Hewlett Packard
Enterprise

HPE Serviceguard for Linux 15.00.01 Release Notes

Part Number: 10-173010-150001
Published: Mar 2023

Contents

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

Overview

This document provides release information about HPE Serviceguard for Linux version 15.00.01

Supported platforms and Linux distributions

HPE Serviceguard for Linux v15 is available on the following Linux distributions:

- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- Oracle Linux 7 (Unbreakable Enterprise Kernel Only)
- Oracle Linux 8 (Unbreakable Enterprise Kernel Only)
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15

NOTE: For more information about supported updates, supported hardware, storage, and other information, see the latest version of HPE Serviceguard for Linux Certification Matrix at https://www.hpe.com/info/sglxsupportmatrix/.

HPE Serviceguard for Linux updates

Features introduced in this version

This version of HPE Serviceguard for Linux introduces:

- Support for Red Hat Enterprise Linux 9.1

Features introduced in A.15.00.00

This section describes the new features and capabilities added in HPE Serviceguard for Linux 15.00.00:

- New workload centric monitoring and administration through Serviceguard Manager+
- Workload mobility across hybrid environment
- Disaster Recovery (DR) rehearsal for workloads
- Support for quarantine and accelerated failover in SAP HANA multitarget deployments
- Cloud enablement on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)
- New and simplified product and licensing structure
- Pre-install and pre-configure checks and validation tool
- Determine the License requirements
- Unix Domain Socket (UDS) based user authorization for Serviceguard commands
- Integration with Zerto

NOTE: For detailed information about Serviceguard for Linux features and solutions, see the following documents available at **https://www.hpe.com/info/linux-serviceguard-docs**

- HPE Serviceguard for Linux Concepts Guide
- HPE Serviceguard for Linux Operational Guide for Workloads and Solutions

New workload centric monitoring and administration through Serviceguard Manager+

Serviceguard Manager+ (note + sign) is a new look workload driven UI that captures various aspects related to workloads running across datacenters spread across on-premise or cloud. Use the Serviceguard Manager+ to discover workloads deployed on on-premise or cloud and monitor them from a single pane.

Serviceguard Manager+ provides capability to monitor replication health of SAP HANA System Replication (HSR), Oracle, and Microsoft SQL Server on Linux Availability Groups. Monitoring capability is also available for workloads that use storage-based replication.

You can use the Serviceguard Manager+ for administrative operations for select workloads such as:

- Start/Stop for SAP HANA Database workloads
- Configuring recovery site for Oracle workloads

NOTE: The traditional Serviceguard Manager UI will continue to be available with 15.00.00 for cluster and package administrative operations till these capabilities are added in subsequent releases of Serviceguard for Linux to Serviceguard Manager+.

Workload mobility across hybrid environments

Serviceguard now supports movement of Oracle and SAP HANA workloads using Serviceguard Manager+ and command line interface options for other workloads. Using Serviceguard Manager+, you can now move workloads to an adoptive node and perform activities such as maintenance or upgrades on active nodes and failback workloads after completing these operations. For other applications one can use command line interface to move workloads from one site to another.

Disaster Recovery rehearsal for Workloads

Serviceguard supports Disaster Recovery (DR) rehearsal for Oracle workloads from Serviceguard Manager+. You can use command line interface for performing rehearsal (fire-drill) for workloads deployed in push-button recovery environments.

Support for Quarantine and Accelerated failover in SAP HANA Multitarget deployments

Serviceguard Quarantine is a feature of the Serviceguard SAP Add-On. It enables a set of accelerated failover capabilities for SAP HANA environment and optionally integrates with HANA as SAP ha_dr_provider to receive SAP-reported software failures fast and reliably. It avoids HANA instance shutdown and fencing delays during failover.

