Version 8.0 Rev.2

Layer 7 Gateway v7.1 to 8.0 Upgrade Guide

LAYER 7 TECHNOLOGIES

1.800.681.9377
info@layer7tech.com
www.layer7tech.com

OASIS MEMBER

WS-I MEMBER

Copyright © 2014 CA. All rights reserved.
This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW OR AS AGREED BY CA IN ITS APPLICABLE LICENSE AGREEMENT, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF M6ERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contents

Chapter One: Overview of Upgrade Process 1
About Version 8.0 1
Audience and Assumptions 1
Contacting Technical Support 1
Scenarios for Using Version 8.0 1
Chapter Two: Upgrading Hardware Appliances 3
Overview 3
Understanding Error Messages 3
Preparation 4
Preparing to Upgrade 4
Pre-Flight Checks 5
Upgrading 6
Start Upgrade 6
First Boot 7
Finish Upgrade 7
Second Boot 8
Post Upgrade Details 9
Customization and Relicensing 9
Post-Flight Checks 9
Acceptance Testing 9
Return to Production 10
Post Upgrade for API Portal Users 10
Cluster Upgrade 10
Reference Procedures 11
Reference A: How to Point a Node to a Single Database 11
Reference B: How to Restore Database Failover 11
Reference C: How to Restart the Gateway Process 12
Scenario A: Replicated Database Setup 12
Scenario B: Single Database Node Setup 16
Collecting Log Files 18
Redirect Syslog Messages 19
Chapter Three: Upgrading Virtual Appliances 21
Upgrading a Standalone Appliance 21
Prepare to Upgrade 21
Back Up the Source Gateway 22
Default Backup 22
Custom Backup 22
Restore to the Target Gateway 23
Post Upgrade 24

Upgrading Clustered Appliances 24
Cluster Upgrade: Hints and Tips 25
Prepare to Upgrade 25
Migrate Database Nodes 26
Migrate Processing Nodes 26
Customization and Relicensing 27
Acceptance Testing 27
Switch to Production 27
In Production 28
Collecting Log Files 28
Redirect Syslog Messages 28
Post Upgrade Verification 28
Chapter Four: Upgrading Software Gateways 31
Overview 31
RHEL/SUSE Linux Upgrade 31
If Using the MySQL Database 31
If Using the Embedded Database 33
Solaris Upgrade 35
If Using the MySQL Database 35
If Using the Embedded Database 36
Migrating to Version 8.0 under RHEL 6 38
Appendix A: Cluster Configuration Worksheet 41
Appendix B: Default Manifest 43

Chapter One: Overview of Upgrade Process

About Version 8.0

The Layer 7 Gateway version 8.0 has been designed to take advantage of the advancements in Red Hat Enterprise Linux 6 (RHEL 6).

RHEL 6 is mandatory for hardware and virtual appliances. Software Gateways may operate on either RHEL 5 or 6.

This guide describes how to install version 8.0 of the Gateway on all three Gateway form factors.

Notes: (1) The upgrade process described in this Guide is *only* used to upgrade a Gateway from version 7.1 to 8.0. For upgrades to other versions, please refer to "Upgrading the Gateway" in the *Layer 7 Installation and Maintenance Manual* for that version. (2) Only version 7.1 can upgrade to version 8.0. If you are currently using a Gateway earlier than 7.1, you must first upgrade to 7.1 before following this Guide.

Audience and Assumptions

The upgrade procedures described in this Guide is highly technical and is intended for users with a good working knowledge of Linux and the Layer 7 Gateway.

Contacting Technical Support

If you require assistance during the upgrade process, please email support@layer7tech.com or call your local Technical Support office (see "Contacting Layer 7 Technologies" in the *Layer 7 Installation and Maintenance Manual)*.

Scenarios for Using Version 8.0

The following are the various scenarios for using version 8.0 of the Gateway:

- If you are currently running a Software Gateway (RHEL/SUSE), version 8.0 can run under RHEL 5 or 6.
- If you are currently running Software Gateway (Solaris), version 8.0 can be installed using the same procedure as in previous releases.
- If you are currently running a Hardware or Virtual Gateway, you will upgrade to RHEL 6 as part of the version 8.0 upgrade.

Note: If you are running version 7.1 and do not plan on upgrading to version 8.0 yet, *do not* upgrade to RHEL 6 (on any Gateway form factor) as the older version 7.1 is not compatible with RHEL 6.

Chapter Two: Upgrading Hardware Appliances

Layer 7 Gateway version 8.0 requires Red Hat Enterprise Linux (RHEL) 6 on hardware appliances. This chapter provides detailed instructions on upgrading your appliance's operating system from RHEL 5 to 6 while upgrading the Gateway to version 8.0.

Tip: If you have purchased new appliances for version 8.0, they will already have RHEL 6 installed.

Overview

The upgrade process to RHEL 6 involves the following stages.

