



Hewlett Packard
Enterprise

HPE Serviceguard for Linux Enterprise edition 12.30.00 Release Notes

Part Number: P04491-002
Published: July 2018

Contents

- Overview..... 6**
- Supported platforms and Linux distributions..... 7**
- Packaging information..... 8**
- Licensing information..... 9**
 - Obtaining a permanent license..... 9
 - Renewing the permanent license..... 9
 - Validating the permanent license..... 10
- HPE Serviceguard for Linux Enterprise edition updates..... 12**
 - Features introduced in this version..... 12
 - Features introduced in earlier versions..... 13
 - Features introduced in A.12.20.00..... 13
 - Features introduced in A.12.10.00..... 13
 - Features introduced in A.12.00.51..... 14
 - Features introduced in A.12.00.50..... 14
 - Features introduced in A.12.00.40..... 15
 - Features introduced in A.12.00.30..... 16
 - Features introduced in A.12.00.22..... 16
 - Features introduced in A.12.00.21..... 16
 - Features introduced in A.12.00.20..... 16
 - Features introduced in A.12.00.00..... 16
 - Common features of Enterprise bundle..... 18
 - Metrocluster with Continuous Access EVA P6000 for Linux..... 19
 - Metrocluster with Continuous Access XP P9000 for Linux..... 19
 - Features not supported..... 20
 - Metrocluster with 3PAR Remote Copy for Linux..... 20
 - Metrocluster with Continuous Access EVA P6000 for Linux..... 20
 - Metrocluster with Continuous Access XP P9000 for Linux..... 21
 - Metrocluster with EMC SRDF..... 21
 - Continentalclusters..... 21
 - Compatibility matrix..... 21
 - Installation..... 21
 - Defects fixed 22
 - Known problems and limitations..... 22
 - Deprecated or obsolete features..... 22
 - References..... 22
- Compatibility and installation requirements..... 24**
 - Hardware requirements..... 24
 - Port requirements..... 24
 - Ports needed for Serviceguard..... 24

Ports needed for authentication.....	24
Ports needed by Serviceguard Manager.....	25
System firewalls.....	25
Supported browsers.....	27
Software prerequisites for Serviceguard for Linux.....	28
Installing Serviceguard for Linux.....	31
Installing Serviceguard for Linux using cminstaller.....	31
Installing Serviceguard for Linux using cmeasyinstall.....	33
Installing Serviceguard for Linux the traditional way.....	35
Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository.....	36
Installing Serviceguard for Linux Update Release.....	37
Post installation.....	40
Rolling software upgrade.....	41
Requirements.....	41
Limitations of rolling upgrades.....	43
Preparation.....	44
Rolling upgrade of a minor OS version of Linux.....	45
Rolling upgrade of major OS version of Linux.....	46
Major OS rolling upgrade of two node cluster running HPE Serviceguard for Oracle Data Guard.....	48
Supported rolling upgrade paths for Serviceguard versions.....	50
Performing rolling upgrades of Serviceguard versions.....	50
Rolling upgrade from 11.20.X to 12.20.00	51
Rolling upgrade from 11.19.X to 12.20.00.....	56
Performing offline rolling upgrade from 11.18.X to 12.20.00.....	57
Rolling upgrade from 12.00.X to 12.30.X.....	58
Rolling upgrade from A.11.19.X to A.12.20.X.....	65
Offline rolling upgrade from A.11.18.X to A.12.20.X.....	65
Upgrading Serviceguard for Linux packages.....	66
Removing Serviceguard for Linux.....	67
Troubleshooting.....	68
Related information.....	73
Documentation feedback.....	74

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 Enterprise edition 12.30.00.

Supported platforms and Linux distributions

Serviceguard for Linux Enterprise edition 12.30.00 is available on the following Linux distributions:

- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise Server 11
- SUSE Linux Enterprise Server 12

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

Packaging information

Serviceguard for Linux 12.30.00 is available on all three editions, namely, Serviceguard for Linux Base, Serviceguard for Linux Advanced, and Serviceguard for Linux Enterprise. Serviceguard for Linux Enterprise edition 12.30.00 July 2018 contains rpms for the following components:

- Serviceguard License
- Serviceguard for Linux
- Serviceguard for Linux snmp
- Serviceguard for Linux WBEM providers
- Serviceguard for Linux analytics
- Serviceguard Quorum Server
- Serviceguard Manager
- Serviceguard Toolkit for Enterprise DB PPAS for Linux
- HPE Serviceguard Toolkit for Oracle Database for Linux
- HPE Serviceguard Toolkit for SAP Sybase ASE and Sybase Replication Server for Linux
- Serviceguard Extension for SAP
- Serviceguard XDC for Linux
- Metrocluster with Continuous Access XP P9000 for Linux
- Metrocluster with 3PAR Remote Copy for Linux
- Metrocluster with SADR for Linux
- Metrocluster with Continuous Access EVA P6000 for Linux
- Serviceguard Toolkit for KVM for Linux
- Metrocluster with EMC SRDF
- HPE Serviceguard Toolkit for Oracle Data Guard for Linux
- HPE Serviceguard Toolkit for Db2 for Linux
- HPE Serviceguard Solutions for Microsoft SQL Server for Linux

Licensing information

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

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

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

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

To obtain a permanent license:

1. Go to <https://myenterpriselicence.hpe.com>.
2. Log into HPE Passport. If you do not have an account, you can create one.
3. Enter Entitlement Order Number and click **Go**.
 - Here are the licenses listed that have been activated and license that have not yet been activated 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 permanent license](#) on page 10.)

Renewing the permanent license

You can renew the permanent license from the Serviceguard Manager.

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

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

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 permanent license key in a file on the system.

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

3. Renew the license:

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

On successful license renewal, it displays the following message:

```
License is successfully installed
```

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

Example

To verify if the license is valid:

- 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
```

Validating the permanent license

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

To validate the permanent license:

1. Run the following command:

```
#cmgetlicense -f line
```

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

