



## **HPE Serviceguard for Linux Base edition**

### **12.50.00 Release Notes**

Part Number: P04490-005  
Published: November 2019

# Contents

|   |           |
|---|-----------|
| <b>Overview.....</b>  | <b>6</b>  |
| <b>Supported platforms and Linux distributions.....</b>       | <b>7</b>  |
| <b>Packaging information.....</b>                             | <b>8</b>  |
| <b>Licensing information.....</b>                             | <b>9</b>  |
| Obtaining a license.....                                      | 9         |
| Renewing the license.....                                     | 9         |
| Validating the license.....                                   | 10        |
| <b>HPE Serviceguard for Linux Base edition updates.....</b>   | <b>12</b> |
| Features introduced in this version.....                      | 12        |
| Features introduced in earlier versions.....                  | 12        |
| Features introduced in 12.40.00.....                          | 12        |
| Features introduced in A.12.30.00 version.....                | 13        |
| Features supported in A.12.20.00.....                         | 13        |
| Features introduced in A.12.10.00.....                        | 13        |
| Features introduced in 12.00.51.....                          | 14        |
| Features introduced in A.12.00.50.....                        | 14        |
| Features introduced in A.12.00.40.....                        | 14        |
| Features introduced in A.12.00.30.....                        | 14        |
| Features introduced in A.12.00.22.....                        | 14        |
| Features introduced in A.12.00.21.....                        | 15        |
| Features introduced in A.12.00.20.....                        | 15        |
| Features introduced in A.12.00.00.....                        | 15        |
| Features not supported.....                                   | 17        |
| Compatibility matrix.....                                     | 17        |
| Defects fixed .....   | 18        |
| Known problems and limitations.....                           | 18        |
| Deprecated or obsolete features.....                          | 20        |
| <b>Compatibility and installation requirements.....</b>       | <b>22</b> |
| Hardware requirements.....                                    | 22        |
| Port requirements.....  | 22        |
| Ports needed for Serviceguard.....                            | 22        |
| Ports needed for authentication.....                          | 22        |
| Ports needed by Serviceguard Manager.....                     | 23        |
| System firewalls.....   | 23        |
| <b>Software prerequisites for Serviceguard for Linux.....</b> | <b>25</b> |

|  |           |
|--|-----------|
| <b>Installing Serviceguard for Linux.....</b>  | <b>28</b> |
| Installing and upgrading Serviceguard for Linux using cminstaller.....                                       | 28        |
| Installing Serviceguard for Linux using cmeasyinstall.....   | 29        |
| Installing Serviceguard for Linux the traditional way.....   | 31        |
| Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository.....                   | 32        |
| Installing Serviceguard for Linux Update Release.....  | 33        |
| Post installation.....   | 35        |
| <br>   |           |
| <b>Rolling software upgrade.....</b>   | <b>36</b> |
| Requirements.....  | 36        |
| Limitations of rolling upgrades.....   | 37        |
| Preparation.....   | 38        |
| Rolling upgrade of a minor OS version of Linux.....  | 39        |
| Rolling upgrade of major OS version of Linux.....  | 40        |
| Supported rolling upgrade paths for Serviceguard versions.....   | 42        |
| Performing rolling upgrades of Serviceguard versions.....  | 42        |
| Rolling upgrade from 11.20.X to 12.20.00 .....   | 43        |
| Rolling upgrade from 11.19.X to 12.20.00.....  | 48        |
| Performing offline rolling upgrade from 11.18.X to 12.20.00.....   | 49        |
| Rolling upgrade from 12.00.X to later versions.....  | 50        |
| Rolling upgrade from A.11.19.X to A.12.20.X.....   | 56        |
| Offline rolling upgrade from A.11.18.X to A.12.20.X.....   | 56        |
| Upgrading Serviceguard Base edition to Advanced edition for Linux using cminstaller or cmupgrade tools.....  | 56        |
| Upgrading Serviceguard Base edition to Enterprise edition for Linux using cminstaller or cmupgrade tool..... | 58        |
| <br>   |           |
| <b>Removing Serviceguard for Linux.....</b>  | <b>61</b> |
| <br>   |           |
| <b>Troubleshooting.....</b>  | <b>62</b> |
| <br>   |           |
| <b>Related information.....</b>  | <b>68</b> |
| <br>   |           |
| <b>Documentation feedback.....</b>   | <b>69</b> |

# Notices

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

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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.

# Overview

This document provides information about HPE Serviceguard for Linux Base edition 12.50.00.

# Supported platforms and Linux distributions

Serviceguard for Linux Base edition 12.50.00 is available on the following Linux distributions:

- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- Oracle Linux 7 (Unbreakable Enterprise Kernel Only)
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15

---

**NOTE:** For more information about supported updates, supported hardware, storage, and other information, see the latest version of *HPE Serviceguard for Linux Certification Matrix Base Edition* at [\*\*http://www.hpe.com/info/linux-serviceguard-docs\*\*](http://www.hpe.com/info/linux-serviceguard-docs).

---

# Packaging information

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

# Licensing information

Starting Serviceguard for Linux 12.00.00 requires licenses on per-socket basis. When you install Serviceguard for Linux Base edition,, an instant-on license valid for 90 days is installed. With the instant-on license, you can use the product even if you do not have a permanent license. You must get a permanent license or term-based license before the grace period expires. The permanent license is perpetual and never expires. The term-based license is valid for one or three years and it must be renewed at the end of the term.

When ordering the licenses, determine the number of active sockets on the server. Order one license for each active socket irrespective of number of cores. A virtualized server may select less than the total number of active sockets if Serviceguard is used within virtual machine. The virtual machines use less than the total number of sockets available. 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 6 to Red Hat Enterprise Linux 7, you can use the same license of Red Hat Enterprise Linux 6 on Red Hat Enterprise Linux 7.
- 

## Obtaining a license

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

To obtain the license:

1. Go to <https://myenterpriselicense.hpe.com>.
2. Log in to **My License Portal** using your HPE Passport account. 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 message appears.
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 license**.)
- 

## Renewing the license

You can renew the license from the Serviceguard Manager.

To renew the license from the CLI after you have obtained the license, follow these steps to renew the license:

---

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

---

## **Procedure**

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 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:

- a. Copy the license file:

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

- b. Run the cmsetlicense command:

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

The mySGlicense file contains the license information.

- c. Run the cmgetlicense command:

```
cmgetlicense -f line
```

- d. 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 Base to Advanced or Enterprise license, repeat steps from 1 to 4.

---

## **Validating the license**

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

To validate the license:

1. Run the following command:

```
#cmgetlicense -f line
```

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

For permanent license

```
# cmgetlicense -f line
node:node1|license_method=PSL
node:node1|license_type=Base
node:node1|total_count=2
node:node1|license_type:Base|count=2
node:node1|license_type:Base|expiry_date=Indefinite
```

For term based license

```
# cmgetlicense -fline
node:node1|license_method=PSL
node:node1|license_type=Base
node:node1|total_count=2
node:node1|license_type:Base|count=1
node:node1|license_type:Base|days_remaining=330
node:node1|license_type:Base|expiry_date=2020/02/20 23:59:59 IST
node:node1|license_type:Base|count=1
node:node1|license_type:Base|days_remaining=1060
node:node1|license_type:Base|expiry_date=2022/02/19 23:59:59 IST
```

---

**NOTE:**

- If you install higher license than the one already installed on the system, the license on the node is upgraded automatically.
- If you have multiple licenses of the same type installed on the system, the `cmgetlicense -f line` command displays the following output:

```
# cmgetlicense -fline
node:node1|license_method=PSL
node:node1|license_type=Base
node:node1|total_count=2
node:node1|license_type:Base|count=1
node:node1|license_type:Base|days_remaining=330
node:node1|license_type:Base|expiry_date=2020/02/20 23:59:59 IST
node:node1|license_type:Base|count=1
node:node1|license_type:Base|days_remaining=1060
node:node1|license_type:Base|expiry_date=2022/02/19 23:59:59 IST
```

---

# HPE Serviceguard for Linux Base edition updates

## Features introduced in this version

Serviceguard 12.50.00 supports the following features:

- Starting with Serviceguard for Linux 12.50.00, cluster generic resources can be defined and operated with scope set to site or cluster in addition to node scope available for use starting from SGLX 12.40.00 release.

Cluster generic resource of type Site or Cluster scope allows you to build resource monitoring scripts which will help convey the resource status information consistently to all nodes identifiable at a Site or Cluster level. The resource monitoring for Site or Cluster scope Cluster generic resources can be performed at one or all nodes attached to Site or Cluster.

All packages having dependency on a Cluster Generic Resource of type Site or Cluster scope will see the same status value of a resource in the cluster. The resource status or up criteria used in the package definition will help determine the overall state of a package running in the site or cluster.

- Serviceguard supports RHEL8.1. You must install the below fixes before installing RHEL8.1.
  - authd-1.4.4-5.el8\_0.1 - <https://access.redhat.com/errata/RHBA-2019:1970>
  - kernel-4.18.0-80.9.el8 - (Yet to get the link from RH)
  - net-snmp-5.8-7.el8\_0.2 & more - <https://access.redhat.com/errata/RHBA-2019:2706>
- Applications can make use of Persistent Memory configured in Storage Over App Direct Mode in Serviceguard environment on physical and VMware virtual machines.
- Serviceguard Package Logging has been enhanced to provide flexibility in specifying the date and timestamp format.
- Serviceguard supports features of HPE Foundation Software on HPE Superdome Flex, specifically GEODID based NIC naming in a Serviceguard cluster.
- Serviceguard cluster supports long network interface names. More specifically the Predictable Network Interface Names.
- Serviceguard supports VMware vVols in all the deployments except the array based replication environments. For more information about the configuration details, see *Manging HPE Serviceguard for Linux* document.

## Features introduced in earlier versions

### Features introduced in 12.40.00

- You can apply Term-Based licenses for Serviceguard from this release. A Term-Based license is typically valid for one or three years. At the end of the term, the license must be renewed for the normal function of Serviceguard. Serviceguard perpetual license will continue to be available for its use as it offers unlimited period of validity.
- Serviceguard can run on Oracle Linux 7.4, 7.5, 7.6 (on all versions of UEK), SLES12 SP4, and SLES 15 operating systems.
- A new parameter `QS_HB_HEALTH` is introduced to enhance the quorum mechanism for two node clusters. Heartbeat health-based quorum mechanism allows the quorum server to consider the real-time heartbeat health status of cluster nodes while resolving split-brain situation.

