Serviceguard Manager Version A.04.00 Release Notes

Manufacturing Part Number: B8325-90046

June 2004

Legal Notices

Corporate Offices:

Hewlett-Packard Co.
3000 Hanover St.
Palo Alto, CA 94304

1 Serviceguard Manager Version A.04.00 Release Notes

Announcements

Serviceguard Manager is the graphical user interface for Serviceguard product. With it, you can monitor, administer, and configure clusters managed by Serviceguard, Serviceguard Extension for RAC, Metrocluster, Continentalclusters, and Serviceguard Extension for Faster Failover.

Serviceguard Manager replaces ClusterView and the SAM High Availability tool. It can be launched independently, from HP Systems Insight Manager, or from OpenView.

You install Serviceguard Manager on a management station, which can be any computer running HP-UX, Linux, or Windows. From there, you connect to a node with Serviceguard version A.11.13 or later. This node becomes your Session Server; it will go out on its subnets and query for information about Serviceguard objects. You can see the discovered clusters, nodes, and packages in your session on the tree and map, and more information in Properties and Alerts.

You can also do administrative commands through the interface, if the Session Server and target clusters are running Serviceguard version A.11.14 or later. The administrative actions are:

- Run or halt a cluster, node, or package
- Move a package to a new node
- Change package- and node-switching flags

You can also create and modify Serviceguard configuration of clusters and packages if the target node or cluster has Serviceguard A.11.16 or later installed.

An icon on the toolbar warns you about new problems, whether the Serviceguard object is in your current view or not. High-availability alerts are posted when Serviceguard Manager polls. The Alerts window has aids for analyzing the problems.

If your HP-UX cluster nodes are configured for SNMP, you can receive their SNMP cluster trap messages in the SNMP Browser window. You can set your management station as a trap destination from a tab in the window. Messages can be sorted and re-organized.

Serviceguard Manager can be installed on HP-UX, Linux, and Windows. The Serviceguard Manager software for all platforms is available free from the web at `http://www.software.hp.com`.. Serviceguard Manager is one of the products delivered on the Distributed Components CD that comes free with Serviceguard:

- Product B8325BA software and license for HP-UX
- Product T1228BA software and license for Linux
- Product B8341BA software and license for Windows

The Serviceguard Manager interface is available in 5 languages:

- English
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

What's in this Version

Serviceguard Manager version A.04.00 supports Serviceguard A.11.16.

- In Serviceguard Manager A.04.00, you can create or modify configuration of clusters and packages on nodes with Serviceguard version A.11.16.

  Many of your configuration options are discovered by Serviceguard and displayed in lists for you to select. The configuration file and control script can be automatically created, then distributed to the nodes by clicking a button.

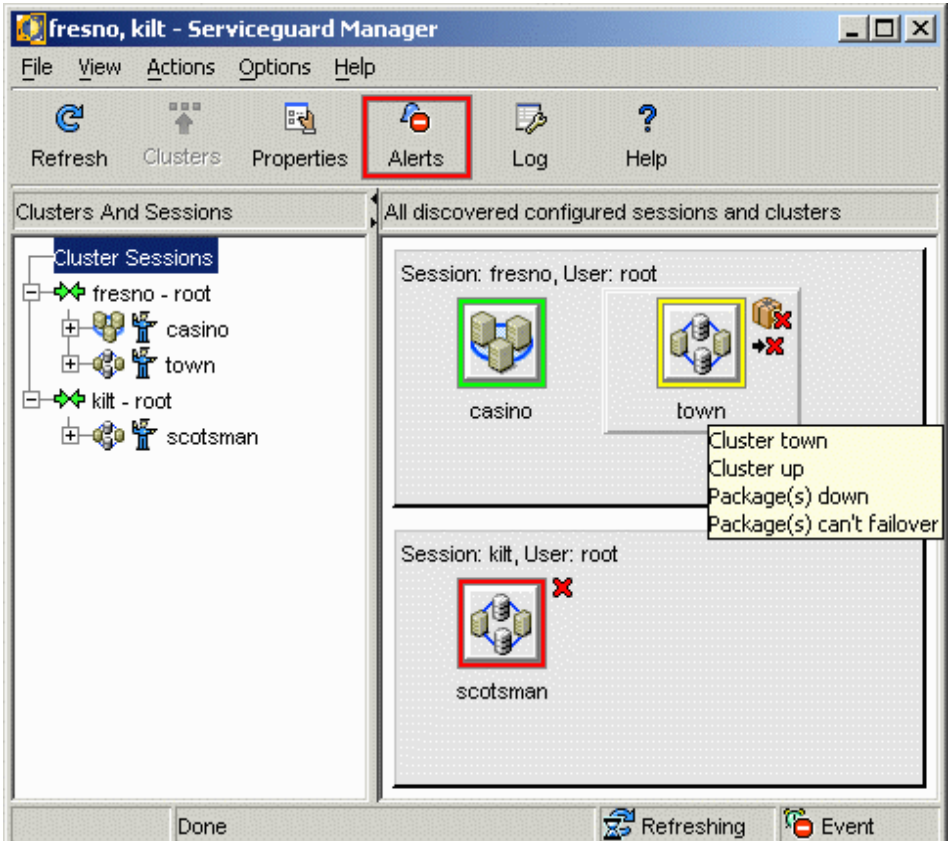
- Serviceguard Manager uses the new Serviceguard non-root access roles to administer Serviceguard Version A.11.16 clusters and packages.
- The Properties have several new tabs, and now display information about physical volumes, volume groups, EMS resources, and access control policies (roles).
- The new Operations Log window shows messages for administration and configuration actions. Messages from all operations are integrated into the one screen.
- If you connect to a session server with Serviceguard A.11.16, it can discover these Serviceguard Extension for RAC clusters:
  - SGeRAC 11.14 clusters with Oracle 8i or Oracle 9i
  - SGeRAC 11.15 clusters with Oracle 8i, Oracle 9i, or Oracle 10g
  - SGeRAC 11.16 with Oracle 9i or Oracle 10g

What You See

The figure below shows an instance of Serviceguard Manager with two sessions. (Up to 10 sessions are supported.) The icon by the connection to Session Server fresno shows that the user's role has an Admin role for those clusters. In the second session, the icon shows the user role is Monitor.

The Alerts button tells you there is information about serious alerts. We can see a red-bordered cluster is down. Also critical are the clusters that have a package icon with a red X, showing they have a package that is down.

Figure 1-1 Serviceguard Manager Map and Tree



With Serviceguard Manager, you see Serviceguard objects three ways.

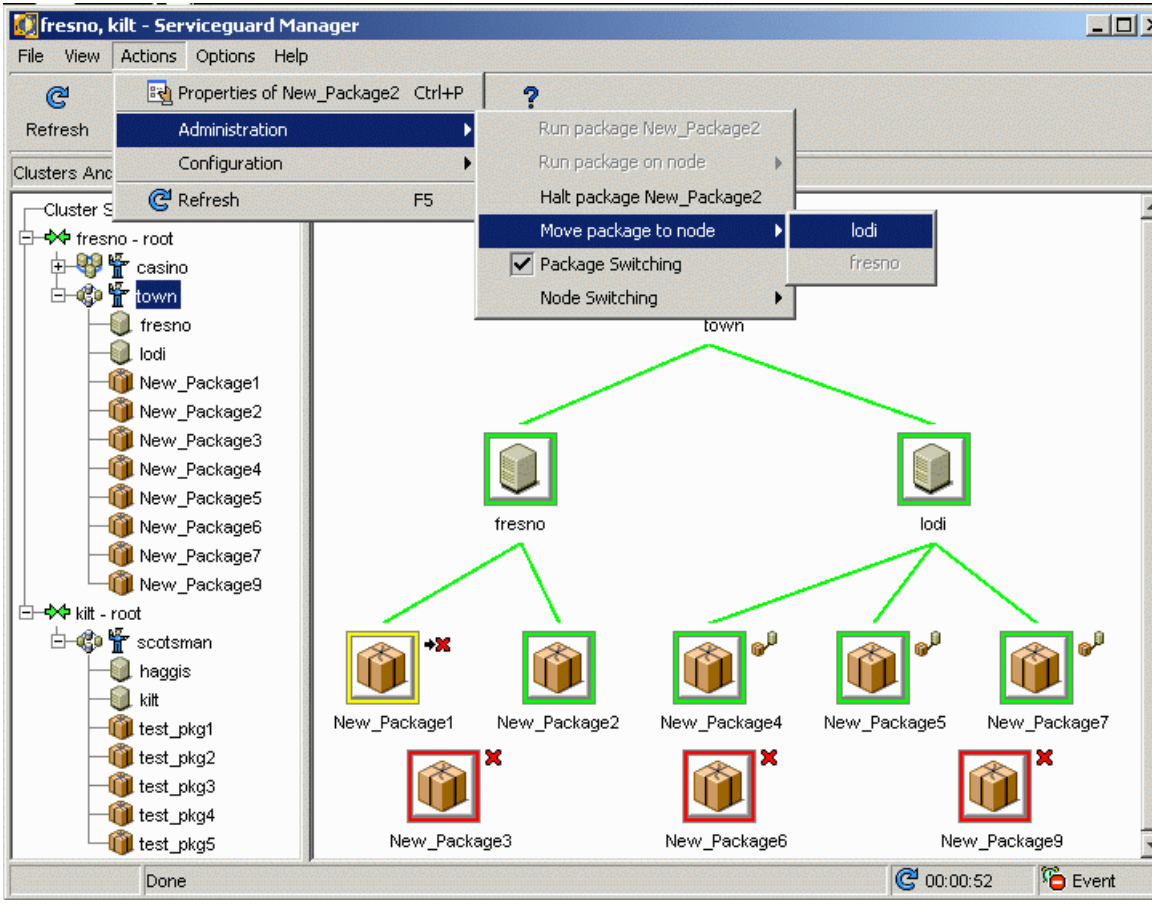
- In the tree on the left pane, you see cluster relationships listed hierarchically.