- HPE Serviceguard for Linux 15.00.00 extends support of all previously available Quarantine functionality to multi-target HANA scale-up environments. Quarantine failover is possible from tier-1 to any of the tier-2 or tier-3 targets. Accelerated failover is also available from tier-2 to tier-3 targets to restore valid failover targets and connected replication streams as fast as possible.
- The ha_dr_provider integration can now be restricted to incidents that impact specific tenants. It can also be extended to non-indexserver process issues.
- In scale-up environments, primary instance process restarts can be triggered for failed software components as fallback strategy if no valid failover target host is available in the cluster in the moment a failure happens. The same fallback can be used if valid failover targets are only available in a remote site, effectively restricting automatic failovers due to software failures to a single datacenter if possible.
- The *cmpushpkg* command got extended with an option that makes use of HANA-halt-detach and Quarantine to enable simple and accelerated changes to the replication connection topology as part of workload placement operations including complex near-zero-downtime rolling kernel upgrade procedures (nZDT rku).
- The *cmsaphdb* command status output got reworked to provide more straight-forward access to information about Quarantine, HANA-halt-detach and double primary resolution states of the cluster.

Cloud enablement on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)

HPE Serviceguard for Linux supports configuring cloud instances as cluster nodes using Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)

The cloud instances as cluster nodes can be deployed as:

- Across availability zones within in a cloud region
- Across cloud regions

New and simplified product and licensing structure

Product Structure

HPE Serviceguard for Linux 15.00.00 is available in two foundational editions:

- HPE Serviceguard for Linux High Availability (HA) E5 edition
- HPE Serviceguard for Linux High Availability (HA) plus Disaster Recovery (DR) E7 edition

Table 1: SGLX Foundational licenses

Sr. No.	SGLX Edition / License Name	Feature
1	HA-E5	• Serviceguard High Availability • Single Target Replications like HANA Scale-up • Zero RPO • Serviceguard Integration with Db2, KVM, Postgres and Sybase Workloads
2	HA-DR-E7	All the features supported with HA-E5, plus Disaster recovery Features: • Hybrid Deployments • RPO sensitive deployment • DR Rehearsal • Multi Target Replication • Scale-Out • Workload Mobility

HPE Serviceguard for Linux 15.00.00 also offers out-of-the-box application integrations through application specific Add-ons. The following Add-On available currently:

- HPE Serviceguard for Linux SAP Add-On (includes SAP NetWeaver, SAP S/4 HANA (application tier), and NFS)
- HPE Serviceguard for Linux Oracle Add-On
- HPE Serviceguard for Linux Microsoft SQL Server Add-On
- HPE Serviceguard for Linux NFS Add-On
- HPE Serviceguard for Linux Flex Storage Add-On

Other workloads Add-Ons: IBM Db2, Sybase, EnterpriseDB PPAS and KVM

These Add-Ons can be configured with E5 or E7. The *cminstaller* tool has been enhanced to install based on the selected workloads and upgrade the product based on the deployed workloads. It has both interactive and non-interactive options.

Licensing Mechanism

The licensing mechanism with A.15.00.00 is based on the number of cores present in the server for deployments on physical systems and number of vCPUs present in the Virtual Machine for deployments on VMs.
The licensing for Flex-Storage-Add-on will continue to be on per-instance basis.

The Instant-on license will be activated after the product is installed, with a validity of 60 days. You can apply valid licenses within 60 days to continue using the product. You can apply the license post validation expiry, but HPE recommends renewing or applying license before expiry for normal product functioning.

License Expiry Notification,
Renewal reminders begin 90 days before the expiry. Product provides the alert messages on CLI, GUI and E-Mail alerts based on configuration.

Post expiry of Licenses,

- Cluster administration commands such as *cmapplyconf*, *cmrunnode*, *cmruncl* and others are blocked.
- The failover capability will be blocked after an additional buffer time of 30 days.
- All the capabilities will be restored once valid licenses are applied.

Pre-Install and Pre-configure checks & validation tool

You can now perform pre-requisite checks on the nodes where Serviceguard for Linux is planned to be installed and configured. This will prevent detecting issues like dependencies, invalid operating system distribution, unavailability of ports, etc. after the product is installed.

Pre-requisite checks can be

- Invoked as part of *cminstaller* available in the Serviceguard for Linux Software or
- Downloaded standalone from here and run individually, to help validate the preparedness of environment even before downloading the Serviceguard for Linux Software.