1. Prepare to upgrade
2. Pre-flight checks
3. Start upgrade
4. First boot
5. Finish upgrade
6. Second boot
7. Customization and relicensing
8. Post-flight checks
9. Acceptance testing
10. Return to production
11. Post Upgrade for API Portal Users

Understanding Error Messages

Generally, all operations are logged with an INFO message throughout the upgrade process. All generated logs are stored in the */home/upgrader/* directory, in both RHEL5 and RHEL 6. The logs are text files containing a series of timestamped messages with severity levels similar to the Syslog levels INFO, WARNING, and ERROR.

The log messages also sent to the Syslog, and all messages sent to the logs are displayed on the screen. The Upgrader will proceed if a WARNING message is logged, but it will stop when an ERROR message is encountered.

Note: If an ERROR message appears, contact Layer 7 Support.

Preparation

Preparing to Upgrade

Before upgrading to RHEL 6, create a backup of your system.

Note: The total time to upgrade from RHEL 5 to RHEL 6 may take up to 4 to 6 hours for each node. Be sure to allocate sufficient time for upgrading.

Ø *To prepare your system for upgrading to RHEL 6:*

1. Copy the following files to the "/home/ssgconfig/" directory on the appliance:

   Layer7_Upgrader_v1.L7P
   Layer7_PlatformUpdate_64bit_v7.1-04-24-2014.L7P
   image.tgz
   packages.tgz

   Note: The *Layer7_PlatformUpdate_64bit_v7.1-04-24-2014.L7P* file is required only if the current Gateway had been upgraded to version 7.1. If you purchased the Gateway at version 7.1 or had your Gateway re-imaged to v7.1, then this file is not required.

2. After copying these files, ensure that the permissions are set correctly for each of them. When using chmod octal notation, the files should be set to **0644**. This means that the files will be readable and writable by the owner, but only readable by the group and other users of the system.

3. Stop the Gateway services by doing the following:

   a. Start the Gateway main menu.

   b. Select option **2** (Display Layer 7 Gateway configuration menu).

   c. In the configuration menu, choose option **7** (Manage Layer 7 Gateway status).

4. If required, upload and install the *Layer7_PlatformUpdate_64bit_v7.1-04-24-2014.L7P* patch file (see Note under step 1 for eligibility). For information on installing patches, refer to "Managing Gateway Patches" in the *Layer 7 Installation and Maintenance Manual*.

   a. Return to the Gateway main menu.

   b. Select option **R** (Reboot the SSG appliance).

5. Upload and install the *Layer7_Upgrader_v1.L7P* patch file.

Pre-Flight Checks

The following is a list of optional but recommended checks to run to ensure an optimum upgrade experience. These checks are performed by logging in as the *upgrader* user and then selecting the menu option “Perform pre-flight checks”. Each check can be performed individually.

- Check for non-standard hardware (which may not be supported in RHEL 6) or failing hardware.
- Check the file system stack for bad disk blocks, failed RAID sets, corrupt file systems (for example, fsck checks) and failed disks (for example, SMART status checks).
- Check the databases for any corrupt database files. This is to ensure that the databases are small enough to be copied and are able to restore replication within an acceptable time window.
- Check for free space and inodes,
- Check for custom assertions. Custom assertions are not migrated by the Upgrader and will need to be reinstalled.
- Check the RPMs for non-standard and missing packages, unknown configuration files, missing dependencies. It also checks for a supported version of the Gateway RPM, as well as a supported version of the nCipher RPM.

  Notes: (1) The Upgrader only supports upgrading from an appliance with Gateway RPM version 7.1 or newer. (2) The *ssg-nshieldpci* RPM must be version 6.0 or newer.

- Check that GRUB is installed correctly.
- Run the option to verify the .TGZ files’ SHA-512 checksums.
- Check that the system has collected the state of the system for post-flight checks. This may include IP addresses assigned, and services/daemons list of ports on which the system is listening that are running.

View the list run. If you see any errors at this stage, contact Layer 7 Tech Support.

Upgrading

Start Upgrade

Note: If you have a Thales nCipher card installed, disable it before proceeding.

Before starting the upgrade process, stop the SSEM service and make sure that the Gateway and MySQL are running. You must also disable any HSM (Hardware Security Module) that is installed.

Ø *To disable the HSM:*

1. From the Gateway main menu, choose option **6** (Manage HSM).
2. Choose the item "Manage Gateway nCipher HSM state".
3. From the submenu, choose "Disable the Gateway use of nCipher HSM".

Ø *To start the upgrade process:*

1. Log in as user **upgrader** and then change the default password.
2. Choose the "Start upgrade" menu item.

Note: You will be prompted for the disk to be zeroed before RHEL 6 is installed. Zeroing your disk is highly recommended if you have reimaged your appliance or installed any other operating systems.

At this stage, the Upgrader will execute the following tasks.

1. Collects system state for Post-flight checks. At this point, the Upgrader checks that the prerequisites are met (the MySQL service is running and the SSEM service is stopped).
2. Creates the migration package.
3. Breaks the existing RAID sets.
4. Creates two RAIDs set on the single disk RAID for RHEL 6. This includes the RAID set for the boot partition and a RAID set for the LVM volumes.
5. Creates the LVM volumes by adhering to the STIG and NSA guidelines on partitioning.