```
#cmgetlicense -f line
```

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

NOTE:

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

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

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

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

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

HPE Serviceguard for Linux Enterprise edition updates

Features introduced in this 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.
- With this release, you can use a single command `cinstaller` 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 `cinstaller` commands see the see the [**Upgrading Serviceguard for Linux using cinstaller tool.**](#)

- With this release, you can implement Oracle single instance, Oracle Data Guard, and both AOFI and AOAI workloads for Microsoft SQL Server on nonvolatile memory on nonvolatile memory (NVM) systems such as NVDIMM and NVMe memory systems. These memory systems are accessed as block devices and bridge the performance and persistence gaps between the traditional DRAM and NAND flash systems. You can store the database, transaction/redo logs, and the temporary files such as hot files, temporary table space, database cache files in the nonvolatile memory systems. Or you can choose to save the combination of any of the data types on the traditional and the nonvolatile memory systems.
- 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.
- You can implement Serviceguard Metrocluster on 3PAR Synchronous Long Distance (SLD) environment. In this configuration Serviceguard can seamlessly orchestrate the primary and secondary roles in a SLD environment and ensure high availability and disaster recovery between sites.

Serviceguard Metrocluster provides RPO sensitive failover within the cluster. It also monitors the replication status across all the three sites and provides user notification appropriately.

- 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.**](#)
- Storage Agnostic Disaster Recovery (SADR) is a DR solution that is agnostic to the underlying array replication and the array type. SADR enables automated failover and failback capability between primary data center and secondary data center, which are connected in replication mode. Functionalities of the Metrocluster, such as role reversal, RPO/RTO monitoring, and automated recovery can be used with this solution.

NOTE: Download and install *SADR template* RPM hosted at <https://myenterpriselicense.hpe.com/cwp-ui/evaluation/SGLX-DR/A.12.30.00/null> to use this feature. This RPM contains two files:

- SADR template file
 - ReadME file
-

Features introduced in earlier versions

Features introduced in A.12.20.00

Serviceguard A.12.20.00 supports the following features:

- Serviceguard provides a robust monitoring system to monitor all disks of a ASM mirrored disk group configured in a Serviceguard package. Serviceguard discovers all the underlying disks of the ASM mirrored disk group and starts monitoring the disks to check their health. If a disk fails in a disk group, Serviceguard notifies the failure to the end user in the form of alerts and notifications. When the failed disk is restored, Serviceguard makes it available to the disk group.
- HPE Serviceguard Solutions for Microsoft SQL Server for Linux provides High Availability and Disaster Recovery solutions for Microsoft SQL Server for Linux. With this toolkit, Serviceguard monitors the health of the database and provides high availability and disaster recovery solutions for Availability Groups or Always on Availability Groups (AOAI) deployment model.

Features introduced in A.12.10.00

Serviceguard A.12.10.00 supports the following features:

- To validate and test the preparedness of disaster recovery site without disrupting the operations of production site, Serviceguard for Linux allows the selection of production workloads at site, node, and package levels for their recovery tests conducted at recovery site. It also prepares a detail report which captures the details of various preparedness tests conducted for audit or compliance purposes.
- Serviceguard for Linux configured cluster nodes in VMware ESXi environment are compatible with VMware Site Recovery Manager (SRM) supported recovery plan executions. With this integration, it facilitates automated disaster recovery with continued HA protection for applications independent of their SRM site of operation.
- VMware's Virtual Machine File System (VMFS) based virtual disks can be configured for Serviceguard Metrocluster with EMC SRDF for Linux based Metrocluster for disaster recovery.
- For easy viewing of multiple packages and their state which need to be examined together to understand the state of a solution level service delivery, Workload view is now available from single resource pane of Serviceguard Manager. You can create the following workload types:
 - Oracle Single Instance DB
 - Oracle Single Instance DB using ASM
- Serviceguard Metrocluster with 3PAR Remote Copy for Linux supports SSH based connections only with 3PAR arrays starting from Inform OS 3.3.1 (Supported from Serviceguard A.12.00.51 and later).

Features introduced in A.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).
- Metrocluster with 3PAR Remote Copy for Linux supports only SSH connection to the 3PAR arrays from Inform OS 3.3.1 onwards.

Features introduced in A.12.00.50

Oracle Data Guard Toolkit for Linux

With Serviceguard 12.00.50 release, a new disaster recovery solution for Oracle workloads based on Oracle dataguard replication is introduced. With this toolkit, Serviceguard manages the Oracle database and Oracle dataguard replication. It performs RPO sensitive automatic role management (failover, switch over) to handle failures, and also supports event notifications.

For more information, see the *HPE Serviceguard Toolkit for Oracle Data Guard on Linux User Guide* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

Metrocluster with 3PAR Remote Copy for Linux

Support for physical servers with disaster recovery solution based on 3PAR peer persistence.

Metrocluster with EMC SRDF for Linux

Metrocluster with EMC SRDF Symmetrix Remote Data Facility is now supported on the following Linux distributions:

- Red Hat Enterprise Linux (RHEL) 7 server
- SUSE Linux Enterprise Server (SLES) 12

Serviceguard Metrocluster for Linux with EMC SRDF B.01.00.00 is now bundled with *Serviceguard for Linux Enterprise Edition A.12.00.50* as *Serviceguard Metrocluster for Linux with EMC SRDF B.12.00.50*. All the features that were supported with Metrocluster EMC SRDF B.01.00.00 are now available for Metrocluster EMC SRDF B.12.00.50 in addition to the following:

- Support for Red Hat Enterprise Linux (RHEL) 7 server
- Support for SUSE Linux Enterprise Server (SLES) 12

Serviceguard Metrocluster for Linux with EMC SRDF B.01.00.00 is no longer available as a standalone product for Serviceguard for Linux Base and Advanced editions.

Following features that were supported with Metrocluster EMC SRDF B.01.00.00 are now bundled with 12.00.50 release:

- Support for Synchronous and Asynchronous Replication mode

Metrocluster with EMC SRDF for Linux includes support for synchronous replication mode. EMC SRDF software offers synchronous and asynchronous data transfer mode between the storage systems. Synchronous data transfer offer the highest levels of data availability. With synchronous operations, both primary and secondary copies are identical and concurrent at all times. Synchronous replication is appropriate when data currency is critical while recovering a business application. In the asynchronous

mode, host writes are performed only on the primary storage array, and the host write is acknowledged as soon as the data is written on the primary storage array.

- Supported for LVM

The LVM is supported with EMC SRDF disk group for Linux.

For more information on supported versions of the volume managers, see the *Serviceguard Disaster Recovery Products Compatibility and Feature Matrix(EMC SRDF disk group)* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- Support for Continentalclusters

EMC SRDF replication is supported with Continentalclusters and can be used to achieve push button automated recovery of EMC SRDF replication pairs. For more information, see the *Continentalclusters for Linux Version B.01.00.00 Release Notes* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- Support for failover polices `site_preferred` and `site_preferred_manual`

For more information on these failover polices `site_preferred` and `site_preferred_manual`, see the *Metrocluster SRDF for Linux B.01.00.00 Guide* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- Support for persistent reservations
- Support for Device Mapper

Features introduced in A.12.00.40

- Extended Distance Cluster (XDC) provides support for XDC based LVM Mirroring (RAID 1).
- Metrocluster with Continuous Access EVA P6000 for Linux provides automated failover of Serviceguard packages on local and remote P6000/EVA series disk arrays.
- Support for VMware Virtual Machine File System (VMFS) on the following Metrocluster products:
 - Metrocluster with 3PAR Remote Copy for Linux
 - Metrocluster with Continuous Access EVA P6000 for Linux
 - Metrocluster with Continuous Access XP P9000 for Linux
 - Extended Distance Cluster (XDC)
- Metrocluster with 3PAR Remote Copy for Linux provides the following features:
 - Support for Recovery Point Object (RPO).
 - Support for Asynchronous Streaming Mode
 - Support for peer persistence environment only if VMware Virtual Machine File System (VMFS) module is configured in the package configuration file. A disaster recovery solution based on 3PAR peer persistence with VMware guest nodes.

Features introduced in A.12.00.30

Support for Smart Quorum. For more information on Smart Quorum, see *Managing HPE Serviceguard A.12.00.30 for Linux*.

