Upgrade Guide

Version 6.1

Guardium®
SAFEGUARDING DATABASES™

Contents

Preface

About this Document

This document describes how to upgrade SQL Guard to version 6.1 from version 6.0. The 6.1 upgrade is ***only*** applicable for version 6.0. If you have an earlier version of SQL Guard (5.1, 5.0, 4.0.4, or 4.0.3, for example) you must upgrade to 6.0 ***before*** upgrading to 6.1.

To upgrade to version 6.1 from any version ***other than*** 6.0, contact Guardium Support to obtain the correct documentation and software.

For a detailed description of the new features in this release, see the updated *SQL Guard Administrator Guide* and the *SQL Guard User Guide*.

Target Audience

This document is intended for SQL Guard administrators.

230 Third Ave, Waltham, Massachusetts 02451 T. 877 487 9400 F. 781 487 7900 www.Guardium.com

Document Version 6.1 August 29, 2007

Upgrade Notes

Before beginning the upgrade process, be sure to read through all of the topics in this section.

Before Upgrading Any Unit

Always perform a full system backup from the CLI before starting the upgrade procedure, regardless of the unit type (collector, aggregator or Central Manager).

Bonding/High-Availability System Upgrades

If your unit is configured for bonding/high-availability, that functionality must be turned off via the CLI, and the unit must be rebooted before performing the upgrade. After the upgrade completes, the bonding/high-availability functionality can be turned on again via the CLI.

Upgrade Sequence for Aggregation Environment

Upgrade an aggregator *before* upgrading any of the units that export data to it. An upgraded aggregator can aggregate data from older releases, but an older aggregator cannot aggregate data from newer releases.

At least one day before updating the aggregator, from the *admin* account, stop the aggregation process (the Export Data schedule) on all collectors that export data to that aggregator. Do not restart the Export Data schedules on the collectors until *after* the aggregator has been upgraded.

Upgrade Sequence for Central Manager Environment

Upgrade the Central Manager to the new release, and then upgrade the managed units, taking care to upgrade an aggregator before upgrading any of the units that export data to it (see above).

Estimated Down Time

The duration of the upgrade depends on the amount of data on your appliance. Plan for about two hours of down time for the upgrade.

Upgrade Procedures

Step 1: Stop S-Taps

Stop all S-Taps that send data to the Guardium server. After the Guardium server has been upgraded, restart any 6.0 S-Taps. The 6.1 Guardium server software supports version 6.0 S-Taps, but older S-Taps must be upgraded before being restarted. For detailed instructions on stopping, restarting, uninstalling or installing S-Taps, see the *Unix* and *Windows S-Tap Guides* (two separate documents).

Step 2: Upgrade Guardium Servers

Follow this procedure to upgrade each SQL Guard Server. These steps are performed from the CLI, so you will need to have the SQL Guard *cli* user password for the unit being upgraded.

Step 2a: Back Up the Pre-Upgrade System

Before running this step, archive and purge all data that you will not need to access on your upgraded system. The less data on your system, the more quickly the upgrade procedures will run. For instructions on how to archive and purge data, see your current version of the *SQL Guard Administrator Guide*.

This step is performed while logged in as the *cli* user on the SQL Guard server.

1. Using an SSH client, log in to the SQL Guard unit as the *cli* user.
2. Enter the following command to back up the SQL Guard system:

   ```
   backup system
   ```

   You will be prompted to supply host, directory and password information for the system to which the backup data will be sent. Respond appropriately, and a series of messages will inform you that various processes or services are being stopped. Ultimately, you will be informed of the result of the backup operation with a message like the one illustrated below:

   ```
   Backup done. Keep the file /<xxx>/<host_name.domain_name-yyyy-mm-dd>.sqlguard.bak
   in a safe place.

   [Press Enter to continue]
   ```

3. Press Enter to complete the operation. A series of messages will display as the SQL Guard system restarts.
4. Log in to the backup host and verify that the backup file has been copied there.

Step 2b: Apply the Upgrade Patch

You can install the upgrade patch directly from a CD, or remotely from an *ssh* host on the network.