You can navigate through the map by clicking an object in the tree. The map pane will show information relevant to the object you clicked. For example, if you click a node, you see that node, its cluster, and the packages configured to run on it.

- In the map on the right pane, you can see configuration relationships by the position of objects in the diagram. You can see status from the colors and symbols. You can also get a small text message about the status if you pause the mouse over a cluster object.
- In Properties, you see more detailed information about any session, cluster, node, or package on your map. To open Properties, select an object, then go to the menu on top. Or right-click an object and use the pop-up menu.

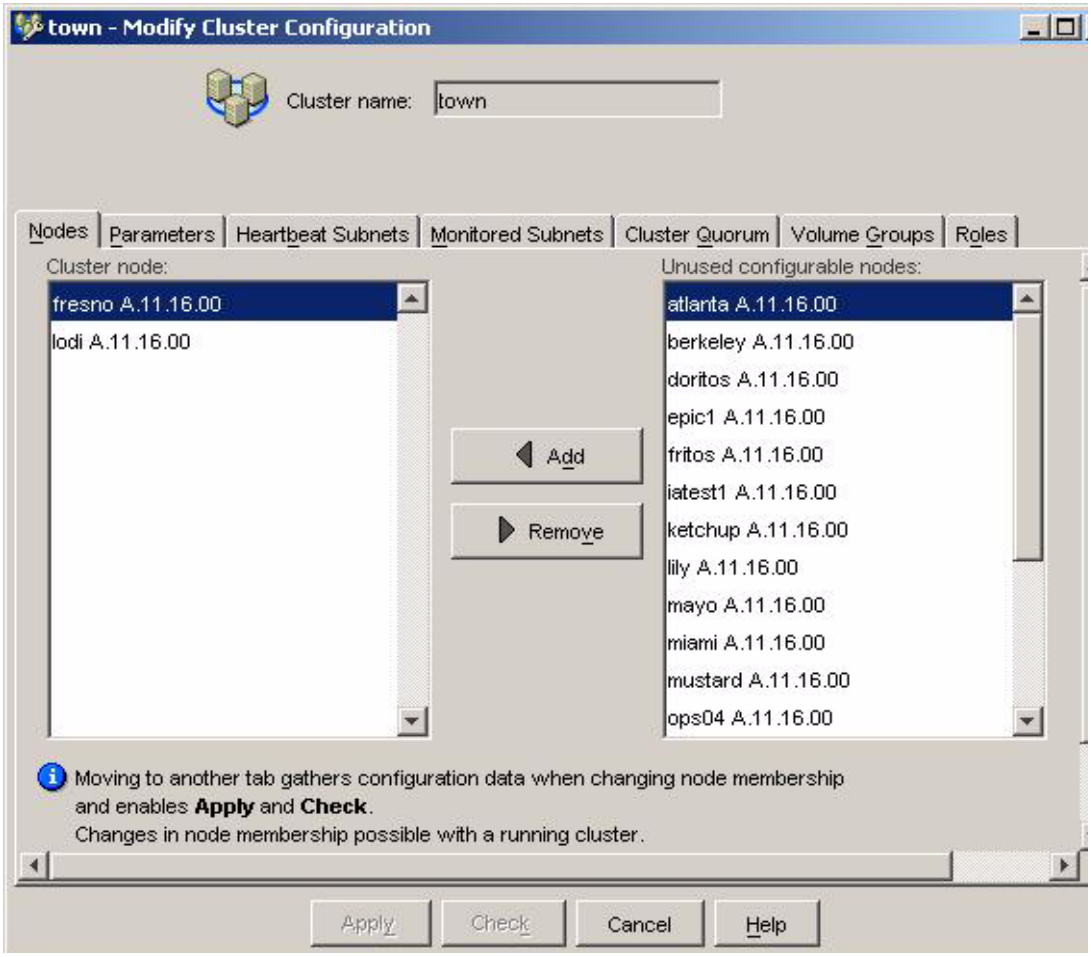
You can issue common administrative commands on your clusters through Serviceguard Manager. WIth Serviceguard A.11.16 clusters, administrators can be specified by configuring a non-root Admin Access Control Policy.

Figure 1-2 Administering clusters with Serviceguard Manager



With Serviceguard A.04.00, you can configure clusters and packages on nodes with Serviceguard A.11.16 installed.

Figure 1-3 Configuring clusters with Serviceguard Manager (Nodes tab)



How it Works

You install Serviceguard Manager on a management station. This can be HP-UX, Linux, or Windows.

From the management station, you connect to a Session Server with Serviceguard installed (HP-UX or Linux). Each Session Server connection is displayed on the tree with the clusters it discovered. The component of Serviceguard that interfaces with Serviceguard Manager is called the COM (Cluster Object Manager). The version of the Session Server's COM is shown in its properties.

When you log in to a Session Server, it goes out on its subnets to discover Serviceguard nodes configured for these types of clusters:

- Serviceguard, Version A.10.10 and later
- Serviceguard Extension for RAC, Version A.11.14.01 or later
- ServiceGuard OPS Edition, Version A.11.13 and later
- Metrocluster, all versions
- Continentalclusters, all versions
- Serviceguard Extension for Faster Failover, all versions.

You can do administrative commands if the Session Server and the target Serviceguard node or cluster has version A.11.13 or later. The rules for access are different in Serviceguard versions A.11.13 to A.11.15 than in version A.11.16. See Table 2-1 on page 18.

The Session Server queries Serviceguard nodes on its subnet for status and configuration information. If the discovered node has allowed the Session Server to query, the information will appear in your map, tree, Properties, and Alerts. (See "Before Installing Serviceguard Manager," below, for a description of configuring node access permissions.)

Note: Because Continental Clusters are always on more than one subnet, Serviceguard Manager sees them as two clusters. To see all the information about a Continental cluster, open two separate sessions, one on each subnet.

What Documentation is Available for This Version

These Release Notes will help you install Serviceguard Manager.

Once Serviceguard Manager is running, online help has the information about how to use the interface. Start with the Help section "Using Serviceguard Manager." If you have installed Serviceguard Version A.11.16 on any nodes, be sure to read the topic "Security, Logons, and Permissions" there.

Documentation for the Serviceguard products themselves is available at http://www.docs.hp.com and is updated regularly. Click High Availability, then scroll through the alphabetical listings.

You will find manuals for Serviceguard, including:

- *Managing Serviceguard*
- *Getting Started with Serviceguard on Linux*
- *Serviceguard for Linux*
- *Using Serviceguard Extension for Real Application Clusters (RAC)*
- *Configuring OPS clusters with Serviceguard OPS Edition*
- *Managing Serviceguard Extension for SAP*
- *Designing Disaster Tolerant High Availability Clusters*

You will also find Release Notes for Serviceguard Manager, Serviceguard, and other High Availability products.

You can order the book *Clusters for High Availability: A Primer of HP Solutions*, second edition, by Peter Weygant (HP Press: Prentice Hall, ISBN 0-13-089355-2). This guide describes basic cluster concepts. To see information about this retail book, go to `http://www.hp.com/hpbooks/` and click search, then enter the first few words of the title.

For information about HP-UX, go to: `http://www.docs.hp.com` and scroll to HP-UX in the alphabetical listing.

For information about Red Hat Linux, go to `http://www.redhat.com`

For information about SuSE Linux, go to `http://www.suse.com`

For information about HP OpenView Operations, IT/Operations, and Network Node Manager, refer to:
`http://www.docs.hp.com/hpux/netsys`

Further Information

Additional information about Serviceguard and high-availability topics may be found on HP's web pages: `http://www.hp.com/hpux/ha` (High Availability) and `http://www.hp.com/linux` (Linux-specific).

Also see `http://www.hp.com/go/ha`.

Support information is available from the Hewlett-Packard IT Resource Center at:

`http://itrc.hp.com (US and Asia Pacific)`
`http://europe.itrc.hp.com (Europe)`

To receive the latest news about recommended patches, product support matrices, and recently supported hardware, go to the IT Resource Center site above, and subscribe to the *High availability programs tips and issues digest*.

The most recent versions of users's guides, release notes, and white papers are available on Hewlett-Packard's documentation web pages: `http://docs.hp.com/hpux/ha` (High Availability) and `http://docs.hp.com/linux` (Linux-specific)

Compatibility Information and Installation Requirements

Before you begin an installation, read this entire document and any other Release Notes or READMEs you have.

Compatability

This section summarizes the compatability of this version of Serviceguard Manager with related products and their versions. For all versions (this and older), see the *Serviceguard Manager Support Matrix* posted on `http://www.docs.hp.com/hpux/ha` -> serviceguard -> white papers

Hardware Requirements

Serviceguard Manager will run on the HP 700 Series workstations and the HP 800 Series servers.

Serviceguard Manager will run on a PC with a Pentium II 450 MHz or higher, and a video adapter with resolution of SVGA or higher.

System Requirements

Serviceguard Manager version A.04.00 can be installed on a computer with one of the following operating systems:

- HP-UX, Version 11.0 or later.