- Unlike prior releases where the https port was fixed, you can now set or modify the https port for Serviceguard Manager. You can set the port at the time of installation or during the upgrade process.
- Quorum Server for Serviceguard can now be deployed in a public or private cloud infrastructure. The Cloud-based Quorum Server deployment model provides flexible options for Quorum server to operate on variety of platforms. The platforms can be physical servers or cloud infrastructure. For more information about the configuration details, see, *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

## Features introduced in A.12.30.00 version

Serviceguard A.12.30.00 supports the following features:

- Serviceguard is safe against the Spectre V2 vulnerability. Starting with Serviceguard Version 12.30.00, Serviceguard complies with the OS vendor specified requirements to protect the system against Spectre V2 vulnerability.
- You can upgrade a major version of Linux operating system and the Serviceguard software on a node at a time without causing downtime to your applications. For more information see, [\*\*Rolling upgrade of major OS version of Linux\*\*](#).
- With this release, you can use a single command `cminstaller` to perform a fresh installation or upgrade HPE Serviceguard bundles. HPE Serviceguard bundle is available in three variants such as HPE Serviceguard for Linux Base, HPE Serviceguard for Linux Advanced and HPE Serviceguard for Linux Enterprise.

For more information about `cminstaller` commands see the see the [\*\*Upgrading Serviceguard for Linux using cminstaller tool\*\*](#).

- Generic resource monitoring mechanism has been enhanced to support cluster generic resource. This is an easy to administer resource monitoring mechanism to monitor the critical resources of a cluster. It can be used to monitor common resources of multiple packages at cluster level and depending upon the status of the resource, you can take appropriate actions at the package level. Use the cluster generic resource to integrate any third party, custom, or user-defined monitoring agents at the cluster level.

## Features supported in A.12.20.00

- Serviceguard Root Disk Monitoring feature provides protection against failure of root disks. When a root disk of a node fails, Serviceguard detects the failure and sends a message about the failure to all member nodes in the cluster. Serviceguard then resets the node associated with the faulty root disk. After the node is reset, all the monitored applications and workloads running on that node fail over to another healthy node.
- Hyper-V based Virtual machines as cluster nodes.

## Features introduced in A.12.10.00

- Serviceguard for Linux 12.10.00 is configurable with any SCSI-3 Persistent Reservation compliant storage array for High Availability(HA) protection of any workload or application. For more information see, *HPE Serviceguard for Linux Certification Matrix* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- You can use the Toolkit Studio for easy, quick, and efficient integration of any application with Serviceguard for Linux cluster. Toolkit Studio is available for custom toolkit development. Toolkit Studio provides a Graphical User Interface for creation and deployment of application toolkit for its integration with Serviceguard for Linux cluster.

- To verify and generate reports for cluster and package configuration, Serviceguard for Linux has intuitive Graphical User Interface which allows flexible selection of various cluster objects for its verification operation. It also has the ability to save and retrieve reports for later reviews based on your preference.
- In addition to Command Line Interface (CLI) and Serviceguard Manager (Graphical User Interface), you can use the RESTful Application Programming Interface (API) to program your infrastructure to configure, monitor, and manage Serviceguard clusters, packages, and workloads.

## Features introduced in 12.00.51

- Serviceguard A.12.00.51 supports the cluster configuration for Virtual Machines deployed on VMware ESXi hosts enabled with Distributed Resource Scheduler(DRS). The DRS manages the allocation of physical resources to a set of virtual machines deployed in a cluster of hosts, each running VMware's ESXi hypervisor.
- Serviceguard supports Application Tuner Express (ATX).

## Features introduced in A.12.00.50

Serviceguard Manager B.12.00.50 introduces a new capability to perform seamless vMotion of Serviceguard cluster nodes VMs with a single click. This feature simplifies the migration of cluster nodes VMs.

Serviceguard Manager has been enhanced to configure the subnets automatically during Serviceguard Manager installation. Prior to the B.12.00.50 Serviceguard Manager release, the user needed to perform a manual step to configure the settings to use Serviceguard Manager.

## Features introduced in A.12.00.40

VMware Virtual Machine File System (VMFS)—Serviceguard for Linux 12.00.40 introduces support for VMFS (Virtual Machine File System) as a supported storage configuration in Serviceguard Packages. This enhancement allows seamless integration with other VMware features as follows:

- vMotion of VMware virtual machines configured as Serviceguard nodes.
- Native Multipathing (NMP) to shared storage from VMware hosts.

For more information on VMFS feature, see *Managing HPE Serviceguard for Linux*.

## Features introduced in A.12.00.30

Serviceguard A.12.00.30 contains the following features:

- Support for Smart Quorum  
For more information on Smart Quorum, see *Managing HP Serviceguard A.12.00.30 for Linux*.
- Support for Red Hat Enterprise Linux (RHEL) 7 and SUSE Linux Enterprise Server (SLES)12.

---

**NOTE:** For RHEL 5, 6, and SLES 11, Serviceguard for Linux A.12.00.30 is available as a patch.

---

## Features introduced in A.12.00.22

There are no new features in this version of the release. The patch contains only defect fixes for the following component:

SGeSAP

---

**NOTE:** For 12.00.22 version, only Advanced and Enterprise edition were released.

---

## **Features introduced in A.12.00.21**

There are no new features in this version of the release.

## **Features introduced in A.12.00.20**

Serviceguard for Linux A.12.00.20 supports these new features:

Serviceguard Analytics for Linux A.12.00.20 supports shared storage option to consolidate all the events of Serviceguard cluster in a common location. After the installation of Serviceguard Analytics for Linux A.12.00.20, it is recommended to configure shared storage to store all cluster events so that cluster analytics daemon can access analytics database from all nodes in the cluster. For information on configuring shared storage, see *Managing HPE Serviceguard A.12.00.20 for Linux* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

Serviceguard for Linux A.12.00.20 also supports the following enhancements from Serviceguard Manager:

- User can perform cluster, node and package operations using Serviceguard manager. These operations status display is enhanced for all operation with detailed description of errors.
- You can view and upgrade Serviceguard cluster licenses from Serviceguard Manager.

For more information about these new features, see the latest *Serviceguard Manager Online Help*.

## **Features introduced in A.12.00.00**

Serviceguard for Linux A.12.00.00 supports these new features

- **Cluster simulation**

Cluster simulation allows administrators to simulate different kinds of failures, such as node, network, and workload failures (that is, Serviceguard packages). Cluster simulation is capable of simulating node and network interface failures. Cluster simulation evaluates and analyzes what happens to the package due to simulated failures, whether the packages will failover and start on a specified node. The cluster states reported by the simulated cluster exactly matches with the real Serviceguard cluster. This helps in analyzing high availability design for various failure scenarios.

`cmsimulatecl` command is introduced as part of this feature. This command allows users to simulate Serviceguard cluster environment to verify high availability design and identify SPOF (single points of failures) in the Serviceguard cluster deployment. For more information about cluster simulation see *Managing HPE Serviceguard A.12.00.00 for Linux* manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Load sensitive package placement**

Serviceguard load sensitive placement for packages enables packages to be placed in such a way that package weights are distributed evenly among the cluster nodes based on each node's capacity. This ensures even distribution of workloads across cluster nodes during failover. For more information about load balancing see *Managing HPE Serviceguard A.12.00.00 for Linux* manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Veritas Volume Manager (VxVM)**

Serviceguard supports the use of Veritas Volume Manager (VxVM) and Veritas File System (VxFs) to meet the data management needs of applications configured in packages. VxVM is a storage management solution that allows you to manage physical and logical devices. VxFs is yet another constituent of Veritas Storage Foundation product suite which provides the file system management functionality. For more information on VxVM and VxFs, see *Managing HPE Serviceguard A.12.00.00 for Linux*. For information on configuring VxVM Diskgroups for Serviceguard Extended Distance Cluster product see *HPE Serviceguard Extended Distance Cluster for Linux A.12.00.00 Deployment Guide* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **btrfs file system**

Serviceguard supports the use of btrfs file systems for application with the packages managed in the cluster. btrfs is a new copy on write (CoW) file system for Linux aimed at implementing advanced features while focusing on fault tolerance, repair, and administration. For more information on btrfs file system see Managing HPE Serviceguard A.12.00.00 for Linux manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Scalable cluster: 32 nodes support**

With this release, the node support in Serviceguard is extended from 16 to 32 nodes, so now the cluster can have upto 32 nodes. For more information see Managing HPE Serviceguard A.12.00.00 for Linux manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Easy deployment to set up cluster - Create a cluster in three simple steps.**

Serviceguard for Linux A.12.00.00 offers quick and easy configuration of a cluster using just a few commands. Easy deployment is a feature that provides quick and simple way to create a cluster. It automates the security, shared storage, and networking configuration required by the package and cluster, it also simplifies cluster lock configuration using these commands:

- cmquerycl—This is an existing command which is enhanced with option –N to query available network configuration and generate network template.
- cmpreparestg—Using this command you can create or modify LVM, VxVM storage shared between Serviceguard nodes.
- cmdeploycl—Using this commands you can deploy the cluster with the previously generated network and storage configuration.

For more information on cmquerycl, cmpreparestg, and cmdeploycl commands see corresponding Manpages.

- **Support for IPV6 address**

You can use both IPv4 or the IPv6 address family for any subnet configured into the cluster, including subnets that carry the cluster heartbeat, and those connected to a Quorum Server. For more information about these modes including restrictions for IPv6-only and mixed modes see Managing HPE Serviceguard A.12.00.00 for Linux manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **New behavior during online reconfiguration of the package**

Serviceguard supports non-disruptive online modification of packages, so the packages will not fail due to any error during online reconfiguration. For more information, see Managing HPE Serviceguard A.12.00.00 for Linux manual available at <http://www.hpe.com/info/linux-serviceguard-docs>

- **License Information**

Serviceguard now requires per-socket license. You can manage the license using the following commands:

- cmgetlicense— This command displays the currently installed Serviceguard License information. When you invoke this command with “-f line” option, it displays the currently installed Serviceguard License information in machine parseable output format. If more than one type of license keys are present, it displays information about the higher license. If more than one similar type of permanent licenses are present, it displays the count of licenses present.
- cmsetlicense— This command renews the Serviceguard license at any time within 90 days or after 90 days of license expiry. You can also run cmsetlicense command while the node is up and running.

