



**Hewlett Packard**  
Enterprise

# HPE Serviceguard for Linux Advanced edition 12.00.50 Release Notes

Part Number: 766796-007  
Published: June 2016

© Copyright 2016 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

#### **Acknowledgments**

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NIS™ is a trademark of Sun Microsystems, Inc.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE® is a registered trademark of SUSE AG, a Novell Business.

# Contents

1 Overview.....	5
2 Supported platforms and Linux distributions.....	5
3 Packaging information.....	5
4 Licensing information.....	6
4.1 Obtaining a permanent license.....	6
4.2 Renewing the permanent license.....	6
4.3 Validating the permanent license.....	7
5 Compatibility and installation requirements.....	8
5.1 Hardware requirements.....	8
5.2 Port requirements.....	8
5.2.1 Ports needed for Serviceguard.....	8
5.2.2 Ports needed for authentication.....	9
5.2.3 Ports needed by Serviceguard Manager.....	9
5.2.4 System firewalls.....	9
5.3 Supported browsers.....	10
5.4 Software prerequisites for Serviceguard for Linux.....	11
5.5 Installing Serviceguard for Linux.....	13
5.5.1 Installing Serviceguard for Linux using cmeasyinstall.....	13
5.5.2 Installing Serviceguard for Linux the traditional way.....	15
5.5.2.1 Changing the Jetty location of Serviceguard Manager.....	16
5.6 Installing Serviceguard for Linux Patch.....	17
5.7 Post installation.....	19
6 Rolling software upgrade.....	19
6.1 Requirements.....	19
6.2 Limitations of rolling upgrades.....	20
6.3 Preparation.....	21
6.4 Rolling upgrade on OS.....	22
6.5 Supported rolling upgrade paths.....	23
6.6 Performing rolling upgrades.....	23
6.6.1 Rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y .....	24
6.6.1.1 Upgrading Serviceguard for Linux using cmupgrade tool.....	24
6.6.1.2 Upgrading Serviceguard for Linux the traditional way.....	25
6.6.1.3 Upgrading Serviceguard for Linux using YUM or Zypper.....	26
6.6.2 Rolling upgrade from A.11.19.X to A.12.00.00.....	29
6.6.3 Performing offline rolling upgrade from A.11.18.X to A.12.00.00.....	30
6.6.4 Rolling upgrade from A.12.00.X to A.12.00.Y.....	31
6.6.4.1 Upgrading Serviceguard for Linux using cmupgrade tool.....	31
6.6.4.2 Upgrading Serviceguard for Linux the traditional way.....	33
6.6.4.3 Upgrading Serviceguard for Linux using YUM or Zypper.....	34
6.6.5 Rolling upgrade from A.11.19.X to A.12.00.X.....	37
6.6.6 Offline rolling upgrade from A.11.18.X to A.12.00.X.....	37
6.6.7 Upgrading Serviceguard Advanced edition to Enterprise edition for Linux using cmupgrade tool.....	37
7 Upgrading Serviceguard for Linux packages.....	39
8 Removing Serviceguard for Linux.....	39
9 Troubleshooting.....	39
10 Related information.....	43
11 Documentation feedback.....	44



# 1 Overview

This document provides information about HPE Serviceguard for Linux Advanced edition 12.00.50.

## 2 Supported platforms and Linux distributions

Serviceguard for Linux Advanced edition 12.00.50 is available on the following Linux distributions:

- Red Hat Enterprise Linux 5 or Advanced platform
- Red Hat Enterprise Linux 6 or Advanced platform
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise Server 11
- SUSE Linux Enterprise Server 12

---

**NOTE:** For more information about supported updates, supported hardware, storage, and other information, see the latest version of *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

---

## 3 Packaging information

Serviceguard for Linux 12.00.50 is available on all three editions, namely, Serviceguard for Linux Base, Serviceguard for Linux Advanced, and Serviceguard for Linux Enterprise.

**IMPORTANT:** Before you install 12.00.50 patch edition, ensure that one of the following Main Release (MR) editions is installed on your system:

- Serviceguard for Linux Advanced edition 12.00.00 or later (Red Hat Enterprise 5, 6, and SUSE Linux Enterprise Server 11)
- Or
- Serviceguard for Linux Advanced edition 12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12)

---

Serviceguard for Linux Advanced edition 12.00.50 June 2016 patch (SGLX\_00530) contains rpms for the following components:

- Serviceguard License
- Serviceguard for Linux
- Serviceguard for Linux snmp
- Serviceguard for Linux WBEM providers
- Serviceguard for Linux analytics
- Serviceguard Quorum Server
- Serviceguard Manager
- Serviceguard Toolkit for Enterprise DB PPAS for Linux
- Serviceguard Toolkit for Oracle Database for Linux
- Serviceguard Toolkit for SAP Sybase ASE and Sybase Replication Server for Linux
- Serviceguard Extension for SAP version

The following is added as new rpm with 12.00.50 version:

- Serviceguard Toolkit for KVM on Linux

## 4 Licensing information

Starting Serviceguard for Linux 12.00.00 requires licenses on per-socket basis. When you install Serviceguard for Linux Advanced, an instant-on license valid for 90 days is installed. With this instant-on license, you can use the product even if you do not have a permanent license. You must get a permanent license before the grace period expires.

When ordering the licenses, determine the number of active sockets on the server and order one license for each active socket irrespective of number of cores. A virtualized server may select less than the total amount of active sockets if Serviceguard is used within virtual machine which utilized less than the total number of sockets. For information about the license terms and supported server models, see the QuickSpecs available at <https://h41370.www4.hpe.com/quickspecs/overview.html>.

- 
- ❗ **IMPORTANT:** If you plan to upgrade to new OS version, you can use the same license that you are currently using. For example, if you are upgrading from Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, you can use the same license of Red Hat Enterprise Linux 5 on Red Hat Enterprise Linux 6.
- 

### 4.1 Obtaining a permanent license

Before your 90 days instant-on license expires, you must obtain and validate the permanent license to continue to use applicable Serviceguard versions beyond the grace period.

To obtain a permanent license:

1. Go to <https://myenterpriselicense.hpe.com>.
2. Log into HP Passport. If you do not have an account, you can create one.
3. Enter Entitlement Order Number and click **Go**.
  - Here are the licenses listed that have been activated and license that have not yet been activated.
4. Check the box that belongs to products you want to activate and click **Next**.
5. Select “if you are activating for yourself” or “if you are activating on behalf of another customer”. If “on behalf of another customer” is selected, you will enter the final user email address.
6. Activation Completes. Save the files. One includes the license key and the other includes additional product information.
7. You will receive a license certificate in your email box. You must retain the email message because this is the valid proof of purchase documentation you may need for future reference or support requests.

- 
- ❗ **IMPORTANT:** Ensure that you save the file and make a note of its path. (See the example in [Validating the permanent license](#).)
- 

### 4.2 Renewing the permanent license

After you have obtained the permanent license, follow these steps to renew the license:

**NOTE:** You must renew or apply the license on each node.

1. Ensure that `$SGCONF/AutoPass/LicFile.txt` exists.

---

**NOTE:** Hewlett Packard Enterprise recommends that you back up the `$SGCONF/AutoPass/LicFile.txt` before renewing the license.

---

2. Place the permanent license key in a file on the system.

**NOTE:** Ensure the file that contains the license key must not have the commented line.

---

3. Renew the license:

```
#cmsetlicense -i <absolute path of the license file>
```

On successful license renewal, it displays the following message:

```
License is successfully installed
```

For more information, see `cmsetlicense(1m)` manpage.

#### Example

To verify if the license is valid:

1. Copy the license file:

```
cp $SGCONF/AutoPass/LicFile.txt $SGCONF/AutoPass/LicFile.txt.sav
```

2. Run the `cmsetlicense` command:

```
cmsetlicense -i /test/mySGlicense
```

The `mySGlicense` file contains the license information.

3. Run the `cmgetlicense` command:

```
cmgetlicense -f line
```

4. If the license is valid, keep the new license file `$SGCONF/AutoPass/LicFile.txt` and delete the old license file `$SGCONF/AutoPass/LicFile.txt.sav`.

If the license is invalid, restore the original license:

```
mv $SGCONF/AutoPass/LicFile.txt.sav $SGCONF/AutoPass/LicFile.txt
```

---

**NOTE:** If you wish to upgrade from Advanced to Enterprise licence, repeat steps from 1 to 4.

---

## 4.3 Validating the permanent license



**IMPORTANT:** Ensure that you validate the permanent license before the 90-day grace period of instant-on license expires.

---

To validate the permanent license:

1. Run the following command:

```
#cmgetlicense -f line
```

2. On successful renewal, the command displays the following output:

```
#cmgetlicense -f line
```

```
node:node1|license_type=Advanced|license_type=Advanced
node:node1|license_type=Advanced|license_count=1
node:node1|license_type=Advnaced|license_valid_for_days=Indefinite
```

---

**NOTE:**

- If you install higher license than the one already installed on the system, the license on the node is upgraded automatically.

For example, if you have Serviceguard for Base and install Serviceguard for Advanced, the license on the node is upgraded to Advanced and the `cmgetlicense -f line` command displays the following output:

```
node:node1|license_type=Advanced|license_type=Advanced
node:node1|license_type=Advanced|license_count=1
node:node1|license_type=Advanced|license_valid_for_days=Indefinite
```

- If you have more than one type of license installed on the system, the `cmgetlicense -f line` command displays the information about highest level license. For example, if you have Serviceguard for Base and Serviceguard for Advanced installed on the system, the `cmgetlicense -f line` command displays the following output:

```
node:node1|license_type=Advanced|license_type=Advanced
node:node1|license_type=Advanced|license_count=1
node:node1|license_type=Advanced|license_valid_for_days=Indefinite
```

- If you have multiple licenses of the same type installed on the system, the `cmgetlicense -f line` command displays the following output:

```
node:node1|license_type=Advanced|license_type=Advanced
node:node1|license_type=Advanced|license_count=3
node:node1|license_type=Advanced|license_valid_for_days=Indefinite
```

---

## 5 Compatibility and installation requirements

### 5.1 Hardware requirements

For more information about hardware requirements, see the latest version of *HPE Serviceguard for Linux Certification Matrix* at <http://www.hpe.com/info/linux-serviceguard-docs>.