  Viewing Serviceguard Manager through Reflection X is not supported.
- Red Hat Linux Advanced Server Version 2.1
- Red Hat Enterprise Linux Version 3
- SuSE Linux Enterprise Server, Version 8 (SLES 8), United Linux version 1.0 (SuSE is available only in English.)
- Microsoft Windows XP Professional Edition, or Windows 2000 Professional with Service Pack 1 or later, with a video adapter of SVGA or higher resolution. (With Serviceguard Manager version A.04.00, Windows NT is no longer supported.)

Memory Requirements

Running on HP-UX, these are the minimum requirements for Serviceguard Manager:

- 256 MB of available memory
- 120 MB of available hard disk space under `/opt`
- 1 MB of available hard disk space under `/usr`
- 1 MB of available hard disk space under `/etc/opt/OV` if OpenView is installed.
- 3-15 MB of available hard disk space under `/var` for log files.

Running on Red Hat or SuSE Linux, these are the minimum requirements for Serviceguard Manager:

- 128 MB of available memory
- 100 MB of available hard disk space under /usr/local
- Up to 33 MB of additional hard disk space during the installation process.
- 15 MB of additional hard disk space available for log files created when Serviceguard Manager is run:
  - Red Hat: `/usr/local/sgmgr/log`
  - SuSE: `/opt/sgmgr/log`
- 100 MB of additional hard disk space in:
  - Red Hat: `/usr/local/sgmgr/`
  - SuSE: `/opt/sgmgr/`
- Up to 33 MB of additional hard disk space during the install process.

Running on Windows, these are the minimum requirements for Serviceguard Manager:

- 256 MB of memory
- 55 MB of available hard disk space
- 1 MB for log files when Serviceguard Manager is run.
- Up to 50 MB of additional hard disk space during the installation process.

Requirements for Capabilities

With Serviceguard version A.04.00, a new capablity was added. Now you can configure clusters and packages using nodes that have Serviceguard version A.11.16. Administration has changed from previous versions as well. Serviceguard version 11.16 now has Role Based Access as a way to assign administrative roles to non-root users to administer Serviceguard clusters and packages, either locally or from outside the cluster.

With Serviceguard Manger A.04.00, some of the capabilities you have depend on the Serviceguard version of the Session Server, the node you log in to and begin a session. Some depend on the target, the Serviceguard node, cluster, or package you will see in your map, tree, and Properties.

The table below summarizes the capabilities of different releases of Session Servers and target nodes in Serviceguard Manager A.04.00. The first column has the Serviceguard versions of the Session Server. The second column lists the Serviceguard version of target clusters you can reach with that Session Server. The next three columns describe the capabilities, and what is required for each: Monitor, Administration, and Configuration.

Table 1-1 Capabilities of Session Servers on Target clusters

Session Server's Service guard version	Target cluster's Service guard version	To Monitor	To Administer	To Configure
A.11.13, A.11.14, and A.11.15	A.11.10, A.11.11, and A.11.12	**User** can be any entry in Session Server's /etc/passwd file **Target** must have <sess.serv><root> in `cmclnodelist` file.	not supported	not supported

Table 1-1 Capabilities of Session Servers on Target clusters (Continued)

Session Server's Service guard version	Target cluster's Service guard version	To Monitor	To Administer	To Configure
A.11.13 A.11.14, and A.11.15	A.11.13 A.11.14, and A.11.15	**User** can be any entry in Session Server's /etc/passwd file **Target** must have <sess.serv><root> in `cmclnodelist` file.	**User** must log in to Session Server as root. **Target** must have <sess.serv><root> in `cmclnodelist` file.	not supported
A.11.13, A.11.14, and A.11.15	A.11.16	**User** can be any entry in Session Server's /etc/passwd file **Target cluster** must have an Access control Policy configured • Host = Session Server • User = any entry in Session Server's /etc/passwd • Role = Monitor	Not supported	Configuration menu available when an A.11.16 object is selected User must supply root password for a cluster node
A.11.16	A.11.13, A.11.14, and A.11.15	**User** can be any entry in Session Server's /etc/passwd file **Target** must have <sess.serv><root> in `cmclnodelist` file.	**User** must log in to Session Server as root. **Target** must have <sess.serv><root> in `cmclnodelist` file.	not supported

Table 1-1 Capabilities of Session Servers on Target clusters (Continued)

Session Server's Service guard version	Target cluster's Service guard version	To Monitor	To Administer	To Configure
A.11.16	A.11.16	**User** can be any entry in Session Server's /etc/passwd file **Target cluster** must have an Access control Policy configured • Host = Session Server • User = any entry in Session Server's /etc/passwd • Role = Monitor	**User** can be any entry in Session Server's /etc/passwd file **Target cluster** must have an Access control Policy configured • Host = Session Server • User = any entry in Session Server's /etc/passwd • Role = Admin	**User** can be any entry in Session Server's /etc/passwd file **Target cluster** User must supply root password for a cluster node

Port Requirements

Serviceguard Manager itself does not have any port requirements. If you want to receive SNMP traps in the Event Browser, you need the SNMP ports 161 and 162.

Serviceguard does have port requirements, particularly when interacting with internal firewalls. If you are using a firewall such as Bastille, and connecting to a Cluster Object Manager outside the cluster, these rules apply:

Each Serviceguard Manager node must allow these connections:

- from the cluster nodes:
  - — udp on port 162
- to the cluster nodes:
  - — udp on port 161

Each Serviceguard node must allow these connections:

- from the Serviceguard Manager node:
  - udp on port 161
- to the Serviceguard Manager node:
  - udp on port 162
- to the COM node:
  - tcp on port 5303 - and allow only packets with SYN flag.

Each cluster node must allow these connections:

- from the COM node to the cluster nodes:
  - tcp on port 5302 and allow only packets with the SYN flag
  - udp on port 5302
- to the COM node from the cluster nodes
  - tcp and udp on port numbers 49152-65535 from the cluster nodes

The node running the COM must allow these connections:

- from Serviceguard Manager to the COM node:
  - tcp on port 5303 - and allow only packets with the SYN flag
- from cluster nodes to the COM:
  - tcp and udp on port numbers 49152-65535 from the cluster nodes
- to the cluster nodes
  - tcp on port 5302 - and allow only packets with the SYN flag
  - udp on port 5302

Each cluster node should allow SNMP connections between it and the Serviceguard Manager node. The Event Browser in Serviceguard Manager can receive messages from SNMP traps. SNMP requires ports 161 and 162. The list of port assignments is in the /etc/services file.

Because SNMP uses a single dedicated port, only one application can receive messages. For more information about SNMP, open online help and go to Troubleshooting Clusters, SNMP Problems.

Installing and Running Serviceguard Manager

Installing Software

You can install Serviceguard Manager on an HP-UX workstation, on an HP-UX server (with or without Serviceguard), on a Linux workstation (with or without Serviceguard), or on a PC with Windows XP Professional Edition or Windows 2000 Professional.

If a previous version of Serviceguard Manager is already installed, stop any instances of Serviceguard Manager running on a node before installing the new version there. See information about uninstalling below.

Before Installing Serviceguard Manager

When deciding where to install Serviceguard Manager, consider the connections from users to the Session Server node, the connection from the Session Server to cluster nodes, and creating the security you want.

Which operators will use the interface, and which capabilities do you want them to have? Which management stations will they sit at, and which computer will they log into to begin a Serviceguard session? See the table “Capabilities of Session Servers on Target clusters” on page 16 for help in planning this. Serviceguard version 11.16 has a new way to setting up access.

Installing Software

You can install Serviceguard Manager on three platforms: HP-UX, Linux, or Windows. The methods are slightly different for each. Use the section below that is appropriate for your type of installation.

There are two ways to install Serviceguard Manager: from the HP Serviceguard Distributed Components disk, or from this web site: `http://www.software.hp.com`. You can choose the English, Japanese, Korean, Simplified Chinese, or Traditional Chinese version.

Serviceguard Manager installs its own JRE (Java Runtime Environment™), and can not use any other JRE that may already be installed.

If you are updating from an earlier version, first uninstall the earlier version.

If you update from a version of Serviceguard Manager earlier than A.03.00, your user preference files will be replaced with newer default settings. Preference files changed inA.03.00.01, and earlier settings cannot be carried over.

NOTE Serviceguard Manager supports system default colors for all platforms. Most system settings work, but a custom color setup could cause problems. For example, you may see what seems to be an empty box. However, when you drag the mouse to highlight it, you may discover that your system is displaying white font on a white background. If you restore the system to default colors, you will be able to see things as they were designed.

Installing Serviceguard Manager on HP-UX You can install version A.04.00 of Serviceguard Manager on a computer with bundles specifically for HP-UX Version 11.x

- To install from the HP Serviceguard Distributed Components disk:

  1. Mount the CD-ROM directory, choosing /SD_CDROM for your mount directory.
  2. Enter the `swinstall` command.
  3. When the window opens, set Source Depot Type to: `LocalCDROM`.

     For Source Depot Path, fill in the appropriate release name. For example, if you have HP-UX 11.23, use:

     `SD_CDROM/SGManager/HP-UX/11.23/sgmanager.depot`
  4. `swinstall` allows you to select: `B8325BA A.04.00 Serviceguard Manager`. Select the appropriate platform, then start the install.

- To install from the web, go to `http://www.software.hp.com`. Click High Availability, then Serviceguard Manager for HP-UX. Fill out the information form. A download window opens.

1. Select your operating system from the “Software Specification” pull-down list. (To see the version of an HP-UX node, use the `uname` command from the node.)
2. Download the depot, and store it on your disk, perhaps in the `/tmp` directory. To save disk space, you can remove this depot from your disk when you have finished installing.
3. Run the `swinstall` command on this depot. The user interface will lead you through the installation (mark, analyze, install). Select the `B8325BA Serviceguard Manager` product.