Support for Asymmetric node configuration in a disaster recovery solution. The following Metrocluster products support asymmetric node configuration for sites:

- Metrocluster with 3PAR Remote Copy for Linux
- Metrocluster with Continuous Access EVA P6000 for Linux
- Metrocluster with Continuous Access XP P9000 for Linux

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 SGeSAP.

Features introduced in A.12.00.21

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

Features introduced in A.12.00.20

- Site Aware Disaster Tolerant Architecture (SADTA) — SADTA is a framework, which enables you to easily deploy disaster recovery solutions for complex multi-instance workloads. You can create Serviceguard cluster to deploy complex workloads with SADTA using Serviceguard Manager. You can also use this framework to build disaster recovery solution for SAP HANA scale out workloads.
- Metrocluster with 3PAR Remote Copy for Linux supports Failsafe mode of 3PAR array.

Features introduced in A.12.00.00

Metrocluster with 3PAR Remote Copy for Linux enables automatic failover of Serviceguard packages between primary and recovery sites. In addition, Metrocluster with 3PAR Remote Copy for Linux provides the following features:

- **Support for Remote Copy volume group monitor**

In a Metrocluster 3PAR environment, Remote Copy volume group (RCVG) monitor provides the capability to monitor the status of the Remote Copy volume group used in a package. It sends notifications to the user via email, syslog, OPC, or console. The notifications are sent when:

- There is a change in a failure or state of Remote Copy volume group.
- The monitor cannot determine the Remote Copy volume group status.

- **Support for easy deployment**

With Metrocluster 3PAR, Metrocluster supports the package easy deployment feature. This feature is only available from the Serviceguard Manager for Linux version B.12.00.00 or later. It provides a simple way to quickly deploy Metrocluster 3PAR modules in supported toolkit applications.

- **Support for online reconfiguration of the packages**

With Metrocluster 3PAR for Linux, you can modify the Metrocluster 3PAR package attributes values while the package is up and running.

- **Support for 3PAR features**

- **Support for synchronous long distance replication**

Metrocluster with 3PAR Remote Copy for Linux includes support for synchronous long distance replication. It supports synchronous and periodic transfer between the primary and secondary and the third datacenters and provides additional data redundancy.

- **Support for synchronous replication mode**

Metrocluster with 3PAR Remote Copy for Linux includes support for synchronous replication mode. It supports synchronous and asynchronous periodic transfer modes between primary and secondary storage systems. Synchronous data transfers offer the highest levels of data availability where with synchronous operations, both the primary and secondary copies are identical and concurrent at all times while recovering a business application.

- **Support for asynchronous periodic mode**

Configure the 3PAR Remote Copy volume group in asynchronous periodic mode when you want no impact on the response time of application.

In the asynchronous periodic mode, host writes are performed only on the primary storage array and the host write is acknowledged as soon as the data is written into cache on the primary storage array. The primary and backup volumes are resynchronized periodically. This is ideal for deployments stretched across longer distances or narrow bandwidths.

- **Support for fully and thinly provisioned virtual volumes**

Metrocluster with 3PAR Remote Copy for Linux supports 3PAR Fully provisioned Virtual Volumes and Thinly Provisioned Virtual Volumes (TPVVs). For TPVVs, all data and snapshot space is allocated on demand from a Common Provisioning Group (CPG), and for fully provisioned virtual volumes, only the snapshot space is allocated on demand from the CPG.

NOTE: Common Provisioning Group (CPG) is a user created pool of storage from which Virtual Volumes are allocated.

As the volumes that draw from the CPG require additional storage, the system automatically creates additional logical disks and adds them to the pool until the CPG reaches the user-defined allocation limit that restricts its maximum size.

- **Support for Remote Copy configurations**

The following Remote Copy configurations are supported in a Metrocluster environment:

- Bidirectional configuration
- N-to-1 configuration
- 1-to-N configuration

For more information on each of these Remote Copy configurations, see the *3PAR Remote Copy User Guide* available at <http://www.hpe.com/info/storage/docs>.

NOTE: Both N-to-1 and 1-to-N configuration can have unidirectional and bidirectional Remote Copy configuration. However, the two arrays that are part of a Metrocluster must have a bidirectional Remote Copy configuration between them.

Synchronous Long Distance and Unidirectional Remote Copy configurations are not supported in a Metrocluster.

- **Support for 3PAR Virtual Domains**

This enables fine grained privileges over system objects such as volumes and hosts. Each domain can be dedicated to a specific application. A subset of the 3PAR storage system users can have varying privileges over the domains. Domains can be useful where a single storage system is used to manage data from several different independent applications.

- Supported volume managers with Metrocluster with 3PAR Remote Copy for Linux

The following volume managers are supported with Metrocluster 3PAR Remote Copy for Linux.

- LVM
- VxVM

For the supported versions of the volume managers, see the *Serviceguard Disaster Recovery Products Compatibility and Feature Matrix (Metrocluster 3PAR Remote Copy)* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

- **Support for HP 3PAR Remote Copy replication in Continentalclusters**

For more information, see the *Continentalclusters for Linux Version B.12.00.00 Release Notes* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

Common features of Enterprise bundle

The following are the common features of Metrocluster products:

- **Serviceguard Manager enablement in disaster recovery configuration**

Starting with HPE Serviceguard Manager B.12.00.00, along with Serviceguard for Linux A.12.00.00, the following Serviceguard Manager operations are supported in a Metrocluster environment:

- Configuring, monitoring, and administration of Metrocluster modular packages.

However, the following is the restriction with Serviceguard Manager in a Metrocluster environment:

The Metrocluster package configuration requires a system administrator to configure data replication, which is not supported by the Serviceguard Manager. This step needs to be performed by the administrator outside of HPE Serviceguard Manager.

- **Support for VMWare virtual machines as Metrocluster nodes**

Metrocluster for Linux includes support for configuring VMWare virtual machines as Metrocluster nodes. All the Serviceguard related restrictions and guidelines for configuring VMWare virtual machines as Serviceguard nodes are also applicable to Metrocluster configurations. In Metrocluster configurations, Raw Device Mapping (RDM) is not supported. You must configure the Fiber channel N-Port ID Virtualization (NPIV) for all the virtual machines. For more information on configuring NPIV, see the *Using HPE Serviceguard for Linux with VMWare virtual machines* whitepaper.

- **Support for Cluster Verification**

Metrocluster for Linux supports verification of its packages. By using the `cmcheckconf -v` command, you can generate a report on the sanity of the cluster configuration. This feature requires Serviceguard for Linux A.11.20.20 or later.

- **Support for failover polices `site_preferred` and `site_preferred_manual`**

Metrocluster for Linux supports Serviceguard failover policies *site_preferred* and *site_preferred_manual*. These failover policies are supported for failover packages configured in a Metrocluster with sites defined in the Serviceguard cluster configuration file. For more information on the *site_preferred* and *site_preferred_manual* failover policies, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>

- *Building Disaster Recovery Serviceguard Solutions Using Metrocluster with 3PAR Remote Copy for Linux*
- *Building Disaster Recovery Serviceguard Solutions Using Metrocluster with Continuous Access EVA P6000 for Linux*
- *Building Disaster Recovery Serviceguard Solutions Using Metrocluster with Continuous Access XP P9000 for Linux*
- **Support for persistent reservations**

Metrocluster for Linux supports configuring persistent reservations (PR) in Metrocluster packages to control access to LUNs. For more information on persistent reservation, see the *Managing HPE Serviceguard A.12.00.00 for Linux* available at <http://www.hpe.com/info/linux-serviceguard-docs>.
- **Support for Device Mapper**

Metrocluster for Linux supports configuring Device Mapper for disks used in Metrocluster packages. All the Serviceguard related restrictions and guidelines for supporting DM-Multipath are also applicable to Metrocluster configurations.
- **Support for Data Replication Storage Failover Preview**

The `cmdrprev` command enables you to preview the preparation process for data replication in a Metrocluster environment and also helps you in identifying any potential problems in the data replication environment, which if left undetected, may result in an unsuccessful Metrocluster failover.

Metrocluster with Continuous Access EVA P6000 for Linux

The B.12.00.00 version of Metrocluster with Continuous Access EVA P6000 for Linux supports the following features:

- **Support for Synchronous Replication Mode**

Metrocluster for Linux supports Synchronous write mode with P6000/EVA arrays. In Synchronous write mode, the data at primary and remote array are identical and concurrent at any point of time. This write mode is required when business application needs concurrent data.