---

**NOTE:** Ensure that you run the cmsetlicense command on each node. When you add a new node to the cluster you must apply the license using the cmsetlicense command.

---

For more information about license see the appropriate release notes as per your bundle (Base, Advanced, and Enterprise) available at <http://www.hpe.com/info/linux-serviceguard-docs>

- **Improved installation and upgrade through `cmeasyinstall` and `cmupgrade` commands**

Serviceguard for Linux A.12.00.00 offers improved installation and upgrade methods through the following commands:

- `cmeasyinstall`—This command helps you to do a fresh installation of HPE Serviceguard and its components such as Serviceguard Extended Distance Cluster, Serviceguard Manager, Oracle toolkit, Enterprise DB toolkit, SAP sybase toolkit and Metroclusters except for SGeSAP from HPE Serviceguard for Linux Base, HPE Serviceguard for Linux Advanced and HPE Serviceguard for Linux Enterprise A.12.00.00 DVD or ISO image.
- `cmupgrade`—This command helps you in upgrading HPE Serviceguard and its components such as Serviceguard Manager, Toolkits, Extended Distance Cluster and Metrocluster except for SGeSAP.

For more information about `cmeasyinstall` and `cmupgrade` commands see the appropriate release notes as per your bundle (Base, Advanced, and Enterprise) available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Using Serviceguard with virtual machines**

For more information about these new features, see latest *Serviceguard Manager Online Help*. In this configuration, the virtual machine is a member of a Serviceguard cluster, allowing failover of application packages between other physical or VM nodes in the cluster. VMware vMotion feature is supported in this release. For more information about VMware features and configurations see Using HPE Serviceguard for Linux with VMware Virtual Machines white paper at <http://www.hpe.com/info/linux-serviceguard-docs>.

### **Cluster analytics**

Serviceguard cluster analytics provides a mechanism to perform "availability audits" on Serviceguard cluster, node, and application packages running on the cluster. New commands introduced as part of this feature are as follows:

- `cmcaadmin`—This command is used to manage cluster analytics daemon.
- `cmcashowkpi`—This command is used to display KPI (Key Performance Indicator) for Serviceguard cluster, node, and package. New Serviceguard Manager also has capabilities to view KPIs in donut charts and graphs. For more information about cluster analytics see Managing HPE Serviceguard A.12.00.00 for Linux manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

## **Features not supported**

### **Serviceguard Manager**

- Deletion of VMware hypervisor/vCenter Server credentials from Serviceguard Credential store (SCS) is not allowed from Serviceguard GUI.
- Updating Serviceguard credential store key is not allowed from Serviceguard GUI.
- Simulating a Serviceguard cluster.
- Localization in Simplified Chinese and Japanese.
- Preview option from UI for all supported Serviceguard admin commands.

## **Compatibility matrix**

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

## Defects fixed

The list of defects fixed in HPE Serviceguard for Linux Base edition 12.20.00 and its relevant details can be found *HPE Serviceguard for Linux Cumulative Update Release changes* guide at [https://support.hpe.com/hpsc/doc/public/display?docId=emr\\_na-a00038449en\\_us](https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00038449en_us).

## Known problems and limitations

This section provides a list of known problems and limitations with HPE Serviceguard for Linux Base edition 12.40.00 as known to HPE at the time of publication. If workarounds are available, they are included.

- The systemd does not have the ordering dependency on Serviceguard configuration sockets during shutdown on SLES15 and RHEL8.1. Because of the lack of ordering dependency the cluster node does not shut down properly.

### Workaround

First, run the cmhaltnode -f command from the command prompt to halt all the nodes. Then run the systemctl command to reboot or systemctl command to shutdown the cluster.

- The device mapper multipath fails to put the registration key after a failed path has recovered on SLES15.

### Workaround

This issue has been fixed with multipath-tools-0.7.3+102+suse.be95116-3.7.1.x86\_64 and later. Ensure that you install this or the later version to avoid this issue.

- Under certain scenarios, the Serviceguard daemons such as cmclld, cmproxy and qsc may fail to start and generate the following message.

### Workaround

To resolve this issue, see the customer advisory available at [https://support.hpe.com/hpsc/doc/public/display?docId=emr\\_na-a00069245en\\_us](https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00069245en_us).

- The pidentd does not support IPv6 addresses on SUSE Linux Enterprise Server 15 GA.

### Workaround

To use IPv6 addresses with Serviceguard, upgrade the pidentd from <https://www.suse.com/support/update/announcement/2018/suse-ru-20182936-1/> to enable it for IPv6 addresses.

- The sg\_persist commands report false return status for certain operations in SLES15.

### Workaround

This issue has been fixed in the subsequent kernel maintenance updates. Ensure to install the appropriate update to avoid this issue. For more information about the updated kernel see, <https://build.opensuse.org/request/show/685279>.

- QXCR1001610482 — Global switching for halted package is re-enabled unexpectedly. This issue occurs in clusters with package dependency configurations. It typically occurs in SGeSAP scale-up HANA clusters, where a primary and a secondary HANA package have a mutual exclusion dependency that prevents them from running on the same node.

### Workaround

Disable the global switching of both mutual exclusion dependency packages before halting the packages.

- QXCR1001605368 — Package fails if out of maintenance mode is reached before service halt timeout. Package fails after being placed out of maintenance mode before service halt timeout number is met if halt on maintenance is yes.
- QXCR1001500925 — During package start time, a warning message WARNING in package log "sg\_activate\_pr: registration failed on disk" appears when a Serviceguard package is configured with 3PAR based storage with multipath paths on Linux. You might receive the reservation conflict errors in package logs and syslog during package start time.

## **Workaround**

You can ignore these error messages.

- QXCR1001517687 — Serviceguard GUI crashes on Chrome version 54.0.2840.99 m.

## **Workaround**

Use a different version of Chrome or any other supported browser to start Serviceguard GUI.

- QXCR1001490615 — For the listed kernel versions of SLES12 and SLES12 SP1 Serviceguard will not work for IPv6 as heartbeat address

SLES 12

-----

3.12.48-52.27.1

3.12.51-52.31.1

SLES12 SP1

-----

3.12.49-11.1

3.12.51-60.20.2

3.12.51-60.25.1

Using IPv6 addresses as heartbeat network will not work in Serviceguard on above mentioned kernel versions. This is due to the issue with `recvfrom()` call which fails to read the UDP packets through IPv6 address.

## **Workaround**

Update the kernel version to latest on SLES12, SLES 12 SP1 systems.

- QXCR1001455844—When multiple VGs based on VMFS type disks are configured in the package, the package may fail back to the node on which it was running. When multiple VGs are configured on VMFS disks, the attach of these disks may take significant time. If the node where package was running had `AUTOSTART_CMCLD` configured as 1, node will join back the cluster and will be eligible to run the package. This will cause volume group tags check on the node where the package is still starting to fail. Package will then move back to the node where it was running earlier.
- QXCR1001435779—Serviceguard Linux patch installation fails due to `xinetd` exit.

On SUSE Linux Enterprise Server, `xinetd` service does not run if no services are configured.

## **Workarounds**

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

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

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

- QXCR1001378236—if you configure cluster and package together using `cmapplyconf` command and then check for package KPIs (Key Performance Indicators), the KPIs value displayed will be incorrect.
- After installing Serviceguard analytics for Linux A.12.00.20 or later, if `cmproxy` daemon is not running on all nodes in a cluster, then providing high availability for cluster analytics daemon is not possible.
- After installing Serviceguard analytics for Linux A.12.00.20 or later, it is recommended to configure shared storage to store all cluster events so that cluster analytics daemon can access analytics database from all nodes in the cluster. If you do not configure shared storage, cluster analytics will display incorrect value for all KPIs. For more information, see *Cluster Analytics Database Migration to Shared Storage* section from *Managing HPE Serviceguard A.12.00.20 for Linux*.

- Serviceguard analytics for Linux A.12.00.10 or later patch must be installed on all nodes of the cluster if it meets the following criteria:
  - Time zone used on the cluster nodes has DST (Daylight Saving Time).
  - Cluster analytics is installed and configured during the standard time period of 2014.

This ensures that cluster analytics computes the correct values for various KPIs (Key Performance Indicators) during the period of transition from standard to DST or vice versa.

If Serviceguard analytics for Linux A.12.00.10 or later patch is installed after the transition to standard time in 2014 or later, then some of the KPIs computed by cluster analytics might be incorrect. To avoid this problem, cluster analytics database must be initialized prior to the installation of A.12.00.10 or later patch.

The procedure for initializing cluster analytics database is as follows:

1. Stop cluster analytics daemon using `$SGSBIN/cmcaadmin stop` command.
  2. Delete the database file located at `$SGCONF/cluster3.db3` prior to installation of A.12.00.10 or later patch.
- QXCR1001251481—RHEL 6.x—Empty XML doc error due to `rpmReadConfigFiles()` failure.

### **Serviceguard Manager**

The known problems and limitations with Serviceguard Manager are as follows:

- QXCR1001433533—Sometimes, Serviceguard Manager fails to load the package monitoring page.
- QXCR1001339661—Nodes are not listed correctly in `Nodes` section.
- Configuration management (**Settings** option in Serviceguard Manager)— While configuring a subnet if certain nodes are not displayed under **Available Subnets**, then ensure that the IP address of all the Subnets of a node that needs to be configured in Serviceguard Manager is present in `/etc/hosts` file along with host name mapping.
- QXCR1001331670—Serviceguard Manager becomes unresponsive when you perform frequent operations on Serviceguard.
- QXCR1001318457—Sometimes all packages disappears for 20 or 30 seconds.
- QXCR1001376462—Multipath devices are not validated for Lock-LUN use during cluster create or edit operation.
- QXCR1001718665—If the host is on Red Hat 8, Serviceguard Manager is not launching in Internet Explorer browser.