   Note: Sizing is based on a percentage-of-disk based scheme with minimum and maximum sizes for each partition. Any extra space is allocated to the database partition.

6. Creates the ext3 file systems.
7. Unpacks the .TGZ into the new file systems.

8. Installs the GRUB.

Note: If there are any failures, the Upgrader will automatically stop. If you see any errors in the log, contact Layer 7 Tech Support.

If no errors are found, then the Upgrader creates the migration package, located under */home/upgrader/migration-package.tgz*.

First Boot

If there are no errors found, you can now reboot. Once the server reboots, it will automatically boot into RHEL 6.

Note: At this point you cannot use SSH because the files, including network configurations, have not been migrated yet.

Ø *To do the first reboot:*

1. Log out of the Upgrader menu.
2. Log in to the Gateway menu.
3. Select option **R** (Reboot the SSG appliance).

Finish Upgrade

Ø *To finish the upgrade:*

1. Log in to the Upgrader menu. Because the password in RHEL 5 is not migrated to RHEL 6, you must enter the default password first, then change the password when prompted.
2. Select option **3** (Finish upgrade) from the Upgrader menu.

Note: At this point, only the “Perform pre-flight checks” and “Start upgrade” options are available in RHEL5, while the “Finish upgrade” and “Perform post-flight checks” options are only available in RHEL 6.

In this stage, the Upgrader performs the following steps.

1. Reinstalls the Gateway, ssg-appliance, SSEM, and MySQL RPMs in RHEL 6.
2. Creates the initial MySQL database file.
3. Stages the operating system configuration files in the migration package for restoration on reboot.
4. Restores the database backups.
5. Upgrades the database content to comply with the requirements in version 8.0.

6. Checks that the file references the correct InnoDB file with the correct min size and log file size.
7. The Upgrader installs packages from the package's .TGZ file. In this process, the Upgrader will do the following.
   a. Copies the pre-flight state file from the RHEL 5 disk, which is used to determine which packages need to be installed in RHEL 6.
   b. Verifies the integrity of the RPMs extracted.
   c. Installs the MySQL RPMs. Note: If there are any integrity failures, the installation fails.
   d. Creates the initial database files.
   e. Starts the MySQL service. An INFO message is displayed before the service is started, due to a 10GB InnoDB data file being created during startup.
8. Runs mysql_upgrade.
9. Drops the "test" database.
10. Finds and installs the RPMs.
11. Sets the ssg-dbstatus and ssgsysconfig services to "start on boot", and finds the ssg-nshieldpci RPMs.
12. Checks if the ssg-nshieldpci RPM was installed in RHEL 5.
    If the pre-flight state file isn't available, the installation of the ssg-nshieldpci RPM is skipped and "ERROR" appears, but the Upgrader can continue.
13. Installs the ssg-nshieldpci RPM (if it was in RHEL 5).

    If the RPM is installed, the nCipher's SNMP service is disabled.
14. Installs any remaining packages from the .TGZ file.
15. Restores the content from the migration package, and patches the SQL upgrade scripts.
16. Upgrades the Gateway database.

Second Boot

If there are no errors found at this point, you can now reboot. Open the Gateway main menu and choose option **R** (Reboot the SSG appliance).

Post Upgrade Details

Customization and Relicensing

If there are no errors after rebooting the system, you can do the following:

- Install any missing RPMs which were installed in RHEL 5.
- Reinstall any custom assertions.
- Relicense the Gateway.

Tip: You can change the default booting operating system by using the "Change default booted operating system" option from the Upgrader menu, if necessary.

Post-Flight Checks

The Upgrader compares the Pre- and Post-flight states of the system. This comparison includes system properties such as network interface names, DNS server IPs and search bases, the routing tables, and the versions of MySQL.

Ø *To perform the post-flight steps:*

1. Log in to the Upgrader menu in RHEL 6.
2. Select option **4** (Perform post-flight checks).
3. Select option **5** (Rebuild RAID Sets) before rebuilding the RAID.

Note: You can choose between RHEL 5 and 6 for testing purposes until you rebuild on a RAID set. If you rebuild on RHEL 5, you will lose all configurations for RHEL 6 and vice-versa.

At this stage, the Upgrader creates a post-flight state file in the same manner as creating the pre-flight state file.

The pre-flight state file is copied from the RHEL 5 disk so that it can be compared to the pre-flight and post-flight state files. If the pre-flight state file cannot be detected, an error will appear. However, unlike in previous steps, even if any differences are found between the pre-flight and post-flight states, the Upgrader will continue to run and the differences will be listed. If there are differences between the MySQL versions, only a warning message appears.

Acceptance Testing

Before rebuilding the RAID sets, perform acceptance testing to determine if the Gateway is behaving as expected.

After the acceptance testing is successful, choose option **5** (Rebuild RAID Arrays) in the Upgrader menu to rebuild the RAID sets.