### 5.2 Port requirements

#### 5.2.1 Ports needed for Serviceguard

Before installing, ensure that no other program uses these ports.

**On Red Hat Enterprise Linux and SUSE Linux Enterprise Server:**

- icmp 8/icmp
- hacl-hb 5300/TCP High Availability (HA) Cluster heartbeat
- hacl-hb 5300/UDP High Availability (HA) Cluster heartbeat
- hacl-cfg 5302/TCP HA Cluster TCP configuration
- hacl-cfg 5302/UDP HA Cluster UDP configuration
- hacl-local 5304/TCP HA Cluster Commands

If you are using SNMP:

- snmp 161/UDP
- snmptrap 162/UDP

If you are using the WBEM provider:

- `wbem-http` TCP/5988
- `wbem-https` TCP/5989

If you are using the Quorum Server:

- `hacl-qs` 1238/TCP HA Quorum Server

If you are using the `appserver` utility:

- `hacl-poll` 5315/TCP

If you are using VMware VMFS volumes:

- `https` 443/TCP

## 5.2.2 Ports needed for authentication

The ports reserved for authentication are also used by Serviceguard:

- `auth` 113/TCP authentication
- `auth` 113/UDP authentication

## 5.2.3 Ports needed by Serviceguard Manager

- 5511 (`http`) and 5522 (`https`), 5301 (multicast port) are used by Serviceguard Manager.
- Serviceguard Manager needs a multicast IP address and a TCP/IP port for auto-discovery of the nodes in the subnet. Serviceguard uses default multicast IP 235.1.1.1 and 5301 port, which are configured in the setting page.

---

**NOTE:** Only IP address can be modified by the user. The default port 5301 cannot be modified.

---

## 5.2.4 System firewalls

System firewalls When using a system firewall with Serviceguard for Linux, you must leave open the ports listed above. For more information, see the latest version of Configuring firewall rules for HP Serviceguard on SUSE Linux Enterprise Server and Red Hat White Paper at <http://www.hpe.com/info/linux-serviceguard-docs> —> Whitepapers.

Serviceguard also uses some dynamic ports for some cluster services. These must be open in the firewall. They are typically in the range 32768-61000 for Red Hat. To determine the range on a given system, check the contents of the file `/proc/sys/net/ipv4/ip_local_port_range`.

If you have adjusted the dynamic port range using kernel tunable parameters, alter your firewall rules accordingly.

- To enable intra-cluster communications, each HEARTBEAT\_IP network on every node in the cluster must allow the following communications in both directions with all other nodes in the cluster:
  - TCP on port numbers 5300 and 5302 – and allow only packets with the SYN flag
  - UDP on port numbers 5300 and 5302
  - TCP and UDP on dynamic ports
- If you use a quorum server, all nodes in the cluster must allow the following communication to the quorum server IP address:

- TCP on port 1238 — and allow only packets with the SYN flag  
Any node providing quorum service for another cluster must allow the following communication from that cluster's nodes:
- TCP on port 1238 — and allow only packets with the SYN flag
- Running the `cmsscanc1` command requires the ssh port be open.  
There are additional firewall requirements to enable execution of Serviceguard commands from nodes outside the cluster, such as those listed in `cmclnodelist`. To allow execution of Serviceguard commands, follow these guidelines:  
All nodes in the cluster must allow the following communications:
- from the remote nodes:
  - TCP on ports 5302 — and allow only packets with the SYN flag
  - UDP on port 5302
- to the remote nodes:
  - TCP and UDP on dynamic ports
 The remote nodes must allow the following communications:
- from the cluster nodes
  - TCP and UDP on dynamic ports
- to the cluster nodes
  - TCP on ports 5302 — and allow only packets with the SYN flag
  - UDP on port 5302
 Authentication communication must allow the following ports:
- from the cluster nodes:
  - TCP and UDP on port 113
- to the cluster nodes:
  - TCP and UDP on port 113

---

**NOTE:** If you suspect that the firewall is blocking communications, you can add `-j LOG` before the last line in your iptables file (for example `/etc/sysconfig/iptables`) to log any blocked ports. Consult your Linux distribution's documentation on firewalls for information on iptables.

---

### 5.3 Supported browsers

Serviceguard Manager supports the following web browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

For latest information about web browser support, see the latest version of *HPE Serviceguard/SGeRAC/Storage Management Suite/Serviceguard Manager Plug-in Compatibility and Feature Matrix - HP-UX and Linux* available at [https://support.hpe.com/hpesc/public/docDisplay?docId=emr\\_na-a00018408ja\\_jp](https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00018408ja_jp).

---

**NOTE:** The recommended screen resolution for Serviceguard Manager is 1280 x 1024 or greater. However, Serviceguard Manager also supports a minimum screen resolution of 1024 x 768.

---

## 5.4 Software prerequisites for Serviceguard for Linux

Before installing Serviceguard for Linux, ensure that all the following software prerequisites are installed:

- Hewlett Packard Enterprise recommends that you must upgrade all components of the cluster to the latest firmware versions before you install Serviceguard.
- Serviceguard for Linux depends on the `xinetd` service. Ensure that the `xinetd` rpm is installed from the distribution source (for example, your Linux installation DVD) and is enabled.

To check if the `xinetd` service is running:

```
#ps -ef | grep xinetd
```

To enable the `xinetd` service:

```
#!/sbin/chkconfig --level 35 xinetd on
```

To enable the `xinetd` service on Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12:

```
systemctl enable xinetd.service
```

---

**NOTE:** On SUSE Linux Enterprise Server, `xinetd` service does not run if no services are configured. This can lead to patch installation failure. To address this, perform the following:

- You can configure `xinetd` with `-stayalive` option to ensure that it is running even when no services are configured.
- Alternatively, you can configure any other service before installing the patch to ensure that `xinetd` always restarts successfully.

For example, you can configure `echo` under `xinetd` using:

```
#!/sbin/chkconfig echo on
```

- 
- [Table 1](#) lists all the software that you need for each distribution before installing Serviceguard for Linux Advanced edition.

**Table 1 RPMs (prerequisites) for installing Serviceguard A.12.00.50 for Linux**

Red Hat Enterprise Linux	SUSE Linux Enterprise Server
lm_sensors	bash
tog-pegasus	pidentd
authd	libblkid1
krb5-libs	sblim-indication_helper
zlib	sblim-sfcb
e2fsprogs-libs (rhel 5)	sblim-sfcc
libblkid (rhel 6)	sblim-cmpi-base
net-snmp	net-snmp
sg3_utils	sg3_utils
sg3_utils-libs	xinetd
xinetd	libnl
libnl (rhel 5, rhel 6)	mdadm
libnl1 (rhel 7)	udev
mdadm	lsscsi
udev (rhel5, rhel 6)	net-tools
lsscsi	systemd (SLES 12)
net-tools	sqlite
systemd (rhel 7)	dmidecode (SLES 12)
polycoreutil (for KVM toolkit on rhel6 when SELinux is enforced)*	pmtools (SLES 11)
checkpolicy (for KVM toolkit on rhel6 when SELinux is enforced )*	open-vm-tools
sqlite	open-vm-tools (VMware only, SLES11 SP4, SLES12, and their respective later releases)**
dmidecode	
open-vm-tools (VMware only rhel7 and their respective later releases)**	

\* The `cmeasyinstall -a` will not automatically install these packages. You have to manually install these packages on an RHEL6 system, if the SELinux is enforced.

\*\*On SLES11 SP4, SLES12, RHEL7 and their respective later releases open-vm-tools are bundled along with distributions. For installation of VMware tools you may refer Installing and Configuring VMware Tools document at <https://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf>.

#### Other software prerequisites

You can download Jetty versions from Jetty web page at <http://www.eclipse.org/jetty>.

For latest information about Java and Jetty support on each Linux OS, see the latest version of *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

**NOTE:** Starting from Serviceguard Manager version A.12.00.30, IBM Java is supported.

You can install all these software prerequisites manually or automatically by using `cmeasyinstall -a` command except for Java and Jetty.

## 5.5 Installing Serviceguard for Linux

If you are installing Serviceguard for Linux for the first time, you can do in the following ways:

- “Installing Serviceguard for Linux using `cmeasyinstall`”
- “Installing Serviceguard for Linux the traditional way”

If Serviceguard version earlier than A.12.00.00 is installed, follow the instructions described in the [Performing rolling upgrades \(page 23\)](#) section to upgrade to latest version.

---

### NOTE:

- Hewlett Packard Enterprise recommends installing all the components that are part of the Serviceguard for Linux Advanced edition 12.00.00 (Red Hat Enterprise Linux 5, 6, and SUSE Linux Enterprise Server 11) or 12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12).
  - Starting Serviceguard 12.00.00 legacy packages are obsolete. If you have configured legacy packages, you must migrate to modular packages before you move to 12.00.00. For more information about how to migrate to modular packages, see the white paper *Migrating packages from legacy to modular style* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
  - When installing Serviceguard for Linux 12.00.00 on HPE BL920s Gen8 servers, you must use the `cmeasyinstall` tool shipped along with Serviceguard for Linux 12.00.10 patch. For information about the Serviceguard patches for each package, see [Table 3](#).
  - You must use the `cmeasyinstall` tool shipped along with Serviceguard for Linux 12.00.30 patch or later to install Serviceguard for Linux 12.00.30 on SUSE Linux Enterprise Server 11 SP4. For information about the Serviceguard patches for each package, see [Table 3](#).
- 

### 5.5.1 Installing Serviceguard for Linux using `cmeasyinstall`

The `cmeasyinstall` tool helps you to install Serviceguard for Linux and its components, such as Serviceguard Manager, Toolkits, Extended Distance Cluster, and Metrocluster except for SGeSAP. You can also execute the `cmeasyinstall` tool from one of the nodes in the specified list, and also the tool has capability to do a fresh installation on the remote nodes that are specified. It also provides an option to install the software prerequisites along with Serviceguard for Linux and its components.

#### Prerequisites

Before you begin to use `cmeasyinstall` tool, ensure that the following prerequisites are met:

- You must be a root user.
- You must have ‘execute’ permission on the node specified.
- All nodes must be reachable using FQDN (Fully Qualified Domain Name) or PQDN (Partially Qualified Domain Name).
- Ensure that all the nodes specified with `cmeasyinstall` are at same major version of the operating system.
- Ensure that PERL is installed on all the systems where you intend to install Serviceguard using the `cmeasyinstall` tool.
- Ensure that YUM (Yellowdog Updater Modified) update service on Red Hat Enterprise Linux Server or Zypper on SUSE Linux Enterprise Server is configured, if you intend to use the `-a` option.