Determine the License requirements

With the change in Licensing Mechanism with A.15.00.00. The command / script *cmmaplicense* provides with a mapping of SGLX licenses applied on existing cluster solutions based on SGLX version 12.XX.YY with the new SGLX version 15.00.00.

cmmaplicense provides with:

- Type of SGLX License Editions, add-ons required based on workloads configured.
- Required number of SGLX Licenses for each Node in the cluster.

cmmaplicense is also available at following location, in addition to the above. It provides with the capability of determining the licensing requirements for fresh SGLX environments also.

UDS based user authorization for Serviceguard commands

HPE Serviceguard for Linux has been using identd protocol to validate the users when Serviceguard commands are executed. With HPE Serviceguard for Linux A.15.00.00, a new method for user validation is introduced where users will be validated using Unix Domain Socket (UDS) on the local system. This enables Serviceguard commands to use SSL method for further communication amongst the trusted nodes only

- This method is supported for TLS version 1.3
- This method provides:
  - An alternative to identd method of user validation
  - Secure communication compared to identd, which is unencrypted

- This method is enabled by default from RHEL9. For prior supported versions, one can enable it optionally
- The SSL certificates needed to perform the SSL communication will be generated during the installation.
- You can also configure email alerts to notify expiration of the certificates.

Integration with Zerto

HPE Serviceguard for Linux integration with Zerto allows recovering the Serviceguard monitored workloads seamlessly when Zerto push button recovery is performed. When you chose to recover the compute using Zerto, Serviceguard for Linux continues to protect availability and data integrity of the applications,

- HPE Serviceguard for Linux integration with Zerto also allows for creating tagged checkpoints for Oracle workloads, allowing workload aware Disaster Recovery in Zerto environment.

Deprecated or obsolete features

- Starting with HPE Serviceguard for Linux release 15.00.00, Web-Based Enterprise Management (WBEM) method of monitoring will no longer be available. You can continue using Simple Network Management Protocol (SNMP-based) tools for cluster, package, node monitoring and event indications.

- The SGeSAP storage connector for SAP HANA host auto failover is getting obsolete as part of HPE Serviceguard for Linux release 15.00.00. Alternative technologies are available from virtual machine vendors.

Known problems and limitations

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

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

   Workaround

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

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

   Workaround

   This issue has been fixed with multipath-tools-0.7.3+102+suse.be95116-3.7.1.x86_64 and later. Ensure that you install this or the later version to avoid this issue.

3. Under certain scenarios, the Serviceguard daemons such as cmcld, cmproxy and qsc may fail to start and generate the following message:
   "Could Not/Failed To Set Realtime Priority"

   Workaround

   To resolve this issue, see the customer advisory available at https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00069245en_us

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

   Workaround

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

5. The sg_persist commands report false return status for certain operations in SLES15.

   Workaround

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

6. IN533111: Global switching for halted package is re-enabled unexpectedly. This issue occurs in clusters with package dependency configurations. It typically occurs in SGeSAP scale-up HANA clusters, where a primary and a secondary HANA package have a mutual exclusion dependency that prevents them from running on the same node.

   Workaround

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

7. IN480961: When multiple VGs based on VMFS type disks are configured in the package, the package may fail back to the node on which it was running. When multiple VGs are configured on VMFS disks, the attach of these disks may take significant time. If the node where package was running had `AUTOSTART_CMCLD` configured as 1, node will join back the cluster and will be eligible to run the package. This will cause volume group tags check on the node where the package is still starting to fail. Package will then move back to the node where it was running earlier.

8. Cross-subnet configurations for SAP are only available for HANA two-instance scale-up.

9. Multi-target HANA clusters do not support the Safesync feature and Multi-SID environments.

10. Clustering of more than one scale-out HANA system of a HANA Multi-SID installation is not supported within the same cluster.

11. HANA scale-out configurations of more than 32 nodes with synchronous or syncmem System Replication configuration must activate the Serviceguard Safesync feature as replication status monitoring method.

12. The general usage of Instance Quarantine as method for HANA primary package failover

(hdb_instance_stop_with_package_failover using_quarantine parameter setting) is not supported in SAP host auto failover (HANA with cold standby node) scale-out configurations. Independent from this, configurations with cold standby can make use of Instance Quarantine for the special use case of a switch_on_indexserver_failure setting in HANA global.ini. Manually triggering instance detach is supported in such setups.

13. Due to limitations in Linux loopback mount handling, clusters that may run a HA NFS package and a Serviceguard SAP Add-On package on the same cluster nodes are not supported with NFSv4.