After swinstall completes, verify the installation:

1. Is the man page installed? (Enter: `man sgmgr`)
2. Was the directory created for log files? (Enter: `ll /var/opt/sgmgr`)
3. Are all the program files in the installation directory? If you install in the default directory, you should see the following when you enter `ll /opt/sgmgr/* :`
   - bin
   - examples
   - jre
   - lib
   - config
   - OV (if HP OpenView is installed)

Serviceguard Manager installs its own JRE (Java™ Runtime Environment) and cannot use any other JRE on the computer.

If you are updating from an earlier version of Serviceguard Manager, your user preference files are replaced with default settings. The new preference files are compatible with Serviceguard Manager Version A.03.00.01 and later. Preferences from earlier versions cannot be carried over.

If you have Network Node Manager or OpenView Operations installed on this computer, also see the section below, *Installing with HP OpenView*.

For more information about installation procedures and related issues, refer to the man page for `swinstall`. Also see the manual *Managing HP-UX Software with SD-UX* , which can be viewed or printed from http://www.docs.hp.com -> HP-UX 11.0 Operating System -> System Administration.

Installing Serviceguard Manager on Linux Install Serviceguard Manager on a computer that has one of these versions of Linux:

- Red Hat Enterprise Linux Version 3
- SuSE Linux Enterprise Server, Version 8 (SLES 8), United Linux version 1.0 (SuSE is available only in English.)

You can install from two places: from the Distributed Components CD or from a browser

- To install from the Serviceguard Distributed Components CD:
  1. Insert the disk and mount the CD-ROM drive. Choose a name for your directory, for example `</SGM_ROM>`.
  2. From `</SGM_ROM>/SGManager/LINUX`, enter:
     — For Red Hat Linux:

     ```
     rpm -i sgmanager-A.04.00.00-1.product.redhat.i386.rpm
     ```

     — For SuSE Linux (32-bit machines):

     ```
     rpm -i sgmanager-A.04.00.00-1.product.suse.i386.rpm
     ```

     — For SuSE Linux (64-bit machines):

     ```
     rpm -i sgmanager-A.04.00.00-1.product.suse.ia64.rpm
     ```
- To install from the web:
  1. Go to `http://www.software.hp.com`. Click High Availability. Click Serviceguard Manager in the alphabetical list.
  2. Save the `sgmanager-A.04.00.00-1.product.redhat.i386.rpm` file to your disk. (To save disk space, you can remove the rpm file when installation is done.)
  3. From the directory where you saved the file, run the install process with this command:
     — For Red Hat Linux:

```
rpm -i sgmanager-A.04.00.00-1.product.redhat.i386.rpm
```

— For SuSE Linux (32-bit machines):

```
rpm -i sgmanager-A.04.00.00-1.product.suse.i386.rpm
```

— For SuSE Linux (64-bit machines):

```
rpm -i sgmanager-A.04.00.00-1.product.suse.ia64.rpm
```

After `rpm` completes, verify the installation:

1. Is the man page is installed? (Enter: `man sgmgr`)
2. Are all the program file directories in the installation directory? By default, the Red Hat default directory is `/usr/local/sgmgr/`. By default, the SuSE install directory is `/opt/sgmgr/`.
   - bin
   - examples
   - jre
   - lib
   - log
   - users
   - config

Serviceguard Manager installs its own JRE (Java Runtime Environment™) and cannot use another JRE already installed on the computer.

If you are updating from an earlier version of Serviceguard Manager, your user preference files are replaced with default settings. The new preference files are compatible with architecture changes in Serviceguard Manager Version A.03.00.01 and later. Your old preferences cannot be carried over.

Installing Serviceguard Manager on Windows Install Serviceguard Manager on a computer that has Microsoft Windows XP Professional Edition or Windows 2000 Professional installed. If you currently have an older version of Serviceguard Manager, uninstall it first: Start -> Programs -> ServiceGuard Manager -> Uninstall.

You can install from two places:

- To install from the Serviceguard Distributed Components CD:

1. Insert the disk in the PC's drive.
2. Click the Start menu in lower left corner of your screen. Choose Settings -> Control Panel. Double-click Add/Remove Programs.
3. Click on Install.
4. Navigate to SGManager\Windows. Select sgmanager.exe.
5. Click Finish and follow installation directions.

- To install from the web:

1. Go to http://www.software.hp.com. Click High Availability, then Serviceguard Manager.
2. Click on the link under Download Software (sgmanager.exe).
3. You can store the file on your system, or run it directly from the website. If you download to your system, you can remove it after installation.
4. On your PC, run sgmanager.exe (or double-click the sgmanager.exe file in Explorer).
5. Choose a language option. The default install directory is: C:\Program Files\Hewlett Packard\ServiceGuard Manager\ but you can choose a custom installation directory.

The SG Manager A.04.00 icon will appear on your desktop.

Using Windows Explorer, verify that these folders are installed:

- bin
- examples
- jre
- lib
- log
- users
- config
- ov (if OpenView Network Node Manager is already installed on the PC)

Serviceguard Manager installs its own JRE (Java Runtime Environment™) and cannot use any other JRE already on the computer.

If you have Network Node Manager installed on this computer, see Installing with OpenView, below.

Verify that the name ServiceGuardManager is listed in Start -> Programs ->. Verify that a SG Manager A.04.00 icon is on your desktop.

If you are updating from an earlier version of Serviceguard Manager, your user preference files are replaced with default settings. The new preference files are compatible with architecture changes in Serviceguard Manager Version A.03.00.01 and later. Your old preferences cannot be carried over.

Installing with HP Systems Insight Manger When you install Serviceguard Manager,it looks to see if you have installed HP Systems InsightManager, version C.04.01.00 or later. If you have, the ServiceguardManager install process automatically registers with InsightManager, and you can launch Serviceguard Manager from within InsightManager.

If you want to install Insight Manager after you have Serviceguard Manager installed, no registration is done. In this situation, uninstall Serviceguard Manger, and then re-install it.

Installing with HP OpenView When you install Serviceguard Manager, it looks to see if you have installed one of these OpenView products:

- NNM (Network Node Manager) Version 7.0, 6.31, 6.3, and 6.2.
- OpenView Operations Version 7.0 and 8.0. (OVO includes NNM.)
- VPO Version 6.0. Serviceguard Manager does not support VPW (Vantage Point for Windows).

If you have installed any of these, the install process automatically does these things:

- Adds a menu item and a button on the toolbar of NNM or OVO to start Serviceguard Manager (“Serviceguard Mgr Launcher”).
- Sends Serviceguard events to be logged in the Event Log. The Serviceguard subagent is responsible for notifying the management station when status or configuration changes. By default, it is installed in `/usr/lbin/cmsnmpd`.
- Adds Serviceguard messages to the OVO Message Browser if assigned, and in the NNM Alarm Browser.

- Modifies the Event Configuration Tool so you can set up automatic actions and filter Serviceguard messages.
- Lets you configure the data collection to get historical MIB data from network nodes, including data stored in Serviceguard MIB objects. The Serviceguard subagent services the Serviceguard MIB objects. By default, it is installed in `/usr/lbin/cmsnmpd`.

Then the installation process looks to see if you have OVO Version 7 or later, or VPO 6.0 or later. If you do, it checks to see if you also have ClusterView.

If you do have ClusterView installed, no files will be overwritten. The launcher will be installed, so you can open an instance of Serviceguard Manager from the OpenView menu.

If you do not have ClusterView, but you do have OVO, tools are added to the Tool Bank, ready for an OpenView administrator to assign them. These tools are listed below.

Assign these tools carefully. Some require root access to the Serviceguard nodes, and some can grant it indirectly.

- Serviceguard Mgr launcher: You can launch Serviceguard Manager from OpenView. Serviceguard Manager is independent of OpenView. It does not use the OV daemons or object database to discover the configuration or status of clusters. Instead, it gets information by connecting to Serviceguard Version A.11.13 or greater; then Serviceguard goes out on its subnets and gathers the information.
- Installs these Tools to work on a selected cluster node:
  - HA Info Tools:
    - Query Cluster Conf: uses `cmquerycl` to gather configuration information
    - Scan Cluster: uses `cmscancl` to display information about cluster configuration, LAN cards, disks, and file systems.
    - View Cluster Binary Config: uses `cmviewconf` to see an ASCII extraction of the binary configuration file.
    - View Cluster Config: uses `cmviewcl` to see cluster configuration and status of running clusters.
    - View System Log: opens `vi` editor to view `/var/adm/syslog/syslog.log`

- HA Admin Tools:
  - Run Cluster: uses the `cmruncl` command to start a cluster from the node you selected
  - Halt Cluster: uses the `sghaltcl` command (a variant of the `cmhaltcl` command) to halt the cluster of the node you selected
  - Run Node: uses the `cmrunnode` command to join the selected node to its cluster
  - Halt Node: uses the `cmhaltnode` command to make the selected node inactive in its cluster
- Net Diag Tools
  - View Interface Config: displays LAN interface configuration parameters
  - LAN Diag and Admin: launches the program `lanadmin`, which administers and tests the local area network.
  - Scan LAN interfaces: uses `lanscan` to display information about each LAN device that has software support on the system.
  - IP Interface Stat: uses `netstat` to display statistics for network interfaces and protocols, as well as the contents of various network-related data structures. (Choose options to filter output.)
- LVM tools.
  - View Logical Volumes: displays the logical volumes currently configured
  - View Volume Groups: uses `vgdisplay` to show information about the volume groups configured.

