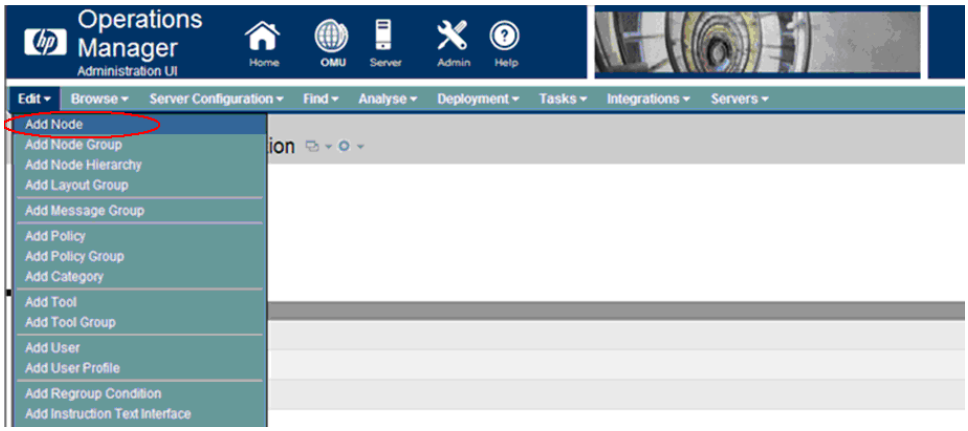
      /opt/OV/bin/OpC/utils/opcnode -add_node node_name=<node_name>
      node_label=<nodelabel> group_name=OpenVMS net_type=NETWORK_IP
      mach_type=MACH_BBC_VMS_IPF64

      For example:

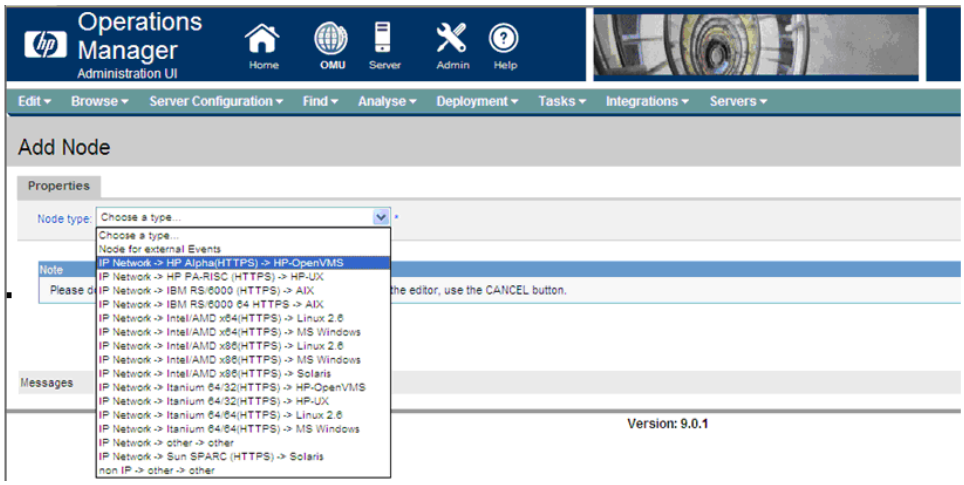
      ```
      /opt/OV/bin/OpC/utils/opcnode -add_node node_name=node2.xyz.com
      node_label=Alex group_name=OpenVMS net_type=NETWORK_IP
      mach_type=MACH_BBC_VMS_IPF64
      ```

   If the Management Server is OML 9.x:

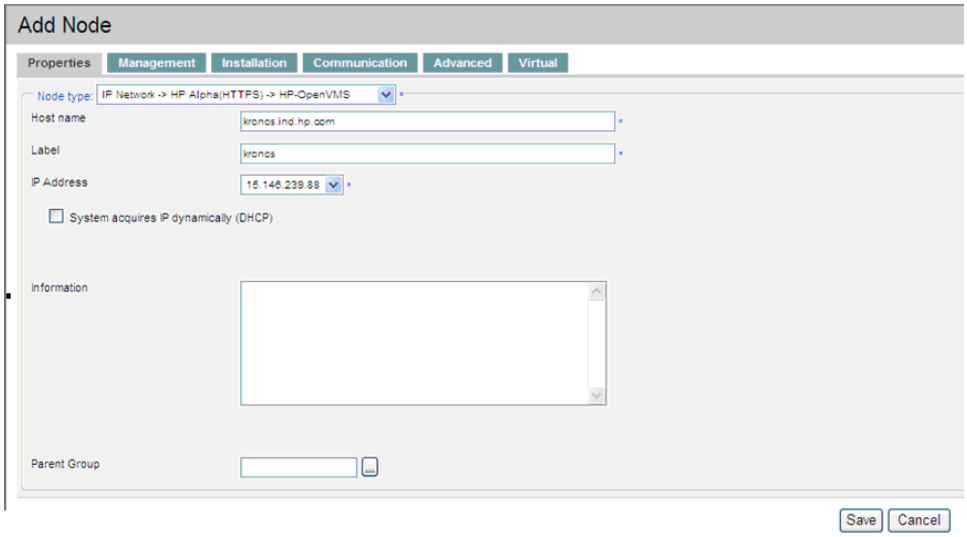
   a. In the **Operations Manager Administration UI** window, go to **Edit** ->**Add Node**.



b. The **Add Node** screen appears. Select the **Node type** as `IP Network -> HP Alpha (HTTPS)-> HP-OpenVMS` for Alpha managed nodes and `IP Network -> Itanium64/32(HTTPS)-> HP-OpenVMS` for Integrity servers managed nodes.



c. Enter the Managed Node Host name and Label as shown in the following figure and click **Save**.



1.2.3.2 Remote Installation

NOTE: Remote installation is not supported when the management server is OMU 9.x HP-UX.

Execute the following steps when the Management Server is OML 9.x:

1. To perform remote installation of agents on a specific OpenVMS node, execute the following perquisite script on the Management Server command line to identify the installation disk.