Return to Production

At this point, you must reconnect the system to a cluster. If this node is a member of a multi-node cluster, refer to the appropriate scenario below, under "Cluster Upgrade":

"Scenario A: Replicated Database Setup" on page 12

"Scenario B: Single Database Node Setup" on page 16

Post Upgrade for API Portal Users

If this Gateway is to be configured for use with the Layer 7 API Portal, it is important to disable the Portal Metrics Synchronization Utility *immediately* upon upgrading to version 8.0, prior to the installation of version 2.5.1.1 of the API Portal. If this is not done, Portal metrics data may be lost.

Ø *To disable the Portal Metrics Sync Utility:*

1. Log in to the Gateway and open a privileged shell. For more information, see "Using the Privileged Shell" in the *Layer 7 Installation and Maintenance Manual*.
2. Enter the following command:

   ```
   # crontab -u gateway –r
   ```

After upgrading the Portal, re-enable the Portal Metrics Sync Utility. This is described in the API Portal installation instructions, but is given below as reference.

Ø *To enable the Portal Metrics Sync Utility:*

1. Open a privileged shell and navigate to the following directory:

   ```
   /opt/SecureSpan/ApiPortal
   ```

2. Enter the following command:

   ```
   crontab -u gateway apiportal.cron
   ```

Cluster Upgrade

Tip: Complete the worksheet in Appendix A prior to upgrading, for backup purposes.

The method of upgrading depends on whether your system has a single node or a replicated database setup. There are two database nodes: node A, which is the primary node, and node B, which is the secondary. It is assumed that all nodes X are using A for their primary JDBC connection and failing over to B.

W A R N I N G

If you are configuring the first node of a cluster, ensure that the database layer has been properly configured for replication and tested. Failure to do this will require complex steps to enable proper operation of the cluster. Replication is described in "Configuring Database Replication" in the *Layer 7 Installation and Maintenance Manual*.

The following procedures will be referenced several times in the cluster upgrade instructions.

Reference Procedures

The two upgrade scenarios in this section call upon the following reference procedures at different points in the upgrade.

Reference A: How to Point a Node to a Single Database

Do the following when a procedure asks to point a node to a single database.

Ø *To point a node to a single database:*

1. Start the Gateway main menu.
2. Choose option **2** (Display Gateway configuration menu), and then choose option **3** (Configure the Gateway).
3. Choose option **1** (Database Connection) and enter the FQDN of database node A when prompted.
4. Choose option **2** (Configure Database Failover Connection).
5. Choose "Yes" when prompted to remove configuration for "Configure Database Failover Connection".
6. Save and exit by choosing option **S** (Save and exit).
7. From the Gateway main menu, choose option **6** (Display the current Layer 7 gateway configuration). Confirm that the node is only connecting to database node A.

Reference B: How to Restore Database Failover

Do the following when a procedure asks to restore database failover.

Ø *To restore database failover:*

1. Start the Gateway main menu.
2. Choose option **2** (Display Gateway configuration menu) and then option **3** (Configure the Gateway).
3. Choose option **1** (Database Connection) and enter the FQDN of database node A when prompted.

4. Choose option **2** (Configure Database Failover Connection).
5. Choose "No" when prompted to remove configuration for "Configure Database Failover Connection".
6. Enter the FQDN of database node B when prompted.
7. Save and exit by choosing option **S** (Save and exit).
8. From the Gateway main menu, choose option **6** (Display the current Layer 7 gateway configuration). Confirm that the node is only connecting to database node A.

Reference C: How to Restart the Gateway Process

Do the following when a procedure asks to restart the Gateway.

Ø *To restart the Gateway:*

1. Access the Gateway main menu.
2. Choose option **2** (Display Layer 7 Gateway configuration menu).
3. Choose option **7** (Manage Layer 7 Gateway status).
4. Choose option **2** to restart the Layer 7 Gateway.

Scenario A: Replicated Database Setup

If you have a replicated database setup, follow the instructions below. A replicated database setup is where there are two databases plus processing nodes and two more processing nodes all running as appliance-imaged virtual machines.

Note: Some audits and service metrics may be lost during the upgrade, due to the fact that replication is unavailable. This can be avoided if audits are configured to be sent to an external location. For more information, see "Managing the Audit Sink" in the *Layer 7 Policy Manager User Manual*.

Ø *To upgrade clusters for a replicated database setup:*

1. Point database node A and all processing nodes X to database node A, with no failover (see "Reference A" on page 11; refer to worksheet that was filled out in Appendix A). Ensure that Node A is using *localhost* and not FQDN. Failure to do so will prevent the database from being migrated into RHEL 6.
2. Restart the Gateway process on node A and all processing nodes X (see "Reference C" on page 12).
3. Verify that no processing nodes are connecting to node B by running this command on node B:

   ```
   # mysql -e 'show processlist;'
   ```

The output should *not* contain any IP addresses or hostnames of processing nodes for the MySQL *gateway* user.

4. Verify that all processing nodes are connecting to node A, by running this command on node A:

   ```
   # mysql -e 'show processlist;'
   ```

   The output should contain any IP addresses and hostnames of all the processing nodes for the MySQL *gateway* user.

5. Remove database node B from the load balancer.

   Note: Do not rely on service availability checks done by the load balancer, as these checks will succeed at times during the upgrade when the node is not ready to receive traffic. This applies to all cases where a node is removed from the load balancer.