---

**NOTE:** The `cmeasyinstall` tool does not install Serviceguard Extension for SAP (SGeSAP) B.06.00.60 (Red Hat Enterprise Linux 5, 6, and SUSE Linux Enterprise Server 11) or B.06.00.60 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) automatically from the ISO or DVD. You must install SGeSAP manually using `rpm -ivh` command. If you are already running SGeSAP A.06.00.20 (Red Hat Enterprise Linux 5, 6, and SUSE Linux Enterprise Server 11) or B.06.00.60 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12), then it is not required to install the product. For more information on SGeSAP installation, see *Serviceguard Extension for SAP B.06.00 Release Notes for Linux*.

Also, the `cmeasyinstall` tool does not install the Quorum Server.

---

The `cmeasyinstall` tool has the following advantages:

- Checks for dependencies and prompts you to install the required software or packages, if not already installed.
- Streamlines the installation of several rpm packages that are included on the DVD or ISO image.
- Reduces the installation from many commands to one command to invoke the tool.
- Takes the list of nodes that are expected to be a part of the cluster and installs the software on all the nodes.

The `cmeasyinstall` tool prompts for the directory path where the Serviceguard for Linux DVD or ISO image is mounted. It checks for Linux packages that are required as prerequisites for Serviceguard for Linux and its components. For more information about software prerequisites, see [“Software prerequisites for Serviceguard for Linux”](#). If not already installed, you will be prompted to install these packages for the installation to complete successfully.

To run the `cmeasyinstall` tool:

1. Mount Serviceguard for Linux DVD or ISO image.
2. Open a terminal window to the server from the console or an ssh client.
3. Execute the `cmeasyinstall` command with appropriate qualifiers. For more information about the command usage and qualifiers, see the Read Me available at `/<DVD_mount_dir>/README_cmeasyinstall.txt`.

The `cmeasyinstall` tool installs the RPMs in the following order:

- `serviceguard-license`
- `serviceguard`
- `serviceguard-snmp`
- `serviceguard-providers`
- `serviceguard-analytics`
- `serviceguard-manager`
- `serviceguard-sybase-toolkit`
- `serviceguard-oracle-toolkit`
- `serviceguard-ppas-toolkit`
- `serviceguard-kvm-toolkit`

In case of SUSE Linux Enterprise Server 11, while installing `serviceguard-snmp`, the following error message might be displayed, if the `xinetd` service is not started:

```
Starting cmsnmpdFailed due to no cmclconfderror:
%posttrans(serviceguard-snmp-A.12.00.00-0.sles11.x86_64) scriptlet
failed, exit status 1
```

After installation is complete, if you see the following error message:

```
nodel:~ # cmviewcl
unable to receive reply from local cmclconfd
Connection timed out Unable to initialize `HOSTNAME_ADDRESS_FAMILY`
```

Then, there is a problem with `xinetd` service. To enable `xinetd` service, see [“Software prerequisites for Serviceguard for Linux”](#)

On successful completion of the script, the following message is displayed:

```
Installation script execution completed successfully <date>
```

---

**NOTE:** You cannot use the `cmeasyinstall` tool to upgrade Serviceguard for Linux and its components. If you have already installed Serviceguard for Linux and its components, the `cmeasyinstall` tool exits with an appropriate error message.

---

## 5.5.2 Installing Serviceguard for Linux the traditional way

If you do not wish to install using the `cmeasyinstall` tool, you must install the Serviceguard for Linux and its components manually in the same order as described in [“Packaging information”](#) section and the location of rpms are described in the [“DVD directory structure”](#) section.

DVD directory structure

[Table 2](#) describes the operating system and the DVD directory structure for Serviceguard for Linux Advanced edition:

**Table 2 DVD directory structure for Serviceguard for Linux Advanced edition**

Operating system	DVD directory structure
Red Hat Enterprise Linux 5	<pre>&lt;DVD-mount-path&gt;/RedHat/RedHat5/Serviceguard/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat5/SGManager/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat5/SGeSAP/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat5/Toolkit/noarch/&lt;*.rpm&gt;</pre>
Red Hat Enterprise Linux 6	<pre>&lt;DVD-mount-path&gt;/RedHat/RedHat6/Serviceguard/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat6/SGManager/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat6/SGeSAP/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat6/Toolkit/noarch/&lt;*.rpm&gt;</pre>
Red Hat Enterprise Linux 7	<pre>&lt;DVD-mount-path&gt;/RedHat/RedHat7/Serviceguard/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat7/SGManager/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat7/SGeSAP/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/RedHat/RedHat7/Toolkit/noarch/&lt;*.rpm&gt;</pre>
SUSE Linux Enterprise Server 11	<pre>&lt;DVD-mount-path&gt;/SLES/SLES11/Serviceguard/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES11/SGManager/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES11/SGeSAP/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES11/Toolkit/noarch/&lt;*.rpm&gt;</pre>
SUSE Linux Enterprise Server 12	<pre>&lt;DVD-mount-path&gt;/SLES/SLES12/Serviceguard/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES12/SGManager/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES12/SGeSAP/x86_64/&lt;*.rpm&gt; &lt;DVD-mount-path&gt;/SLES/SLES12/Toolkit/noarch/&lt;*.rpm&gt;</pre>

To install Serviceguard for Linux and its components, use `rpm -ivh [<product>]` command. For example,

On Red Hat Enterprise Linux 5:

```
rpm -ivh serviceguard-A.12.00.00-0.rhel5.x86_64.rpm
```

On Red Hat Enterprise Linux 6:

```
rpm -ivh serviceguard-A.12.00.00-0.rhel6.x86_64.rpm
```

On Red Hat Enterprise Linux 7:

```
rpm -ivh serviceguard-A.12.00.30-0.rhel7.x86_64.rpm
```

On SUSE Linux Enterprise Server 11:

```
rpm -ivh serviceguard-A.12.00.00-0.sles11.x86_64.rpm
```

On SUSE Linux Enterprise Server 12:

```
rpm -ivh serviceguard-A.12.00.30-0.sles12.x86_64.rpm
```



---

**IMPORTANT:** After the Serviceguard Manager RPM installation is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management.

**Note:** Only `sgmgr` user can perform configuration tasks.

A replicated user is a user created on one or more systems with same `user name` and `password`. A replicated user on all systems or a user in the central directory services like LDAP is necessary to perform multi-cluster management.

If the LDAP central directory service is not configured and you want to perform multi-cluster management, you must create replicated users as necessary.

**Note:** If you already have `sgmgr` user created on the system or if the LDAP is configured, the following procedure to create a replicated user is optional.

To create a replicated user:

1. Export the `SGMGR_ENV` environment variable:

```
SGMGR_ENV=<replicated user password>
```

where, `<replicated user password>` is the password that you want to set for Serviceguard Manager (`sgmgr`) user.

---

**NOTE:** Installation of Serviceguard Manager for Linux B.12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) or Serviceguard Manager for Linux B.12.00.00 (Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and SUSE Linux Enterprise Server 11) automatically creates a user called `sgmgr` and password for this user is taken from the `SGMGR_ENV` environment variable.

---

2. Run the following command:

```
/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup -u  
-l <jetty location> -o config
```

```
/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup -u  
-l <jetty location> -o config -m 5301
```

---

### 5.5.2.1 Changing the Jetty location of Serviceguard Manager

To change the Jetty location of Serviceguard Manager:

1. Ensure that the Serviceguard Manager version A.12.00.10 or later is installed.

2. Run the following commands:

```
# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup
-l <existing-jetty-location> -o erase

# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup
-l <new-jetty-location> -o config
```

3. Verify the Jetty location:

```
#service jetty-sgmgr status
```

---

**NOTE:** Ensure that the value of `JETTY_HOME` is pointing to the new Jetty location.

---

## 5.6 Installing Serviceguard for Linux Patch

Starting Serviceguard for Linux 12.00.00, the patches are available on three different packages, namely, Serviceguard for Linux Base edition, Serviceguard for Linux Advanced edition, and Serviceguard for Linux Enterprise edition. For information about the components available in each package, see “[Packaging information](#)”.

[Table 3](#) provides details about the Serviceguard patches for each package. You can download the latest Serviceguard patches for Linux 12.00.X from Hewlett Packard Enterprise Support Center at <http://www.hpe.com/info/hpesc>.

**Table 3 Serviceguard patches for Linux**

Serviceguard Version	Packages	Patches <sup>1</sup>
12.00.50	Serviceguard for Linux Advanced edition	SGLX_00530.tar
12.00.40	Serviceguard for Linux Advanced edition	SGLX_00525.tar
12.00.30	Serviceguard for Linux Advanced edition	SGLX_00519.tar
12.00.20	Serviceguard for Linux Advanced edition	SGLX_00495.tar
12.00.10	Serviceguard for Linux Advanced edition	SGLX_00490.tar
12.00.01	Serviceguard for Linux Advanced edition	SGLX_00483.tar

<sup>1</sup> These patches may not include all the components as described in the “[Packaging information](#)” section.

---

**NOTE:** The A.12.00.50 release delivers a new KVM toolkit for linux product, which gets automatically installed with `cmupgrade`.

For latest information on supported OS for patches, see the latest version of *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

To install the patch:

1. Download the patch depending on the package from the Hewlett Packard Enterprise Support Center at <http://www.hpe.com/info/hpesc>.

① **IMPORTANT:** Before you install the patch, ensure that Serviceguard for Linux Advanced edition 12.00.00 (Red Hat Enterprise Linux 5, 6, and SU2SE Linux Enterprise Server 11) or 12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) is installed on your system.

2. Extract the patch files from the `<filename.tar>` file.
3. Verify the signature of the RPM. For more information about how to verify the signature of the RPM, see <http://www.hpe.com/info/swdepot/LinuxCodeSigning>.

4. Upgrade Serviceguard for Linux in one of the following way:
  - [Upgrading Serviceguard for Linux using cmupgrade tool](#)
  - [Upgrading Serviceguard for Linux the traditional way](#)
  - [Upgrading Serviceguard for Linux using YUM or Zypper](#)
5. Repeat steps from 2 to 4 on all the nodes in a cluster.

