GuardianOS Version 7.7.236 Release Announcement

April 2021

Preface

This Product Information Bulletin announces the release of GuardianOS® Version 7.7.236 for selected SnapServer® systems.

Models Affected

GuardianOS Version 7.7.236 supports the SnapServer XSR Series™ appliances (XSD 40, XSR 40, and XSR 120), the SnapExpansion XSR™, the SnapServer DX Series™ appliances (DX1 and DX2), and the SnapExpansion DX.

IMPORTANT: For SnapServer DX1 or DX2 appliances, this version of GuardianOS is only supported as an upgrade for GuardianOS 7.2.130 or later. For servers running older versions of GuardianOS, you must first upgrade to GuardianOS 7.2.132. Do NOT attempt to upgrade to 7.2.130!

Upgrade Considerations

When upgrading to GuardianOS 7.7.236, there are a few factors to consider before performing the upgrade:

- Backup the system prior to any GuardianOS upgrade.
- Reboot the system prior to any GuardianOS upgrade to ensure the server starts the upgrade from a clean state.
- After upgrading, it is recommended that a disaster recovery image be created to ensure the recovery of the system should a hardware failure occur.
- For servers running older versions of GuardianOS, upgrade to GuardianOS 7.2.132 first. Do NOT attempt to upgrade to 7.2.130!

Downgrades are Not Supported

As with all previous GuardianOS releases, downgrades are not supported.

GuardianOS 7.7.236 Changes and Enhancements

The following changes are included since the previous GuardianOS 7.7 release (7.7.236):

- Support for Veeam 10 and 11 backup repository functionality.
- Redirected noisy sudo logging out of the main Event Log.
- Fix for diagnostic log collection on systems in DynamicRAID mode with large drives.
- Fix for a rare access denied message when opening a file over SMB in Windows.
- Fix for an error submitting support case information in Maintenance > Support.

- Fix for an issue writing files over SMB that originated from servers running GOS 8.x.
- Improved chassis fan monitoring on XSD40 to prevent erroneous fan failure errors.

Previous GuardianOS 7.7 Changes and Enhancements

This is a cumulative release and includes all upgrades, feature enhancements, and bug fixes from previous GuardianOS 7.7 releases:

- Fixed a problem causing erroneous "Disk is too small to add as a member" and "New disk detected" messages when growing a DynamicRAID storage pool by replacing members with larger drives. The fix prevents the problem from occurring and should be applied before attempting to grow a storage pool using this procedure. The fix will not repair a system that has already exhibited the problem—contact Tech Support if this occurs.
- Fix for the occasional RDX job failure due to timeouts.
- Miscellaneous fixes for other rare problems.
- Several improvements to Snap ECR stability and functionality.
- Fix for Samba remote code execution vulnerability CVE-2017-7494.
- Several fixes for Active Directory domain controller discovery for more reliable authentication and clock synchronization.
- RDX Backup Schedules allows the user to backup selected directories to a specific cartridge at a specific time. This provides a means of generating off-site backups without interrupting working day operations.
- Snap ECR now retains sparseness when replicating files.
- High capacity native SAS drives larger than 1.8TB are supported. GuardianOS 7.7.220 or higher is required for use of these larger drives.
- Internet Explorer now loads the web management interface in standard view rather than compatibility view (addressing a number of rendering problems in some versions of Internet Explorer).
- Snap ECR updated to v1.4 for future compatibility with SnapScale clusters.

  NOTE: ECR 1.4 is not compatible with ECR 1.3. All source/target peers running ECR 1.3 must be upgraded to ECR 1.4 to maintain replication functionality.