6. Point database node B to itself with no failover (see "Reference A" on page 11). You must use *localhost*, and not the FQDN of node B.

7. Restart the Gateway process on node B (see "Reference C" on page 12).

8. Modify the iptables rules to block the MySQL replication port on nodes A and B. Ensure that the changes below are saved to disk (so that they are migrated into RHEL 6).

   a. Run the following commands on node A:

      ```
      # iptables -I INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3306
      -j REJECT
      ```

      ```
      # iptables -I INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3307
      -j REJECT
      ```

   b. Edit */etc/sysconfig/iptables* and add the following lines before the ACCEPT rule for dport 3306:

      ```
      [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3306 -j
      REJECT
      [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3307 -j
      REJECT
      ```

   c. Run the following commands on node B:

      ```
      # iptables -I INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3306
      -j REJECT
      ```

      ```
      # iptables -I INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3307
      -j REJECT
      ```

   d. Edit */etc/sysconfig/iptables* by adding the following commands just before the ACCEPT rule for dport 3306:

```
[0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3306 –j
        REJECT
[0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3307 –j
        REJECT
```

e. At this point, replication will be failing on nodes A and B. You will need to complete the following steps in a timely fashion to ensure that replication can be restored. To confirm that replication is failing:

- Run the following commands on both nodes A and B:

  # mysql -h OTHER-DB-NODES-IP -u root -p

  # mysql -h OTHER-DB-NODES-IP -u root -p --port 3307

  Enter the password for the database's root user. You should see an error message stating that it cannot connect.

9. Once you have confirmed that replication is failing, perform the cluster upgrade.

Ø *To perform the cluster upgrade:*

1. Run the Upgrader on node B and leave B in RHEL 6.

   To run the Upgrader:

   a. Log in as user **upgrader.**

   b. Choose the "Start upgrade" menu item.

2. Relicense node B. For more information, see “Managing Gateway Licenses” in the *Layer 7 Policy Manager User Manual*.

3. Customize the node to match its RHEL5 state. For example, install any custom assertions or unsupported RPMs.

4. Perform acceptance testing on node B.

   Note: If your node B is a database + processing node, replace all nodes in the load balancer with B. All traffic will now be flowing through a single node until everything is upgraded.

5. For each processing node X, do the following:

   a. Remove node X from the load balancer, if it has not been done already.

   b. Run the Upgrader on node X and leave X in RHEL 6.

   c. Point node X at node B with no failover (see “Reference A” on page 11).

   d. Restart the Gateway process on each processing node X (see “Reference C” on page 12).

   e. Customize the node to match its RHEL5 state. For example, reinstall any custom assertions or unsupported RPMs.

   f. Perform acceptance testing on node X.

g. Add node X to the load balancer. Note: If X is the first processing node being added to the load balancer, be sure to remove all the other non-RHEL 6 nodes first.

6. Run the Upgrader on node A and leave A in RHEL 6.
7. Customize the node to match its RHEL5 state. For example, install any custom assertions or unsupported RPMs.
8. Perform acceptance testing on node A.
9. Restore replication between nodes A and B.

   Do the following on node A:

   a. Run the following commands.

   ```
   # iptables -D INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3306
   j REJECT
   ```

   ```
   # iptables -D INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3307
   j REJECT
   ```

   b. Next, edit */etc/sysconfig/iptables* by removing the following lines, just before the ACCEPT rule for dport 3306:

   ```
   [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3306 –j
   REJECT
   [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-B-IP --dport 3307 –j
   REJECT
   ```

   Do the following on node B:

   a. Run the following commands.

   ```
   # iptables -D INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3306
   -j REJECT
   ```

   ```
   # iptables -D INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3307
   -j REJECT
   ```

   b. Next, edit */etc/sysconfig/iptables* and remove the following lines just before the ACCEPT rule for dport 3306:

   ```
   [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3306 -j
   REJECT
   [0:0] -A INPUT -i eth0 -p tcp -m tcp -s NODE-A-IP --dport 3307 -j
   REJECT
   ```

10. If node A is a database + processing node, do the following.

    a. Point node A at node B with no failover (see “Reference A” on page 11).

    b. Restart the Gateway (see “Reference C” on page 12).

    c. Add node A to the load balancer.

11. Run the following command on node A first, and then on node B:

    ```
    # /opt/SecureSpan/Appliance/bin/restart_replication.sh
    ```

    When prompted for the “IP for the MASTER”, enter the other database node's IP.

12. To verify that replication has been restored on both nodes A and B:

a. Run the following command.

```
# mysql -e 'show processlist;'
```

The output should show a connection from the other DB node as the user *repluser* (provided that the default username “repluser” was used during setup of the cluster).

b. Next, run the command:

```
# mysql -e 'show slave status\G;'
```

The fields “Slave_IO_Running” and “Slave_SQL_Running” should both be set to “Yes”. If not, wait approximately two minutes before re-running the command, to allow enough time for the slaves to reconnect to their masters.