   ```
   # cd /opt/OV/bin/OpC/agtinstall
   # ./getinstdisk.sh <Node Name>
   ```

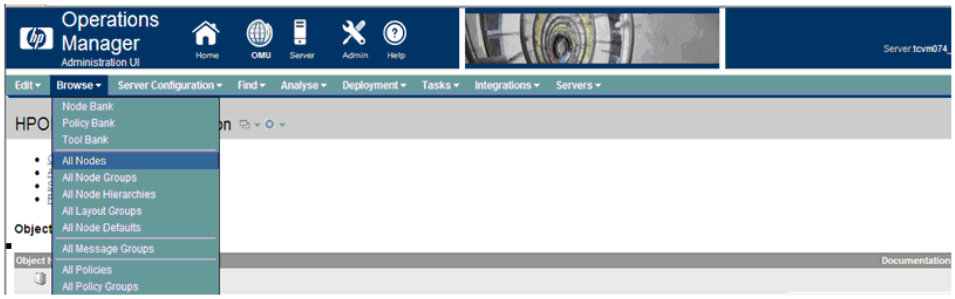
   For example:

   ```
   ./getinstdisk.sh abc.xyz.com
   ```

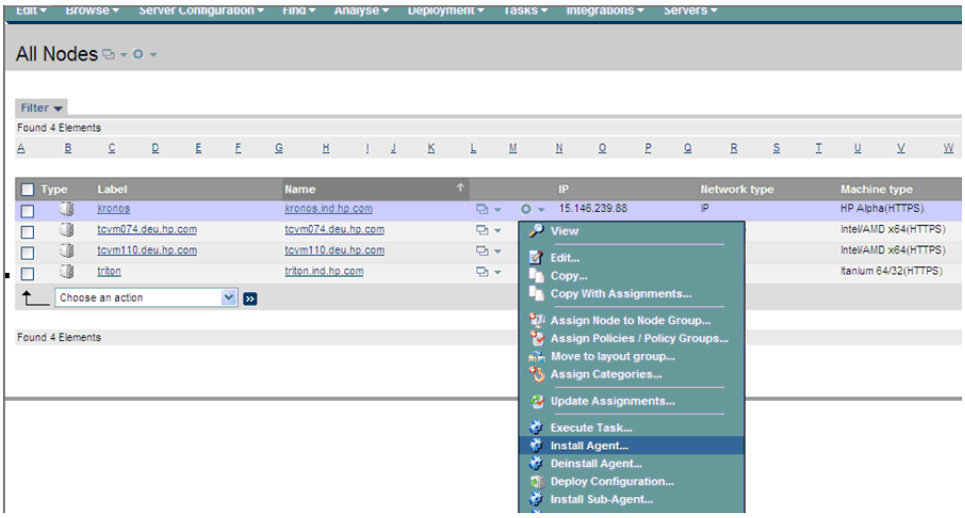
   When you run the script, it prompts as follows:

   - Enter the SYSTEM password.
   - Lists all the ODS-5 disks available on the Managed Node.
   - When it prompts again, enter the disk on which you want to install the agents.
   - Then, it verifies minimum disk space requirement and marks the disk to install the agent software. When remote installation is initiated, it installs agent software on the disk.

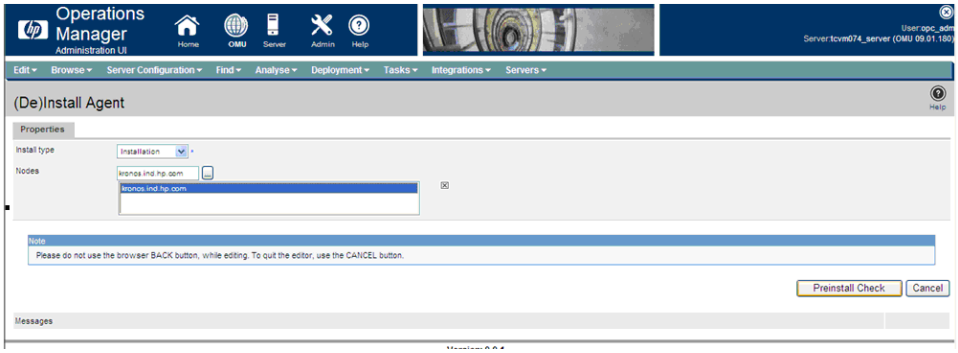
2. In the **Operations Manager Administration UI** window, go to **Browse** —>**All Nodes**. This displays all the nodes added to this management server.



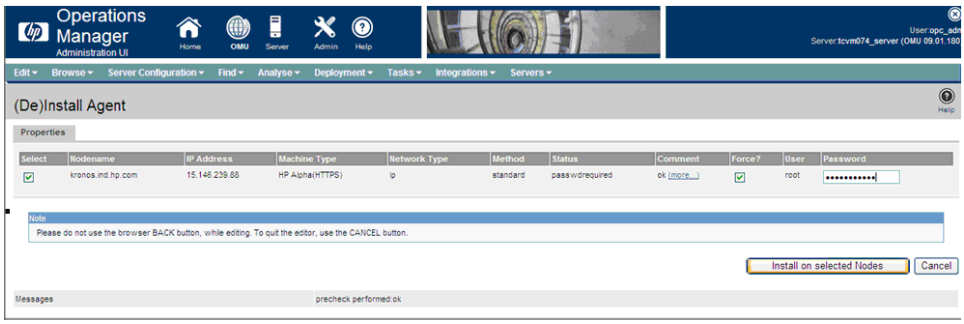
3. In the **All Nodes** window, go to Managed Node's **Action Menu** and select **Install Agent…**



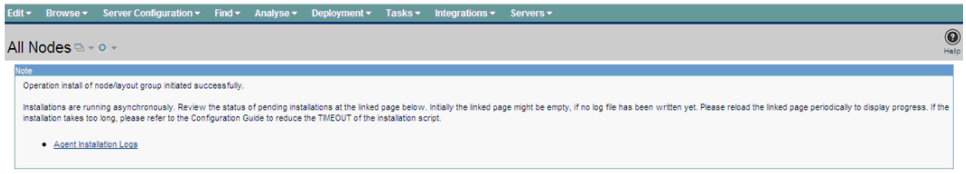
4. The **(De)Install** screen appears. Select Install type as 'Installation' and click **Preinstall Check**.



