GuardianOS Version 8.2.030 (alpha) Release Announcement

July 2022

Preface

This Product Information Bulletin announces the release of GuardianOS® Version 8.2.030 (alpha) for selected SnapServer® systems. This is an alpha release with limited testing and should only be installed to preview new features or to address critical issues if necessary.

Models Affected

GuardianOS version 8.2.030 (alpha) is available as an upgrade for existing SnapServer appliances running GuardianOS 8.1.119 or later, including DX1, later-model DX2, XSD40, XSR40, XSR120, and XSR122 models. The server must upgrade to 8.1.119 or later before installing 8.2.030.

Migration to GuardianOS 8.1 from Pre-8.0

Due to fundamental changes in storage and iSCSI configuration, upgrade to GuardianOS 8.1 is not possible from pre-8.0 versions. However, a migration process is available that requires a fresh install and restore of data from a backup. For more information on migration from pre-8.0 GuardianOS, see the document *Fresh Install Migration to GuardianOS 8.0+* in the Guardian OS 7.7 to 8.x Migration package at https://www.snapserver.com/support.

Downgrades

As this is an alpha preview release, the server can be downgraded to an older release if necessary. However it should only be downgraded to 8.1.119 or later -- downgrades to older GuardianOS versions can result in critical failures in some cases.

Downgrades are not supported using the standard upgrade process in the web management interface. A special manual process is required to bypass the downgrade restriction. To downgrade the server from GuardianOS 8.2.030:

1. Download the GSU for GuardianOS 8.1.119 or later from http://support.snapserver.com.
2. Copy the GSU to a share on the SnapServer, e.g. SHARE1.
3. Point a web browser to the SnapServer's debug console at http://servername/debug.cgi where "servername" is the servername or IP address normally used to connect to the SnapServer's web management interface. Login as an admin user when prompted.

4. Enter the following in the Command box to copy the GSU from the share to the /updater directory, then click the OK button to issue the command:

```
cp /shares/SHARE1/GuardianOSImage.gsu /updater/
```

5. Enter the following in the Command box to extract the GSU, then click the OK button to issue the command:

```
/ramdisk/bin/imageextract /updater/GuardianOSImage.gsu
```

This should produce output similar to the following:

```
CRC ok on image
Platform Bytes of Image File match this machine: 07.09.00

Successfully extracted /updater/fullimage.txt
Successfully extracted /updater/install.sh
Successfully extracted /updater/pre_install.sh
Successfully extracted /updater/platformbytes.txt
Successfully extracted /updater/osupdate.msg
Successfully extracted /updater/need_bios_update.sh
OK to leave .tgz file in OS image
File /updater/root400.tgz was not extracted
```

6. Enter "reboot" into the Command box and click the OK button to initiate the reboot, or alternatively reboot the server as usual. The server will perform the downgrade and reboot to the older GuardianOS version.

GuardianOS 8.2.030 Changes and Enhancements

GuardianOS 8.2.030 is an **alpha release** with limited QA testing. **should only be installed to preview new features or to address critical issues if necessary.** As with all upgrades, **a complete backup of all data should be made before performing the upgrade**, and this is particularly important for an alpha release.

- Two-factor authentication option for administrative users in the administrative interfaces (Web Management Interface, SSH).
- Remove default root password and no longer sync with admin (root password can be set in CLI if necessary).
- Require non-default admin password to be configured in initial setup.
- Remove the lighttpd Rescue Web Interface to eliminate a common source of security vulnerabilities (can be temporarily launched manually if necessary).
- Properly clean drives when deleting a storage pool or RAID to avoid errors when subsequently creating a new storage pool or RAID, and better handle leftover residue from previous configuration when creating a new storage pool or RAID.
- Several improvements to robustness of storage pool modification operations (resize, etc.).
- Support email notification via SMTP servers that require TLS 1.2, e.g. Microsoft 365.
- Retry failed email notification until successfully sent.
- Send email notification for hard drive hot remove events.
- Support the Broadcom BCM57416 dual-port 10GBE card.