Uninstalling Serviceguard Manager

Uninstalling from HP-UX On HP-UX, uninstall Serviceguard Manager by running this command:`swremove B8325BA`

After uninstalling Serviceguard Manager, you can remove the Serviceguard Manager logs; if you are not going to re-install, you can remove the entire directory (by default, `/var/opt/sgmgr/`). If you are not going to re-install, you can also remove the preferences that are stored in the user's home directory, under the .sgmgr directory.

Uninstalling from Linux On Linux, uninstall Serviceguard Manager by running this command:

```
rpm -e sgmanager
```

After uninstalling, you can remove the Serviceguard Manager logs; if you are not going to re-install, you can remove the entire directory (by default, `/usr/local/sgmgr` on Red Hat and `/opt/sgmgr` on SuSE). If you get a message about "unable to remove." you can ignore the ones about error messages. If you are not going to reinstall, you can remove the preferences that are stored in the user's home directory, under the.sgmgr/users directory.

Uninstalling from Windows On Windows, there are two ways to uninstall Serviceguard:

- From the Start menu, choose Programs -> ServiceGuard Manager -> Uninstall.
- From the Start menu, choose Settings -> Control Panel -> Add/Remove Programs. Select Serviceguard Manager from the list.

After uninstalling Serviceguard Manager, you can delete the log files; if you are not going to re-install, you can remove the entire directory: `C:\Program Files\Hewlett-Packard\ServiceGuard Manager\log` folder. If you are not going to re-install, you can also remove the user preferences folder. In Windows, by default, preferences are in: `C:\Program Files\Hewlett-Packard\ServiceGuard Manager\users`

Removing Serviceguard Manager - OpenView Integration In addition to doing the `swremove` of Serviceguard Manager, you need to manually do the following things if you integrated Serviceguard Manager into OpenView.

- If you have NNM only (not OVO):

  1. Remove event templates: Go to the NNM menu and select Options -> Event Configuration. From the list, delete the following event groups:

— hpEMSTraps

— hpmcMgmt Traps

— hpmcSGTraps

2. Remove SGMgr MIBs: Go to the NNM menu and select Options -> Load/Unload MIBs:SNMP. Unload the following MIBs:

— hp-cluster

— hp-sgcluster

- If you have OVO (which includes NNM):

1. Remove messaging: Go to the Message Group Bank, and delete Message Group HA.

2. Remove templates and monitors: Open the Message Source Templates window. By default, the following are visible on the top level. Remove them:

— Syslog

— SG_check_cmsnmpd

— EMS SNMP Traps

— HA Cluster SNMP Traps

3. Remove Application Tools: From the Application Bank, remove these tool groups:

— HA Info

— HA Admin

— LVM

— Net Diag

Uninstalling: Removing SNMP Trap Destinations If you are not going to re-install, and you do not wish to receive SNMP traps anymore, you need to “unset” the trap destinations on the sending nodes.

1. First get a list of the nodes that are sending traps to your computer. Select Event Browser from the View menu. Click the Configuration tab. Make a note of the nodes and IP addresses.

Notice that the configuration tab shows only the nodes in your current map. If you have several subnets, connect to a Session Server in each, and use the View All option.

2. Log in to each node and edit the /etc/snmpd.conf file to remove your computer from the list.
3. Stop and re-start the SNMP Master Agent on the node.
   a. Find the process ID number, using: `ps -ef | grep snmp`.

      The master agent will show as `snmpd`, and the subagent will show as `cmsnmpd`.

   b. Stop that process, using: kill <*pid*>
   c. Restart the agents.

      Use: `/sbin/init.d/SnmpMaster start` for the master agent

      Use: `/sbin/lbin/cmsnmpd` for the subagent.

Setting up Serviceguard Manager

Security, Logins, and Access Policies

In version A.11.16, Serviceguard changed its method of controlling and assigning logins, and roles. Therefore, the way you open Serviceguard sessions and discover Serviceguard objects is quite different in version A.11.16 and later than it is in earlier versions.

Logins and roles, Version A.11.16 and later: Creating or modifying configuration still requires Root access (UID=0) on a cluster's nodes. Starting in Serviceguard version A.11.16, however, a root user can configure clusters and packages using Serviceguard Manager or on the command line.

In addition, there are four possible non-root roles that can be defined in the cluster's configuration files. These can be specified as Access Control Policies in the cluster and package configuration files. Each Access Policy has three parts:

- User: A username from the host's /etc/passwd file
- Host: Where the user will issue the command. For Serviceguard Manager, this is the Session Server node

- Role: Which commands the user may issue on the cluster where the policy is configured. There are 4 non-root roles:
  - — monitor (view, read-only): in cluster configuration file.

    This is the only role that does not require a Host with Serviceguard A.11.16.
  - — (single package) package admin: defined in that package's configuration file
  - — (all cluster packages) package admin: defined in the cluster configuration file
  - — full admin (cluster and its packages): defined in the cluster configuration file

For more information about access control policies, see the online help for Configuring Clusters: Roles.

If you upgraded a cluster to Serviceguard A.11.16, its cmclnodelist has been migrated into Access Control Policies. With A.11.16, `cmclnodelist` is gone. If your previous `cmclnodelist` file listed the pair <sess.server><user> your cluster configuration now has an Access Control Policy that lists this triplet:

- USER_NAME <user>
- USER_HOST <sess.serve>
- USER_ROLE Monitor (All migrated pairs have Monitor, the view-only role.)

If your old cmclnodelist had the wildcard +, the configuration file now has an Access Control Policy with wildcards in triplet:

- USER_NAME ANY_USER
- USER_HOST ANY_SERVICEGUARD_NODE
- USER_ROLE MONITOR (All migrated pairs have Monitor, the view-only role.)

Only a root user can modify configuration to change Access Control Policies. You do not have to halt the cluster, or any packages, to add, modify, or delete an Access Control Policy.

Bootstrapping a new A.11.16 node If you have a cluster on an A.11.16 node, be sure to configure at least one Access Control Policy if you want to see the cluster and its nodes in Serviceguard Manager. Once a cluster is configured, Serviceguard will only check access in the cluster's configuration files. It will ignore the .rhosts file and the `cmclnodelist` file.

If no cluster is configured, you can create a `cmclnodelist` file to act as a "bootstrap" for access. Once done, you will be able to see information about the node on the Serviceguard Manager map and tree, and in Properties. If it is not a part of a cluster now, it will still show up in the Unused Nodes list. To configure it later, you can connect to a Session Server with Serviceguard version A.11.16, select the node from Unused Nodes, and select Configuration from the Actions menu.

To create a bootstrap file:

1. Create the file `/etc/cmcluster/cmclnodelist` on the node.
2. Using any ascii editor, add a comment like this:

   ```
   ##########################################

   # Do not try to configure access in this file.

   # This is for bootstrapping only, before a cluster is configured.

   # Once a cluster exists, Serviceguard will ignore this file.

   ##########################################################
   ```

3. Below the comment, create monitor access so Serviceguard can discover and display the node as an unused node.

   It may be easiest to add a wildcard + (plus) below the comment. This is equivalent to granting the view-only Monitor role to Any User from Any Serviceguard Node. It will allow any session on the node's subnet to query the cluster and display its information in any session of Serviceguard Manager.

   Alternately, you can list any number of <hostname> <username> pairs. Hostname can be any Session Server's name, and user can be any name in that Session Server's /etc/passwd file.

Now you will be able to see your new A.11.16 node in a Serviceguard Manager session. If the Session Server also has version A.11.16, you can configure this node into a cluster. You will be prompted for the node's root password.

Logins, roles and security, Version A.11.15 and earlier:

If you are an experienced Serviceguard user, you may think there is a similarity between the command-line user's `cmviewcl` command and the way Serviceguard Manager user gets information about remote clusters with Serviceguard version A.11.15 and earlier. Using Serviceguard Manager, certain users can also relay the most common administrative commands to these Serviceguard clusters, and the effect seems the same as logging into the node and issuing the command on the command line.

Please notice, however, that the permissions and access mechanisms are *not* the same. In version A.11.15 and earlier, the Serviceguard Manager user's permissions depend on his login to the *Session Server*, not the cluster node. It is the Session Server that interacts with the cluster nodes on the user's behalf, through the Cluster Object Manager, a Serviceguard API.

A Serviceguard Manager user does not need to directly access target nodes to do configuration of Serviceguard version 11.16. Users can log into a Session Server as any user. However, before the user can configure any object they see in the map or tree they must give a root password for at least one of the cluster nodes.

If the target node has version A.11.15 or earlier, the Session Server node must always use user= root to access it. The recommended access mechanism is to include the Session Server name or IP address in the target nodes' `cmclnodelist` file. A less secure way is to include the Session Server node in a target node's `.rhosts` file. Listing in `cmclnodelist` allows contact to Serviceguard alone; a listing in `.rhosts` grants wider access.

If the user is logged in as root to a Session Server node with version A.11.15 or earlier, the Session Server node will also display certain common administrative commands in the menu. The Session Server relays these commands to the clusters in the session for the users.

If you are updating from an earlier version, think about permissions on your HP-UX nodes with Serviceguard Version A.11.13, A.11.14, and A.11.15. Any person who can log in to that node as root may be able to do administrative commands on any cluster objects on that node's subnets. If you do not want access, you can limit the root logins on that node, or limit that node's access to particular clusters on its subnets.

Making a Highly Available Connection

If you wish, you can create a Serviceguard package that will keep the connection between your monitoring station and the Session Server highly available. If there is a failure in the connection, you might see the "Connection Dropped" message flash momentarily, but Serviceguard will maintain your connection. It will fail the connection over from one node in a Serviceguard cluster to another node in the same cluster.