- **Support for Enhanced Asynchronous Replication Mode**

Metrocluster for Linux does not support the Basic Asynchronous mode. The asynchronous replication process reads the I/O from the journal and replicates it, using current methodologies, to destination P6000/EVA.

Metrocluster with Continuous Access XP P9000 for Linux

Metrocluster with Continuous Access XP P9000 for Linux provides automated failover of Serviceguard packages between primary and recovery sites.

In addition, Metrocluster with Continuous Access XP P9000 for Linux B.12.00.00 provides the following new features:

- **Support for Device Group Monitor**

DGM provides the capability to monitor the status of the Continuous Access device groups configured in a Metrocluster package. Device Group Monitor provides the following functionalities:

- Sends a notification message upon the change in a device group status.
 - Performs automatic resynchronization of the Continuous Access device group upon link recovery.
- **Support for HPE XP P9000 Storage Family**
Starting with this version, Metrocluster with Continuous Access XP P9000 for Linux includes support for XP20000/XP24000/P9500 disk arrays.

- **Support for Remote Command Device**

Metrocluster with Continuous Access XP P9000 for Linux includes support for remote command device. A remote command device is a device to which a command device in a remote P9000 array is mapped. A remote array P9000 RAID Manager must be configured using the remote command device. Using a remote array RAID manager instance, it is possible to get the status of the device group on the remote P9000 array even when the remote hosts are inaccessible.

The remote command device can be configured using one of the following methods:

- Using the P9000 external storage feature
- Using an extended SAN

Features not supported

The following features are not supported:

- You can deploy SAP workload from Serviceguard Manager workloads page. SAP workload feature is not supported and it is currently not recommended for deployment or monitoring of SAP workloads.
- Localization in Simplified Chinese and Japanese.
- Alert generation for manual site switching failover mode.

Metrocluster with 3PAR Remote Copy for Linux

- Unidirectional Remote Copy configuration
- 3PAR Remote Copy volume groups configured with `fail_wrt_on_err` policy
- Failover to the third data center (DC3)

Metrocluster with Continuous Access EVA P6000 for Linux

The following P6000 Continuous Access features are not supported with Metrocluster with Continuous Access EVA P6000 for Linux:

- Asynchronous Replication Mode
- Failsafe-Locked Mode

- Storage Management Appliance (SMA)
- No support for online reconfiguration of the package

HPE Serviceguard Manager (UI) for Linux does not support configuration, monitoring, and administration of Metrocluster modular packages with EVA P6000.

Metrocluster with Continuous Access XP P9000 for Linux

The following features introduced in HPE Storage P9000 RAID Manager are not supported with Metrocluster:

- Virtual Command Device via LAN
- Copy Group configuration based on RAID
- User Authentication based on Command Device
- Resource Group Control

Online modification of the package

Metrocluster with Continuous Access XP P9000 for Linux does not support online reconfiguration of the package.

HPE Serviceguard Manager (UI) for Linux does not support configuration, monitoring, and administration of Metrocluster modular packages with Continuous Access XP P9000.

Metrocluster with EMC SRDF

HPE Serviceguard Manager (UI) for Linux does not support configuration, monitoring, and administration of Metrocluster modular packages with EMC SRDF.

Continentalclusters

Creating and Monitoring Continentalclusters from SGMgr is not supported.

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>.

Installation

With A.12.00.50 release, the following components are introduced with Enterprise bundle:

- Oracle Data Guard Toolkit for Linux
- Metrocluster with EMC SRDF

For more information on installation instructions, see the *HPE Serviceguard for Linux Enterprise edition Release Notes* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

Defects fixed

The list of defects fixed in HPE Serviceguard for Linux Enterprise edition 12.20.00 and its relevant details can be found in *HPE Serviceguard for Linux Cumulative Update Release changes* guide at https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00038449en_us.

Known problems and limitations

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

QXCR1001555757 — SSH connection to 3PAR arrays might occasionally fail with return code 254 & 255.

The following are the known issues with Serviceguard Manager:

- QXCR1001379443—Adding a new site must not affect the existing site definition
- QXCR1001621395—Workload discovery and deployment fails if there is a mismatch in the hostname
- QXCR1001621396—Workload discovery and deployment incorrectly obtains remote node's DC RCVG name

There are no known problems and limitations for Oracle Data Guard toolkit.

There are no other known problems and limitations in Metrocluster with 3PAR Remote Copy for Linux, Metrocluster with Continuous Access EVA P6000 for Linux, Metrocluster with Continuous Access XP P9000 for Linux, and Metrocluster with SRDF for Linux.

Deprecated or obsolete features

Serviceguard A.12.10.00 onwards is not supported on RHEL 5.

References

The following are the references available for Metrocluster:

- *Understanding and Designing Serviceguard Disaster Recovery Architectures*
- For 3PAR Storage Systems and 3PAR Remote Copy documents, see the following documents:
 - *3PAR Remote Copy User Guide* available at <http://www.hpe.com/info/storage/docs>.
 - *3PAR InForm OS Concepts Guide* available at <http://www.hpe.com/info/storage/docs>.
 - *3PAR CLI Administrator Manual* available at <http://www.hpe.com/info/storage/docs>.
- For more information on P6000/EVA disk array with P6000 Continuous Access, see the following list of the documents:
 - HP P6000 Enterprise Virtual Array Compatibility Reference Guide
 - HP P6000 Command View User Guide
 - HP P6000 Command View Release Notes
 - HP P6000 Command View Installation Guide
 - HP Storage System Scripting Utility Reference Guide

- HP P6000 Replication Solution Manager User Guide
- HP P6000 Continuous Access EVA Replication Performance Estimator Application Notes
- For documentation on P9000 disk arrays with Continuous Access for P9000, see the following documents:
 - *HP StorageWorks P9000 Business Copy User Guide*
 - *HP StorageWorks P9000 Continuous Access User Guide*
 - *HP StorageWorks P9000 Raid Manager User Guide*
 - *HP StorageWorks P9000 Remote Web Console User Guide*
- For documentation on XP disk array with Continuous Access XP, see the following documents:
 - *HP StorageWorks Disk Array XP Business Copy User's Guide*
 - *HP StorageWorks Disk Array XP Continuous Access User's Guide*
 - *HP StorageWorks Disk Array XP Raid Manager User's Guide*
 - *HP StorageWorks Disk Array XP Remote Web Console User's Guide*
- For Metrocluster with EMC SRDF document, see the following documents:
 - HPE Serviceguard Metrocluster with EMC SRDF for Linux B.12.00.50 for Linux user Guide available at <http://www.hpe.com/info/linux-serviceguard-docs>.
 - EMC® Symmetrix® Remote Data Facility (SRDF®) Product Guide at <http://support.emc.com>.
Building Disaster Recovery Serviceguard Solutions Using Metrocluster with EMC SRDF for Linux B.01.00.00

Compatibility and installation requirements

Hardware requirements

For more information about hardware requirements, see the latest version of *HPE Serviceguard for Linux Certification Matrix Enterprise 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 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

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

NOTE:

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

System firewalls

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

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

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

- To enable intra-cluster communications, each HEARTBEAT_IP network on every node in the cluster must allow the following communications in both directions with all other nodes in the cluster:
 - TCP on port numbers 5300 and 5302 – and allow only packets with the SYN flag
 - UDP on port numbers 5300 and 5302
 - TCP and UDP on dynamic ports
- If you use a quorum server, all nodes in the cluster must allow the following communication to the quorum server IP address:
 - TCP on port 1238 — and allow only packets with the SYN flag
Any node providing quorum service for another cluster must allow the following communication from that cluster's nodes:
 - TCP on port 1238 — and allow only packets with the SYN flag
- Running the `cmscancel` 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 `cmclodelist`. 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.

Supported browsers

Serviceguard Manager supports the following web browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

For latest information about web browser support, see the latest version of *HPE Serviceguard for Linux Certification Matrix Enterprise Edition* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

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

Software prerequisites for Serviceguard for Linux

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

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

To check if the `xinetd` service is running:

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

To enable the `xinetd` service:

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

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

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

NOTE: On SUSE Linux Enterprise Server, `xinetd` service does not run if no services are configured. This can lead to 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
```