### Example

To install the patch using `cmupgrade` tool:

1. Download `SGLX_00530.tar` patch file for Serviceguard for Linux Advanced edition.
2. Extract the patch file:

```
#tar -xvf SGLX_00530.tar
```

The contents of the `.tar` file are:

```
cmeasyinstall
cmupgrade
install
SGLX_00530.text
public_key/HP-RPM-GPG-2048-KEY-1.pub

Common/SGManager/x86_64/\
serviceguard-manager-B.12.00.50-0.linux.noarch.rpm

<dist>/<distro_version>/repodata/filelists.xml.gz
<dist>/<distro_version>/repodata/primary.xml.gz
<dist>/<distro_version>/repodata/other.xml.gz
<dist>/<distro_version>/repodata/repomd.xml
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-analytics-A.12.00.50-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-A.12.00.50-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/SGManager/x86_64/\
serviceguard-manager-B.12.00.50-0.linux.noarch.rpm
<dist>/<distro_version>/QuorumServer/x86_64/\
serviceguard-qs-A.12.00.50-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-sybase-toolkit-A.12.00.40-00.redhat.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-oracle-toolkit-A.12.00.50-00.redhat.noarch.rpm
<dist>/<distro_version>/SGeSAP/x86_64/\
serviceguard-extension-for-sap-B.06.00.80-0.sles12.x86_64.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-kvm-toolkit-A.12.00.50-00.sles.noarch.rpm
```

where:

`<dist>` is the value that can be either RedHat or SLES based on the operating system.

`<distro_version>` is the value that can be either RedHat5, RedHat6, RedHat7, SLES11, or SLES12 based on the operating system.

`<os_version>` is the value that can be either rhel5, rhel6, rhel7, sles11, or sles12 based on the operating system.

3. Verify the signature of the RPMs. For more information about how to verify the signature of the RPM, see <http://www.hpe.com/info/swdepot/LinuxCodeSigning>.

---

**NOTE:** Each RPM contains corresponding signature file with an extension `.sig`.

---

4. Upgrade Serviceguard for Linux Advanced edition.

## 5.7 Post installation

After the installation is complete, you need to configure the cluster. For more information about how to configure the Serviceguard cluster, see chapter 5 of *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

## 6 Rolling software upgrade

You can upgrade the Linux operating system and the Serviceguard software on a node at a time without bringing down your clusters. This process can also be used any time when a node in the cluster must be taken offline for hardware maintenance or patch installations. **Until the process of upgrade is complete on all nodes, you cannot change the cluster configuration files, and you will not be able to use any of the features of the new Serviceguard release.**

---

**NOTE:** Starting Serviceguard 12.00.00 legacy packages are obsolete. If you have configured legacy packages, you need to migrate to modular packages before you move to 12.00.00. For more information about how to migrate to modular packages, see the white paper *Migrating packages from legacy to modular style* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

---

### 6.1 Requirements

#### △ CAUTION:

- Special considerations apply to a rolling or non-rolling upgrade to Serviceguard A.12.00.00 or later.
  - If you are using an alternate address, then you must upgrade the Quorum Server to version A.12.00.00 before you proceed. For more information, see *HPE Serviceguard Quorum Server Version A.12.00.00 Release Notes* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- 

To upgrade a Linux Serviceguard node to a newer Serviceguard release, you must ensure the following:

- The node must be running with a supported version of Linux (Red Hat Enterprise Linux 5.x, Red Hat Enterprise Linux 6.x, Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11, or SUSE Linux Enterprise Server 12).
  - The node must be running a supported release of Serviceguard.
- 

**NOTE:** If the target version of Serviceguard does not support the version of operating system on the node currently, then you must upgrade the operating system before upgrading Serviceguard.

---

- All members of the cluster must be upgraded to the same version of OS and the Serviceguard.
- Ensure that all applications that run on the current OS are also supported with the new OS.
- Verify that the new OS supports the current cluster hardware configuration and drivers (network interfaces, bonding driver, and shared disk storage).
- Do a full backup on each node.

---

**NOTE:** Hewlett Packard Enterprise recommends you to use the rolling upgrade process which:

- Helps you upgrade to the latest software version.
- Preserves the current OS and cluster configuration.
- Keeps running your mission-critical applications.

Before you upgrade, ensure that you read the “[Limitations of rolling upgrades](#)” and complete the entire upgrade process before you can use any Serviceguard commands.

---

**△ CAUTION:** If a failure occurs on one node while you are upgrading another, packages, and the applications they contain may not be able to fail over to the node being upgraded.

---

## 6.2 Limitations of rolling upgrades

- During rolling upgrade, you must issue Serviceguard commands (other than `cmrunnode` and `cmhaltnode`) on nodes that have been upgraded to latest revision of Serviceguard software. Issue of commands on yet to be upgraded nodes in the cluster will result in failure or inconsistent execution.
- You cannot modify the cluster or package configuration until the upgrade is complete. You *cannot* modify the hardware configuration including the cluster’s network configuration during rolling upgrade. This means that you must upgrade all nodes to the new release before you can modify the configuration file and copy it to all nodes.
- None of the features of the newer release of Serviceguard are allowed until all nodes have been upgraded.
- Binary configuration files may be incompatible between releases of Serviceguard. Do *not* manually copy configuration files between nodes. The Serviceguard binary configuration file (`cmclconfig`) must be in the correct directory or the cluster will not behave properly.
- Within a Serviceguard cluster, no more than two versions of Serviceguard can be running while the rolling upgrade is in progress.
- All nodes must be running the same releases of Linux and Serviceguard before the upgrade.
- Rolling upgrades are not intended as a means of using mixed releases of Serviceguard or Linux within the cluster. It is highly recommended that you upgrade all cluster nodes as quickly as possible to the new release level.
- You cannot delete Serviceguard software (via `rpm -e`) from a node while the cluster is in the process of rolling upgrade.
- This procedure depends on the upgrade or re-install keeping the same device naming convention and general system configuration. It is possible for devices to change names or be changed in the scan order in a way that cannot be corrected. If this happens, the cluster must be recreated rather than to be upgraded.
- SGMgr does not detect the rolling upgrade status of that cluster, hence you must use `sgmgr` after rolling upgrade is complete. `Sgmgr` assumes that the cluster is not under rolling upgrade.

## 6.3 Preparation

---

- ⓘ **IMPORTANT:** Ensure that there is a supported upgrade path from your current Linux and Serviceguard versions to the new versions. For more information, see the latest version of *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

There is no upgrade path between some Linux OS releases. In such cases, you must install a new OS (cold install).

---

- ⚠ **CAUTION:** No package can be in maintenance mode, whether it is running or not, when you perform an upgrade from Serviceguard A.11.19 to any later version, including an upgrade from the initial release of A.11.19 to the July 2009 or later patch.

This means:

- You must ensure that no packages are in maintenance mode when you start the upgrade.
- You must not put any package in maintenance mode until all the nodes are upgraded.

Breaking this rule will leave the cluster in an inconsistent state. To recover, you must halt the cluster and then upgrade all the nodes.

For more information, see “Maintaining a Package: Maintenance Mode” section in the *Managing HPE Serviceguard for Linux A.12.00.50* manual.

---

Before you start doing the following:

1. Record the hostname and its entire network interface IP addresses. Record each MAC address of each interface and its network assignment (for example, `eth1: HWaddr 00:0B:CD:69:F4:68`)
  2. Record all network information, such as network mask, gateway address, DNS server address, its broadcast address, and so on. This information can be useful, if you are installing a new OS.
- 

**NOTE:** Ensure that all your network and storage interfaces are supported by the new OS.

---

3. Record the storage configuration, such as all LVM information, and if possible, collect a list of hardware disks configured, for example, `sfdisk -l`.

On SUSE Linux Enterprise Server, you may need to run YAST or YAST2.

4. Back up the following files on media that can be easily recovered by the node after its upgrade or a new OS installation:
  - Host files: `/root/.rhosts`, `/etc/hosts`, `/etc/profile`, and the network information (including the bonding configurations):
    - Red Hat Enterprise Linux: `/etc/sysconfig/network-scripts/ifcfg*`
    - SUSE Linux Enterprise Server: `/etc/sysconfig/network/ifcfg*`
5. Ensure you have the latest versions of the software listed in the “[Software prerequisites for Serviceguard for Linux](#)” section.
- SG files: `$SGCONF/*`: all current package control and configuration files, including their log files.

## 6.4 Rolling upgrade on OS

1. Halt the node you want to upgrade (`cmhaltnode -f`). This will cause the node's packages to start up on an adoptive node.
2. Install the new Serviceguard from the DVD in the same order as described in the “[Packaging information](#)”.
3. Upgrade the node to latest patch.

---

**NOTE:** Before you upgrade from SUSE Linux Enterprise Server 11 SP3 to SP4, ensure that you have installed Serviceguard for Linux 12.00.30.

---

4. After completing the OS upgrade for the node, restore all its previously saved Host files: `/root/.rhosts`, `/etc/hosts`, `/etc/profile`, `/etc/profile`, `/etc/sysconfig/network/ifcfg*`(or `/etc/sysconfig/network-scripts/ifcfg*`) and bonding files.

Verify that the network configurations are the same prior to the upgrade or the new installation. Check the current interface `eth0` has the same corresponding Mac address before and after.

5. Verify that all disks and their file systems are the same prior to this OS upgrade or new installation.

Check and compare with the disk layout collected before the upgrade. Use command `vgscan` to ensure the node with new OS sees all its previously configured LVM disks.

6. Follow the instructions in the `README` file in the directory of each driver. If you have installed a new OS version, you must run a convert program. This will convert the binary file (`cmclconfig`) to its new release format. To run the program on the upgraded node, enter: `$SGGSBIN/convert`

- a. Reboot the node.
- b. After the node is rebooted, verify the cluster status using `cmviewcl`, and also verify all file systems with `fsck`.
- c. Restart Serviceguard on this node using `cmrunnode`. Check that the node joins the cluster successfully, and if necessary, move the packages back onto the node.
- d. Edit the following file to include the line: `AUTOSTART_CMCLD = 1`

For Red Hat Enterprise Linux: `/usr/local/cmcluster/conf/cmcluster.rc`

For SUSE Linux Enterprise Server: `/opt/cmcluster/conf/cmcluster.rc`

- e. Check if `sgmgr` service is running on the node:

```
# service jetty-sgmgr status
```

- f. Repeat this process for each node in the cluster.