Serviceguard Manager gets its information by connecting to a Session Server with Serviceguard A.11.13 or later. A component of Serviceguard, the Cluster Object Manager, polls the available subnets to discover other Serviceguard objects. It collects status and configuration information, and sends the information back to Serviceguard Manager.

To set up the highly-available connection between Serviceguard Manager and Session Server nodes in a cluster, follow these steps:

Create the package in a cluster with Serviceguard. For viewing, use Serviceguard A.11.12 or later. For administration commands use Serviceguard A.11.13 or later.

See "Creating the Package Configuration" chapter in the Serviceguard manual. All Serviceguard manuals are posted on the web and you can view or print them there. Go to `http://www.docs.hp.com` and click High Availability; the products are listed alphabetically.

1. Get an IP address to use as the package's relocatable address. You can use `nslookup` to be sure the package name and IP address are correctly associated in your DNS table.
2. When naming the package, choose one that your users will recognize, such as `Clus3Srvr`. The first time a user opens Serviceguard Manager they will see the Connect dialog box. They can type this name in for the server connection. After that, the name will appear in a list every time that user opens Serviceguard Manager.
3. Make only these two modifications to the package configuration file template, and leave the defaults for the other fields:
   - List the package nodes. For high-availability, it is best to list all the nodes in the cluster.
   - For the run and halt scripts pathname, specify the control script name and path for the run and halt script. (The default path is in the documentation.)

4. Open the control script template. Make just two modifications, and leave the defaults for the other fields. These will allow the connection between your client (Serviceguard Manager management node) and the Session Server:
   - Insert the IP address associated with your package (the package's relocatable address).
   - Insert the address of the subnet.

Assigning and Configuring New OpenView OVO Tools

When you install Serviceguard Manager, it checks to see if you have OpenView OVO installed. If you do, it checks to see if you have the tools listed in "Installing with HP OpenView" above. If you do not have those tools, it installs them for you.

To Restore Default Configuration If the Serviceguard Manager configuration gets lost or corrupted, follow these steps to restore the default configuration that came with Serviceguard Manager:

1. Exit all OVO user sessions.
2. Stop the OVO server process with the `/opt/OV/bin/ovstop opc` command.
3. Go to `/opt/sgmgr/OV` and untar the configurations files in with the `tar -xvf ito-ux.tar` command.
4. Go to `/opt/OV/bin/OpC` and upload the new configuration with the `opccfgupld -replace -subentity /opt/sgmgr/OV/SGOpC` command.
5. Stop and restart the OVO package with the `/opt/OV/bin/OpC/opcsv -stop` and `/opt/OV/bin/OpC/opcsv -start` commands.

Launching Serviceguard Manager

You can starting Serviceguard Manager directly from HP-UX, Linux, and from Windows.You can also start Serviceguard Manager from within HP Sytems Insight Manager or HP OpenView.

Launching Serviceguard Manager from HP-UX

To launch Serviceguard Manager, standalone, in HP-UX, go to the Serviceguard Manager directory (by default, `/opt/sgmgr/bin`) and enter the `sgmgr` or `./sgmgr` command, plus any options you want. To see the full command, enter `man sgmgr`. The options are also listed below in *sgmgr Command Syntax*.

You can also create a script or alias that includes the options you want.

Launching Serviceguard Manager from Linux

To launch Serviceguard Manager in Linux, go to the Serviceguard Manager directory (by default, Red Hat is `/usr/local/sgmgr/bin` and SuSE is `/opt/sgmgr/bin`). Enter the `sgmgr` or `./sgmgr` command, plus any options you want. To see the full command, enter `man sgmgr`. The options are also listed below in *sgmgr Command Syntax*

Launching Serviceguard Manager from Windows

Here are 3 ways to launch Serviceguard Manager in Windows:

- By default, a shortcut icon is placed on your desktop (labelled SG Manager A.04.00). Click it to launch the program. When installed, it has the simple command without options. You will be prompted to enter the options once the program opens. You can modify the icon's properties to use any of these options: your name, password, Session Server to connect to, and clusters to discover. If you want to modify it follow the steps below:

  1. Right-click on the icon, then choose Properties from the popup menu.
  2. Add options to the command in "Target." The options are listed below in *sgmgr Command Syntax*.

     It is best to put quotes around command and file path names; Windows allows spaces and other characters in directories, and that could cause parsing errors.

- From the *Start* menu, select Programs -> Serviceguard Manager. This launches the simple command, with no options.

- Open a *DOS* window. At the DOS prompt, enter the `SGMgrDOS.exe` command. Depending on your system path setup, you may have to enter the SGMgr directory (by default C:\Program Files\Hewlett-Packard\ServiceGuard Manager\bin). You can also enter options, as listed below in *sgmgr Command Syntax*.

  It is best to put quotes around command and file path names.

Launching Serviceguard Manager fromHP Insight Manger or OpenView

Within Insight Manager or OpenView, you can launch SGMgr from themenu bar or by clicking the SGMgr icon.

When Serviceguard Manager installs, it checks to see if HP Insight Manager or OpenView are installed. If either are present, Serviceguard registers itself with the program. Therefore, if you have both, you want to install Serviceguard Manager *after* you installInsight Manager or OpenView. If you already have Insight Manager or OpenView installed, simply de-install Serviceguard Manager, then re-install it.

sgmgr Command Syntax

The basic command to launch Serviceguard Manager in Linux or HP-UX is `sgmgr`. In Windows, it is `SGMgr.exe` or `SGMgrDOS.exe`. The options are listed below. If you do not mention an option with the command, you will be prompted to specify it in a window after the interface opens.

- To open a saved (static) file:
  - The -f <`filename`> option opens a saved .sgm file. Enter the pathname of the saved file, in quotes. This option is not used with any other options.
- To open a Session Server connection and see a map that you can update; repeat these options for each session:
  - The -s <`servername`> option specifies a node with Serviceguard A.11.13 or later. This node will become your Session Server. Serviceguard will discover the other clusters on its subnet, and report back their configuration and status information.
  - If you specify the -s option, you may also specify the -l <`username`> option to give the logon name of a user on that server.

— If you specify the -l option, you may also specify the -p <password> option to give that user's password.

— The -c <clustername> option specifies the clusters you want the Session Server to discover. (The Session Server can discover only the nodes on its subnets.) These clusters will be displayed on your map, under the Session Server's name. Repeat the -c option for several clusters in this session.

— The -local option will discover the cluster where the Session Server is configured, whether it is specifically listed in the -c option or not.

— Specify -un TRUE to see the unused nodes discovered by this Session Server on its subnets. These are nodes that have Serviceguard installed, but are not currently configured in any cluster.

- To open another session, repeat these steps.

When the interface opens, you will see what you have chosen, and you will be given a chance to fill in any options you have not yet chosen.

Using the Interface

When Serviceguard Manager opens, you have a chance to choose Connect or Open (unless you have already specified one of them in the command line).

Use Open to see any saved "snapshot" file (one with .sgm extension). To get acquainted with the program, Open a supplied Example file.

To see your own clusters "live", use Connect. You need to have a logon for a node that is running Serviceguard A.11.13 or later. This will be your Session Server. It can discover clusters on its subnets, if they have granted it access.

For the rules about access for admin capability, see Table 1-1 on page 16

Once you have a session open, open Help from the toolbar. Open the Getting Started topic from the Help window's Table of Contents. *Using Serviceguard* is a good place to start. *Map Legend* explains status, colors, and symbols on the map.

Select a tree or map object, and choose Properties from the Actions menu.

Select a tree or map object and look at Actions. You will see Administration if you have permission. If you select an object with Serviceguard A.11.16, you will also see Configuration.

Patches and Fixes in this Version

This section lists known patches, defects that have been fixed in this version, and current known defects and workarounds.

Please consult the Release Notes for the language you will install, to find information about language-specific patches, defects, and known problems.

Required and Recommended Patches

This section lists patches required or recommended for Serviceguard Manager Version A.04.00. This list is subject to change without notice. Contact your HP support representative for up-to-the-moment information. Patches can be superseded or withdrawn at any time, so always be sure to check the status of any patch before downloading it.

An updated list of patches is available on the Hewlett-Packard IT Resource Center: `http://itrc.hp.com` (Americas and Asia Pacific) and `http://europe.itrc.hp.com` (Europe).

In non-English locales, when installing on HP-UX 11.0 or 11.11, install the TrueType Fonts patch:

- HP-UX 11.0:
  - Japanese: PHSS_26972
  - Korean: PHSS_26974
  - Chinese-Simplified: PHSS_26976
  - Chinese-Traditional: PHSS_24937
  - Font Server: PHSS_25091
- HP-UX 11.11
  - Japanese: PHSS_26971
  - Korean: PHSS_26973
  - Chinese-Simplified: PHSS_26975
  - Chinese-Traditional: PHSS_24977
  - Font Server: PHSS_25092

Before you use the Event Browser, install a patches on all HP-UX nodes in the clusters that will *send* the SNMP traps to your Serviceguard Manager Event Browser. The patch numbers are:

- PHSS_26724 for HP-UX 10.x
- PHSS_27858 for HP-UX 11.x

Serviceguard Manager installs its own JRE (Java Runtime Environment). Check for defects for each platform's JRE:

- On HP-UX, Serviceguard Manager automatically installs JRE Version 1.4.2.00.
- On Linux, Serviceguard Manager automatically installs JRE Version 1.4.2_02
- On Windows, Serviceguard Manager automatically installs JRE Version 1.4.2_02

Check your operating system for patches:

- For HP-UX, check patches at: `http://www.itrc.hp.com (Americas and Asia Pacific)` or `http://www.europe.itrc.hp.com (Europe)`.
- For Linux, check patches at: `http://www.redhat.com`
- For Windows PC, check Service Pack at: `http://microsoft.com/ms.htm`.