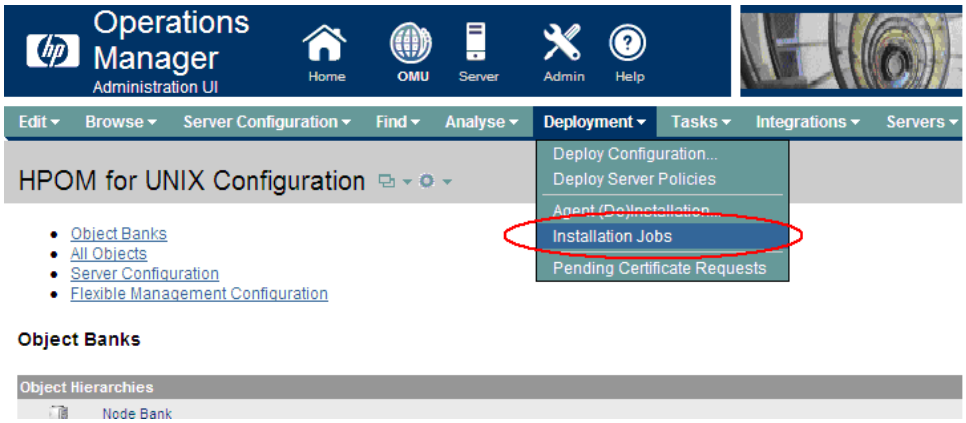
5. Enter the SYSTEM password for the node and click **Install on selected Nodes**.



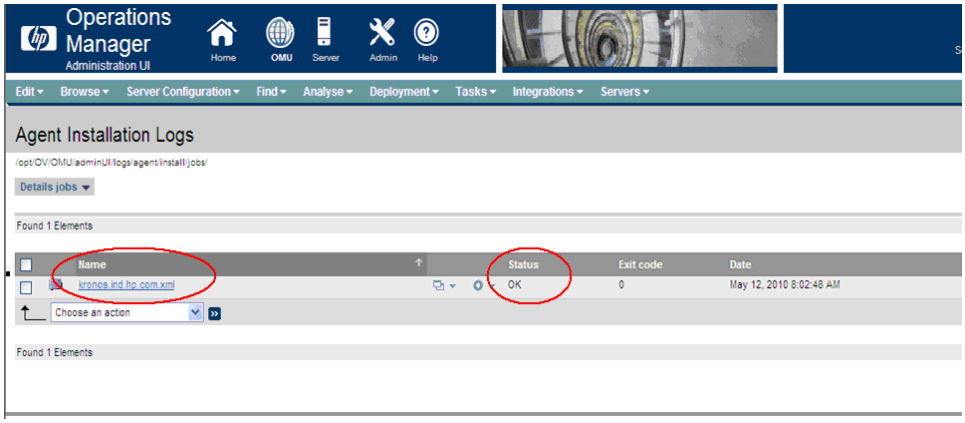
This installs the agent's software on the Managed Node and displays the following message:



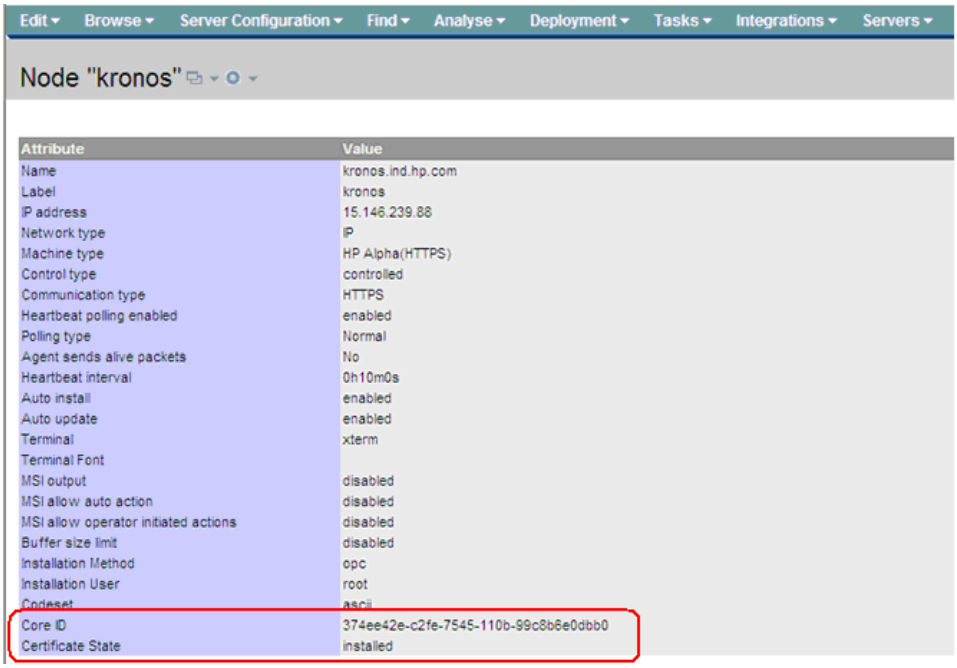
6. After the installation is complete, check the installation log file for remote installation status.
   a. In the **Operations Administration UI** windows, go to **Deployment —>Installation Jobs**.



   b. The **Agent Installation Jobs** screen appears. Open the node specific XML file and check the installation status.



7. After the installation completes, check whether `OVCOREID` of the node is registered in the management server To do so, follow these steps:
   a. In the **Operations Manager Administration UI** window, go to **Browse —>All nodes**.
   b. Click on managed node link. The **Node properties** screen appears. Check the `Core ID`.



8. Login into the OpenVMS agent and check whether all the process are running.

```
$ ovc
ovcd      OV      Control CORE                      (1135) Running
obbccb    OV      Communication Broker CORE         (1136) Running
opcacta   OVO     Action Agent AGENT,EA             (1138) Running
opcle     OVO     Logfile Encapsulator AGENT,EA     (1140) Running
opcmona   OVO     Monitor Agent AGENT,EA            (1141) Running
opcmsga   OVO     Message Agent AGENT,EA            (1137) Running
opcmsgi   OVO     Message Interceptor AGENT,EA      (1142) Running
ovconfd   OV      Config and Deploy COREXT          (1139) Running
```

9. Check whether valid certificate is installed on the Managed Node.

```
Ovcert -list
Ovcert -check
```

If there is no valid certificate installed, see Section 1.2.3.4 (page 26) to manually install the certificate request from the managed node.