### **Workarounds**

- IE browser launch works when LEGACY protocols are enabled in Red Hat 8. Read the warning note carefully in the below link before enabling the LEGACY protocols.  
[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/security\\_hardening/using-the-system-wide-cryptographic-policies\\_security-hardening](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening)
- Login as replicated user in non-Red Hat 8 Serviceguard Manager nodes in Internet Explorer and manage the Red Hat 8 nodes using the Multi cluster management functionality.

## **Deprecated or obsolete features**

Serviceguard A.12.10.00 and later is not supported on RHEL5 and Serviceguard A.12.50.00 and later is not supported on SLES11.

Starting with Serviceguard A.12.00.00, legacy packages are obsolete and only modular packages are supported. 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\*\*](http://www.hpe.com/info/linux-serviceguard-docs).

# Compatibility and installation requirements

## Hardware requirements

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

## Port requirements

### Ports needed for Serviceguard

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

#### On Red Hat Enterprise Linux, Oracle 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

### Ports needed for authentication

The ports reserved for authentication are also used by Serviceguard:

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

## **Ports needed by Serviceguard Manager**

- Ports 5511 (http), 5522 (the default https port, if not configured) and 5301 (multicast port) are used by Serviceguard Manager.
- You can set the https port instead of 5522 to user specified port number at the time of installation or upgrade of the Serviceguard Manager RPM.
- 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 is configured in the setting page.

---

**NOTE:** Only IP address and the port 5522 (https) can be modified by the user. The default multicast port 5301 and the http port 5511 cannot be modified.

---

For more information about set-up or modify the https port, see the section *Setting up https port for Serviceguard Manager* in the *Managing HPE Serviceguard for Linux User Guide*.

## **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 dynamic ports for 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, then 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 cmscanc1 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.

---

# 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, Oracle Linux, and SUSE Linux Enterprise Server:

```
#systemctl enable xinetd.service
```

---

**NOTE:** On SUSE Linux Enterprise Server, xinetd service does not run if no services are configured. This can lead to update 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 update to ensure that xinetd always restarts successfully.

For example, you can configure echo under xinetd using:

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

---

**NOTE:** The xinetd service is not available on SUSE Linux Enterprise Server 15 and RHEL8.1. Serviceguard configuration services are directly managed by systemd. Ensure that the `systemd` sockets `hacl-cfg.socket` and `hacl-cfgudp.socket` are enabled and running. You can use the commands `systemctl status hacl-cfg.socket` and `systemctl status hacl-cfgudp.socket` to check the status of the `systemd` sockets.

---

The table lists all the software that you need for each distribution before installing Serviceguard for Linux Base Edition.

**Table 1: RPMs (prerequisites) for installing Serviceguard for Linux**

| <b>Red Hat Enterprise Linux, Oracle Linux</b>   | <b>SUSE Linux Enterprise Server</b>  |
|---|--|
| lm_sensors  | bash   |
| tog-pegasus   | pidentd  |
| authd   | libblkid1  |
| krb5-libs   | sblim-indication_helper  |
| zlib  | sblim-sfcb   |
| libblkid(rhel6)   | sblim-sfcc   |
| net-snmp  | libnl1 (SLES 12)   |
| sg3_utils   | libnl3 (SLES 15)   |
| sg3_utils-libs  | sblim-cmpi-base  |
| xinetd  | net-snmp   |
| libnl   | sg3_utils  |
| mdadm   | xinetd   |
| udev (rhel 6)   | mdadm  |
| lsscsi  | udev   |
| net-tools   | lsscsi   |
| systemd (rhel7, rhel8, OL7, SLES 12 and SLES 15)  | net-tools  |
| sqlite  | systemd (SLES 12, SLES 15)   |
| dmidecode   | sqlite   |
| open-vm-tools (VMware only rhel7, rhel8, OL7, and their respective later releases) <sup>2</sup> | dmidecode (SLES 12, SLES 15)   |
| libnl3  | open-vm-tools (VMware only, SLES12, SLES 15, and their respective later releases) <sup>2</sup> |
|   | rhel8  |

<sup>1</sup> 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.

<sup>2</sup> On SLES12, SLES 15, RHEL7, OL7 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>.

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

#### **Other software prerequisites**

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

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

---

**NOTE:** The pidentd does not support IPv6 addresses on SUSE Linux Enterprise Server 15 GA. To use IPv6 addresses with Serviceguard, upgrade the pidentd from <https://www.suse.com/support/update/announcement/2018/suse-ru-20182936-1/> to enable it for IPv6 addresses.

---

# Installing Serviceguard for Linux

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

- **Installing and upgrading Serviceguard for Linux using cminstaller**
- **Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository**

---

#### **NOTE:**

- The `cmeasyinstall` tool will be obsoleted in the upcoming releases. Use `cminstaller` tool to perform installation and uninstallation of Serviceguard and its components.
- Hewlett Packard Enterprise recommends installing using `cminstaller` or SDR mechanisms for installation or upgrade of Serviceguard.
- 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>.

---

## Installing and upgrading Serviceguard for Linux using cminstaller

HPE recommends to use the `cminstaller` tool which helps you to install Serviceguard for Linux and its components, such as Serviceguard Manager, Toolkits, Extended Distance Cluster, Metrocluster, and SGeSAP. You can also execute the `cminstaller` 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.

---

**NOTE:** Changes suggested in **Customer Advisory** for real time priority issue can be reverted.

---

#### **Prerequisites**

Before you begin to use `cminstaller` 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 `cminstaller` are at same major version of the operating system.
- Ensure that PYTHON, PYTHON-BASE Version 2.X and later is installed on all the systems where you intend to install Serviceguard using the `cminstaller` tool.
- Ensure that a soft link from /usr/bin/python to python2 or python3 exists.

---

**NOTE:** On some operating systems, like RHEL8.1, the soft link does not come by default. In this case, user needs to create a soft link before using cminstaller.

An example to create soft link is `ln -s /usr/libexec/platform-python /usr/bin/python`.

cminstaller can also be executed with `/usr/libexec/platform-python cminstaller <options>`.

- 
- Ensure that YUM (Yellowdog Updater Modified) update service on Red Hat Enterprise Linux Server and Oracle Linux or Zypper on SUSE Linux Enterprise Server must be configured.

---

**NOTE:**

- The `cminstaller` tool does not install the Quorum Server.
- When you install Serviceguard bundle through `cminstaller` method, ensure that you have installed `mssql-tools` RPM on all the servers you intend to install the bundle on. The Serviceguard Solutions for Microsoft SQL Server for Linux is dependent on this RPM and only this solution is not installed if the RPM is not available on the node. `cminstaller` will continue to install the rest of the Serviceguard components.

For more information on `mssql-tools` RPM see, the Microsoft SQL Server for Linux documentation.

---

The `cminstaller` tool has the following advantages:

- Checks for dependencies using `-c` or `--dependency-check` option. This option displays the required software or packages and repository names, 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.

Use `-d` option along with `cminstaller` tool to specify 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 `cminstaller` 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 `cminstaller` command with appropriate qualifiers. For more information about the command usage and qualifiers, see the `Read_Me` available at `/<DVD_mount_dir>/README_cminstaller.txt`.

The `cminstaller` tool installs the RPMs.

## 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, Metrocluster, and 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 PYTHON, PYTHON-BASE Version 2.X and later is installed on all the systems where you intend to install Serviceguard using the cmeasyinstall tool.
  - Ensure that a soft link from /usr/bin/python to python2 or python3 exists.
- 

**NOTE:** On some operating systems, like RHEL8, the soft link does not come by default. In this case, user needs to create a soft link before using cmeasyinstall.

An example to create soft link is ln -s /usr/libexec/platform-python /usr/bin/python.

---

- Ensure that YUM (Yellowdog Updater Modified) update service on Red Hat Enterprise Linux Server and Oracle Linux or Zypper on SUSE Linux Enterprise Server is configured, if you intend to use the –a option.
- 

**NOTE:**

- The cmeasyinstall tool does not install the Quorum Server.
- When you install Serviceguard bundle through cmeasyinstall method with –a option, ensure that you have installed mssql-tools RPM on all the servers you intend to install the bundle on. The Serviceguard Solutions for Microsoft SQL Server for Linux is dependent on this RPM and the installation fails if the RPM is not available on the node. Alternatively you can use cmeasyinstall without –a option.

For more information on mssql-tools RPM see, the Microsoft SQL Server for Linux documentation.

---

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.

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

Installation script execution completed successfully <date>

**NOTE:** If Serviceguard is already installed, use cmupgrade tool to upgrade Serviceguard for Linux and its components. 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.

## Installing Serviceguard for Linux the traditional way

If you do not wish to install using the cminstaller or SDR mechanisms, 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

The following table describes the operating system and the DVD directory structure for Serviceguard for Linux Base edition:

**Table 2: DVD directory structure for Serviceguard for Base**

| Operating system           | DVD directory structure  |
|----------------------------|--|
| Red Hat Enterprise Linux 6 | <DVD-mount-path>/RedHat/RedHat6/Serviceguard/x86_64/<br><*.rpm><br><br><DVD-mount-path>/RedHat/RedHat6/SGManager/x86_64/<*.rpm>  |
| Red Hat Enterprise Linux 7 | <DVD-mount-path>/RedHat/RedHat7/Serviceguard/x86_64/<br><*.rpm><br><br><DVD-mount-path>/RedHat/RedHat7/SGManager/x86_64/<*.rpm>  |
| Red Hat Enterprise Linux 8 | Red Hat Enterprise Linux 8 /RedHat/RedHat8/Serviceguard/<br>x86_64/<br><br><*.rpm> /RedHat/RedHat8/SGManager/x86_64/<*.rpm> /RedHat/<br>RedHat8/SGeSAP/x86_64/<*.rpm> /<br><br>RedHat/RedHat8/Toolkit/noarch/<*.rpm> /RedHat/RedHat8/<br>Metrocluster/x86_64/<br><br><*.rpm> |
| Oracle Linux 7             | <DVD-mount-path>/Oracle_Linux/Oracle_Linux7/Serviceguard/<br>x86_64/<*.rpm><br><br><DVD-mount-path>/Oracle_Linux/Oracle_Linux7/SGManager/<br>x86_64/<*.rpm>  |