Fixed in Version A.04.00

The problems listed below were fixed for the A.04.00 release.

- JAGae87041 - In SuSE Linux on IPF, Serviceguard Manager sometimes did not run. Although it installs correctly, sometimes Serviceguard Manager will not run because it can not find a library.
- JAGae81488 - A PC hung. The cause is apparently some interaction between the graphics accelerator card and JRE 1.4.1-01.b0.
- JAGae69297 - Man page formatting issue / only available in English: The `sgmgr` man page is not correctly formatted. Also, the man page is available in less languages that the interface is.
- JAGae68450 - Sometimes map connecting lines between node and package are missing, (Rare.)

- JAGae67456 - Using RemoteX, “Save Map” creates empty file. This is a defect in Serviceguard Manager A.03.00.01 on Linux. The Save Map functionality has changed in A.04.00
- JAGae67232 - Right click in tree may cause an exception (Fixed in A.03.00.01)Commands do not always complete if user right-clicks on an object that is *not selected*.
- JAGae64679 - HP-UX/OpenView installation doesn’t show IPv6 traps IPv6 trap template should be overwritten when Serviceguard is installed on an OpenView system. However, it isn’t.
- JAGae62189 - Incorrect executing command message in halt node progress dialog (Fixed in A.03.00.01) Halt node progress dialog says command executing is `cmhaltcl -v -f`. It should say `cmhaltnode -v -f`.
- JAGae55465 - sgmgr core dumps when executed by non-root user (JRE directory permission problem) (Fixed in A.03.00.01) On some HP-UX systems, a JRE file permission problem causes Serviceguard Manager to core dump when a non-root user opens the interface
- JAGae51034 - Event notification not supported by SG 11.12 Object Manager (Fixed in A.03.00.01)
- JAGae50988 - Trap status is “trap Setting” if IP address is unresolved (Fixed in A.03.00.01)
- JAGae50948 - Event Browser reports “HA Cluster Node Joined Cluster” when it should report “HA Cluster Node Up.” (Fixed in A.03.00.01)
- JAGae50883 - Event Browser Time/Date sort does not work correctly (Fixed in A.03.00.01)
- JAGae50816 - “Java Webstart not installed” message displayed when using Netscape. The problems occurs when using Service Control Manager. Serviceguard Manager 4.0 no longer supports using Service Control Manager.
- JAGae50813 Cannot launch Serviceguard Manager 3.00 from Service Control Manager 3.0 (Webstart not available). Servcieguard Manager version 4.0 does not use Service Control Manager.
- JAGae50772 - Rendering issues for non-English locales running W2P (English Version) Certain non-English characters were not rendered correctly.

- JAGae50769 - In Simplified Chinese and Traditional Chinese locales on Windows, installer renders buttons as squares. (Fixed in A.03.00.01)
- JAGae50746 - “Include Unused SG nodes” button does not work in Change Sessions dialog
- JAGae50692 - Can not read .sgm files saved from Serviceguard Extension for RAC (Fixed in A.03.00.01)
- JAGae50336 - Alerts Panel: package status unknown for some newly added packages
- JAGae50003 - SNMP Event Browser cannot be scrolled during arrival of burst of events
- JAGae49513 - Cluster Properties shows Rolling Upgrade = yes if node version is unknown.
- JAGae48058 - View-Tree menu unclick does not remove tree. Session disconnects if trying to discover many clusters with bad configurations.
- JAGae45299 - Printing Help pages may use 100% CPU (Java problem) When trying to print a Help topic, CPU usage may suddenly jump to 100% of capacity, and stay there.
- JAGae42868 - File Chooser window for file Open and Save can be slow to pop up.

Known Problems and Workarounds

The following lists known problems for Serviceguard Manager version A.04.00 at time of publication. This list is subject to change without notice. Contact your HP support representative for up-to-the-moment information. More recent information on known problems and workarounds may be available on the Hewlett-Packard IT Resource Center: `http://www.itrc.hp.com (Americas and Asia Pacific)` or `http://www.europe.itrc.hp.com (Europe)`.

JAGaf21135 - The map also disappears when you hide the tree. Re-enabling does not work.

- *What is the problem?* Do not hide the tree. If you click the box to remove the “Tree” check from the View menu, the map and the tree become blank, and cannot be re-enabled.

- *What is the workaround?* Do not hide the tree. If you do, you have to close Serviceguard Manager and open a new instance.

JAGaf19307 - Serviceguard/SIM integration does not un-install properly

- *What is the problem?* After Serviceguard Manager is uninstalled, it is still on the menu. If you click on it, it says “Error 404 not found.”
- *What is the workaround?* There is no workaround.

JAGaf18740 - Sometimes, Linux rpm manager warns file conflict for SIM integration files

- *What is the problem?* When installing SGMgr on a linux machine with SIM (Systems Insight Manager) already installed, user may see the following errors:

```
# rpm -Uvh sgmanager-A.04.00.00-1.product.redhat.i386.rpm

Preparing...

########################################### [100%]
file /opt/hpwebadmin/lib/sgmgrLauncher.properties from install of
sgmanager-A.04.00.00-1 conflicts with file from package
hpsim-C.04.01.00.00R41_QA9-1
file /opt/hpwebadmin/lib/sgmgrLauncher_ja.properties from install of
sgmanager-A.04.00.00-1 conflicts with file from package hpsim-
C.04.01.00.00R41_QA9-1
file /opt/hpwebadmin/webapps/sgmgr/WEB-INF/web.xml from install of
sgmanager-A.04.00.00-1 conflicts with file from package
hpsim-C.04.01.00.00R41_QA9-1
file /opt/hpwebadmin/webapps/sgmgr/sgmgrLauncher.jsp from install of
sgmanager-A.04.00.00-1 conflicts with file from package
hpsim-C.04.01.00.00R41_QA9-1
```

The Serviceguard Manager files are meant to replace the hpsim package files

- *What is the workaround?* Force replacement files, regardless of the warnings.

```
rpm -i --replacefiles sgmanager-A.04.00.00-1.product.redhat.i386.rpm
```

JAGaf18743 - InstallAnywhere does not suport Win 2003 Server

- *What is the problem?* System Insight Manger supports Windows 2003 server, but Serviceguard Manager does not.

- *What is the workaround?* Install Serviceguard Manager on one of the platforms it supports.

JAGaf18880 - Serviceguard Manager integration with OVO 8.0 is not complete

- *What is the problem?* Serviceguard Manger does not completely integrate with OVO 8.0. The tools are missing, although you can manually install the other functionality is there. OVO 8.0 includes NNM 7.1, and the NNM 7.1 functionality does install without problem. (This does not happen with OVO 6.0 or 7.0.)
- *What is the workaround?* When using swinstall to install Serviceguard Manager a user sees that NNM-UX (and/or NNM-JPN-UX) fileset(s) are installed, if OVO 8.0 is installed on the machine. SG mib and SG snmp event templates will be available in OVO 8.0. The following steps need to be performed manually for SGMgr icon and launcher menu item to appear in OVO:

  Register the SGMgr application with the user opc_adm.

  ```
  cd /etc/opt/OV/share/conf/OpC/mgmt_sv/ui/registration/C/
  opc_adm/
  sbin/ln -fs ../../../../../../../registration
  /C/sgmgr.arf ./sgmgr.arf
  ```

  And if you have Japanese version of OVO 8.0:

  ```
  cd /etc/opt/OV/share/conf/OpC/mgmt_sv/ui/registration
  /ja_JP.SJIS/opc_adm/
  sbin/ln -fs ../../../../../../../
  registration/ja_JP.SJIS/sgmgr.arf ./sgmgr.arf
  ```

  However, the SG OVO tools are not avaiable for OVO 8.0. There is currently no workaround ways of installing them for this release.

JAGaf17398 - Creating new cluster with embedded “#” character fails (API JAGaf12270)

- *What is the problem?* Using Serviceguard Manager, you cannot create a cluster with the pound (#) character in the name. One example is the name “cluster#27.” Other non-alphanumeric characters may not be accepted.

When you click Apply, you will get an internal error, “Null pointer exception.” In the Operations Log, after Operation Completed”, you may see a message like this: “Error: Missing ‘{’ in Component definition.”

- *What is the workaround?* Try to create clusters with alpha-numeric characters in the name. If you use other keyboard characters, check the log file carefully.

JAGaf17035 Some accessibility short cut keys do not work in non-English locale**.**

- *What is the problem?* Some accessibility short-cut keys do not work in traditional Chinese, simplified Chinese, Korean, or Japanese.
- *What is the workaround?* There is no workaround. If you require short-cut keys, install the English version.

JAGaf15152 Package with all nodes (*) causes problem when adding node to cluster.

- *What is the problem?* If a configuration uses a wild card to set node membership to all nodes, you will have trouble adding a new node to the cluster.
- *What is the workaround?* On the package configuration screen, remove the “all nodes” star wildcard. Select all the nodes in the list, adding them one at a time. Then add the new node. Be sure the configuration and control script are added to the new node before you do any more changes.

JAGaf14625 Problems creating and modifying packages that contain non-alphanumeric characters (,*,$,#, ...).

- *What is the problem?* All alphanumeric characters are accepted as package names. However, you cannot use most of the other characters on a keyboard. (For the exact list, see the Help topic for Configuring Packages.)

  The packages appear to be added. However, if you select one in the tree or map, you will get a connection error. You will also get an error if you try to open the properties for the package or its cluster.