1.2.3.3 Manual Installation

Management server is Operations Manager for Windows (OMU 9.x and OML9.x)

1. See Section 1.2.3.1 (page 18) and complete Step 1 through Step 6.
2. Download `OpenVMS-OA-8.6.030C.tar` from the web to a temporary directory on the OpenVMS Managed Node and untar it by logging into managed node as 'SYSTEM'.

   If tar utility is not available on the OpenVMS node, then download VMSTAR.ALPHA_EXE (for Alpha) or VMSTAR.IA64_EXE (for Integrity servers) from the web.

   Execute the following commands to untar:

   ```
   $ set proc/par=ext
   $ tar :==$[<temporary directory>]:VMSTAR.IA64_EXE (For Integrity servers)
   ```

   Or

   ```
   $ tar :==$[<temporary directory>]:VMSTAR.ALPHA_EXE (For Alpha)
   $ tar -xvf OpenVMS-OA-8^.6^.030C.tar
   ```

   This untars the files in the OVMS8_60 directory under the temporary directory.
3. Change directory to OVMS8_60 and execute the script `OA_SETUP.COM` as 'SYSTEM':

   ```
   $ @OA-SETUP.COM -i -srv <<management server>> -cert_srv <<certificate server>>
   ```

   For example,

   ```
   $ @OA-SETUP.COM -i -srv abc.def.hp.com -cert_srv ghi.jkl.hp.com
   ```
4. Provide the ODS-5 disk details when prompted for installation disk. The installation of agents starts.
5. To check if the agents are installed successfully, execute the following commands:

   ```
   $PRODUCT SHOW PRODUCT OV*,VMSSPI
   $ovc –status
   $ovcert –list
   ```

   The output of the commands must be as follows:

   ```
   $PRODUCT SHOW PRODUCT OV*, VMSSPI
   ---------------------------------- ----------- ---------
   PRODUCT                            KIT TYPE    STATE
   ---------------------------------- ----------- ---------
   HP I64VMS OVBBC V8.6-1             Full LP     Installed
   HP I64VMS OVCONF V8.6-1            Full LP     Installed
   HP I64VMS OVCTRL V8.6-1            Full LP     Installed
   HP I64VMS OVDEPL V8.6-1            Full LP     Installed
   HP I64VMS OVEAAGT V8.6-1           Full LP     Installed
   HP I64VMS OVSECCC V8.6-1           Full LP     Installed
   HP I64VMS OVSECCO V8.6-1           Full LP     Installed
   HP I64VMS OVXPL V8.6-1             Full LP     Installed
   HP I64VMS VMSSPI V8.6-1            Full LP     Installed
   ---------------------------------- ----------- ---------
   9 items found
   $ovc -status
   ovcd        OV Control                          CORE         (95D)    Running
   opcacta     OVO Action Agent                    AGENT,EA     (960)    Running
   opcle       OVO Logfile Encapsulator            AGENT,EA     (963)    Running
   opcmona     OVO Monitor Agent                   AGENT,EA     (964)    Running
   opcmsga     OVO Message Agent                   AGENT,EA     (95F)    Running
   opcmsgi     OVO Message Interceptor             AGENT,EA     (965)    Running
   ovbbccb     OV Communication Broker             CORE         (95E)    Running
   ovconfd     OV Config and Deploy                COREXT       (961)    Running

   $ovcert -list
   +-------------------------------------------------------+
   | Keystore Content                                      |
   +-------------------------------------------------------+
   | Certificates:                                         |
   ```

```
+------------------------------------------------------------+
| Trusted Certificates:                                      |
+------------------------------------------------------------+
```

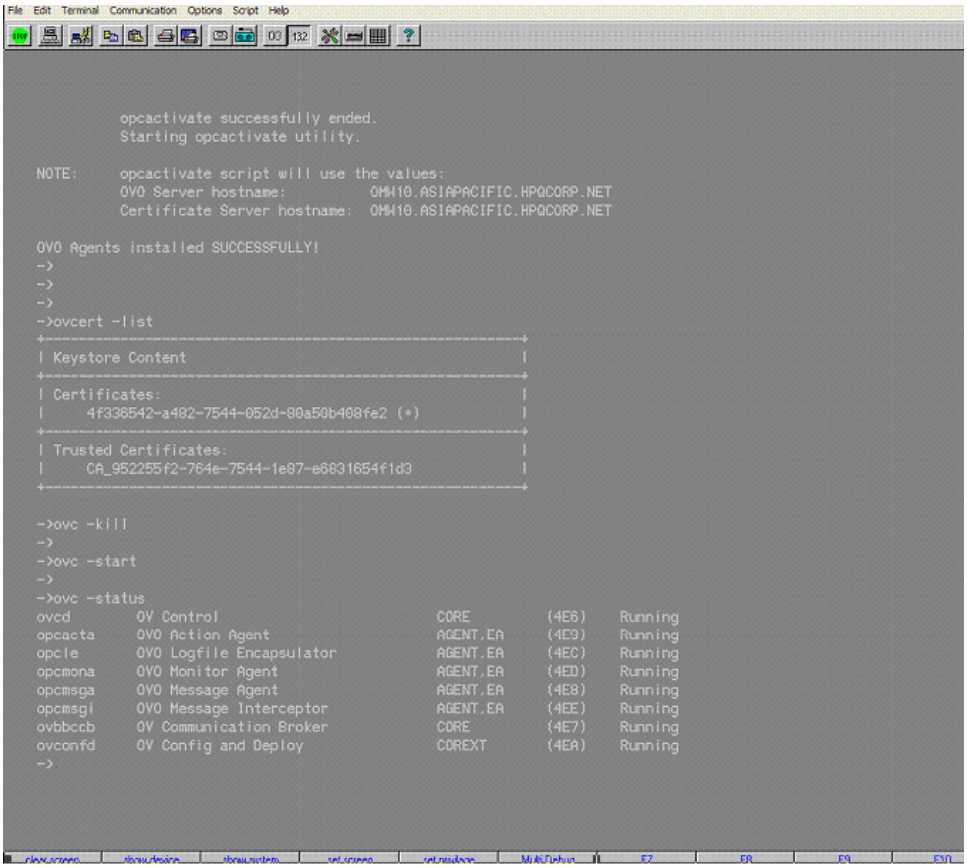
6. Login to the OMU9/OML9 Management Server to check whether a certificate request has been received for the OpenVMS node. Note that this certificate request is automatically initiated as part of installation.