14. The possibility to do a package failover or a site switch in reaction to a HANA indexserver failure depends on notification events from the SAP HANA nameserver. In multiple failure cases where an indexserver and the active master nameserver fail at the same time, no notification will be sent. If the HANA instance is configured to repair itself by restarting a failed indexserver, it will attempt to do so. If the HANA instance fails to repair itself, the standard package failover/site-switch is triggered afterwards.

15. SAP HANA packages currently do not support csh default shell for sidadm.

16. Graceful Shutdown of HANA packages with Instance Quiescing is only supported for SAP Netweaver instances on Suse/Redhat Linux hosts. Windows application servers are not covered.

17. During upgrade of serviceguard-kmod rpm following error might be logged.
"*serviceguard-kmod-A.15.00.00-0.rhwarning: file /usr/local/cmcluster/drivers/RHEL9/deadman.ko: remove failed: No such file or directory*"
This warning can be ignored.

18. In some scenarios, Serviceguard deadman module might fail to load after reboot post RHEL9.0 to RHEL9.1 upgrade. This could happen if SELinux policy is set to Enforcing.

    Workaround

    Post reboot execute below commands.

    # depmod -a
    # systemctl restart SGSafetyTimer.service

Troubleshooting & Workaround

- Ensure that java version 1.8 is installed on all the systems where you intend to install Serviceguard software. Also ensure that a soft link of /usr/bin/java is pointing to JDK 1.8 version.

  NOTE: On some operating systems, like RHEL8.6 and later, the rpm database may not be properly updated with java version even though OpenJDK 1.8 version is installed on the system. In this case, the user needs to first install the default java (Ex: java-11-openjdk) software by using *"yum install java"* command and later install the java-1.8.0-openjdk version using *"yum install java-1.8.0-openjdk"* command. Post this step user must change the soft link of java to point to Open JDK 1.8 version.

  An example to create a soft link is *ln -s /etc/alternatives/java /usr/bin/java* or use the command *"alternatives --config java*" and choose the Command path which provides the java-1.8.0-openjdk.

  Example output of soft links is shown below:

  [root@node1 ~] # file /usr/bin/java

  /usr/bin/java: symbolic link to /etc/alternatives/java

  [root@node1 ~] # file /etc/alternatives/java

  /etc/alternatives/java: symbolic link to /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.322.b06-9.el9.x86_64/jre/bin/java

Installing / Upgrading Serviceguard for Linux

For information on pre-requisites, installation and upgrade of Serviceguard for Linux, see the *HPE Serviceguard for Linux Operational Guide for Workloads and Solutions* guide available at
http://www.hpe.com/info/linux-serviceguard-docs

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
https://www.hpe.com/info/sglxsupportmatrix/

Checksum information

The table below provides checksum information for HPE Serviceguard for Linux bundles

Checksum reported here is obtained via running the command “sha256sum <ISO image or tar file>”.

Example:

To verify checksum of A.15.00.00 bundle (SGLX_150000.iso)

a) Download required bundle and execute the command “*sha256sum*” by providing the path to downloaded bundle as an argument:

```
# sha256sum SGLX_150000.iso
a4a96c619816c7ee1dff06d8230370f89a085eef565b74e6e7c198139cea4d1d  SGLX_150000.iso
```

b) Output in first column of above command “a4a96c619816c7ee1dff06d8230370f89a085eef565b74e6e7c198139cea4d1d” is the checksum for the given file (SGLX_150000.iso) and this value is expected to match with the value mentioned in table below for A.15.00.00

Table 2: HPE Serviceguard for Linux Release, Updates, Patch Checksum information

SGLX Version	Checksum
A.15.00.01	“9b88c7f2647a74f99fd72aed47e8db31bcff68c4478772b5bad489d2fc60afed”
A.15.00.00	“a4a96c619816c7ee1dff06d8230370f89a085eef565b74e6e7c198139cea4d1d”

Open-source software components

The source code of the open-source software binaries used by Serviceguard Manager are available in the below location
https://github.com/HewlettPackard/serviceguard/tree/master/sglx_serviceguardmanager

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the **Feedback** button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. All document information is captured by the process.