*Table Continued*

---

|                                    |  |
|------------------------------------|--|
| SUSE Linux Enterprise Server<br>12 | <DVD-mount-path>/SLES/SLES12/Serviceguard/x86_64/<*.rpm><br><DVD-mount-path>/SLES/SLES12/SGManager/x86_64/<*.rpm>  |
| SUSE Linux Enterprise Server<br>15 | <DVD-mount-path>/SLES/SLES15/Serviceguard/x86_64/<*.rpm><br><DVD-mount-path>/SLES/SLES15/SGManager/x86_64/<*.rpm><br><DVD-mount-path>/SLES/SLES15/SGeSAP/x86_64/<*.rpm><br><DVD-mount-path>/SLES/SLES15/Toolkit/noarch/<*.rpm><br><DVD-mount-path>/SLES/SLES15/Metrocluster/x86_64/<*.rpm> |

---

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

On Red Hat Enterprise Linux 6:

```
rpm -ivh serviceguard-A.12.XX.YY-0.rhel6.x86_64.rpm
```

On Red Hat Enterprise Linux 7:

```
rpm -ivh serviceguard-A.12.XX.YY-0.rhel7.x86_64.rpm
```

On Red Hat Enterprise Linux 8:

```
rpm -ivh serviceguard-A.12.XX.YY-0.rhel8.x86_64.rpm
```

On Oracle Linux 7:

```
rpm -ivh serviceguard-A.12.XX.YY-0.ol7.x86_64.rpm
```

On SUSE Linux Enterprise Server 12:

```
rpm -ivh serviceguard-A.12.XX.YY-0.sles12.x86_64.rpm
```

On SUSE Linux Enterprise Server 15:

```
rpm -ivh serviceguard-A.12.XX.YY-0.sles15.x86_64.rpm
```

Serviceguard manager RPM installation requires replicated user `sgmgr` for performing multi-cluster management.

Before installing the RPM, ensure that the user `sgmgr` exists in the system. If not the installation fails. If the `sgmgr` does not exist in the system, complete the steps to create the `sgmgr` as part of installation of Serviceguard Manager RPM.

Export the `SGMGR_ENV` environment and run the RPM command:

```
export SGMGR_ENV=<password>; rpm -ivh <serviceguard-manager>.rpm
```

---

**NOTE:** Installation of Serviceguard Manager for Linux B.12.10.00 onwards (Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Oracle Linux 7, SUSE Linux Enterprise Server 11, 12, and 15) automatically creates a user called `sgmgr` and password for this user is taken from the `SGMGR_ENV` environment variable.

---

## Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository

You can install or upgrade Serviceguard for Linux A.12.10.00 and later using HPE Software Delivery Repository (SDR). SDR hosts Serviceguard for Linux product repositories and enables you to use Linux-native software configuration manager such as `yum` or `zypper` to install or upgrade Serviceguard for Linux.

Using SDR to install or upgrade Serviceguard for Linux, provides the following benefits:

- You will receive notifications of the latest updates available for Serviceguard for Linux
- Provides easy and hassle-free installation or upgrade experience with all the dependencies taken care of
- Provides familiar Linux-native software configuration manager to install or upgrade
- Provides easy to integrate environment for any of your custom installation or upgrade scripts

### Prerequisites

You must be an authorized user to be able to access the HPE Software Delivery Repository site.

### Procedure

1. Navigate to the HPE SDR website at <http://downloads.linux.hpe.com/>  
The **Software Delivery Repository** page appears.
2. From the **Browse repository** column, select **sglx**.
3. Select the appropriate Serviceguard repository, from the **Subscribe** column, such as **Serviceguard for Linux Base**, **Serviceguard for Linux Advanced**, or **Serviceguard for Linux Enterprise** depending on the product or the subscription you have purchased.
4. Complete the instructions provided on the SDR page to install the selected version of Serviceguard.

## Installing Serviceguard for Linux Update Release

Serviceguard for Linux updates are available on three different editions 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 update, see [Packaging information](#).

- You can install Serviceguard using HPE Software Delivery Repository (SDR) at <http://downloads.linux.hpe.com/>. You can install only Serviceguard version A.12.10.00 and later using SDR.  
SDR hosts Serviceguard for Linux product repositories and enables you to use Linux native software configuration manager such as yum or zypper to install or upgrade Serviceguard for Linux. For more information about installing Service through SDR see, [Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository](#).
- Or you can install or upgrade Serviceguard by downloading the latest Serviceguard updates for Linux from Software updates and licensing site at <http://www.hpe.com/downloads/software>.

To install it from the Software updates and licensing site, complete the following steps. You can download the latest Serviceguard updates for Linux from Software updates and licensing at <http://www.hpe.com/downloads/software>.

**Table 3: Serviceguard updates for Linux**

| Serviceguard Version | Packages                            | Updates        |
|----------------------|-------------------------------------|----------------|
| 12.30.00             | Serviceguard for Linux Base edition | SGLX_00xxa.iso |

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

To install the update:

### Procedure

1. Download the update depending on the required edition, from the Hewlett Packard Enterprise Support Center at <http://www.hpe.com/info/hpesc>.

---

**!** **IMPORTANT:** Use `cmeasyinstall` if you are installing Serviceguard for the first time on the machine. Use `cmupgrade` if you are upgrading Serviceguard to the next version.
2. Mount the Serviceguard for Linux DVD or ISO image.
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. If you are installing Serviceguard for Linux for the first time, then use one of the following ways to install Serviceguard for Linux update release:
  - [\*\*Installing Serviceguard for Linux using cminstaller\*\*](#)
  - [\*\*Installing Serviceguard for Linux using cmeasyinstall\*\*](#)
  - [\*\*Installing Serviceguard for Linux the traditional way\*\*](#)
5. Upgrade Serviceguard for Linux in one of the following way:
  - [\*\*Upgrading Serviceguard for Linux using cminstaller tool\*\*](#)
  - [\*\*Upgrading Serviceguard for Linux using cmupgrade tool\*\*](#)
  - [\*\*Upgrading Serviceguard for Linux the traditional way\*\*](#)
  - [\*\*Upgrading Serviceguard for Linux using YUM or Zypper\*\*](#)

### Example

To install or upgrade the update complete the following steps:

1. Download `SGLX_00xxa.iso` bundle for Serviceguard for Linux Base edition.
2. The contents of the DVD or ISO are:

```
cminstaller  
cminstaller_utils/cminstaller_utils.py  
cminstaller_utils/log.py  
cminstaller_utils/yum_zypper.py  
cmeasyinstall  
cmupgrade  
End_User_License_Agreement.pdf  
README_cmeasyinstall.txt  
README_cmupgrade.txt  
Readme_Before_Install.txt  
Common/SGManager/x86_64/\  
serviceguard-manager-B.12.20.00-0.linux.noarch.rpm  
<dist>/<distro_version>/repodata/other.xml.gz  
<dist>/<distro_version>/repodata/repo-md.xml  
<dist>/<distro_version>/repodata/filelists.xml.gz  
<dist>/<distro_version>/repodata/primary.xml.gz
```

```
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-analytics-A.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-A.12.20.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-license-A.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-snmp-A.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Serviceguard/x86_64/\
serviceguard-providers-A.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/SGManager/x86_64/\
serviceguard-manager-B.12.20.00-0.linux.noarch.rpm
<dist>/<distro_version>/SGManager/x86_64/\
serviceguard-manager-B.12.20.00-0.linux.noarch.rpm
<dist>/<distro_version>/QuorumServer/x86_64/\
serviceguard-qs-A.12.10.00-0.<os_version>.x86_64.rpm
```

where:

<dist> is the value that can be either RedHat, Oracle\_Linux, or SLES based on the operating system.

<distro\_version> is the value that can be either RedHat6, RedHat7, Oracle\_Linux7, rhel8, or SLES12 based on the operating system.

<os\_version> is the value that can be either rhel6, rhel7, rhel8, sles12, or sles15 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. Install or upgrade Serviceguard for Linux Base edition.

## 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

# 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 be used any time when a node in the cluster must be taken offline for hardware maintenance or update installations. It can also be used when a node in the cluster must be updated to new major OS release 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 offered by the new Serviceguard release.**

The supported and recommended method of upgrading the major OS versions of Serviceguard node is to remove the existing node from the Serviceguard cluster configuration having the older version of the OS and add a new node with fresh install of new major OS version. Prior to adding the new node to the cluster, all the configuration changes must be done on the new node which should allow it to host or start an application or workload of an existing cluster package.

---

**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>.

---

## 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, Oracle Linux, SUSE Linux Enterprise Server).
- 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.

---

- For minor OS upgrade, 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.
- Supported rolling upgrade of major operating system versions are from Red Hat Enterprise Linux 6.x to Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11 to SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 12 to SUSE Linux Enterprise Server 15.
- Verify that the new OS supports the current cluster hardware configuration and drivers (network interfaces, bonding driver, and shared disk storage).
- Administrator or the customers are responsible for verifying, validating, and maintaining the version compatibility for any third party applications installed on their HPE Serviceguard environment which is being upgraded.
- Supportability and compatibility of applications (which are configured on the packages or workload) between the two major OS version must be checked and tested before starting any upgrade procedure.

- Customers are responsible for capturing and documenting all configuration details for any third party software prior to an OS installation, and then reinstalling those applications post OS installation.
- Configuration of applications during major OS upgrade must be tested and verified while moving from one major OS to other.
- Do a full backup on each node.
- For major OS upgrade, the Serviceguard version installed on all the cluster nodes (running different OS version) should be common minimum supported version of Serviceguard.

For example, Serviceguard A.12.00.30 is minimum version supported for SLES 11 SP4 and A.12.00.50 is the minimum version supported for SLES 12 SP1. Then during rolling upgrade, in a cluster of two nodes each running SLES 11SP4 and SLES 12SP1 required Serviceguard version will be A.12.00.50, which is the common minimum version supported.

---

**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, for minor OS upgrade.
- 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:**

- During minor OS upgrade, 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.
- During rolling upgrade sequence, any failures in starting an application package on a node which has undergone OS upgrade will result in downtime to that application package. Refer to package and syslog on the node where the package failed for more information and correct them to bring up the packages.
- Before upgrading any node in the cluster, ensure the packages hosted on it are moved to standby node for its continuous availability.
- During major OS rolling upgrade only failover operation of package is supported. All other features may result in incorrect or inconsistent behavior. For example running cluster verification during rolling upgrade may produce inconsistent results.