The “Seconds_Behind_Master” field should be decreasing with repeated runs of the command.

13. Restore failover for all nodes (see “Reference B” on page 11”).
14. Restart the Gateway process on all nodes X (see “Reference C” on page 12).
15. Rebuild the RAID sets on all nodes. This is done through the Upgrader menu. Tip: This is best performed when the demand on the Gateway is lighter, as this may affect performance.

You have now upgraded clusters for a replicated database setup.

Scenario B: Single Database Node Setup

If you have a single-node setup, follow these instructions. A single-node setup is where there is a single database, or a database plus processing node in a cluster.

Note: The Gateway will be unavailable while the database node is being set up.

Ø *To upgrade clusters for a single database node setup:*

1. Verify that each processing node X is pointing to database node A (see “Reference A” on page 11; refer to the worksheet that was filled out in Appendix A if necessary). For more information on how to do this, see “Configure Authentication Method” in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

   Note: If database node A is also a processing node, it must use *localhost* and not FQDN. Failure to do so will cause the database to not be migrated into RHEL 6.

   ---

2. Restart the Gateway process on database node A and for all processing nodes X (see “Reference C” on page 12).

3. Verify that all processing nodes are connecting to node A. To do this, run the following command on node A.

   ```
   # mysql -e 'show processlist;'
   ```

   The output should contain any IP addresses and hostnames of all the processing nodes for the Gateway user.

4. Remove all nodes from the load balancer.

   Note: Do not rely on service availability checks done by the load balancer as these checks will succeed at times during the upgrade when the node is not ready to receive traffic. This applies to all cases where a node is removed from the load balancer.

5. Power off each processing node.
6. Run the Upgrader on node A and leave it in RHEL 6.

   To run the Upgrader:

   a. Log in as user **upgrader.**
   b. Choose the "Start upgrade" menu item.

7. Relicense node A. For more information, see “Managing Gateway Licenses” in the *Layer 7 Policy Manager User Manual*.
8. Customize the node to match its RHEL 5 state. For example, install any custom assertions or unsupported RPMs.
9. Perform acceptance testing on node A.
10. If node A is a database + processing node, add that back into the load balancer.

    All traffic will now be flowing through a single node until the remainder is upgraded.

11. Repeat the following steps for each processing node X:

    a. Power on the processing node X.
    b. Run the Upgrader on node X and leave X in RHEL 6.
    c. Customize the node to match its RHEL 5 state. For example, install any custom assertions or unsupported RPMs.
    d. Perform acceptance testing on node X.
    e. Add node X to the load balancer.

12. Rebuild the RAID sets on all nodes. You do this through the Upgrader menu.

You have now upgraded clusters for a single-node setup.

After your system is reconnected with the cluster, rebuild the RAID to minimize impact on performance.

Ø *To rebuild the RAID:*

1. Log in to the Upgrader menu for your operating system.

   W A R N I N G

   It is very important to choose the correct operating system. Logging into the Upgrader menu for RHEL 5 and rebuilding the RAID sets will destroy the RHEL 6 installation. Likewise, logging into RHEL 6 and rebuilding will destroy RHEL 5.

2. Select the “Rebuild RAID arrays for current operating system” option.
3. Agree to the displayed warning that the operation is irreversible and can cause potential loss of data. The Upgrader begins rebuilding the RAID array for the /boot partition and will not continue until it finishes rebuilding. This will take approximately a few minutes.

   W A R N I N G

   You must wait for the /boot partition to rebuild to prevent a kernel panic halfway through a system boot. If the system reboots at anytime during the rebuild, you can no longer boot the system.

4. Once the /boot partition RAID set is finished rebuilding, the Upgrader menu appears. However, before returning the system to production, it is recommended that you wait until the RAID sets have finished rebuilding. See the section “To monitor the rebuild of the RAID sets” below.

Ø *To monitor the rebuild of the RAID sets:*

1. Log in to the Upgrader menu and select the “Check status of RAID arrays” option.
2. The Upgrader displays the current state of the RAID sets. To refresh the display of progress, choose the option again.

Collecting Log Files

All log files for the Upgrader are stored in */home/upgrader*. The portions of the upgrade performed in RHEL 5 are stored on the RHEL 5 disk. For RHEL 6 the portions are stored on the RHEL 6 disk. Use the “Change default booted operating system” option from the Upgrader menu to switch between the two operating systems.

The log files can be copied by logging in as user *upgrader* and using a SFTP client

Tip: Include all files from the */home/upgrader* directory when opening a ticket with Layer 7 Support.

Redirect Syslog Messages

You can send any messages, such as errors, info and debug, to any Syslog server. These messages usually are stored in */var/log/messages* or other */var/log* folders on the Gateway. To ensure that a record of the upgrade is preserved, it is recommended that you redirect to external Syslog servers. This allows you to centralize all logs and make backups easier to manage.

Chapter Three: Upgrading Virtual Appliances

This chapter describes how to upgrade from version 7.1 to 8.0 of the Layer 7 Gateway on virtual appliances. The instructions below will back up your data from your v7.1 Gateway and then migrate it to a new v8.0 virtual appliance.