- *What is the workaround?* In package names, do not use any of the special characters listed. If you have an existing package with these special characters, you will not be able to configure it through Serviceguard Manager unless you change its name.

JAGaf14600 Package and property sheets show non-configured cluster monitored subnets.

- *What is the problem?* This happens if a node in the cluster has a lan card that has more than one IP address, and the addresses are for different subnets. If the subnet of one of the IP addresses is specified as monitored, both subnets may show up in the list of monitored subnets. This is especially likely with IPv6 addresses
- *What is the workaround?* There is no workaround.

JAGaf16670 - Startup issues with Java Webstart

- *What is the problem?* There are two problems:
  - First: With non-Windows systems running Mozilla, you have to manually register Webstart as a helper application.
  - Second: When updating Serviceguard Manager on the client side, the SIM client Java Web Start uses the old jar files.
- *What is the workaround?* There are two workarounds:
  - First: With non-Windows systems running Mozilla, go to the browser menu and select Preferences -> Navigator -> Helper App. For the setting Field Value, put the following:

    extension jnlp

    mime type application/x-java-jnlp-file

    handled by application <patch-to-javaws>/javaws.exe
  - Second: When updating, you need to manually clear the Java Web Start cache on the SIM client side. It contains the jar files downloaded from the server. Before installing the new Serviceguard Manager, clear the cache and the server will automatically download the new jar files.

JAGaf12970 Service commands that contain quotes are not passed to control script.

- *What is the problem?* This happens when you are using Guided Mode and letting Serviceguard Manager create your control script automatically. If you enter a service command with quotes in it, such as `/usr/bin/X11/xclock -title "My Xclock"`, your quotes will be ignored when they are transferred.

  After the script is Applied, the target control script in `/etc/cmcluster/<pkgName>/<pkgName>.sdf.sh` contains something like this: SERVICE_CMD[0]="/usr/bin/X11/xclock -title My Xclock"

- *What is the workaround?* Do not use quotes in service commands if you are creating the control script through Guided Mode.

JAGef13948 Property sheets appear to hang when storage is bad.

- *What is the problem?* The timeout for checking storage status may not work. When you open Properties, Serviceguard issues an ioscan to find status of the disks. If you have a bad disk in your cluster, you may see “Please wait” on the network tab for a very long time, perhaps more than an hour. It appears that Serviceguard Manager has hung; actually, it is not timing out when the status request is not returned. This can also happen when you do a `Save As` command.

- *What is the workaround?* If you wait a long time after a `Save As` or on the Network Tab of properties, check the disks from the command line, using ioscan or through SAM. If they have zero length, your disk is bad.

JAGaf13925 SGMgr allows conflicting roles for clusters and packages (API JAGaf08686).

- *What is the problem?* Serviceguard Manager will allow you to configure conflicting or redundant roles. This is especially likely when using wild-cards. For example, you may be able to configure an Admin role for ANY_USER from node1 and then a Monitor role for user1 from node1. Since user1 is included in ANY_USER, this should not be allowed.

- *What is the workaround?* Check your roles to be sure none are redundant or conflicting.

JAGaf11256 Serviceguard Manager won't discover nodes if another cluster has the same name.

- *What is the problem?* Once Serviceguard Manager discovers a cluster, it will ignore any others that have the same name. For example, imagine that one subnet has a cluster named node1 and node2. Now imagine that another subnet has a cluster named clus1, whose members are nodeX and nodeY.

  The situation is not common because Serviceguard insists that the cluster name must be unique in its environment. However, the Session Server may be able to see clusters that cannot see each other. If it does, it will display the first clus1 that it encounters during discovery, and ignore the other.

- *What is the workaround?* There is no workaround.

JAGaf09768 More than one config screen can be opened for one cluster.

- *What is the problem?* Serviceguard Manager does not stop you from opening two configuration screens at the same time. If you enter changes in both screens, thinking there is only one, you may not Apply the configuration that you expected

- *What is the workaround?* There is no workaround.

JAGaf08484 Null Pointer exception search string "ss" in help window (Javahelp bug).

- *What is the problem?* If you enter a string of two or more s's (ss, sss, etc), in the Help Search window, you get an error. This is a known defect in Javahelp. It causes a NullPointerException.

- *What is the workaround?* There is no workaround.

JAGaf03220 User preferences saved in A.03.00 or A.03.01 are ignored by A.04.00.

- *What is the problem?* Because of extensive changes to Serviceguard Manager version A.04.00, preferences are not carried over from version A.03.00.

- *What is the workaround?* There is no workaround.

JAGae71073 Search Help Index with “enter” key does not work in Japanese or Korean.

- *What is the problem?* In Japanese and Korean versions, Serviceguard Manager will freeze if you type local characters into the Index tab of Help and then type `enter`.
- *What is the workaround?* Use the Search tab instead.

JAGae69202 - Rarely, cannot start program when running on SuSE via ReflectionX

- *What is the problem?* Occasionally, an exception happens when using ReflectionX to remotely start Serviceguard Manager on SuSE Linux. (SuSE Linux is supported for English only.)
- *What is the workaround?* This is related to a problem in the Java Runtime Environment. There is no workaround. Often it will work if you try again.

JAGae67613 Timing problem with Options -> Welcome Dialog.

- *What is the problem?* A timing problem cause unsynchronized behavior of the Options-> Dialog box settings. Here is one scenario:
  1. First, click on the button to un-set Options -> Welcome Dialog box.
  2. Exit Serviceguard Manager, then restart
  3. The Welcome Dialog does not show, which is correct behavior
  4. Click on Options->Welcome Dialog box to re-set it.
  5. Exit Serviceguard Manager again, then restart again
  6. This time the Welcome Dialog does not appear at startup, and the box is not clicked. After discovery is complete, however, the Welcome Dialog does appear, and the box is clicked.
- *What is the workaround?* There is no workaround.

JAGae50775 In Traditional Chinese locale, in HP-UX, need to use Java OOB tool prior to install

- *What is the problem?* Java performance is bad on HP-UX in the Traditional Chinese.

- *What is the workaround?* Before installing Serviceguard Manager on Traditional Chinese version of HP-UX, HP recommends running the Java Out-Of-The-Box tool to modify kernel parameters. Please refer to `http://www.hp.com/products1/unix/java/java2/outofbox/infolibrary/release_notes_java_oob.html`.

JAGae50774 In Traditional Chinese and Simplified Chinese, the license agreement radio button text is illegible.

- *What is the problem?* In the installer, the Licence Agreement window shows a radio button to check, confirming that the user agrees with the license terms. The text is too small to be easily read in Chinese.
- *What is the workaround?* Remember that the first button says “I accept the terms of the license agreement” and is checked by default. The other button says “I do NOT accept the terms of the license agreement.”

JAGae50773 In non-English locales, installer shows “OK” in first panel

- *What is the problem?* When installing Korean, Simplified Chinese, and Traditional Chinese, the first panel in the installer gives the customer the local choice in a pull-down menu. The button beside the choose reads “OK” in all languages. This button should be localized, but is not.
- *What is the workaround?* To proceed with install, press “OK.”

JAGae50727 In non-English locales, typed characters not visible in HP-UX

- *What is the problem?* When running non-English versions of SGMgr on HP-UX, typed non-English characters are invisible in the input text boxes. The characters can be read by the program, but not seen by the user. This occurs in the text fields of Alerts: Search and Help: search.
- *What is the workaround?* The computer is printing white characters on a white background, making them invisible. Set the system colors of the CDE Style Manager from the HP-UX toolbar. Choose a color set with a black foreground color, like Alpine or Wheat.

JAGae50110 Welcome Dialog and others: Mnemonic underline indicator can be incorrect in non-English interfaces

- *What is the problem?* In non-English interfaces, the keyboard mnemonics are indicated by underlining a letter in parentheses. This indicates that the item can be accessed by holding the alt key while pressing that letter. In some translations, the underline is misplaced.
- *What is the workaround?* Use the letter in parentheses for the alt-key short-cut, even if the underline has moved into a word.

JAGae45132 New session screen does not allow for blank password.

- *What is the problem?* If you try to connect with a user name, but leave the password field empty, the connect button stays greyed out.
- *What is the workaround?* There is no workaround. Do not use blank password.

JAGae40370 - Alerts dialog Apply button should accept the Enter key.

- *What is the problem?* You cannot use the Enter key to activate the Apply button in the Alerts dialog box.
- *What is the workaround?* Use the mouse to click the button, or tab to it to select it, then use the Return key to activate it.

JAGae40298 - Alerts and Tally for Status not always affected by filters

- *What is the problem?* The Alert icon on the toolbar and the Status title bar reflect the Show Clusters filter in the Alert page, but not the Search filter.
- *What is the workaround?* There is not workaround.

JAGad80600 - Certain progress messages are not localized.

- *What is the problem?* Serviceguard Manager displays progress messages directly from Serviceguard as administration commands are processed. Serviceguard does not localize these messages and

Serviceguard Manager can only translate the start and end messages for every admin operation. The intermediate messages are only in English.

- *What is the workaround?* There is no workaround.

Software Availability in Native Languages

Serviceguard Manager Version A.04.00 interface is available in five language options:

- ABA American English
- ABJ Japanese
- AB0 Simplified Chinese
- AB1 Korean
- AB2 Traditional Chinese

Please consult the Release Notes for the language you will install, to find information about language-specific patches, defects, and known problems.

The following Serviceguard Manager Release Notes are available from `http://docs.hp.com`.

- American English (B8325-90046)
- Japanese (B8325-90047)
- Korean (B8325-90048)
- Simplified Chinese (B8325-90049)
- Traditional Chinese (B8325-90050)