---

## Limitations of rolling upgrades

- During minor OS 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 must not 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. This restriction is applicable when you are upgrading Serviceguard from version 11.xx to 12.xx.yy.
- 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 version 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 for longer duration. It is highly recommended that you upgrade all cluster nodes as quickly as possible to the new release level.
- 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.
- Before major OS rolling upgrade, all nodes must be running the same releases of Linux (for example cluster must contain only SLES11 SPx OS version or RH 6.x OS version) and Serviceguard.
- Any configuration changes of newly added node (post new major OS install) of cluster, which is not compatible to failover the package from the older OS version to newer version will result in unexpected downtime to applications.
- Using Serviceguard Manager during major or minor OS rolling upgrade may lead to unexpected behavior. Use Serviceguard Manager after rolling upgrade is completed on all nodes of the cluster.
- Rolling upgrade of major OS of a cluster which is configured with SAP HANA is not supported.
- During major OS rolling upgrade, recommended cluster operations are:
  - Online cluster reconfiguration to remove the node from the cluster configuration.
  - Online package reconfiguration to remove the node information from the package configuration.
  - Online cluster reconfiguration to add the newly installed node into the existing cluster configuration.
  - Online package reconfiguration to add the node information into the package configuration.

Any operation which is not listed above on cluster or package configuration may result in failure or inconsistent execution state.

## 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 Base Edition* 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 or update release.

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* 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 or Oracle 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.

Serviceguard files: \$SGCONF/\*: all current package control and configuration files, including their log files.

---

**NOTE:** 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 6 to Red Hat Enterprise Linux 7, you can use the same license of Red Hat Enterprise Linux 6 on Red Hat Enterprise Linux 7.

## Rolling upgrade of a minor OS version of Linux

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 update release.

---

**NOTE:** If the target version of OS does not support the currently installed version of Serviceguard on the node, then you must upgrade the Serviceguard to a supported version before upgrading the OS. For supported Serviceguard versions see, *HPE Serviceguard for Linux Certification Matrix Base Edition* at <http://www.hpe.com/info/linux-serviceguard-docs>.

4. After completing the OS upgrade for the node, restore all its previously saved Host files: /root/.rhosts, /etc/hosts, /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.

---

**NOTE:** Before you reboot node running on SLES operating system, ensure that `sles-release` rpm is updated properly and also ensure that the `/etc/SuSE-release` file has the right patch version. If this rpm and file is not updated, Serviceguard commands fails after you reboot the node.

In the above procedure, in case you have not updated the `/etc/SuSE-release` file before the reboot, then you can update the file and restart the `SGSafetyTimer` service post reboot.

---

- 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 or Oracle 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:

For all SLES run # `service jetty-sgmgr status`

For SLES12 or higher run `systemctl status jetty-sgmgr`

- 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 `cmrunc1` command from a node which has been upgraded to the latest revision of the software.

---

---

**NOTE:**

- 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.
- 

## **Rolling upgrade of major OS version of Linux**

### **Prerequisites**

- Before starting the rolling upgrade, read the **Requirements** section.
- If the target version of the OS does not support the currently installed version of Serviceguard on the node, then you must upgrade the Serviceguard to a supported version before you upgrade the OS. For supported Serviceguard versions

see, *HPE Serviceguard for Linux Certification Matrix Enterprise Edition* at <http://www.hpe.com/info/linux-serviceguard-docs>.

## Procedure

1. Run the `cmmodpkg` command to enable the global switching and node switching of all the packages which are running on the node.

```
#cmmodpkg -e pkg1
```

2. Halt the node you want to upgrade. Halting the node causes all the packages running on the node to failover to an adoptive node.

```
#cmhaltnode -f
```

3. Remove the node information (`node_name`) from the package configuration by doing online reconfiguration of the package. This step is not required if the packages are configured to run on all the cluster nodes, that is `node_name` asterisk (\*) in the package configuration. Use the `cmgetconf` to retrieve the package configuration and `cmaplyconf` command to reconfigure the package.

```
#cmgetconf -p pkg1 pkg1.ascii  
#cmaplyconf -P pkg1.ascii
```

4. Remove the node from the cluster through online reconfiguration of the cluster. For more information see the section, *Removing Nodes from the Cluster while the Cluster Is Running* from *Managing HPE Serviceguard for Linux* manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.

5. Install the new major OS on the removed node. Here you can follow either one of two approaches listed below:

- a. You can perform fresh installation of OS on a node which is removed from the cluster. Post configuration, the node can be prepared to install Serviceguard software.
- b. You can perform a fresh install and configuration of OS on a completely new hardware. Ensure that system has adequate resource capacity to accommodate the cluster packages during their failover operation.

---

**NOTE:** HPE recommends that you retain the same host name (earlier removed node name) for the freshly installed node. Retaining the existing name avoids multiple configuration changes to package configuration file.

---

6. Configure the required network and storage of the newly installed node.

Ensure that the configuration is similar to the node that was removed from the cluster configuration. This ensures that the package starts on the new node, from the older OS version node in the cluster, when a failover is triggered.

- a. Restore all the previously saved host files on the new node, after completing the OS upgrade for the node. The `/root/.rhosts`, `/etc/hosts`, `/etc/profile`, `/etc/sysconfig/network/ifcfg*` or `/etc/sysconfig/network-scripts/ifcfg*` and the bonding files. Use these files as the reference files for configuring the network settings on new node.

---

**NOTE:** HPE recommends keeping the subnet of the new node to be same for package subnet compatibility.

---

- b. Verify that all disks and their file systems are the same prior to this new OS installation. Check and compare with the disk layout collected before the upgrade.
- c. Run the command `vgscan` to ensure that the new node recognizes all the previously configured LVM disks.

7. Install and configure the new version of the Serviceguard software on the newly installed node.

---

**NOTE:** The existing version of Serviceguard must be removed and then proceed with installation of new version of Serviceguard.

---

8. Add the newly installed node into the running cluster, after the required configurations are complete. For more information, see the section *Adding Nodes to the Configuration While the Cluster is Running* from *Managing HPE Serviceguard for Linux* manual available at <http://www.hpe.com/info/linux-serviceguard-docs>.
9. Restart Serviceguard on this node using `cmrunnode` and ensure that the node joins the cluster successfully.
10. Add the node information (`node_name`) to the package configuration through online reconfiguration of the package which is running on the yet to be updated node. This step will allow the user to move the packages from currently running node to newly updated node. This step is not required if the packages are configured to run on all the cluster nodes (`node_name asterisk (*)`) in the package configuration).
11. Run the `cmhaltnode -f` command on the node which is running the packages, to move the packages from the old node to new node. During this process, any failures to running packages will result in downtime to applications.
12. Repeat all the steps for each node in the cluster to move all the nodes of cluster to latest major OS.

## Supported rolling upgrade paths for Serviceguard versions

The following table describes the supported upgrade paths for Serviceguard for Linux:

**Table 4: Upgrade paths**

| Serviceguard version  | Rolling upgrade using<br>cmupgrade tool | Rolling upgrade the<br>traditional way | Offline upgrade |
|---|---|--|-----------------|
| To upgrade from A.12.00.X to A.12.20.Y, see<br><b><u><a href="#">Rolling upgrade from 12.00.X to later versions</a></u></b> .                           | Yes                                     | Yes                                    | Yes             |
| To upgrade from A.11.19.X to A.12.20.00, see<br><b><u><a href="#">Rolling upgrade from 11.19.X to 12.20.00</a></u></b> .                                | No                                      | Yes                                    | Yes             |
| To upgrade from A.11.18.X to A.12.20.00, see<br><b><u><a href="#">Performing offline rolling upgrade from 11.18.X to 12.20.00</a></u></b> .             | No                                      | No                                     | Yes             |
| To upgrade from A.11.20.X to A.12.20.00 or<br>from A.11.20.X to A.12.20.Y, see <b><u><a href="#">Rolling upgrade from 11.20.X to 12.20.00</a></u></b> . | Yes                                     | Yes                                    | Yes             |

## Performing rolling upgrades of Serviceguard versions

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 12.00.X to later versions](#)**
- **[Rolling upgrade from 11.20.X to 12.20.00](#)**
- **[Rolling upgrade from 11.19.X to 12.20.00](#)**

- **Performing offline rolling upgrade from 11.18.X to 12.20.00**
- **Rolling upgrade from A.11.19.X to A.12.20.X**
- **Offline rolling upgrade from A.11.18.X to A.12.20.X**

You can also upgrade from Serviceguard for Linux Base edition to Serviceguard for Linux Advanced edition or 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](#).

## **Rolling upgrade from 11.20.X to 12.20.00**

You can perform rolling upgrade of Serviceguard for Linux either from 11.20.x to 12.20.00 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**

### **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.

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 Base Edition* at <http://www.hpe.com/info/linux-serviceguard-docs>.

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 PYTHON, PYTHON-BASE Version 2.X and later is installed on the system to run the `cmupgrade` tool.
- Ensure that a soft link from /usr/bin/python to python2 or python3 exists.

---

**NOTE:** On some operating systems, like RHEL8.1, the soft link from /usr/bin/python to python2 or python3 does not come by default. In this case, user needs to create a soft link before using `cmupgrade`.

An example to create soft link is `ln -s /usr/libexec/platform-python /usr/bin/python`.

---

- Ensure that you run the `cmupgrade` tool on all the nodes that are part of the cluster.
- Ensure that the Java is 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 11.20.x to 12.20.00 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.12.20.00 or later (Red Hat Enterprise Linux 7, Oracle Linux 7, SUSE Linux Enterprise Server 11, SUSE Linux Enterprise Server 12, and SUSE Linux Enterprise Server 15) or A.12.20.00 (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>}

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

**NOTE:** The `cmupgrade` tool does not install or upgrade Quorum Server.

- c.** If you plan to upgrade node 1 to A.12.20.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.12.20.Y: # cmupgrade {-d extracted\_update\_release\_location}

**NOTE:** 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

## Upgrading Serviceguard for Linux the traditional way

To perform the rolling upgrade from A.11.20.X to A.12.20.00 or from A.11.20.X to A.12.20.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 6 x86\_64

```
#rpm -Uvh serviceguard-A.12.20.00-0.rhel6.x86_64.rpm
```

4. If you plan to upgrade node 1 to A.12.20.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 6 x86\_64

```
#rpm -Uvh serviceguard-A.12.20.Y-0.rhel6.x86_64.rpm
```

- 
- !** **IMPORTANT:** Serviceguard manager requires a replicated user `sgmgr` created on the node. Before installing or upgrading Serviceguard Manager RPM, ensure that `sgmgr` user is created on all the nodes. You can also create the `sgmgr` user during the installation process by specifying environment variable `SGMGR_ENV=` followed by `rpm -Uvh` command.