   If the certificate request for the OpenVMS node is not listed, login to the OpenVMS node as SYSTEM and execute the following commands to initiate a certificate request:

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

   ```
   $ovcert -certreq
   ```

7. Map the certificate request to the OpenVMS node on the Management Server. To grant the certificate see Page 26.
8. On the OpenVMS node, verify that certificate is granted and then restart agents.



1.2.3.4 Manually Requesting the Certificate from the Managed Node

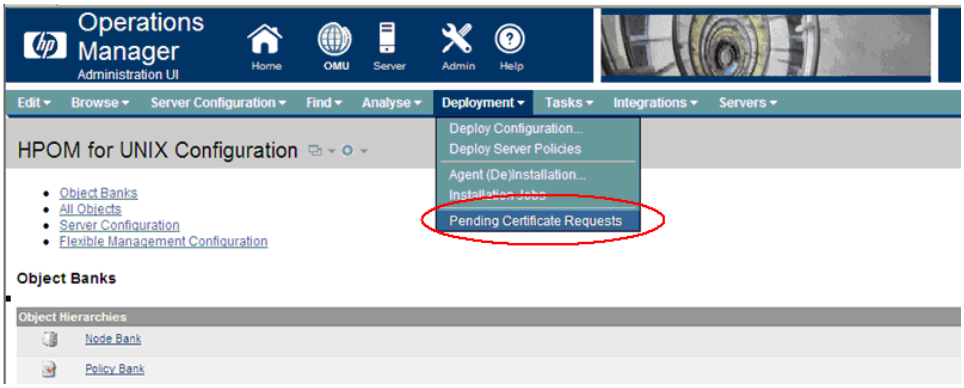
If a valid certificate is not installed on the managed node, perform the following steps to install the certificate

1. Login to the OpenVMS Managed Node as SYSTEM and execute the following commands to initiate a certificate request:

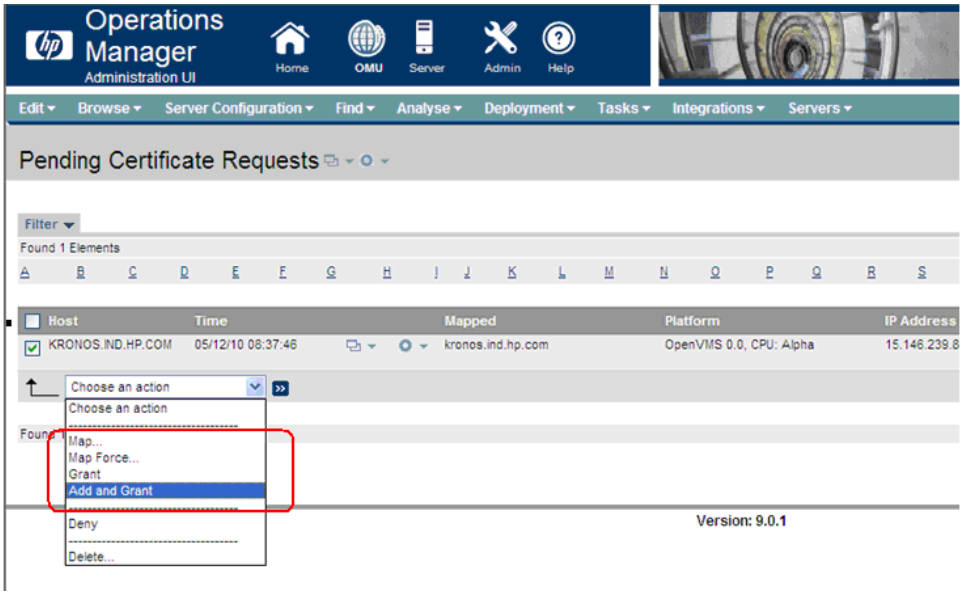
   ```
   $ @SYS$STARTUP:OVO8$DEFINE.COM
   ```

   ```
   $ ovcert -certreq
   ```

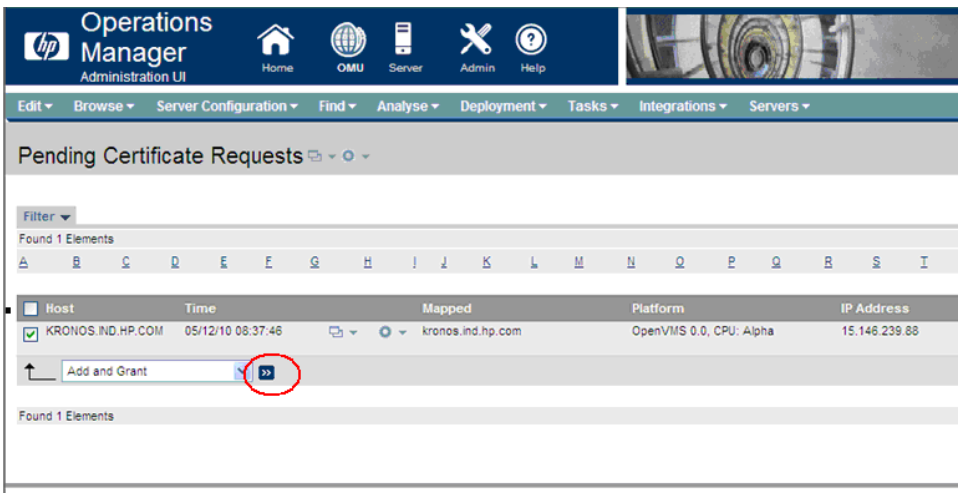
2. In the **Operations Manger Administration UI** Window, go to **Deployment** —> **Pending Certificate Requests**.