- Collect complete SMART information in diagnostic logs ("sysfiles", a.k.a. "syswrapper").
- Permit NTP for clock sync when joined to a Windows domain, and offer NTP configuration in the Initial Setup wizard.
- Properly publish NFS exports when exportfs takes more than 5 seconds to run.
- Support login over SMB for users with '$' in their password.
- Several other bug fixes and improvements.

GuardianOS 8.1.121 Changes and Enhancements

GuardianOS 8.1.121 is a **beta release** with limited QA testing. **It should only be installed to address the specific issue detailed below.** As with all upgrades, **a complete backup of all data should be made before performing the upgrade**, and this is particularly important for a beta release.

- Updated Netatalk (the package providing AFP for MacOS clients) to address several security vulnerabilities, including a remote code execution exploit (CVE-2022-23121) and several related issues (CVE-2021-31439, CVE-2022-23123, CVE-2022-23122, CVE-2022-23125, CVE-2022-23124, CVE-2022-0194).

GuardianOS 8.1.120 Changes and Enhancements

- Fix for a rare condition in which a crash following certain unusual file operations can subsequently cause the server to hang during boot on "Quotacheck needed: Please wait" while initializing the user filesystem.
- Fix to properly automatically run repair on the root filesystem during boot following an unclean shutdown.
- Fix for frequent internal faults in /usr/bin/rsync during ECR replication.

GuardianOS 8.1.119 Changes and Enhancements

- Fix for storage reset performing an unintended system reset to defaults.
- Fix for ECR failure to start following unclean shutdown.
- Fix for ECR policy failure to resume after pausing.

GuardianOS 8.1.117 Changes and Enhancements

- Improved chassis fan monitoring on XSD40 to prevent erroneous fan failure errors.
- Redirected noisy sudo logging out of the main Event Log.
- Fix for an issue writing files over SMB that originated from other servers running GOS 8.x.
- Fix for an error submitting support case information in Maintenance > Support.

GuardianOS 8.1.114 Changes and Enhancements

- SMBv3 encryption configurable globally or per share. Snap CLI only -- see the following CLI commands:

```
windows set smb-encryption=auto|default|required
```

```
share set smb-encryption=default|auto|desired|required
```

- Various fixes for storage pool, volume, and expansion unit management.
- Various fixes for iSCSI disk management.
- Fix to support slashes in filenames from MacOS AFP clients.
- Fix for share target paths with spaces.
- Fix for data import into the root of a volume.
- Fix to properly update CPU microcode.
- Fix for "invalid duplex" errors for some TCP/IP and Ethernet configuration operations.

GuardianOS 8.1.037 Changes and Enhancements

- Encryption at rest for volumes and iSCSI disks.
- Write caching for iSCSI disks to improve performance, responsiveness, and connection reliability. Enabled by default and for existing disks on upgrade; can be enabled or disabled in the web UI or Snap CLI.
- Improved background disk scan I/O throttling and reduced frequency to reduce system load. In addition, Snap CLI contains new commands to enable or disable background disk scan and adjust I/O throttling for both Dynamic RAID and traditional RAID (see “storagepool settings set” and “raidsettings set” commands).
- Improved handling of directory move and rename operations on ECR source servers to prevent full re-replication of moved and renamed directories.
- Re-enabled NTLMv1 and raw NTLMv2 to support some SMB clients (for example, Mobotix cameras). Configurable with the Snap CLI “windows set ntlm auth” and “windows set raw NTLMv2 auth” commands.
- Configurable FTP server passive mode port range via the Snap CLI “ftp set min-PASV-port” and “ftp set max-PASV-port” commands (improves passive FTP mode support behind a firewall).
- Support for over-the-wire data compression in Snap ECR to reduce network I/O overhead.
- Many other bug fixes and improvements for iSCSI, Snap ECR, RDX copy/backup, Dynamic RAID management, and Windows domain membership.
- Fixed support for older serial-only APC UPS models with the IOGear GUC232A USB to Serial Adapter Cable.
- NTLMv1 authentication is now enabled for compatibility with older Windows/SMB clients and MOBOTIX cameras. NTLMv2 and Kerberos authentication continue to be available for newer clients.
- Various fixes for RDX backup job management and functionality.
- New command in CLI to disable RAID scan on DynamicRAID to reduce negative performance impact.
- New default minimum TLS protocol 1.1, and a new CLI command to set the minimum protocol to SSLv3, TLS 1.0, 1.1, or 1.2.
- Fix for failure to add iSCSI storage to a Hyper-V cluster.
- Fix for frequent link drops on the XSR 120 and DX2 onboard 1-gigabit Ethernet interfaces under heavy I/O load (“NIC Link is down/up” in the server Event Log).
- Various miscellaneous fixes for rare problems.