- Workaround for Snap EDR master consoles to address agent certificate renewal failures. See Snap EDR SSLv3 for Agent Registration and Certificate Updates for details.
- Fixes for various security vulnerabilities.
- Snap ECR™ (Snap Encrypted Continuous Replication™) – GuardianOS 7.7 introduces the Snap ECR feature which supports point-to-point near continuous replication over an encrypted connection.
- SnapSync™ – Also new in GuardianOS 7.7 is SnapSync version 2.3.4, a replacement of Sync 2.2.5 included in previous GOS releases. SnapSync is fully compatible with other Sync clients of the same version, and on upgrade to GOS 7.7 existing Sync installations are updated in place with all configuration preserved.
- Simplified Default Windows ACL – The Windows ACL created on new volumes has been simplified for easier file sharing between different users. Existing volumes are unaffected.
- Phone home and phone home commands are available in the CLI.
- Added support for 3TB RDX cartridges.
- SSM has been re-branded from "SnapServer Manager" to "SnapStorage Manager" to reflect enhancements to manage all Snap products.

  NOTE: When installing SnapStorage Manager on a system that has SnapServer Manager already installed, uninstall the existing installation first or install it in a different directory.

Snap EDR SSLv3 for Agent Registration and Certificate Updates

NOTE: This section is for EDR Administrators.

Snap EDR requires SSLv3 to be enabled on the master console SnapServer when registering agents and updating certificates. However, SSLv3 is disabled by default in GuardianOS for security compliance and compatibility with current browsers that block HTTPS access to servers that support SSLv3.

Enable SSLv3 to Register New Snap EDR Agents

SSLv3 can be temporarily enabled on the master console SnapServer when registering new Snap EDR Agents and disabled afterward if necessary:

1. Connect to the **master console SnapServer** at http://<servername_or_IP>/sadmin/debug.cgi, and login with administrative credentials.
2. Enter the following in the **Command box** to enable SSLv3:

   ```
   cli sslv3 set enable=yes
   ```

3. Click OK.
4. Install and register **new agents** as usual.
5. Enter the following in the **Command box** to disable SSLv3:

   ```
   cli sslv3 set enable=no
   ```

6. If necessary, reboot the **master console SnapServer** to restore access to the Web Management Interface.

Certificate Expiration on Legacy Snap EDR Installations

Older Snap EDR installations used certificates with annual expiration dates to validate agent and master console identities. Certificates near the expiration date were replaced using SSLv3 to communicate with the EDR master console SnapServer, requiring SSLv3 to be permanently or periodically enabled throughout the year. Otherwise certificates would expire causing jobs to fail with the error "Secure sockets layer (SSL) handshake failure on the process control server: sslv3 alert certificate expired."

This is no longer necessary for new installations using the current version of Snap EDR available at https://support.overlandstorage.com since March 2018.

For older installations subject to the problem, a hot fix is available from Overland and HVE tech support to either proactively fix the problem or to repair existing installations after certificates expire and jobs fail with the handshake error.

Third Party Product Support

NOTE: Refer to the Compatibility Guide on the Overland Storage Support website for a list of compatible operating systems, software and hardware.

- **Windows Hardware Certification** - Microsoft Windows Hardware Certification has been completed for the following iSCSI targets:
  - Windows Server 2012
  - Windows Server 2008 R2 x64
  - Windows Server 2008 x64 & x86
  - Windows Server 2003 R2 x64 & x86

- **Third Party Backup Products** - The following third party backup agents have been qualified with GuardianOS 7.7:
  - Symantec Backup Exec 2010R3 - 20.2
  - Symantec NetBackup 7.5
  - CA ARCserve 11.5, 12.0
  - EMC Networker 7.3, 7.4
  - Veeam 9 - 11 (as a backup repository only)
- **VMware iSCSI and NFS Certification** - VMware ESXi 5.1 certification for iSCSI (software initiators) has been completed.
- **Citrix iSCSI and NFS Certification** - Citrix XenCert 6.0.2 storage hardware certification.

Downloads

GuardianOS 7.7.236 is available for download for supported SnapServer users with active software entitlement agreements from the SnapServer support site:

http://www.snapserver.com/support

Additional documentation on how to operate, configure, and support your SnapServer is also available on this site.

2901 Summit Avenue, Suite 100 | Plano, TX | 75074 USA
T 866.958.6384 | F 866.203.0622 | www.hveconnexions.com