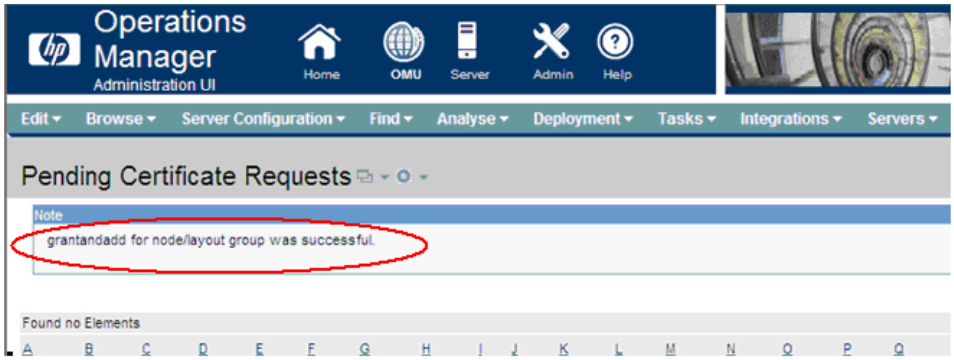
3. The **Pending Certificate Requests** screen appears. If the certificate request is not mapped, select Map Force… option from the List menu to map the pending certificate request to the Managed Node.



4. Select 'Add and Grant' option from the List Menu to grant the certificate. Click **<<figu;re>>** button.



This grants the certificate requests and displays the following message:



5. On the OpenVMS node, verify that certificate is granted and then restart agents.

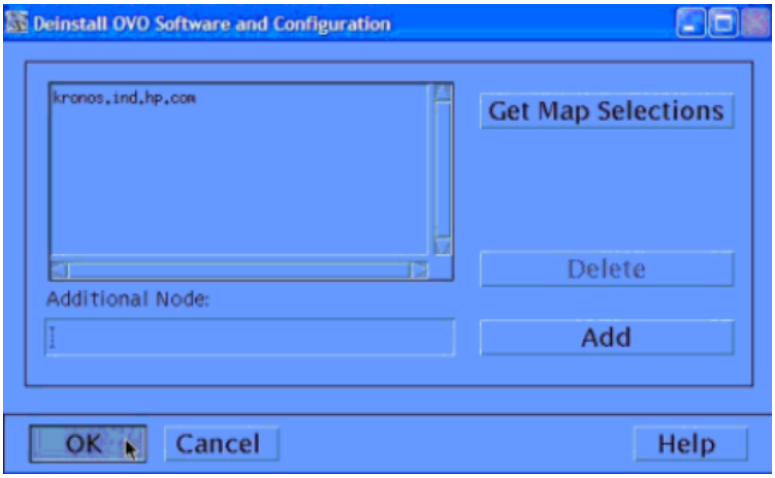
```
$
$
$
$
$ @sys$startup:ovo8$define.com
$ ovcert -list
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
+-------------------------------------------------------+

$
$
$ ovcert -certreq
INFO:    Certificate request has been successfully triggered.
$
$
$ ovcert -list
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
|    90210daa-ba4a-7545-0d78-f28277862ea7 (*)           |
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|    CA_25111388-0af6-7545-1064-e778e7a9085e            |
+-------------------------------------------------------+

$
$
$
```

1.3 Uninstalling HPOM Software from the Managed Node

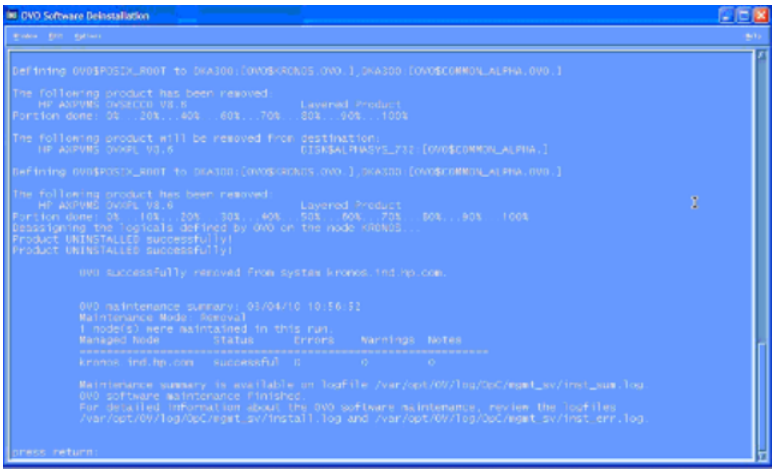
1.3.1 Management server is Operations Manager for UNIX (OMU 8.3x)

To uninstall the HPOM software, follow these steps:

1. Select the Node that you want to uninstall in the `Node Group` window.
2. Click **Actions** and select **Agents**.
3. Click **Deinstall**. The **Deinstall OVO Software and Configuration** screen appears.



4. Click **OK**.
5. Enter the password of the managed node and the system displays product unistalled successfully.



1.3.2 Management Server is Operations Manager for Windows (OMW 8.x)

To uninstall operations manager for Windows, login to the OpenVMS managed node as SYSTEM and execute the following script:

```
$@SYS$MANAGER:OPC_UNINST
```

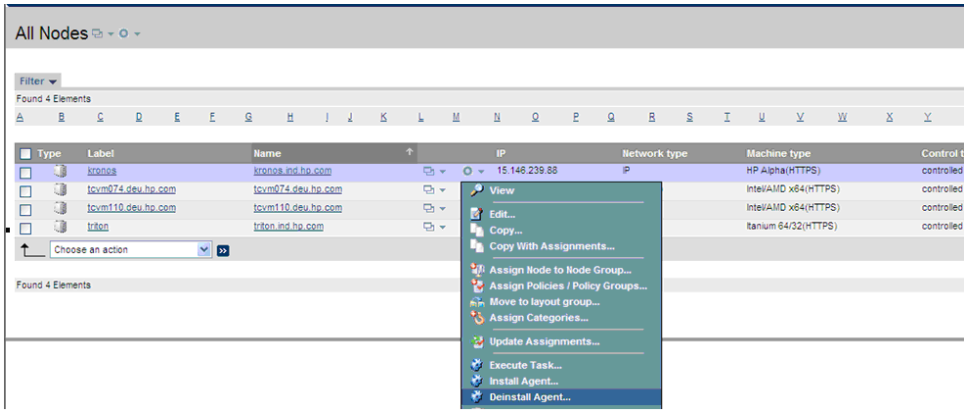
NOTE: During the unistallation of OVO HTTPS agents, the following messages may be displayed. These messages can be ignored:

```
OVO HTTPS Agents UNINSTALLED successfully!
Product UNINSTALLED successfully!
%RMS-E-FNF, file not found
%RMS-F-ISI, invalid internal stream identifier (ISI) value
$
```