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

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

Red Hat Enterprise Linux	SUSE Linux Enterprise Server
lm_sensors	bash
tog-pegasus	pidentd
authd	libblkid1
krb5-libs	sblim-indication_helper
zlib	sblim-sfcb
libblkid(rhel6)	sblim-sfcc
net-snmp	libnl (SLES 11)
sg3_utils	libnl1 (SLES 12)
sg3_utils-libs	sblim-cmpi-base
xinetd	net-snmp
libnl	sg3_utils
mdadm	xinetd
udev (rhel 6)	mdadm
lsscsi	udev
net-tools	lsscsi
systemd (rhel 7)	net-tools
policycoreutil (for KVM toolkit on rhel6 when SELinux is enforced) ¹	systemd (SLES 12)
checkpolicy (for KVM toolkit on rhel6 when SELinux is enforced) ¹	tog-pegasus (For HPE Metrocluster with Continuous Access EVA P6000)
tog-pegasus (For HPE Metrocluster with Continuous Access EVA P6000)	sqlite
mssql-tools (rhel 7)	dmidecode (SLES 12)
unixODBC (rhel 7)	pmtools (SLES 11)
sqlite	open-vm-tools
dmidecode	open-vm-tools (VMware only, SLES11 SP4, SLES12, and their respective later releases) ²
open-vm-tools (VMware only rhel7 and their respective later releases) ²	mssql-tools (SLES 12)
	unixODBC (SLES 12)

¹ 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.

² On SLES11 SP4, SLES12, RHEL7 and their respective later releases open-vm-tools are bundled along with distributions. For installation of VMware tools you may refer Installing and Configuring VMware Tools document at <https://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf>.

For latest information about Java on each Linux OS, see the latest version of *HPE Serviceguard for Linux Certification Matrix Enterprise 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 Enterprise 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.

Installing Serviceguard for Linux

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

- **Installing Serviceguard for Linux using `cminstaller`** on page 31
- **Installing or upgrading Serviceguard for Linux using HPE Software Delivery Repository** on page 36
- **Installing Serviceguard for Linux using `cmeasyinstall`** on page 33
- **Installing Serviceguard for Linux the traditional way** on page 35

If Serviceguard version earlier than A.12.00.00 is installed, follow the instructions described in the **Performing rolling upgrades of Serviceguard versions** on page 50 section to upgrade to latest version.

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 all the components that are part of the Serviceguard for Linux Enterprise edition (Red Hat Enterprise Linux 6, 7 and SUSE Linux Enterprise Server 11, 12).
- Starting Serviceguard 12.00.00 legacy packages are obsolete. If you have configured legacy packages, you must migrate to modular packages before you move to 12.00.00. For more information about how to migrate to modular packages, see the white paper *Migrating packages from legacy to modular style* available at <http://www.hpe.com/info/linux-serviceguard-docs>.

Installing 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.

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 and PYTHON-BASE Version 2.X 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 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.