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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

## 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 Base 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.12.20.00 or from A.11.20.X to A.12.20.Y using YUM:

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

The `cmmodpkg` command enables switching of the package.

```
#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.

```
#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 6 or Red Hat 7.

4. Run the following command:

```
#yum clean all
```

5. If you plan to upgrade to A.12.20.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/sglxupdate.repo YUM repository configuration file with the following contents:

```
[sglxupdaterepo] name=sglxupdaterpms baseurl=file://<dir_location>/RedHat/<distro_update_ver> enabled=1
```

where:

<dir\_location> is the extracted update release location.

<distro\_major\_ver> is the value that can be either Red Hat 6 or Red Hat 7.

- b. Run the following command:

```
#yum clean all
```

- c. Export SGMGR\_ENV creating replicated user for Serviceguard-manager RPM Upgrade all rpms using yum upgrade serviceguard-\* command.

- d. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using YUM:

```
#yum upgrade serviceguard-manager
```

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. To upgrade serviceguard-manager rpm:

```
export SGMGR_ENV=<password>; yum upgrade serviceguard-manager
```

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* 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.12.20.00 or from A.11.20.X to A.12.20.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. To upgrade Serviceguard-manager RPM using zypper, you must first export SGMGR\_ENV variable. This variable when initialized is used by RPM to create an user if it does not exist.

```
export SGMGR_ENV=<password>;zypper upgrade serviceguard-manager
```

6. If you plan to upgrade to A.12.20.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/sglxupdate.repo Zypper repository configuration file with the following contents:

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

where:

<dir\_location> is the extracted update release location.

- b. Run the following command:

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

- c. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using Zypper:

```
export SGMGR_ENV=<password>;zypper upgrade serviceguard-manager
```

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 8 for all the nodes.

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

## Upgrading Serviceguard for Linux using Live Application Detach (LAD)

There may be circumstances to do maintenance that involves halting a node, or the entire cluster, without halting or failing over the affected packages. Such maintenance might consist of anything short of rebooting the node or nodes, but a likely case is networking changes that will disrupt the heartbeat.

This kind of maintenance can be done with Live Application Detach (LAD), when the packages are still running. The packages are no longer monitored by Serviceguard, but the applications continue to run. Packages in this state are called detached packages.

After the necessary maintenance, you can restart the node or cluster, and normal monitoring will resume on the packages.

## Detaching a node with Live Application Detach

### Procedure

1. Detach the node using `cmhaltnode -d` command.
2. Upgrade Serviceguard and its components.
3. Reattach the node using `cmrunnode` command.

---

**NOTE:** The monitoring scripts of the detached package may require to restart the package after upgrade. The package can be restart using `cmhaltpkg` and `cmrunkpkg` commands.

---

4. Repeat the preceding steps on all nodes of the cluster one after the other.

## Detaching a cluster with Live Application Detach

### Procedure

1. Detach the cluster using `cmhaltcl -d` command.
2. Upgrade Serviceguard and its components.

---

**NOTE:** The monitoring scripts of the detached package may require to restart the package after upgrade. The package can be restart using `cmhaltpkg` and `cmrunkpkg` commands.

---

3. Reattach the node back using `cmrunc1` command.

For more details about LAD feature, see *Managing HPE Serviceguard for Linux* document.

## Rolling upgrade from 11.19.X to 12.20.00

To perform the rolling upgrade from A.11.19.X to A.12.20.00:

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.XX.YY-0.rhel6.x86_64.rpm
```

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

For example, Serviceguard rpm for Red Hat 6 x86\_64

```
#rpm -Uvh serviceguard-A.12.XX.YY-0.rhel6.x86_64.rpm
```

---

**NOTE:** You can use YUM or Zypper to perform rolling upgrade from A.11.19.X to A.12.20.00. For more information about how to upgrade using YUM or Zypper, see [Upgrading Serviceguard for Linux using YUM or Zypper](#).

---

7. Restart cluster on first node.

For example, #`cmlrunnode -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.

## Performing offline rolling upgrade from 11.18.X to 12.20.00

To perform offline rolling upgrade from A.11.18.X to A.12.20.00:

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.12.20.00-0.rhel6.x86_64.rpm
```

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

For example, Serviceguard rpm for Red Hat 6 x86\_64

```
#rpm -Uvh serviceguard-A.12.20.00-0.rhel6.x86_64.rpm
```

---

**NOTE:** You can use YUM or Zypper to perform rolling upgrade from A.11.19.X to A.12.20.00. For more information about how to upgrade using YUM or Zypper, see [Upgrading Serviceguard for Linux using YUM or Zypper](#).

---

6. Repeat steps from 2 to 5 on each node of the cluster.

7. After all nodes are upgraded, restart the cluster.

```
#cmrunc1
```

## Rolling upgrade from 12.00.X to later versions

You can perform rolling upgrade of Serviceguard for Linux from A.12.00.XX to latter versions in the following ways. You can use the `cminstaller` tool to upgrade only from Serviceguard version 12.20.00 onwards.

- **Upgrading Serviceguard for Linux using cminstaller tool**
- **Upgrading Serviceguard for Linux using cmupgrade tool**
- **Upgrading Serviceguard for Linux the traditional way**
- **Upgrading Serviceguard for Linux using YUM or Zypper**

---

**NOTE:** To perform configuration changes to the cluster or package during a rolling upgrade, ensure that you initiate the configuration commands from a node running Serviceguard version 12.XX.YY.

---

### Upgrading Serviceguard for Linux using `cminstaller` tool

You can perform rolling upgrade from Serviceguard A.12.20.YY to the current version (A.12.XX.YY) using `cminstaller` tool. The `cminstaller` tool does not install or upgrade the Quorum Server.

#### Prerequisites

- 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 `cminstaller` are at same major version of the operating system.
- Ensure that PYTHON, PYTHON-BASE Version 2.X and later is installed on all the systems where you intend to install Serviceguard using the `cminstaller` tool.
- Ensure that YUM (Yellowdog Updater Modified) update service on Red Hat Enterprise Linux Server and OL or Zypper on SUSE Linux Enterprise Server must be configured.

#### Procedure

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

The `cmmodpkg` command enables switching of the package.

```
#cmmodpkg -e pkg1
```

2. Halt the node you want to upgrade.

The packages in the node start up on an adoptive node. The Serviceguard daemon on node 1 is halted.

```
#cmhaltnode -f node1
```

3. Stop cluster analytics daemon if configured.

```
#cmcaadmin stop
```

4. Export SGMGR\_ENV file, if you have configured Serviceguard Manager and must change the Serviceguard Manager password credentials on local node and the remote node.

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 or upgrade of Serviceguard Manager for Linux B.12.30.00 (Red Hat Enterprise Linux 6 and 7, OL 7, and SUSE Linux Enterprise Server 11 and 12) requires a replicated user sgmgr. During the installation or upgrade process, a user sgmgr is automatically created if the SGMGR\_ENV environment is set.

5. Download the latest ISO from <http://www.hpe.com/downloads/software> and mount the ISO.

6. Upgrade node 1 to the current version (A.12.XX.YY).

7. Export SGMGR\_ENV file, if you have configured Serviceguard Manager.

```
export SGMGR_ENV=<password>;cminstaller -d  
<extracted_update_release_location>
```

Starting from Serviceguard analytics for Linux A.12.00.20, Hewlett Packard Enterprise recommends that you 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](#) available at <http://www.hpe.com/info/linux-serviceguard-docs>.

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

8. Run cminstaller tool to upgrade Serviceguard version of multiple remote nodes from single node, if cluster is halted on remote nodes.

```
cminstaller -d <extracted_update_release_location> -n node2 -n node3
```

9. Rejoin the node on to the cluster.

```
#cmrunnode -n node1
```

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

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

12. After all the nodes are upgraded to the current version and if you have already configured cluster analytics, then start analytics daemon.

## Upgrading Serviceguard for Linux using cmupgrade tool

To perform the rolling upgrade from A.12.00.X to A.12.20.XX 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 or upgrade of Serviceguard Manager on Linux B.12.20.00 or later (Red Hat Enterprise Linux 6, 7, Oracle Linux 7, SUSE Linux Enterprise Server 11, 12, 15 and Oracle Linux 7) requires a replicated user sgmgr. During the installation or upgrade process, a user sgmgr is automatically created if the SGMGR\_ENV environment is set.

---

- b. Download and mount the ISO

You can download the latest Serviceguard updates for Linux from Software updates and licensing at [\*\*http://www.hpe.com/downloads/software\*\*](http://www.hpe.com/downloads/software).

- c. Upgrade node 1 to A.12.20.00 if step a is required, then:

```
export SGMGR_ENV=<password>; cmupgrade { -d  
extracted_update_release_location}
```

- d. 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* available at [\*\*http://www.hpe.com/info/linux-serviceguard-docs\*\*](http://www.hpe.com/info/linux-serviceguard-docs).

- e. 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* available at [\*\*http://www.hpe.com/info/linux-serviceguard-docs\*\*](http://www.hpe.com/info/linux-serviceguard-docs).
- 

**NOTE:** The cmupgrade tool does not install or upgrade Quorum Server.

4. 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.

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

6. Once all the nodes are upgraded to A.12.20.XX and if you have already configured cluster analytics, then start analytics daemon.