Previous GuardianOS 8.0 Changes and Enhancements

This is a cumulative release and includes all upgrades, feature enhancements, and bug fixes from previous GuardianOS 8.0 releases:

- The scheduled RDX backup job option “Create a new folder for each backup” now only backs up changed files for each subsequent backup, with each versioned directory containing a full set of changed and unchanged files via hard links.
- Updated Snap EDR Agent Certificates and SSLv3 Configuration section.
- Updated OS kernel and software packages for improved stability, functionality, and performance.
- Improved Windows client support:
- Support for SMB 3.1.1, the latest version of the Windows file networking protocol with improved performance, TCP multichannel, and encryption over the wire.
- Better integration into Windows Active Directory environments.
- Improved MacOS client support:
- Support for AFP 3.4, the latest version of the MacOS file networking protocol.
- Bonjour discovery in MacOS Finder.
- Full support for Time Machine, including automatic discovery and configuration in the Time Machine control panel.
- New iSCSI implementation:
- Better protocol compliance and performance than previous GuardianOS releases.
- iSCSI targets are allocated as block devices directly on the Traditional RAID or DynamicRAID storage pool.
- Improved Web Management Interface that is more intuitive, providing critical system information in a simple, easy-to-read format. It provides a cleaner, modern look that includes icons that better represent functions, toggle switches for faster option changes, and faster refreshes.
- New DynamicRAID implementation including several enhancements:
- Storage pool local hot spare drives.
- User quotas on volumes.
- Snapshots on individual volumes instead of the entire storage pool.
- Manage Volume Sizes interface to dynamically reduce or increase volume sizes for more efficient storage pool space allocation.
- Snapshot enhancements:
- Snapshot reservation replaces snapshot space to allow snapshots to consume extra unallocated space on the RAID or storage pool if necessary.
- DynamicRAID snapshots are independent instead of chained and can be deleted without affecting other snapshots.
- Improved USB 3.0 functionality and support for the latest Tandberg RDX drives.

Additional Changes from Pre-8.x Releases

- Security models are now configured on entire volumes and can no longer be set on traditional RAID subdirectories.
- Volume security reset to defaults has been removed in favor of re-applying a volume's security model with “reset permissions” selected.

- Group quotas are no longer available.
- SnapSync is no longer available in GuardianOS 8.0.

Snap EDR Agent Certificates and SSLv3 Configuration

NOTE: This section is for EDR Administrators.

Snap EDR agents and master consoles exchange certificates to ensure secure control communications. When a new agent registers with an EDR master console it uses SSLv3 to generate and exchange certificates. Therefore SSLv3 must be enabled on the master console when registering new agents, and can be disabled afterward.

To enable SSLv3 on the master console and register a new agent:

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

   ```
   web set https-min-protocol=SSLv3
   ```

3. Click OK. The web server restarts and will be available again within a minute.
4. Register one or more new **EDR agents** with the master console as usual.
5. After all new EDR agents have been registered, run the following **command** on the master console at http://<servername_or_IP>/sadmin/debug.cgi to disable SSLv3:

   ```
   web set https-min-protocol=TLSv1.1
   ```

Downloads

GuardianOS 8.2.030 (alpha) is available for download for supported SnapServer users with active software entitlement agreements from the SnapServer support website:

http://www.snapserver.com/support

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