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

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

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

```
node1:~ # cmviewcl  
unable to receive reply from local cmclconfd  
Connection timed out Unable to initialize `HOSTNAME_ADDRESS_FAMILY`
```

Then, there is a problem with `xinetd` service. To enable `xinetd` service, see **Software prerequisites for Serviceguard for Linux**.

NOTE: The `cinstaller` does not install Serviceguard Metrocluster with Continuous Access EVA P6000 for Linux Enterprise on SUSE Linux Enterprise Server version 11. You need to do the following:

1. Install `tog-pegasus rpm`:

```
#rpm -ivh --nodeps tog-pegasus-2.8.0-3.5.x86_64.rpm
```

For more information about `tog-pegasus rpm` version, see HPE Serviceguard for Linux Version 12.00.50 Release Notes available at <http://www.hpe.com/info/linux-serviceguard-docs>.

2. Install Serviceguard Metrocluster with Continuous Access EVA P6000:

```
#rpm -ivh
```

```
serviceguard-metrocluster-caevap6000-B.12.00.00-0.sles11.x86_64.rpm
```

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 and PYTHON-BASE Version 2.X and PERL is installed on all the systems where you intend to install Serviceguard using the `cmeasyinstall` tool.
- Ensure that YUM (Yellowdog Updater Modified) update service on Red Hat Enterprise Linux Server or Zypper on SUSE Linux Enterprise Server is configured, if you intend to use the `-a` option.

NOTE:

- The `cmeasyinstall` tool does not install 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.



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

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

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

```
node1:~ # cmviewcl  
unable to receive reply from local cmclconfd  
Connection timed out Unable to initialize `HOSTNAME_ADDRESS_FAMILY`
```

Then, there is a problem with `xinetd` service. To enable `xinetd` service, see **Software prerequisites for Serviceguard for Linux**.

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

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

NOTE: 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.

NOTE: The `cmeasyinstall` does not install Serviceguard Metrocluster with Continuous Access EVA P6000 for Linux Enterprise on SUSE Linux Enterprise Server version 11 when you are using `-a` option. You need to do the following:

1. Install tog-pegasus rpm:

```
#rpm -ivh --nodeps tog-pegasus-2.8.0-3.5.x86_64.rpm
```

For more information about tog-pegasus rpm version, see HPE Serviceguard for Linux Version 12.00.50 Release Notes available at <http://www.hpe.com/info/linux-serviceguard-docs>.

2. Install Serviceguard Metrocluster with Continuous Access EVA P6000:

```
#rpm -ivh
```

```
serviceguard-metrocluster-caevap6000-B.12.00.00-0.sles11.x86_64.rpm
```

Installing Serviceguard for Linux the traditional way

If you do not wish to install using the `cmeasyinstall` tool, you must install the Serviceguard for Linux and its components manually in the same order as described in **Packaging information** on page 8 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 Enterprise edition:

Table 2: DVD directory structure for Serviceguard for Linux Enterprise edition

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

Table Continued

SUSE Linux Enterprise Server 11	<pre><DVD-mount-path>/SLES/SLES11/Serviceguard/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES11/SGManager/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES11/SGeSAP/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES11/Toolkit/noarch/<*.rpm> <DVD-mount-path>/SLES/SLES11/Metrocluster/x86_64/<*.rpm></pre>
SUSE Linux Enterprise Server 12	<pre><DVD-mount-path>/SLES/SLES12/Serviceguard/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES12/SGManager/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES12/SGeSAP/x86_64/<*.rpm> <DVD-mount-path>/SLES/SLES12/Toolkit/noarch/<*.rpm> <DVD-mount-path>/SLES/SLES12/Metrocluster/x86_64/<*.rpm></pre>

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 SUSE Linux Enterprise Server 11:

```
rpm -ivh serviceguard-A.12.XX.YY-0.sles11.x86_64.rpm
```

On SUSE Linux Enterprise Server 12:

```
rpm -ivh serviceguard-A.12.XX.YY-0.sles12.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, SUSE Linux Enterprise Server 11 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.

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](#) on page 8.

- 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 Enterprise edition	SGLX_00xxc.iso

For latest information on supported OS for updates, see the latest version of *HPE Serviceguard for Linux Certification Matrix Enterprise 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_00xxc.iso` bundle for Serviceguard for Linux Enterprise 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/repomd.xml
<dist>/<distro_version>/repodata/filelists.sqlite.bz2
<dist>/<distro_version>/repodata/filelists.xml.gz
```

```

<dist>/<distro_version>/repodata/other.sqlite.bz2
<dist>/<distro_version>/repodata/primary.sqlite.bz2
<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>/Serviceguard/x86_64/\
serviceguard-xdc-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>/QuorumServer/x86_64/\
serviceguard-qs-A.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-sybase-toolkit-A.12.10.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-oracle-toolkit-A.12.20.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/SGeSAP/x86_64/\
serviceguard-extension-for-sap-B.12.20.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-kvm-toolkit-A.12.10.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-dataguard-toolkit-A.12.20.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-ppas-toolkit-A.12.10.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-db2-toolkit-A.12.20.00-00.<dist>.noarch.rpm
<dist>/<distro_version>/Toolkit/noarch/\
serviceguard-extension-for-mssql-A.12.20.00-0.<dist>.noarch.rpm
<dist>/<distro_version>/Metrocluster/noarch/\
serviceguard-metrocluster-3parrc-B.12.20.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Metrocluster/noarch/\
serviceguard-metrocluster-caevap6000-B.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Metrocluster/noarch/\
serviceguard-metrocluster-caxpp9000-B.12.10.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Metrocluster/noarch/\
serviceguard-metrocluster-emcsrdf-B.12.20.00-0.<os_version>.x86_64.rpm
<dist>/<distro_version>/Metrocluster/noarch/\
serviceguard-metrocluster-addons-B.12.10.00-0.<os_version>.x86_64.rpm

```

where:

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

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

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

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

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

4. Install or upgrade Serviceguard for Linux Enterprise 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 causing downtime to your applications. 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 6.x, Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11, or SUSE Linux Enterprise Server 12).
- The node must be running a supported release of Serviceguard.

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

- 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 and SUSE Linux Enterprise Server 11 to SUSE Linux Enterprise Server 12.
- 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** on page 43 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 Manger during major or minor OS rolling upgrade may lead to unexpected behavior. Use Serviceguard Manger 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 Enterprise 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: `/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** on page 8.
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 Enterprise 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/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. If this rpm is not updated, Serviceguard commands will fail after you reboot the node.

- b. After the node is rebooted, verify the cluster status using `cmviewcl`, and also verify all file systems with `fsck`.