1. Using an SSH client, log in to the SQL Guard unit as the *cli* user.
2. Do one of the following:

   If installing from the CD, insert the upgrade patch CD into the Guardium CD drive, enter the following command, and skip ahead to step 3:

   ```
   store system patch install cd
   ```

   If installing from a network location, enter the following command, using either the **ftp** or **scp** transfer method, as appropriate for system on which the patch is stored:

   ```
   store system patch install [ftp | scp]
   ```

   And respond to the following prompts:

   ```
   Host to import patch from:
   User on <hostname>:
   ```

```
Full path to patch, including name:
<user@host> password:
```

3. You will be prompted to select the patch to apply:

   ```
   Please choose one patch to apply (1-n,q to quit):
   ```

   Typically there will be only one patch on an upgrade patch file. Type the number that identifies the upgrade patch – for example *SqlGuard-Upgrade60to61.tgz* – and then press Enter.

4. During the upgrade process, the SQL Guard unit will restart/reboot a few times. That is expected and does not require any action. You will need to respond to several system prompts:

   - Would you like to keep your current panes and menus structure instead of using the new V<*version.number*> default structure for regular users?
   - Would you like to keep your current panes and menus structure instead of using the new V<*version.number*> default structure for the admin user?

   We recommend that to reply **n** (for no) in both cases. When you do that, the upgrade will install the new standard tab layout, which will include all of the new features and reports. Your custom reports will be preserved and placed under a separate tab on the portal.

   You will also be prompted:

   - Would you like to keep the rollback capability (yes/no)?

   We recommend that you reply **no**. The rollback capability is unnecessary if you performed a full backup as described in the first procedure above. Choosing the rollback option will add a substantial amount of time to upgrade process.

   After the installation of this patch completes, and the system restarts, verify that the process has been successful by using a Web browser to log into the SQL Guard *admin* user account, and one or more of the other accounts. Check that all expected reports and other components are present.

Step 2c: Apply Maintenance Patches (Optional)

After restarting the system, apply any maintenance patches that you have received for the new release. *Initially, there will be no maintenance patches to apply.* Patches are distributed as Unix compressed archive files, either on CD or on your Guardium FTP account. There may be more than one patch in a compressed archive file. You can install patches directly from the CD, or remotely from a network location.

1. Log in to the SQL Guard unit as the *cli* user.
2. Do one of the following:

   If installing from a patch CD, Insert the CD into the Guardium CD drive, enter the following command, and skip ahead to step 3:

   ```
   store system patch install cd
   ```

   If installing from a network location, enter the following command:

   ```
   store system patch install [ftp | scp]
   ```

   And respond to the following prompts (be sure to supply the full path name to the patch file):

   ```
   Host to import patch from:
   User on <hostname>:
   Full path to patch, including name:
   Password:
   ```

3. You will be prompted to select the patch to apply:

   ```
   Please choose one patch to apply (1-n,q to quit):
   ```

   Type the number of the patch to apply, and then press Enter.

4. To install additional patches from the CD, repeat steps 2 and 3 above. Or to install additional patches from the compressed patch file just copied to the Guardium server, repeat the following commands:

   ```
   store system patch install sys
   ```

   And respond to the prompt:

   ```
   Please choose one patch to apply (1-n,q to quit):
   ```

   Type the number of the patch to apply, and then press Enter.

Step 3: Install New S-Taps

If you are upgrading from 6.0, you just need to restart the 6.0 S-Taps, which are compatible with the 6.1 Guardium server software. If the S-Taps are from an earlier release, install and start the 6.1 S-Taps. For detailed S-Tap installation instructions, refer to the *Unix* or the *Windows S-Tap Guide* (two separate documents).

Where to go from here…

The upgraded system is now ready to use. If you have added any new separately licensed components for this release (CAS or Informix database monitoring, for example) you will need to install a new license key before you can use that feature. The new license key will be provided by Guardium Support, and you can install it via the CLI interface or the Administrator Console, as described in the *SQL Guard Administrator Guide*.