Prerequisites:

- An operational version 7.1 virtual appliance
- A version 8.0 virtual appliance as delivered by Layer 7, with networking configured. (No database should be configured.)
- The *vm-migration.sh* file, which can be downloaded from the Layer 7 Technical Support download site.

Version 7.1 virtual appliances not being upgraded: If you intend to retain some Gateways at version 7.1 (for example, as a fallback during the v8.0 upgrade), it is highly recommended that you install the 7.1 April 2014 Platform Patch on those Gateways. See step 4 on page 4 for details.

Upgrading a Standalone Appliance

This section describes the upgrade procedure for a single virtual Gateway (in other words, a “cluster” of one).

Tip: If the Layer 7 Enterprise Service Manager is present, the upgrade script will automatically include its database during backup and restore.

Prepare to Upgrade

Before upgrading, you need to copy over the upgrade script and stop the Gateway services.

Ø *To prepare for the upgrade:*

1. Log in as *ssgconfig* on the Gateway virtual appliance running v7.1 and open a privileged command shell from the Gateway configuration menu.
2. Copy the *vm-migration.sh* file to the virtual appliance (any directory).
3. Change to that directory and change the permissions with this command:

   ```
   chmod a+x vm-migration.sh
   ```

4. If the Enterprise Service Manager is installed, stop it with this command:

   ```
   # service ssem stop
   ```

Back Up the Source Gateway

There are two options for backing up the source Gateway:

- **Default Backup:** This backs up your v7.1 database, plus all the OS-level files specified in the default manifest. For more information, see Appendix B. The option is recommended for most users.
- **Custom Backup:** This backs up your v7.1 database, plus only the OS-level files specified in a customized manifest. This option is recommended for advanced users only.

Note: If a particular file cannot be read, it will not be backed up. Be sure to check the log file for warning messages.

Default Backup

Ø *To perform a default backup:*

1. Navigate to the directory containing the *vm-migration.sh* file (see “Prepare to Upgrade” on page 21).
2. Run the following command:

   ```
   # ./vm-migration.sh --verbose --backup
   ```

   This backs up the database and OS-level files from the source Gateway to a file named *migration-package.tgz* in the current directory.

   Tip: You can specify your own backup package name and path by adding the “- -file” parameter:

   ```
   --file /tmp/<backupName>.tar.gz
   ```

   ---

3. Copy both the backup and the script files to the target Gateway running v8.0:

   migration-package.tgz
   vm-migration.sh

To restore the backup, see “Restore to the Target Gateway” on page 23.

Custom Backup

Ø *To create a custom backup:*

1. Navigate to the directory containing the *vm-migration.sh* file (see “Prepare to Upgrade” on page 21).
2. Create the default manifest with this command:

   ```
   # ./vm-migration.sh --verbose --default --manifest /tmp/<manifestName>
   ```

   This extracts the default manifest to a text file named <*manifest.Name*> in the */tmp* directory.

3. Edit <*manifest.Name*> to include only the OS-level files you wish to back up.

- To exclude a configuration file from the backup, remove the line for that file.
- To include a file in the backup, add its file name and path in a new line.

IMPORTANT: Editing the manifest should only be attempted by system administrators or advanced users who have a solid understanding of the internal Gateway system files. Including or excluding critical files may render the target Gateway inoperable after restoring.

4. Perform the backup using your custom manifest:

```
# ./vm-migration.sh --verbose --backup --manifest /tmp/<manifestName>
```

This backs up the database and OS-level files listed in <*manifestName*> from the source Gateway to a file named *migration-package.tgz* in the current directory. It

Tip: You can specify your own backup package name and path by adding the "- -file" parameter:

```
--file /tmp/<backupName>.tar.gz
```

5. Copy both the backup and the script files to the target Gateway running v8.0:

migration-package.tgz
vm-migration.sh

Restore to the Target Gateway

When a backup is restored on a target Gateway, all files in the manifest (either default or customized) are restored. Note: Any errors or warnings generated during the backup may reduce the number of files being restored.

Ø *To restore to the target Gateway:*

1. Ensure the backup and the script files have been copied to the target Gateway.
2. In the directory containing the copied files, update the permissions as follows:

```
# chmod a+x vm-migration.sh
```

3. Restore the backed-up files with this command:

```
# ./vm-migration.sh --verbose --restore
```

This command will look for a backup package named *migration-package.tgz* in the current directory and use it to restore the v7.1 database plus all OS-level files in the default manifest.

Tip: To specify a different backup package name and path, add the "- -file" parameter:

```
--file /tmp/<backupName>.tar.gz
```

4. Reboot the server.

Post Upgrade

Perform the following tasks after upgrade is complete:

- Connect to the v8.0 Gateway using the Layer 7 Policy Manager and install the new license file. Tip: Be sure to use the new v8.0 license file provided; your old v7.1 license will no longer work.
- Any custom assertions present in v7.1 will need to be reinstalled and reregistered after upgrading to version 8.0. For more information, see the *Layer 7 Custom Assertions Installation Manual*.
- Assertion files that were not included by default in your v7.1 system will need to be copied back to the following directory on the v8.0 Gateway:

  runtime/modules/assertions

  An example of non-default files are the .AAR files for modular assertions.
- Similarly, .JAR files will need to be copied over again to the following directories for some features to work (for example, JDBC or JMS):

  /runtime/lib/ext
  /runtime/lib

Upgrading Clustered Appliances

This section describes the upgrade procedure for a cluster of two or more virtual Gateways. The upgrade process involves the following stages:

1. Prepare to upgrade
2. Migrate database nodes
3. Migrate processing nodes
4. Customization and relicensing
5. Acceptance testing
6. Switch to production
7. In production

Each stage is described in detail below.