- c. Restart Serviceguard on this node using `cmrunnode`. Check that the node joins the cluster successfully, and if necessary, move the packages back onto the node.
- d. Edit the following file to include the line:`AUTOSTART_CMCLD = 1`
For Red Hat Enterprise Linux: `/usr/local/cmcluster/conf/cmcluster.rc`
For SUSE Linux Enterprise Server: `/opt/cmcluster/conf/cmcluster.rc`
- e. Check if `sgmgr` service is running on the node:
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 `cmruncl` 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 `cmapplyconf` command to reconfigure the package.

```
#cmgetconf -p pkg1 pkg1.ascii
#cmapplyconf -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.
 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.

Note: Rolling upgrade of a solution involving HPE Serviceguard Toolkit for Oracle Data Guard requires additional steps to be completed along with above steps. Refer to the **Rolling upgrade of a cluster running HPE Serviceguard Toolkit for Oracle Data Guard** section for detailed instructions and steps for Oracle Data Guard setup.

Major OS rolling upgrade of two node cluster running HPE Serviceguard for Oracle Data Guard

This is an example procedure to upgrade major OS of a two node cluster running HPE Serviceguard toolkit for Oracle Data Guard. The configuration consists of Oracle Data Guard configuration with a production database on the first node and the standby database on the second node. Both the nodes (node1 and node 2) of the cluster are running on SLES11 SP4 operating system with Oracle Data Guard. This is an example procedure to upgrade the node1 OS version from SLES11 SP4 to SLES12 SP2.

Here, node1 is configured for primary DB and node2 is configured for secondary DB and consists of three packages, that is, primary DB package, standby DB package and role management package running across two nodes.

- Example Role Management Package name - DG1_RM
- Example Primary Database/DB1 Package name - DG1_DC1_orcl
- Example Standby Database/DB2 Package name - DG1_DC2_orcl

Procedure

1. Run the `cmmodpkg` command to enable the global switching for the role management package running on node1.

```
# cmmodpkg -e DG1_RM
```

2. Halt the first node.

Halt the node you want to upgrade.

```
# cmhaltnode -f node1
```

The packages on the node failover to the adoptive node. The Serviceguard daemon on node 1 is halted.

3. Edit the `DG1_RM` package configuration and remove the node1 name from the `node_name` section. Remove the node information (`node_name`) from the role management package configuration.

4. Run the `cmcheckconf` command to verify the configuration and the `cmapplyconf` command to apply the configuration of the package.

```
#cmcheckconf -P DG1_RM.conf  
#cmapplyconf -P DG1_RM.conf
```

5. Take a backup of package `DG1_DC1_orcl` configuration and delete it from the cluster configuration.

The package is not required as node1 is being removed for upgrading to newer major OS.

- a. Before deleting the `DG1_DC1_orcl` package, take a backup of the package configuration.

The backup is required when the new OS node is added back to cluster.

```
# cmgetconf -p DG1_DC1_orcl DG1_DC1_orcl.conf.bak
```

- b. Delete the package from the cluster configuration

```
# cmdeleteconf -p DG1_DC1_orcl
```

6. Remove the node1 from the cluster through online reconfiguration of the cluster.

- a. Run the `cmgetconf` command to obtain a current copy of the configuration details of the cluster.

```
# cmgetconf -c sg_odg_cls -C clus.ascii
```

- b. Edit the `clus.ascii` file and remove the node1 information from the ASCII file.


- c. Verify the new configuration

```
# cmcheckconf -C clus.ascii
```

- d. From node2, apply the changes to the configuration and distribute the new binary configuration file to the cluster node.

```
# cmapplyconf -C clus.ascii
```

7. Make a fresh install of the new major OS (SLES12 SP2) on the removed node.

 **TIP:** If required take a backup of the storage, network and Serviceguard related files for reference. Retain the hostname as node1 for upgraded node.

8. Install and configure the required new Serviceguard rpms of SLES12 SP2 version on the new node.

9. Install and configure the required Oracle Data Guard rpms of SLES12 SP2 version on the new node.

10. Configure the required network and storage for joining back to the existing cluster. The configuration must be similar to earlier node which is deleted in step 5.

11. Install and configure the Oracle DB and other software that were installed when the node was running with SLES11 SP4 version. This is required to retain the same configuration as that of earlier.

12. After the required configurations are complete, add the newly installed OS node into running cluster. While adding the node ensure to configure it for standby DB.

- a. Do a `cmquerycl` with newly added node or get the existing cluster configuration and add the node1 information. Specify a new node to be configured and generate a template of the new configuration (all on one line).

```
cmquerycl -C clconfig.conf -c sg_odg_cls -n node1 -n node2
```

- b. Edit `clconfig.conf` to check the information about the new node.

- c. Verify the new configuration.

```
cmcheckconf -C clconfig.conf
```

- d. Apply the changes to the configuration and send the new binary configuration file to all cluster nodes.

```
cmapplyconf -C clconfig.conf
```

13. Rejoin the node to the cluster, which is added in step 12.

```
# cmrunnode -n node1
```

14. Add the node information (`node_name node1`) to the role management package (`DG1_RM.conf`) configuration and add the `DG1_DC1_orcl` package back to cluster through online reconfiguration.

```
#cmapplyconfconf -P DG1_RM.conf -P DG1_DC1_orcl.conf.bak
```

15. Run the `DG1_DC1_orcl` package.

```
# cmrunpkg DG1_DC1_orcl
```

NOTE: Post this step the newly added node must be in a position to take back the primary role for Oracle DB with SLES12 SP2 OS.

16. Halt the second node (`node2`) and move the packages from `node2` to `node1`. Make sure that the packages are failed over successfully and the Oracle is started successfully before upgrading the next node to newer OS version.

```
#cmhaltnode -f node2
```

17. Follow the steps as described for `node1` to upgrade the `node2` to SLES12 SP2 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 cmupgrade tool	Rolling upgrade the traditional way	Offline upgrade
To upgrade from A.12.00.X to A.12.20.Y, see <u>Rolling upgrade from 12.00.X to 12.30.X</u> on page 58.	Yes	Yes	Yes
To upgrade from A.11.19.X to A.12.20.00, see <u>Rolling upgrade from 11.19.X to 12.20.00</u> on page 56.	No	Yes	Yes
To upgrade from A.11.18.X to A.12.20.00, see <u>Performing offline rolling upgrade from 11.18.X to 12.20.00</u> on page 57.	No	No	Yes
To upgrade from A.11.20.X to A.12.20.00 or from A.11.20.X to A.12.20.Y, see <u>Rolling upgrade from 11.20.X to 12.20.00</u> on page 51.	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 12.30.X** on page 58
- **Rolling upgrade from 11.20.X to 12.20.00** on page 51

- [Rolling upgrade from 11.19.X to 12.20.00](#) on page 56
- [Performing offline rolling upgrade from 11.18.X to 12.20.00](#) on page 57
- [Rolling upgrade from A.11.19.X to A.12.20.X](#) on page 65
- [Offline rolling upgrade from A.11.18.X to A.12.20.X](#) on page 65

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](#) on page 51
- [Upgrading Serviceguard for Linux the traditional way](#) on page 52
- [Upgrading Serviceguard for Linux using YUM or Zypper](#) on page 53

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 Enterprise 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 PERL is installed on the system to run the `cmupgrade` tool.
- Ensure that you run the `cmupgrade` tool on all the nodes that are part of the cluster.
- Ensure that the 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](#) on page 35.

NOTE: Installation of Serviceguard Manager for Linux B.12.20.00 (Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 12) 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** on page 8.

For example, Serviceguard rpm for Red Hat 6 x86_64

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

NOTE:

- To upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:
 - *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes*
 - To upgrade `servicgurad-xdc` prior to version A.11.20.20: `rpm -Uvh --nopreun <xdc-rpm-name>`
-

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** on page 8.

For example, Serviceguard rpm for Red Hat 6 x86_64

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

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

HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes

- ❗ **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 Enterprise edition using YUM or Zypper. You must upgrade in the same order as described in the **Packaging information** on page 8 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.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

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

For example, `#cmhaltnode -f node1`

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

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

where:

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

`<distro_major_ver>` is the value that can be either Red Hat 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** on page 55.

- 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
```