---

**NOTE:** Be sure to plan sufficient system capacity to allow moving the packages from node to node during the process without an unacceptable loss of performance. If the cluster fails before the rolling upgrade is complete (because of a catastrophic power failure, for example), you can restart it by entering the `cmruncl` command from a node which has been upgraded to the latest revision of the software.

---

**NOTE:**

- Serviceguard does not support major OS upgrades, for example, Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7 or SUSE Linux Enterprise Server 11 to SUSE Linux Enterprise Server 12. On Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12, you must do a fresh installation of Serviceguard.
  - If you plan to upgrade to new OS version, you can use the same license that you are currently using. For example, if you are upgrading from Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, you can use the same license of Red Hat Enterprise Linux 5 on Red Hat Enterprise Linux 6.
  - Warning messages might appear during rolling upgrade while a node is determining the software version that is running. This is a normal occurrence and not a cause for concern.
  - If you change kernel parameters as a part of doing a rolling upgrade, ensure to make the same changes on all nodes that can run the same packages.
- 

## 6.5 Supported rolling upgrade paths

Table 4 describes the supported upgrade paths for Serviceguard for Linux:

**Table 4 Upgrade paths**

Serviceguard version	Rolling upgrade using <code>cmupgrade</code> tool	Rolling upgrade the traditional way	Offline upgrade
To upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y, see <a href="#">Rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y</a> .	Yes	Yes	Yes
To upgrade from A.11.19.X to A.12.00.00, see <a href="#">Rolling upgrade from A.11.19.X to A.12.00.00</a> .	No	Yes	Yes
To upgrade from A.11.18.X to A.12.00.00, see <a href="#">Performing offline rolling upgrade from A.11.18.X to A.12.00.00</a> .	No	No	Yes
To upgrade from A.12.00.X to A.12.00.Y, see <a href="#">Rolling upgrade from A.12.00.X to A.12.00.Y</a> .	Yes	Yes	Yes

## 6.6 Performing rolling upgrades

You can perform online or offline rolling upgrade of Serviceguard for Linux across major versions starting A.11.20.X and later in the following ways:

- “Rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y ”
- “Rolling upgrade from A.11.19.X to A.12.00.00”
- “Performing offline rolling upgrade from A.11.18.X to A.12.00.00”
- “Rolling upgrade from A.12.00.X to A.12.00.Y”

- “Rolling upgrade from A.11.19.X to A.12.00.X”
- “Offline rolling upgrade from A.11.18.X to A.12.00.X”

You can also upgrade from Serviceguard for Linux Advanced edition to Serviceguard for Linux Enterprise edition, in which case the additional components are installed. For more information on how to upgrade, see “[Upgrading Serviceguard for Linux packages](#)”.

## 6.6.1 Rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y

You can perform rolling upgrade of Serviceguard for Linux either from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y in the following ways:

- “[Upgrading Serviceguard for Linux using cmupgrade tool](#)”
- “[Upgrading Serviceguard for Linux the traditional way](#)”
- “[Upgrading Serviceguard for Linux using YUM or Zypper](#)”

### 6.6.1.1 Upgrading Serviceguard for Linux using cmupgrade tool

The `cmupgrade` is the new tool introduced in Serviceguard for Linux A.12.00.00 which helps you in upgrading Serviceguard and its components, such as, Serviceguard Manager, Toolkits, Extended Distance Cluster, and Metrocluster except for SGeSAP.

The `cmupgrade` tool can be used to perform the previously mentioned upgrades on all Linux distros supported by Serviceguard. For information about supported versions, see *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

#### Prerequisites

Before you begin to use the `cmupgrade` tool, ensure that the following prerequisites are met:

- You must be a root user to run the `cmupgrade` tool.
- You must have execute permission to run the `cmupgrade` tool.
- Ensure that PERL is installed on the system to run the `cmupgrade` tool.
- Ensure that you run the `cmupgrade` tool on all the nodes that are part of the cluster.
- Ensure that the Jetty server and Java are installed on the nodes before you run the `cmupgrade` tool. Also, ensure that `java -version` command displays the version greater than or equal to 1.7.0 in the output.

To perform the rolling upgrade from A.11.20.X to A.12.00.00 or A.11.20.X to A.12.00.Y using `cmupgrade` tool:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

3. You can upgrade node as follows:

- a. Export the `SGMGR_ENV` environment variable:

```
SGMGR_ENV=<replicated user password>
```

where, `<replicated user password>` is the password that you want to set for Serviceguard Manager user.

For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

---

**NOTE:** Installation of Serviceguard Manager for Linux B.12.00.30 (Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 12) or A.12.00.00 (Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, or SUSE Linux Enterprise Server 12) automatically creates a user called `sgmgr` and password for this user is taken from the `SGMGR_ENV` environment variable.

---

- b. Upgrade node 1:

```
#cmupgrade [-a <automatic-installation-of-pre-requisites>] {-d  
<mount-path-where-DVD-is-mounted>} {-j <jetty location>}
```

For more information, see `cmupgrade (1m)` manpage.

---

**NOTE:** The `cmupgrade` tool does not install or upgrade Serviceguard Extension for SAP (SGeSAP) to version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12) automatically. You must upgrade SGeSAP manually using `rpm -Uvh` command. If you are already running SGeSAP version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12), then it is not required to upgrade or reinstall the product. It is recommended to upgrade SGeSAP to the latest patch, for more information on installing or upgrading SGeSAP, see *Serviceguard Extension for SAP B.06.00 for Linux Release Notes*.

Also, the `cmupgrade` tool does not install or upgrade Quorum Server.

---

- c. If you plan to upgrade node 1 to A.12.00.Y, then follow the steps listed below. If not, you can skip this step and proceed to step 4.

- i. Upgrade node 1 to A.12.00.Y:

```
# cmupgrade {-d extracted_patch_location} {-j jetty-location}
```

**NOTE:** The `cmupgrade` tool does not install or upgrade Serviceguard Extension for SAP (SGeSAP) to version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12) automatically. You must upgrade SGeSAP manually using `rpm -Uvh` command. If you are already running SGeSAP version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12), then it is not required to upgrade or reinstall the product. It is recommended to install or upgrade SGeSAP to latest patch, for more information on installing SGeSAP, see *Serviceguard Extension for SAP B.06.00 for Linux Release Notes*.

Also, the `cmupgrade` tool does not install or upgrade Quorum Server.

---

4. Restart cluster on first node.

For example, `#cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

5. Repeat steps from 2 to 4 for all the nodes.

6. If you plan to configure Serviceguard analytics for Linux, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

#### 6.6.1.2 Upgrading Serviceguard for Linux the traditional way

To perform the rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y the traditional way:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

3. You can upgrade node 1 in the same order as described in the “Packaging information”.

For example, Serviceguard rpm for Red Hat 5 x86\_64

```
#rpm -Uvh serviceguard-A.12.00.00-0.rhel5.x86_64.rpm
```

---

**NOTE:** When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:

- *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes Version A.12.00.00*

4. If you plan to upgrade node 1 to A.12.00.Y, then follow the steps outlined below. If not, you can skip this step and proceed to step 5.

- a. Upgrade node 1 in the same order as described in the “Packaging information”.

For example, Serviceguard rpm for Red Hat 5 x86\_64

```
#rpm -Uvh serviceguard-A.12.00.Y-0.rhel5.x86_64.rpm
```

---

**NOTE:** To upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:

- *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes Version A.12.00.00*

- 
- ① **IMPORTANT:** After the Serviceguard Manager RPM installation is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see “Installing Serviceguard for Linux the traditional way”.

5. Restart the cluster on first node.

For example, `#cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

6. Repeat steps from 2 to 5 for all the nodes.

7. If you plan to configure Serviceguard analytics for Linux, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

### 6.6.1.3 Upgrading Serviceguard for Linux using YUM or Zypper

If you have configured YUM update service on Red Hat Enterprise Linux Server or Zypper on SUSE Linux Enterprise Server, you can upgrade Serviceguard for Linux Advanced edition using YUM or Zypper. You must upgrade in the same order as described in the “Packaging information” section.

## On Red Hat Enterprise Linux

To perform the rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y using YUM:

1. Enable global switching for packages running on node 1.  
The `cmmodpkg` command enables switching of the package.  
For example, `#cmmodpkg -e pkg1`
2. Halt first node.  
Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.  
For example, `#cmhaltnode -f node1`
3. Create a `/etc/yum.repos.d/sglxrel.repo` YUM repository configuration file with the following contents:

```
[sglxrelrepo]
name=sglxrelrpms
baseurl=file://<dir_location>/RedHat/<distro_major_ver>
enabled=1
```

where:

`<dir_location>` is the mount path where ISO image or DVD is mounted for the main release.

`<distro_major_ver>` is the value that can be either Red Hat 5 or Red Hat 6.

4. Run the following command:  
`#yum clean all`
5. If you plan to upgrade to A.12.00.Y, then follow the steps listed below. If not, you can skip this step and proceed to step 6.

- a. Create a `/etc/yum.repos.d/sglxpatch.repo` YUM repository configuration file with the following contents:

```
[sglxpatchrepo]
name=sglxpatchrpms
baseurl=file://<dir_location>/RedHat/<distro_patch_ver>
enabled=1
```

where:

`<dir_location>` is the extracted patch location for a patch.

`<distro_major_ver>` is the value that can be either Red Hat 5 or Red Hat 6.