For example, #cmcaadmin start

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

To perform the rolling upgrade from A.12.00.X to A.12.XX.YY 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

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

For example, Serviceguard rpm for Red Hat 7 x86\_64:

```
#rpm -Uvh serviceguard-A.12.20.00.Y-0.rhel7.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. 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* 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

**4.** 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.

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

**6.** Once all the nodes are upgraded to A.12.XX.YY and if you have already configured cluster analytics, then start analytics daemon.

For example, #cmcaadmin start.

## Upgrading Serviceguard for Linux using YUM or Zypper

If you have configured YUM update service on Red Hat Enterprise Linux Server and OL or Zypper on SUSE Linux Enterprise Server, you can upgrade Serviceguard for Linux Base 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 update release.

---

### On Red Hat Enterprise Linux or Oracle Linux

To perform the rolling upgrade from A.12.00.X to A.12.XX.YY 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

3. You can access the repositories to upgrade through two methods:

- You can upgrade Serviceguard for Linux A.12.10.00 and later using HPE Software Delivery Repository (SDR). To access the repository from SDR and install see, [\*\*Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository\*\*](#)
- To upgrade from the ISO, create a /etc/yum.repos.d/sglxrel.repo YUM repository configuration file with the following contents:

**For RHEL:**

```
[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 6 or Red Hat 7.

**For OL:**

```
[sglxolrepo]
name=sglxolrpms
baseurl=file://<dir_location>/Oracle_Linux/<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 Oracle\_Linux7.

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* available at [\*\*http://www.hpe.com/info/linux-serviceguard-docs\*\*](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
- 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- 
- !** **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.** 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.
- 8.** Repeat steps from 2 to 8 for all the nodes.
- 9.** Once all the nodes are upgraded to A.12.XX.YY 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.XX.YY using Zypper:
- Enable global switching for packages running on node 1.  
The cmmodpkg command enables switching of the package.  
For example, #cmmodpkg -e pkg1
  - 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
    - If you have configured cluster analytics, stop cluster analytics daemon. For example, #cmcaadmin stop.
  - 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:<br/><dir_location> is the extracted update release location.
```
  - Run the following command:  
#/usr/bin/zypper clean

5. 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
  6. 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* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
  7. Upgrade all the RPMs. For example, to upgrade Serviceguard Manager RPM using Zypper:  

```
#zypper -n upgrade serviceguard-manager
```
- 
- !** **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, [Installing Serviceguard for Linux the traditional way](#).
- 
8. Restart cluster on first node.  
For example, `#cmrundnode -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 9 for all the nodes.

## **Rolling upgrade from A.11.19.X to A.12.20.X**

To perform the rolling upgrade from A.11.19.X to A.12.20.X:

Upgrade node 1 to A.12.20.00. For more information on how to upgrade to A.12.20.00, see [Rolling upgrade from 11.19.X to 12.20.00](#).

## **Offline rolling upgrade from A.11.18.X to A.12.20.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 11.18.X to 12.20.00](#).
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 12.00.X to later versions](#).

## **Upgrading Serviceguard Base edition to Advanced edition for Linux using cminstaller or cmupgrade tools**

---

**NOTE:** It is assumed that you already have Base MR and certain patch already installed on your system. You may or may not have the latest Base 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](#).

---

**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 Base bundle patch release (PR) to latest Base bundle patch release (PR) to upgrade all the existing Serviceguard product.

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

**NOTE:**

- Base bundle patch must be SGLX\_00529 or higher when using cmupgrade.
- Make sure you use only cminstaller or cmupgrade, which is part of latest Base bundle patch tar file.
- Specify untar location of latest patch with option -d.

c. Now upgrade node 1 from Base bundle latest patch release (PR) to Advanced bundle MR to install all additional Serviceguard products.

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

**NOTE:**

- Base bundle patch must be SGLX\_00529 or higher when using cmupgrade.
- Make sure you use only cminstaller or cmupgrade, which is part of latest Base bundle patch tar file, and which has been used in previous cminstaller or cmupgrade in step b.
- Specify mounted ISO image location of Advanced bundle MR with option -d.

d. Now upgrade node 1 from Advanced bundle MR to Advanced bundle latest patch release (PR) to upgrade all additional Serviceguard products.

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

---

**NOTE:**

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

- 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 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 for Linux* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- a. 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.
- b. Repeat steps from 2 to 4 for all the nodes.
  - c. 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`

## Upgrading Serviceguard Base edition to Enterprise edition for Linux using `cminstaller` or `cmupgrade` tool

---

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

---

**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 Base bundle patch release (PR) to latest Base bundle patch release (PR) to upgrade all existing Serviceguard product.

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

---

**NOTE:**

- Base bundle patch must be SGLX\_00529 or higher when using cmupgrade.
  - Make sure use only cminstaller or cmupgrade, which is part of latest Base bundle patch tar file.
  - Specify untar location of latest patch with option -d.
- 

- c.** Now upgrade node 1 from Base bundle latest patch release (PR) to Enterprise bundle MR to install all additional Serviceguard products.

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

---

**NOTE:**

- Base bundle patch must be SGLX\_00529 or higher when using cmupgrade.
  - Make sure use only cminstaller or cmupgrade, which has been used in previous cminstaller or cmupgrade *step b*.
  - Specify mounted ISO image location of Enterprise bundle MR with option -d.
- 

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

```
cminstaller/cmupgrade {-d extracted_patch_location}
```

---

**NOTE:**

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

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

- a.** 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.

- b.** Repeat steps from 2 to 4 for all the nodes.
- c.** 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

# 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>}  
[-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>
```

# Troubleshooting

## Cause

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
```

### 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 9

To configure Jetty 9 with custom certificates:

- a. Perform the following tasks:

- I. **Generating Key Pairs and Certificate**

- II. **Requesting a Trusted Certificate**

- III. **Loading Keys and Certificates**

- IV. 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:1vny1zlo1x8elvnw1vn61x8g1zlulvn4"/></Set>
    <Set name="KeyManagerPassword"><Property name="jetty.keymanager.password"
        default="OBF:1u2u1wm11z7s1z7a1wnl1u2g"/></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:1vny1zlo1x8elvnw1vn61x8g1zlulvn4"/></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

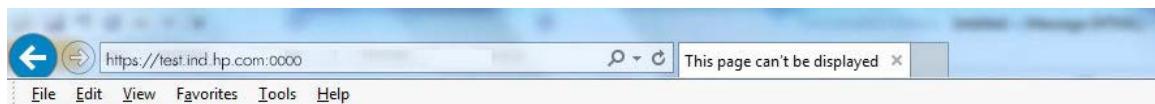
---

**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.



# This page can't be displayed

Turn on SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 in Advanced settings and try connecting to <https://test.ind.hp.com:0000> again.

[Change settings](#)

**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:
  - I. Go to the **Tools** menu, click on **Internet Options**.
  - II. Go to **Advanced** tab.
  - III. Under Security section, locate **Use TLS** options.
  - IV. Check whether these options **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2** are selected.
  - V. If the options are not selected, then select them.
  - VI. 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:

The screenshot shows the 'Analytics' section of the Serviceguard Manager interface. On the left, there's a sidebar with 'Key Performance Indicators' and dropdown menus for 'Failure Protection Level', 'Number of Reformations', 'Reformed On', 'Created On', and 'Modified On'. On the right, there's a 'Specify Range' section with 'From' set to '07/31/2015 12:33:53 GMT+5:5 Hours' and 'To' set to '08/07/2015 12:33:53 GMT+5:5 Hours'. A red error message at the bottom states: 'The "To" date specified is greater than the current server date. Specify a different "To" date.'

**Figure 2: Analytics error**

### 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. 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.

## Cause

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

### 1. Problem

Serviceguard processes cmclld, cmproxyd, quorum server(qsc), and cmanalyticsd may fail to start on the some systems. In operating systems using systemd, sometimes these processes are unable to get realtime priority. To get realtime priority, a new slice, sg.slice, is created, and all the services are attached to that slice.

---

**NOTE:** cmclld is started by cmruncl/cmrunnode command , which may timeout.

cmanalyticsd is started by cmcaadmin start command, which may fail.

Other process cmproxy & quorum server are started by their respective services, which may fail.

---

#### a. Scenario 1

Following error will be logged in systemd logs.

ERROR: sg.slice does not have the complete quantum value. Serviceguard needs complete quantum 950000 to operate. For more information on how to resolve it please refer to the HPE Serviceguard for Linux documentation on the HPE Support Center at <https://support.hpe.com/hpsc/home>. A Customer Advisory is published with additional information on this problem.

#### Solution

The Serviceguard slice, sg.slice, needs the complete quantum to operate.

Ensure that the file /sys/fs/cgroup/cpu/sg.slice/cpu.rt\_runtime\_us has the complete quantum value 950000.

Restart the service after ensuring the same

#### b. Scenario 2

If some other slice (say XXX.slice) is already present on the system and using some part of the quantum (i.e. have non-zero value for cpu.rt\_runtime\_us ).

ERROR: The cpu.rt\_runtime\_us value of XXX.slice is YYY. Serviceguard slice (sg.slice) needs the complete realtime quantum (950000) to operate and will be unable to do so if there is another slice with a realtime quantum. For more information on how to resolve it please refer to the HPE Serviceguard for Linux documentation on the HPE Support Center at <https://support.hpe.com/hpsc/home>. A Customer Advisory is published with additional information on this problem.

#### Solution

To resolve the above issue, ensure that value of /sys/fs/cgroup/cpu/XXX.slice/cpu.rt\_runtime\_us is 0. Serviceguard slice sg.slice needs the complete quantum and cannot co-exist with any other slice. After executing the above command, restart the service.

---

**NOTE:** Services attached to other slices (like XXX.slice) will not be able to get realtime priority after performing the above operations.

---

#### c. Scenario 3

Downgrade from Serviceguard version A.12.50.00

Once Serviceguard version A.12.50.00 is installed, if one tries to go back to lower versions, Serviceguard process cmclld, cmproxyd and quorum server will fail to start with the following message:

Failed to set realtime priority. This could be seen if CPU Accounting is enabled on the system by any of the systemd services. For more information on how to resolve it please refer to the HPE Serviceguard for Linux documentation on the HPE Support Center at <https://support.hpe.com/hpsc/home>.

#### Solution

This is because CPU Accounting gets enabled upon the installation of Serviceguard 12.50 and cannot be disabled when Serviceguard for Linux 12.50 is uninstalled. Refer to [\*\*Customer Advisory\*\*](#), to address this issue.

# Related information

The latest documentation for HPE XP Storage Plug-in for VMware vCenter is available at [http://www.hpe.com/info/  
storage/docs](http://www.hpe.com/info/storage/docs).

Available documents include the *HPE XP Storage Plug-in for VMware vCenter User Guide*.

# 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.