- 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.

- To upgrade serviceguard-manager rpm:

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

- Repeat steps from 2 to 8 for all the nodes.
- 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:

- 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`

- 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.

- Run the following command:

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

- 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
```

- 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>.

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** on page 8.

For example, Serviceguard rpm for Red Hat 6 x86_64

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

NOTE:

- When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:
 - *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes*
- 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** on page 53

7. Restart cluster on first node.

For example, `# cmrunnode -n node1`

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

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

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 `pidntd` rpm.

```
#rpm -e --nodeps pidntd-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** on page 8.

For example, Serviceguard rpm for Red Hat 6 x86_64

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

NOTE:

- When you upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:
 - *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes*
 - *HPE Serviceguard Toolkit for SAP Sybase ASE and SAP Sybase Replication Server for Linux Release Notes*
 - *HPE Serviceguard Toolkit for Oracle on Linux Release Notes*
- 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** on page 53.

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

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

```
#cmruncl
```

Rolling upgrade from 12.00.X to 12.30.X

You can perform rolling upgrade of Serviceguard for Linux from A.12.00.XX to A.12.30.YY 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** on page 58
- **Upgrading Serviceguard for Linux using `cmupgrade` tool** on page 60
- **Upgrading Serviceguard for Linux the traditional way** on page 61
- **Upgrading Serviceguard for Linux using YUM or Zypper** on page 62

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 and PYTHON-BASE Version 2.X 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 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 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](#) on page 35.

NOTE: Installation or upgrade of Serviceguard Manager on Linux B.12.20.00 (Red Hat Enterprise Linux 6 and 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.

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>.

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>.

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>.

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** on page 8.
- For example, Serviceguard rpm for Red Hat 7 x86_64:

```
#rpm -Uvh serviceguard-A.12.20.00.Y-0.rhel7.x86_64.rpm
```

NOTE:

- To upgrade toolkits, use `rpm -Uvh` with appropriate qualifiers. For more information about qualifiers, see the following documents available at <http://www.hpe.com/info/linux-serviceguard-docs>:
 - *HPE Serviceguard Toolkit for Enterprise DB PPAS for Linux Release Notes*
- To upgrade `servicgurad-xdc` prior to version A.11.20.20: `rpm -Uvh --nopreun <xdc-rpm-name>`

! **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** on page 35.

- 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 or Zypper on SUSE Linux Enterprise Server, you can upgrade Serviceguard for Linux Enterprise edition using YUM or Zypper. You must upgrade in the same order as described in the **Packaging information** on page 8 section.

NOTE: Ensure that major version of Serviceguard is installed before you upgrade to update release.

On Red Hat Enterprise 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:

```
[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 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>**.
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](#) on page 35.

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:

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

The `cmmodpkg` command enables switching of the package.

For example, `#cmmodpkg -e pkg1`

2. Halt first node.

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

For example, `#cmhaltnode -f node1`

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

3. Create a `/etc/zypp/repos.d/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 extracted update release location.

4. 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** on page 35.

8. Restart cluster on first node.

For example, `#cmrunnode -n node1`

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

9. Repeat steps from 2 to 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** on page 56.

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** on page 57.
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 12.30.X** on page 58.

Upgrading Serviceguard for Linux packages

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

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:1vn1z1o1x8e1vnw1vn61x8g1z1u1vn4"/></Set>
<Set name="KeyManagerPassword"><Property name="jetty.keymanager.password"
default="OBF:1u2u1wml1z7s1z7a1wn1lu2g"/></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:1vn1z1o1x8e1vnw1vn61x8g1z1u1vn4"/></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.

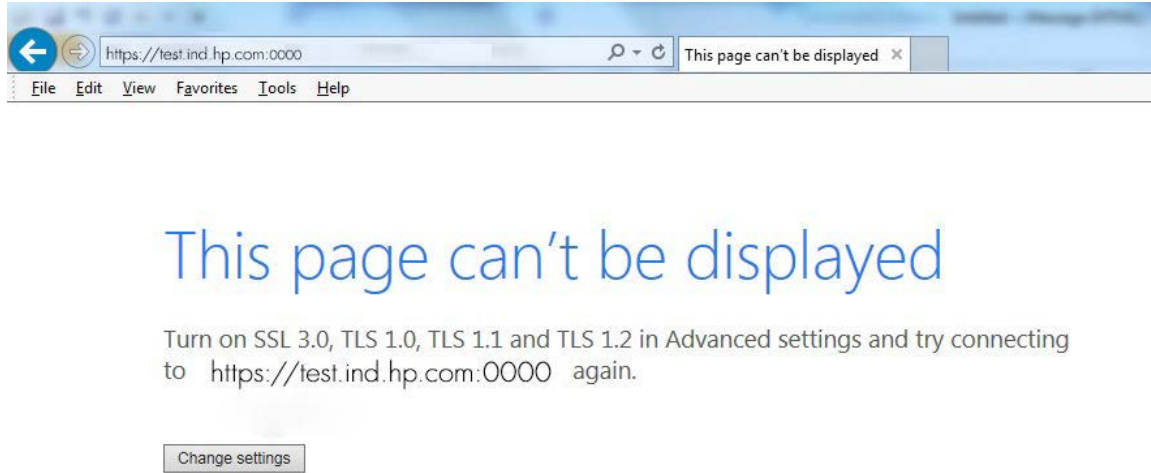


Figure 1: Error while accessing Serviceguard Manager

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:



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.

Related information

The latest documentation for HPE XP Storage Plug-in for VMware vCenter is available at <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). 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.