- b. Run the following command:  
`#yum clean all`
- c. If you are upgrading Serviceguard Manager RPM, do the following:  
`#!/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-1  
<jetty location> -o erase`
- d. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using YUM:  
`#yum upgrade serviceguard-manager`

- 
- ① **IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see [“Installing Serviceguard for Linux the traditional way”](#).
- 
6. Restart the cluster on first node.  
For example, `#cmrunnode -n node1`  
Check that the node joins the cluster successfully, and if necessary, move packages back to the node.
    - a. If you are upgrading Serviceguard Manager RPM, do the following:  
`#/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l <jetty location> -o erase`
    - b. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using YUM:  
`#yum upgrade serviceguard-manager`
    - c. Starting Serviceguard Manager for Linux A.12.00.Y perform the following step:  
`# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup -l <jetty location> -o config`
  7. Repeat steps from 2 to 8 for all the nodes.
  8. If you plan to configure Serviceguard analytics for Linux, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

### On SUSE Linux Enterprise Server

To perform the rolling upgrade from A.11.20.X to A.12.00.00 or from A.11.20.X to A.12.00.Y using Zypper:

1. Enable global switching for packages running on node 1.  
The `cmmodpkg` command enables switching of the package.  
For example, `#cmmodpkg -e pkg1`
2. Halt first node.  
Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.  
For example, `#cmhaltnode -f node1`
3. Create a `/etc/zypp/repos.d/sglxrel.repo` Zypper repository configuration file with the following contents:  

```
[sglxrelrepo]
name=sglxrelrpms
baseurl=file://<dir_location>/SLES/SLES11/
enabled=1
```

where:  
<dir\_location> is the mount path where ISO image or DVD is mounted for the main release.
4. Run the following command:  
`#!/usr/bin/zypper clean`

5. If you are upgrading Serviceguard Manager RPM, do the following:
 

```
#/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l
<jetty location> -o erase
```
6. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using Zypper:
 

```
#zypper -n upgrade serviceguard-manager
```
7. If you plan to upgrade to A.12.00.Y, then follow the steps listed below. If not, you can skip this step and proceed to step 8.
  - a. Create a `/etc/zypp/repos.d/sglxpatch.repo` Zypper repository configuration file with the following contents:
 

```
[sglxpatchrepo]
name=sglxpatchrpms
baseurl=file://<dir_location>/SLES/SLES11/
enabled=1
```

 where:
   
`<dir_location>` is the extracted patch location for a patch.
  - b. Run the following command:
 

```
#!/usr/bin/zypper clean
```
  - c. If you are upgrading Serviceguard Manager RPM, do the following:
 

```
#/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l
<jetty location> -o erase
```
  - d. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using Zypper:
 

```
#zypper -n upgrade serviceguard-manager
```

---

① **IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see [“Installing Serviceguard for Linux the traditional way”](#).

---

8. Restart cluster on first node.
 

```
For example, #cmrunnode -n node1
```

 Check that the node joins the cluster successfully, and if necessary, move packages back to the node.
9. Repeat steps from 2 to 8 for all the nodes.
10. If you plan to configure Serviceguard analytics for Linux, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

### 6.6.2 Rolling upgrade from A.11.19.X to A.12.00.00

To perform the rolling upgrade from A.11.19.X to A.12.00.00:

1. Enable global switching for packages running on node 1.
 

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

3. Uninstall `sg_pidentd` rpm.

---

**⚠ CAUTION:** Serviceguard commands will not work unless step 5 is complete. You cannot change the cluster configuration files until the process of upgrade is complete on all nodes.

---

For example, `#rpm -e --nodeps sg_pidentd-3.0.19-2`

**Note:** This step is applicable only on Red Hat Enterprise Linux.

4. Install `authd` rpm from the Linux Distribution DVD or Repository.

For example, `#rpm -i <authd rpm>`

**Note:** This step is applicable only on Red Hat Enterprise Linux.

5. Upgrade `serviceguard-license` before you upgrade to Serviceguard. For example,

`#rpm -Uvh serviceguard-license-A.12.00.00-0.rhel5.x86_64.rpm`

6. Upgrade node 1 in the same order as described in the “[Packaging information](#)”.

For example, Serviceguard rpm for Red Hat 5 x86\_64

`#rpm -Uvh serviceguard-A.12.00.00-0.rhel5.x86_64.rpm`

---

**NOTE:** When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:

- *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes Version A.12.00.00*
- 

**① IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

---

7. Restart cluster on first node.

For example, `# cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

8. Repeat steps from 2 to 7 for all the nodes.

### 6.6.3 Performing offline rolling upgrade from A.11.18.X to A.12.00.00

To perform offline rolling upgrade from A.11.18.X to A.12.00.00:

1. Halt the cluster.

For example, `#cmhaltcl -f`

2. Select a node you want to upgrade and uninstall `pidentd` rpm.

`#rpm -e --nodeps pidentd-3.0.19-0`

**Note:** This step is applicable only on Red Hat Enterprise Linux.

3. Install `authd rpm` from distro.

```
#rpm -i <authd rpm>
```

**Note:** This step is applicable only on Red Hat Enterprise Linux.

4. Install `serviceguard-license` before you upgrade to Serviceguard. For example,  
`rpm -ivh serviceguard-license-A.12.00.00-0.rhel5.x86_64.rpm`
5. Upgrade node 1 in the same order as described in the “[Packaging information](#)”.

For example, Serviceguard rpm for Red Hat 5 x86\_64

```
#rpm -Uvh serviceguard-A.12.00.00-0.rhel5.x86_64.rpm
```

---

**NOTE:**

- When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:
  - *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes Version A.12.00.00*
  - *HPE Serviceguard Toolkit for SAP Sybase ASE and SAP Sybase Replication Server for Linux Release Notes Version A.12.00.00*
  - *HPE Serviceguard Toolkit for Oracle on Linux Release Notes Version A.12.00.00*
- You can use YUM or Zypper to perform rolling upgrade from A.11.19.X to A.12.00.00. For more information about how to upgrade using YUM or Zypper, see “[Upgrading Serviceguard for Linux using YUM or Zypper](#)”.

---

①

**IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

6. Repeat steps from 2 to 5 on each node of the cluster.
7. After all nodes are upgraded, restart the cluster.

```
#cmruncl
```

### 6.6.4 Rolling upgrade from A.12.00.X to A.12.00.Y

You can perform rolling upgrade of Serviceguard for Linux from A.12.00.X to A.12.00.Y in the following ways, for example, X is A.12.00.00 and Y is A.12.00.10 and Y is always greater than X:

- “[Upgrading Serviceguard for Linux using cmupgrade tool](#)”
- “[Upgrading Serviceguard for Linux the traditional way](#)”
- “[Upgrading Serviceguard for Linux using YUM or Zypper](#)”

---

①

**IMPORTANT:** Before you upgrade to the patch, ensure that Serviceguard for Linux Advanced edition 12.00.00 (Red Hat Enterprise Linux 5, 6, and SUSE Linux Enterprise Server 11) or 12.00.30 ((Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) is installed on your system.

#### 6.6.4.1 Upgrading Serviceguard for Linux using `cmupgrade` tool

To perform the rolling upgrade from A.12.00.X to A.12.00.Y using `cmupgrade` tool:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

- a. If you have configured cluster analytics, stop cluster analytics daemon. For example,  
`#cmcaadmin stop`

3. You can upgrade the node as follows:

- a. If you have configured Serviceguard Manager and you are required to change the `sgmgr` user password then export the `SGMGR_ENV`.

```
SGMGR_ENV=<replicated user password>
```

where, `<replicated user password>` is the password that you want to set for Serviceguard Manager user.

For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

---

**NOTE:** Installation of Serviceguard Manager for Linux B.12.00.00 (Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and SUSE Linux Enterprise Server 11) or Serviceguard Manager for Linux B.12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) automatically creates a user called `sgmgr` and password for this user is taken from the `SGMGR_ENV` environment variable.

---

- b. Upgrade node 1 to A.12.00.Y:

```
# cmupgrade {-d extracted_patch_location} {-j jetty-location}
```

---

**NOTE:** Starting from Serviceguard Manager version B.12.00.20, you can specify the new or existing Jetty location while upgrading Serviceguard Manager using `cmupgrade` tool. Prior to Serviceguard Manager version B.12.00.20, you must specify the same Jetty location.

---

- c. Starting Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends you to use NFS shared storage to create cluster analytics database. For information about how to configure NFS as shared storage, see *Managing HPE Serviceguard A.12.00.50 for Linux* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- d. If you have already configured cluster analytics and plan to use the existing analytics database, see section “Cluster Analytics Database Migration to Shared Storage” in the *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

---

**NOTE:** The `cmupgrade` tool does not install or upgrade Serviceguard Extension for SAP (SGeSAP) to version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12) automatically. You must upgrade SGeSAP manually using `rpm -Uvh` command. If you are already running SGeSAP version B.06.00.70 (Red Hat Enterprise Linux 5, 6, 7, and SUSE Linux Enterprise Server 11, 12), then it is not required to upgrade or reinstall the product. It is recommended to upgrade SGeSAP to the latest patch, for more information on installing or upgrading SGeSAP, see *Serviceguard Extension for SAP B.06.00 for Linux Release Notes*.

Also, the `cmupgrade` tool does not install or upgrade Quorum Server.

---

4. Rejoin the node to the cluster, which was halted in setp 2.

For example, `# cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

5. Repeat steps from 2 to 4 for all the nodes.
6. Once all the nodes are upgraded to A.12.00.Y and if you have already configured cluster analytics, then start analytics daemon.

For example, `#cmcaadmin start`

#### 6.6.4.2 Upgrading Serviceguard for Linux the traditional way

To perform the rolling upgrade from A.12.00.X to A.12.00.Y the traditional way:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

- a. If you have configured cluster analytics, stop cluster analytics daemon. For example, `#cmcaadmin stop`
- b. If you have configured serviceguard-manager, do the following:

```
# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup  
-l <jetty location> -o erase
```

3. You can upgrade node 1 in the same order as described in the [“Packaging information”](#).

For example, Serviceguard rpm for Red Hat 5 x86\_64:

```
#rpm -Uvh serviceguard-A.12.00.Y-0.rhel5.x86_64.rpm
```

---

**NOTE:** When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:

- *HPE Serviceguard Toolkit for Enterprise DB PPMAS for Linux Release Notes Version A.12.00.00*

---

① **IMPORTANT:** After the Serviceguard Manager RPM installation is complete, you must follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

- a. Starting Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends you to use NFS shared storage to create cluster analytics database. For information about how to configure NFS as shared storage, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- b. If you have already configured cluster analytics and plan to use the existing analytics database, see section “Cluster Analytics Database Migration to Shared Storage” in the *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

4. Starting Serviceguard Manager for Linux A.12.00.Y do the following:

```
# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup  
-l <jetty location> -o config
```

5. Rejoin the node to the cluster, which was halted in step 2.

For example, `#cmrunnode -n node1`.