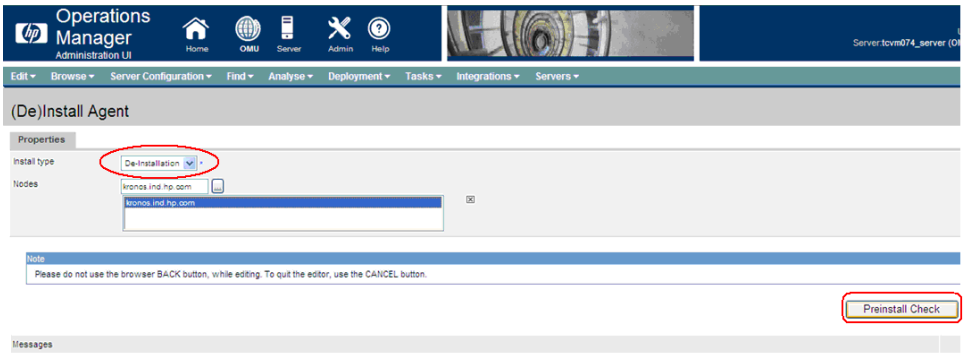
1.3.3 Management Server is Operations Manager for UNIX (OMU 9.x or OML 9.x)

To uninstall operations manager for UNIX, follow these steps:

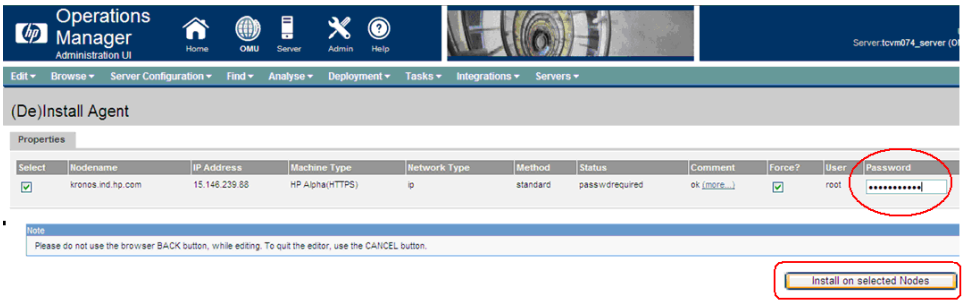
1. In the **Operations Manager Administration UI** window, go to **Broswe** -> **All Nodes**. This displays all the nodes added to this management server.
2. In the **All Nodes** window, go to Managed Node's **Action Menu** and select **Deinstall Agent…**



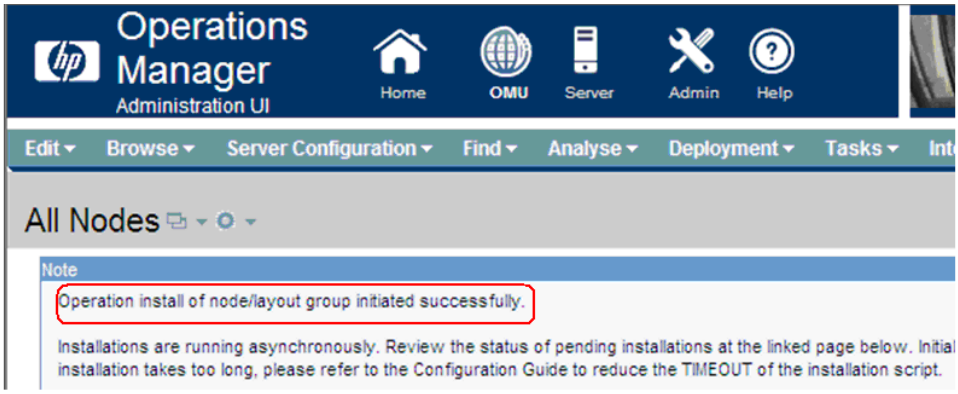
3. The **(De)Install** screen appears. Select Install type as **De-installation** and click **Preinstall Check**.



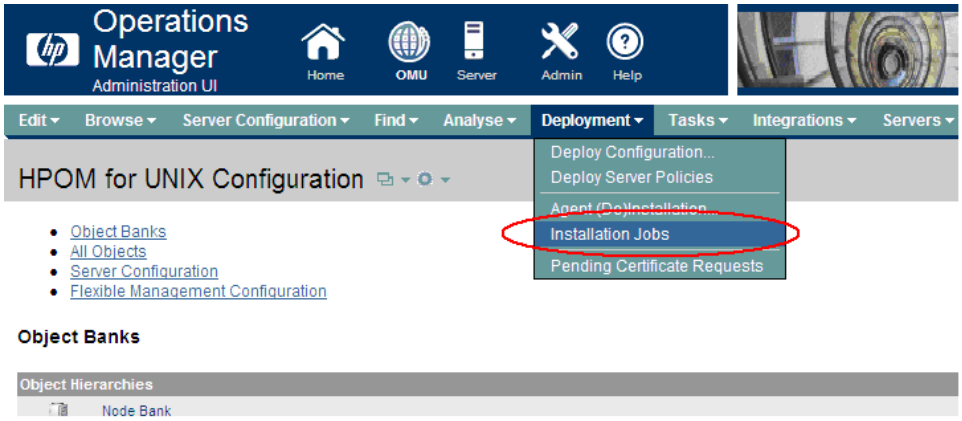
4. Enter the SYSTEM password for the node and click **Install on selected Nodes**.



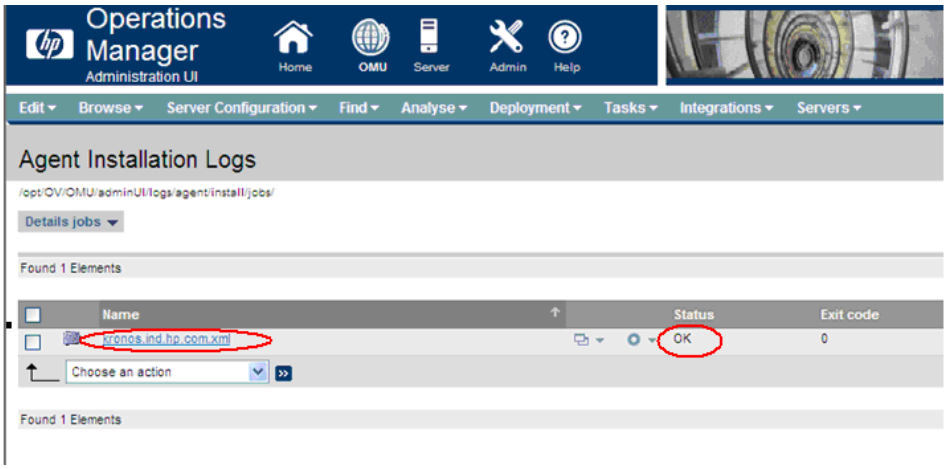
This uninstalls the agent's software on the Managed Node and displays the following message:



5. Check the log file for remote de-installation status To do so, follow these steps:.
   a. In the **Operations Administration UI** windows, go to **Deployment —>Installation Jobs**.



   b. The **Agent Installation Jobs** screen appears. Open the node specific XML file and check the de-installation status.



