GuardianOS Version 7.7.224 Release Announcement

August 2017

Preface

This Product Information Bulletin announces the release of GuardianOS® Version 7.7.224 for selected SnapServer® systems.

Models Affected

GuardianOS Version 7.7.224 supports SnapCLOUD™, 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 7.7.224, 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.
- 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 7.7.224 Changes and Enhancements

- 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.

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:

- 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 Agent Certificates and SSLv3 Configuration 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 Agent Certificates and SSLv3 Configuration

NOTE: These section is for EDR Administrators.

Snap EDR agents and master consoles exchange certificates to ensure secure control communications. Agents attempt to update certificates with their master consoles once a day within 30 days of the one-year certificate expiration date. Since multiple agents registered with a master console can have certificates with different expiration dates, the required time to update can be unpredictable.

The certificate update requires SSLv3 to be enabled on the master console. However, SSLv3 was disabled in GuardianOS 7.6 for security compliance and compatibility with current browsers that block HTTPS access to servers that support SSLv3. This prevents agents from updating certificates. If an agent passes the expiration date without updating certificates, it can become non-functional, requiring a complex workaround or re-installation of the EDR software to repair it.

There are two ways to avoid this problem:

Option 1

Permanently enable SSLv3 on the master console. This does not expose a security vulnerability on the server, but will cause most current browsers to block HTTPS connections. If HTTPS communication with the server is unnecessary, this is the simplest solution. To permanently enable SSLv3 on the master console:

1. Connect to the server at **http://<servername** or **IP/sadmin/debug.cgi**, and login with administrative credentials.
2. Enter the following in the **Command** box:
   ```
   cli sslv3 set enable=yes
   ```
3. Click **OK**.

   The web server will restart and be available again within a minute.

Option 2

Enable periodic SSLv3 configuration on the master console. With this configuration, the server automatically enables SSLv3 for a period of 26 hours at midnight Saturday through 2am Monday once a week to allow agents to perform certificate updates. During these weekly periods, most current web browsers will prevent HTTPS connections to the server. To enable weekly SSLv3 configuration for agent updates:

1. Connect to the server at http://<servername or IP/sadmin/debug.cgi and login with administrative credentials.
2. Enter the following in the **Command** box:
   ```
   configini set edr ssl3certrenew yes
   ```
3. Click **OK**.

   The web server will not need to be restarted.

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, 2012
  - Symantec NetBackup 7.5
  - CA ARCserve 11.5, 12.0
  - EMC Networker 7.3, 7.4
- **VMware iSCSI and NFS Certification** - VMware ESXi 5.1 certification for iSCSI (software initiators) has been completed. You can see a complete listing of the certification testing completed on the VMware Compatibility Guide web page.
- **Citrix iSCSI and NFS Certification** - Citrix XenCert 6.0.2 storage hardware certification.

Downloads

GuardianOS 7.7.224 is available for download for supported SnapServer users with active software entitlement agreements from the Overland NAS support website:

http://support.overlandstorage.com/support/snapserver-nas.htm

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