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

6. Repeat steps from 2 to 4 for all the nodes.

7. Once all the nodes are upgraded to A.12.00.Y and if you have already configured cluster analytics, then start analytics daemon.

For example, `#cmcaadmin start`.

#### 6.6.4.3 Upgrading Serviceguard for Linux using YUM or Zypper

If you have configured YUM update service on Red Hat Enterprise Linux Server or Zypper on SUSE Linux Enterprise Server, you can upgrade Serviceguard for Linux Advanced edition using YUM or Zypper. You must upgrade in the same order as described in the “[Packaging information](#)” section.

---

**NOTE:** Ensure that major version of Serviceguard is installed before you upgrade to patch.

#### On Red Hat Enterprise Linux

To perform the rolling upgrade from A.12.00.X to A.12.00.Y using YUM:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

- a. If you have configured cluster analytics, stop cluster analytics daemon. For example,  
`#cmcaadmin stop`
- b. If you are upgrading Serviceguard Manager RPM, do the following:  
`#/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l  
<jetty location> -o erase`

3. Create a `/etc/yum.repos.d/sglxpatch.repo` YUM repository configuration file with the following contents:

```
[sglxpatchrepo]
name=sglxpatchrpms
baseurl=file://<dir_location>/RedHat/<distro_patch_ver>
enabled=1
gpgcheck=0
```

where:

`<dir_location>` is the extracted patch location for a patch.

`<distro_major_ver>` is the value that can be either Red Hat 5 or Red Hat 6.

4. Run the following command:

```
#yum clean all
```

5. If you have already configured cluster analytics and plan to use the existing analytics database, see section “Cluster Analytics Database Migration to Shared Storage” in the *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
6. You can upgrade node 1 in the same order as described in the "Packaging information". For example, to upgrade Serviceguard Manager RPM using YUM:

```
#yum upgrade serviceguard
```

- If you are upgrading Serviceguard Manager RPM, do the following:  
`#/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l  
<jetty location> -o erase`
- Starting Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends you to use NFS shared storage to create cluster analytics database. For information about how to configure NFS as shared storage, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- Starting Serviceguard Manager for Linux A.12.00.Y perform the following step:  
`# /opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup  
-l <jetty location> -o config`

---

① **IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you need to follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see “[Installing Serviceguard for Linux the traditional way](#)”.

---

7. Rejoin the node to the cluster, which was halted in setp 2

For example, `#cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

8. Repeat steps from 2 to 9 for all the nodes.
9. Once all the nodes are upgraded to A.12.00.Y and if you have already configured cluster analytics, then start analytics daemon.

For example, `#cmcaadmin start`

### On SUSE Linux Enterprise Server

To perform the rolling upgrade from A.12.00.X to A.12.00.Y using Zypper:

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

- a. If you have configured cluster analytics, stop cluster analytics daemon. For example, `#cmcaadmin stop`

3. Create a `/etc/zypp/repos.d/sglxpatch.repo` Zypper repository configuration file with the following contents:

```
[sglxpatchrepo]
name=sglxpatchrpms
baseurl=file://<dir_location>/SLES/SLES11/
enabled=1
```

where:

`<dir_location>` is the extracted patch location for a patch.

4. Run the following command:

```
#!/usr/bin/zypper clean
```

5. If you are upgrading Serviceguard Manager RPM, do the following:

```
#!/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup/-l
<jetty location> -o erase
```

6. Starting Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends you to use NFS shared storage to create cluster analytics database. For information about how to configure NFS as shared storage, see *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
7. If you have already configured cluster analytics and plan to use the existing analytics database, see section "Cluster Analytics Database Migration to Shared Storage" in the *Managing HPE Serviceguard for Linux A.12.00.50* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
8. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using Zypper:  

```
#zypper -n upgrade serviceguard-manager
```

- 
- ① **IMPORTANT:** After the Serviceguard Manager RPM upgrade is complete, you need to follow the procedure described later in this section to start `sgmgr` service and also create a user which can be used as a replicated user for multi-cluster management. For more information about how to create a replicated user, see [“Installing Serviceguard for Linux the traditional way”](#).
- 

9. Restart cluster on first node.

For example, `#cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

10. Repeat steps from 2 to 9 for all the nodes.

### 6.6.5 Rolling upgrade from A.11.19.X to A.12.00.X

To perform the rolling upgrade from A.11.19.X to A.12.00.X:

1. First upgrade node 1 to A.12.00.00. For more information on how to upgrade to A.12.00.00, see [“Rolling upgrade from A.11.19.X to A.12.00.00”](#) (page 29).
2. Then, upgrade node 1 to A.12.00.Y. For more information on how to upgrade to A.12.00.Y, see [“Rolling upgrade from A.12.00.X to A.12.00.Y”](#) (page 31).

### 6.6.6 Offline rolling upgrade from A.11.18.X to A.12.00.X

To perform offline rolling upgrade from A.11.18.X to A.12.00.X:

1. First upgrade node 1 to A.12.00.00. For more information on how to upgrade to A.12.00.00, see [“Performing offline rolling upgrade from A.11.18.X to A.12.00.00”](#) (page 30).
2. Then, upgrade node 1 to A.12.00.Y. For more information on how to upgrade to A.12.00.Y, see [“Rolling upgrade from A.12.00.X to A.12.00.Y”](#) (page 31).

### 6.6.7 Upgrading Serviceguard Advanced edition to Enterprise edition for Linux using `cmupgrade` tool

---

**NOTE:** It is assumed that you already have Advanced MR and certain patch already installed on your system. You may or may not have the latest Advanced bundle patch.

---

1. Enable global switching for packages running on node 1.

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

Halt the node you want to upgrade. This results in the node's packages to start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

For example, `#cmhaltnode -f node1`

- a. If you have configured cluster analytics, stop cluster analytics daemon. For example, `#cmcaadmin stop`
3. You can upgrade the node as follows:
    - a. If you have configured Serviceguard Manager and you are required to change the `sgmgr` user password then export the `SGMGR_ENV`. `SGMGR_ENV=` where, is the password that you want to set for Serviceguard Manager user. For more information about how to create a replicated user, see [“Installing Serviceguard for Linux the traditional way”](#) (page 15).

---

**NOTE:** Installation of Serviceguard Manager for Linux B.12.00.00 (Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and SUSE Linux Enterprise Server 11) or Serviceguard Manager for Linux B.12.00.30 (Red Hat Enterprise Linux 7 and SUSE Linux Enterprise Server 12) automatically creates a user called `sgmgr` and password for this user is taken from the `SGMGR_ENV` environment variable.

---

- b. Upgrade node 1 from Advanced bundle patch release (PR) to latest Advanced bundle patch release (PR) to upgrade all the existing Serviceguard product.

```
cmupgrade {-d extracted_patch_location} {-j jetty-location}
```

---

**NOTE:**

- Advanced bundle patch must be SGLX\_00530 or higher.
  - Make sure use only `cmupgrade`, which is part of latest Advanced bundle patch tar file.
  - Specify untar location of latest patch with option `-d`.
- 

- c. Upgrade node 1 from Advanced bundle latest patch release to Enterprise bundle MR to upgrade all additional Serviceguard products.

```
cmupgrade {-d extracted_patch_location} {-j jetty-location}
```

---

**NOTE:**

- Make sure use only `cmupgrade`, which is part of latest Advanced bundle patch tar file (SGLX\_00530 or higher), and which has been used in previous `cmupgrade` [step b](#).
- Specify mounted ISO image location of Enterprise bundle MR with option `-d`.

**NOTE:** Starting from Serviceguard Manager version B.12.00.20, you can specify the new or existing Jetty location while upgrading Serviceguard Manager using `cmupgrade` tool. Prior to Serviceguard Manager version B.12.00.20, you must specify the same Jetty location.

---

- d. Upgrade node 1 from Enterprise bundle MR to Enterprise bundle latest patch release (PR) to upgrade all additional Serviceguard products.

```
cmupgrade {-d extracted_patch_location} {-j jetty-location}
```

---

**NOTE:**

- Enterprise bundle patch must be SGLX\_00531 or higher.
- Make sure use only `cmupgrade`, which is part of latest Enterprise bundle patch tar file.
- Specify untar location of latest patch with option `-d`.

**NOTE:** Starting from Serviceguard Manager version B.12.00.20, you can specify the new or existing Jetty location while upgrading Serviceguard Manager using `cmupgrade` tool. Prior to Serviceguard Manager version B.12.00.20, you must specify the same Jetty location.

---

- e. Starting Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends you to use NFS shared storage to create cluster analytics database. For information about how to configure NFS as shared storage, see *Managing HPE*

Serviceguard A.12.00.50 for Linux available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- f. If you have already configured cluster analytics and plan to use the existing analytics database, see Cluster Analytics Database Migration to Shared Storage section in the *Managing HPE Serviceguard A.12.00.50 for Linux* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

1. Rejoin the node to the cluster, which was halted in setp 2.

For example, # `cmrunnode -n node1`

Check that the node joins the cluster successfully, and if necessary, move packages back to the node.

2. Repeat steps from 2 to 4 for all the nodes.
3. Once all the nodes are upgraded to A.12.00.Y and if you have already configured cluster analytics, then start analytics daemon.

For example, #`cmcaadmin start`

## 7 Upgrading Serviceguard for Linux packages

You can use the `cmupgrade` tool to upgrade the packages from Serviceguard for Linux Advanced MR to Serviceguard for Linux Enterprise MR, in which case the additional components are installed.

## 8 Removing Serviceguard for Linux

To remove Serviceguard for Linux and its components do one of the following:

- Use `cmeasyinstall` tool to remove the Serviceguard and its components:

```
#cmeasyinstall [-e <uninstall serviceguard>] {-n <nodes including execution node>}
               {-j <location of Jetty server common across all nodes>}
               [-l <do not add sgmgr user as ldap is configured on all the nodes>]
```

- Use traditional way to remove the Serviceguard for Linux and its components:

```
rpm --e <rpm>
```

---

### NOTE:

- To remove Serviceguard Manager components from Jetty server path:

```
#!/opt/hp/cmcluster/serviceguardmanager/Serviceguard_manager_setup
-l <jetty location> -o erase
```

If Serviceguard version earlier than A.12.00.00 is installed, follow the instructions described in the [Performing rolling upgrades \(page 23\)](#) section to upgrade to latest version.