1.4 Agent Processes on HTTPS Managed Nodes

The Operations Manger Agent is comprised of several processes that handle sub-tasks such as transmitting messages and monitoring threshold values on a node. The agent supports a library

of APIs that interact with various processes to give developers access to the capabilities of the agent.

- Message Agent

  The Message agent receives messages from log file encapsulator, monitor agent and message interceptor and forwards the messages to the management server.

- Monitor Agent

  Monitor agent checks the values it finds against predefined thresholds and if a threshold is exceeded, a message is generated and forwarded to message agent.

- Action Agent

  Agents support the execution of various actions (automatic and user-initiated). Actions are defined in the message policies that are installed on the agent.

- Message Interceptor

  The message interceptor intercepts messages written to the Message Interceptor queue.

- Log File Encapsulator

  The log file encapsulator scans log files for messages or patterns. It forwards the scanned and filtered messages to the message agent.

- Control Daemon

  The Control Daemon starts, stops, and controls other agent processes.

- Communication Broker

  The communication broker acts as a proxy and provides a central point of entry to the managed node for all applications on that managed node.

- Configuration and Deployment process

  It is used for deployment of policies, instrumentation and so on, on the managed node.

1.5 APIs and Libraries

How to compile and link an application program using OpenView Agent Message and Monitor APIs?

- Programs calling APIs must include a call to the `OVO$VMS_INITIALIZE` routine before calling an API routine. Application program must check for successful execution of OVO$VMS_INITIALIZE from its return status. If this check is not done and `OVO$VMS_INITIALIZE` fails, application program may display an error indicating that some of the files in the directory structure cannot be found.

  For example, Internal error: Cannot open message catalog `/opt/OV/lib/nls/C/opcagt.cat`

- The program must be linked against the shared image `OVO$LIBOPC_R.EXE`. You can do this by including the following line in an options file, `SYS$SHARE:OVO$LIBOPC_R/SHARE`.
- The program must be run from the SYSTEM ACCOUNT.

```
OVO$VMS_INITIALIZE()
Int OVO$VMS_INITIALIZE()

Parameters
       None

Description
This routine does the initialization that is required on the managed node
It defines SYS$POSIX_ROOT .  It must be called before any opc  API
calls are made.

Return Values
```

```
SS$_NORMAL   : Normal Successful completion
SS$_NOLOGNAM   : OpenView agents are  not installed on the node
SS$_EXLNMQUOTA  : Unable to create SYS$POSIX_ROOT logical due to insufficient quota
SS$_INSFMEM   : Unable to create SYS$POSIX_ROOT logical insufficient dynamic memory
```

opcmsg()

```
#include opcapi.h
int opcmsg (
const int severity, /* in */
const char * application, /* in */
const char * object, /* in */
const char * msg_text, /* in */
const char * msg_group, /* in */
const char * nodename, /* in */
);
```

Parameters

severity Severity level of the new message.
application Application of the message source.
object Object of the message source.
msg_text Message text.
msg_group Message group.
nodename Name of the node originating the message.

Description

Use the function opcmsg() to send a message, created on the managed node, to the management server.

Return Values

OPC_ERR_OK: OK
OPC_ERR_APPL_REQUIRED: attribute OPCDATA_APPLICATION not set
OPC_ERR_OBJ_REQUIRED: attribute OPCDATA_OBJECT not set
OPC_ERR_TEXT_REQUIRED: attribute OPCDATA_MSGTEXT not set
OPC_ERR_INVAL_SEVERITY: set severity invalid
OPC_ERR_MISC_NOT_ALLOWED: message group ‘misc.’ not allowed
OPC_ERR_NO_MEMORY: out of memory

opcmon()

```
#include opcapi.h
int opcmon (
const char *objname, /* in */
const double monval /* in */
);
```

Parameters

objname Name of the monitored object.
monval Actual value of the monitored object.

Description

Use the function opcmon() to send a monitor value, created on the managed node, to its management server.

Return Values

OPC_ERR_OK: OK
OPC_ERR_OBJNAME_REQUIRED: objname is NULL
OPC_ERR_NO_AGENT: agent is not running
OPC_ERR_NO_MEMORY: out of memory

Sample Program

This is a sample program TEST.C to send a message from managed node to the management server (15.14.23.11).

```
#include<stdio.h>
#include<opcapi.h>
```

```
extern Int OVO$VMS_INITIALIZE();

int main()
{
const int severity = 64;
const char * application="app";
const char * object="obj";/* in */
const char * msg_text="MYOPCMSG: Testing with sample program"; /* in */
const char * msg_group="Test"; /* in */
const char * nodename="15.14.23.11"; /* in */

int status;

status = OVO$VMS_INITIALIZE();
   if ( ! (status & 1) )
      return (status);
status = opcmsg (severity, application, object, msg_text, msg_group, nodename);

printf("opcmsg is called and the status is %d\n", status);
}
```

To run the TEST.C program, follow these steps:

1. Compile `TEST.C  CC /INCLUDE=OVO$POSIX_ROOT:[OPT.OV.INCLUDE] TEST.C`
2. Use `TEST.OPT` for linking.

   ```
   $ type TEST.OPT
   $ SYS$SHARE:OVO$LIBOPC_R/SHARE
   ```

3. Link TEST

   ```
   $ link TEST, TEST.OPT/OPT
   ```

4. $ run TEST.EXE

1.6 HP Encourages Your Comments

HP welcomes your comments on this document.

Send comments to the following address:

openvmsdoc@hp.com