You can also use the `cmeasyinstall` tool to remove Serviceguard for Linux and its components version 12.00.00 and later.

---

## 9 Troubleshooting

The following are list of issues with respective solutions related to Serviceguard Manager installation:

### 1. Problem

The `sgmgr` user is not created during installation of Serviceguard Manager.

### Solution

You must create the **sgmgr** user manually and the password must be same as on the other system. To create the **sgmgr** user manually:

- a. Add the user:

```
useradd sgmgr
```

- b. Enter the password:

```
passwd sgmgr
```

## 2. Problem

The **sgmgr** user is not created during installation of Serviceguard Manager.

### Solution

*For Local user:*

- Check if PAM module and x64 bit JRE is installed in your Linux system.
- If you do not find the required node in Serviceguard Manager, try logging into that node through CLI using login credentials; this will confirm if the login credentials are valid for that node.

*LDAP user:*

Check if the user credentials are valid on the nodes where LDAP is configured, then ensure that the logged in credentials are working with LDAP.

## 3. Problem

If nodes are not getting detected by Serviceguard Manager or Serviceguard Manager is unable to launch, ensure that the product is installed and configured completely on those nodes.

### Solution

- a. Check the Jetty status:

```
# service jetty-sgmgr status
```

- b. If not, restart the Jetty server:

```
#service jetty-sgmgr restart
```

- c. If step **b** did not help, then run the following commands as sequenced below:

```
/opt/hp/cmcluster/serviceguardmanager/  
Serviceguard_manager_setup -l -o erase  
  
/opt/hp/cmcluster/serviceguardmanager/  
Serviceguard_manager_setup -l -o config -m 5301
```

---

### NOTE:

- Ensure that the Jetty server instance is running as mentioned earlier and the firewall has no reject rules for port 5511 and 5522 or HTTP/HTTPS traffic.
  - Ensure that the multicast port must be 5301 on all nodes and is not used by any other applications.
- 

## 4. Problem

If nodes are not getting detected by Serviceguard Manager or Serviceguard Manager is unable to launch, ensure that the product is installed and configured completely on those nodes.

### Solution

#### Jetty 8

To configure Jetty 8 with custom certificates:

- a. Perform the following tasks:
  - 1) **Generating Key Pairs and Certificate**
  - 2) **Requesting a Trusted Certificate**
  - 3) **Loading Keys and Certificates**
  - 4) Configure Serviceguard Manager for Jetty 8  
To configure Serviceguard Manager for Jetty 8, follow step b.
- b. Edit `sslContextFactory` object attributes in `<jetty location>/etc/jetty-ssl-sgmgr.xml` file.

```
<New id="sslContextFactory" class="org.eclipse.jetty.http.ssl.SslContextFactory">
  <Set name="KeyStore"><Property name="jetty.home" default="." />/etc/keystore</Set>
  <Set name="KeyStorePassword">OBF:lvnylzl0lx8elvnwlvn6lx8glzlulvn4</Set>
  <Set name="KeyManagerPassword">OBF:lu2ulwml1z7slz7alwnllu2g</Set>
  <Set name="TrustStore"><Property name="jetty.home" default="." />/etc/keystore</Set>
  <Set name="TrustStorePassword">OBF:lvnylzl0lx8elvnwlvn6lx8glzlulvn4</Set>
```

## Jetty 9

To configure Jetty 9 with custom certificates:

- a. Perform the following tasks:
  - 1) **Generating Key Pairs and Certificate**
  - 2) **Requesting a Trusted Certificate**
  - 3) **Loading Keys and Certificates**
  - 4) Configure Serviceguard Manager for Jetty 9  
To configure Serviceguard Manager for Jetty 9, follow step b.
- b. Edit `sslContextFactory` object attributes in `<jetty location>/etc/jetty-ssl-sgmgr.xml` file.

```
<New id="sslContextFactorySgmgr" class="org.eclipse.jetty.util.ssl.SslContextFactory">
  <Set name="KeyStorePath"><Property name="jetty.base" default="." /><Property name="jetty.keystore"
  default="etc/keystore"/></Set>
  <Set name="KeyStorePassword"><Property name="jetty.keystore.password"
  default="OBF:lvnylzl0lx8elvnwlvn6lx8glzlulvn4"/></Set>
  <Set name="KeyManagerPassword"><Property name="jetty.keymanager.password"
  default="OBF:lu2ulwml1z7slz7alwnllu2g"/></Set>
  <Set name="TrustStorePath"><Property name="jetty.base" default="." /><Property name="jetty.truststore"
  default="etc/keystore"/></Set>
  <Set name="TrustStorePassword"><Property name="jetty.truststore.password"
  default="OBF:lvnylzl0lx8elvnwlvn6lx8glzlulvn4"/></Set>
```

Edit the following attributes of Jetty to make use of the newly generated KeyStore:

- a. KeyStore (Jetty 8), KeyStorePath (Jetty 9)
- b. KeyStorePassword
- c. KeyManagerPassword
- d. TrustStore (Jetty 8), TrustStorePath (Jetty 9)
- e. TrustStorePassword

---

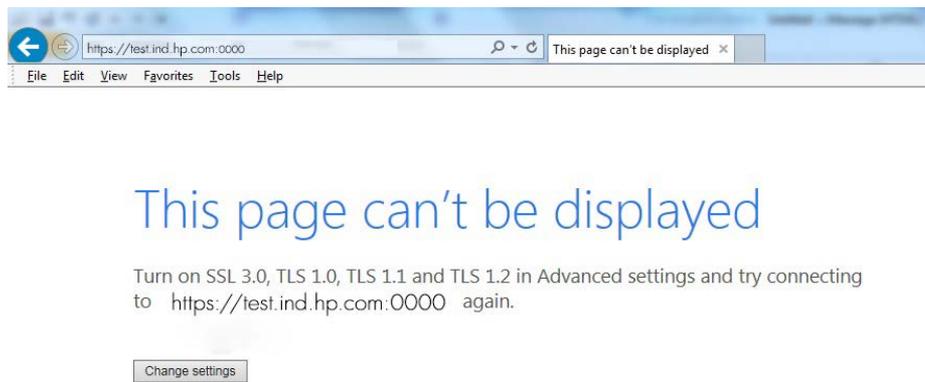
**NOTE:** The KeyStorePassword can be in plain text, obfuscated, checksummed, or encrypted to increase security. To generate password in these formats, see <http://eclipse.org/jetty/documentation/current/configuring-security-secure-passwords.html>.

---

## 5. Problem

Serviceguard Manager is not accessible on Internet Explorer or if you see an error message on Internet Explorer browser as shown in [Figure 1](#).

**Figure 1 Error while accessing Serviceguard Manager**



### **Solution**

You can either change Internet Explorer settings or configure Jetty with custom certificates.

- If you select to change Internet Explorer settings, then follow the procedure outlined in step **b**.
- If you want to configure Jetty with custom certificates, see problem **4**.

---

**NOTE:** Before you make any changes, ensure that you verify the Jetty server is running. To do so, see step **a**.

- 
- a.** Verify whether the Jetty server is running using `service jetty-sgmgr status` and check if the `Jetty running pid` message is displayed.
- If `Jetty running pid` message is not displayed, start Jetty using `service jetty-sgmgr start` and access Serviceguard Manager on Internet Explorer.
  - If `Jetty running pid` message is displayed, follow step **b**.
- b.** Verify the Internet Explorer settings:
- 1) Go to the **Tools** menu, click on **Internet Options**.
  - 2) Go to **Advanced** tab.
  - 3) Under **Security** section, locate `Use TLS` options.
  - 4) Check whether these options `Use TLS 1.0`, `Use TLS 1.1`, and `Use TLS 1.2` are selected.
  - 5) If the options are not selected, then select them.
  - 6) Click **Apply**.

---

**NOTE:** Before you access the Serviceguard Manager on Internet Explorer, ensure that at least one of these `Use TLS 1.0` and `Use TLS 1.1` is selected.

---

### **6. Problem**

When Serviceguard Manager is launched, analytics graph is missing on Node, Cluster, or Package page, or if you see an error message as shown in **Figure 2**:

## Figure 2 Analytics error

### Analytics

Cluster Analytics Start  
Time

Key Performance Indicators

Failure Protection Level -

Number of Reformatations -

Reformed On -

Created On

Modified On

Specify Range

From 07/31/2015 12:33:53 GMT+5.5 Hours To 08/07/2015 12:33:53 GMT+5.5Hours

The "To" date specified is greater than the current server date. Specify a different "To" date.

### Solution

Verify if the current system time on client (where Serviceguard Manager is launched) is in sync with the server time.

When Serviceguard Manager is launched on a client system, from dashboard, when you go to Cluster or Package or Node page, Analytics graph is not displayed because it takes the current client system time by default in `To` field to create and display the graph. If the client system time (selected in "To" field) is ahead of the server time, then the graph is not displayed and an error message is displayed as shown in [Figure 2](#). In this case, you must specify a different time range in `To` field to see the graph.

## 7. Problem

If you get a warning message with `cmupgrade` as follows:

**⚠ WARNING!** Failed to update multicast port to 5301 on <node Name>.The multicast port must be changed to 5301 on <node Name> before proceeding with any further operations. Log in to \$node using Serviceguard Manager GUI to do the same.

### Solution

Verify the multicast port configured in setting page of the node by logging in Serviceguard Manager GUI as "sgmgr" user, edit settings, and update the multicast port to 5301.

**NOTE:** You must update the multicast port to 5301 on all the nodes, which are required to be managed by the Serviceguard Manager.

You must also ensure that the multicast port must be 5301 on all the nodes and is not used by any other applications.

## 10 Related information

The latest documentation for Serviceguard for Linux Advanced edition 12.00.50 is available at <http://www.hpe.com/info/linux-serviceguard-docs>. Available documents include component release notes which contains the new features, problems fixed, known issues and limitations, and guides:

- *HPE Serviceguard for Linux Version 12.00.50 Release Notes*
- *HPE Serviceguard Contributed Toolkit Suite on Linux Release Notes Version A.12.00.00*
- *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes Version A.12.00.00*

- *HPE Serviceguard Toolkit for NFS on Linux Release Notes Version A.12.00.30*
- *HPE Serviceguard Extension for SAP Version B.06.00 Release Notes for Linux*

## 11 Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hpe.com](mailto:docsfeedback@hpe.com)). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.