Tip: If the Layer 7 Enterprise Service Manager is present, the upgrade script will automatically include its database during backup and restore.

Cluster Upgrade: Hints and Tips

The following are some hints and tips to ensure a successful cluster upgrade:

- Ensure that replication has started in the v7.1 cluster *before* beginning the upgrade to v8.0.
- If you need to reboot the cluster or a single node within the cluster, note that there may be a delay of several minutes before replication starts. To verify that replication has started, see the Tip under "Configure Replication" in the *Layer 7 Installation and Maintenance Manual, v8.0 (Appliance Edition)*.
- Allow several minutes for the Gateway to become available after rebooting. When testing connections to a processing node (during the "Acceptance Testing" stage), wait at least 5 minutes after the last reboot completes before determining whether a node is incorrectly configured or otherwise unavailable.

Prepare to Upgrade

Ø *To prepare to upgrade:*

1. Configure your v7.1 Gateways to redirect audit messages to an external destination. This will minimize the backup size and reduce resource requirements on the database during the upgrade.

   For more information, see "Managing the Audit Sink" in the *Layer 7 Policy Manager User Manual*.

2. Start up an equal number of v8.0 virtual Gateways, using the steps described in the *Layer 7 Virtual Appliance User Manual*.

   a. Ensure that any resource management policies (for example, VMware's Resource Pools) are applied correctly to the new virtual appliances.

   b. Configure networking on the v8.0 virtual appliances, using the Gateway main menu. Note: Be sure to assign new IP addresses for each node in the v8.0 Gateway cluster.

   c. Configure database replication if the v8.0 cluster will contain two database nodes. For details, see "Configuring Database Replication" in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

   Note: Do ***not*** create a new database for the new cluster. Your v7.1 database will be backed up, restored, and upgraded.

3. Copy the *vm-migration.sh* script file to the following directory on both the v7.1 and v8.0 virtual appliances:

   /home/ssgconfig/

4. Optionally, move the *vm-migration.sh* script into **/root**.

5. For clusters with two database nodes, ensure that all nodes in the v7.1 cluster are using the primary database, with no failover.

Migrate Database Nodes

Note: The vm-migration.sh script file must be run by the *root* user.

Ø *To migrate database nodes:*

1. Perform the following on each database node:
   a. Back up the v7.1 Gateway node using one of the scenarios described under "Back Up the Source Gateway" on page 22 (performing a default or custom backup as required). Tip: When creating a custom manifest, ensure that any additional files are readable by the *layer7* user.
   b. Copy the resulting migration package to the corresponding v8.0 node.
   c. Restore the migration package on the v8.0 node using the instructions under "Restore to the Target Gateway" on page 23.
2. If any database node that is also a processing node, you need to reconfigure the Gateway to point to the primary and secondary v8.0 database nodes, instead of to the primary and secondary v7.1 database nodes. To do this:
   a. Start the Gateway main menu.
   b. Choose option **2** (Display Gateway configuration menu) and then option **3** (Configure the Gateway).
   c. Choose option **1** (Database Connection) and enter the FQDN of the primary node when prompted.
   d. Choose option **2** (Configure Database Failover Connection).
   e. Choose "Yes" when prompted to remove configuration for "Configure Database Failover Connection".
   f. Enter the FQDN of the secondary node when prompted.
   g. Save and exit by choosing option **S** (Save and exit).
   h. From the Gateway main menu, choose option **6** (Display the current Layer 7 Gateway configuration). Confirm that the node is connecting to the primary and failing over to the secondary node.

Migrate Processing Nodes

To migrate the processing nodes, follow the steps under "Migrate Database Nodes" above for each processing node.

Customization and Relicensing

After the migration package is successfully restored onto the v8.0 Gateways, manually reapply any customizations and the licensing:

1. Adjust the ownership and/or permissions on restored files and directories that should not be owned by the *root* user.
2. Install the new v8.0 license files. For more information, see "Managing Licenses" in the *Layer 7 Policy Manager User Manual*.
3. Reinstall any custom assertions that were present in v7.1, including any dependencies. For installation directions, see the *Layer 7 Custom Assertions Installation Manual*.
4. Files that were not included by default in your v7.1 system will need to be copied back to the following directory on the v8.0 Gateway:

   runtime/modules/assertions

   An example of non-default files are the .AAR files for modular assertions.
5. Similarly, .JAR files will need to be copied over again to the following directories for some features to work (for example, JDBC or JMS):

   /runtime/lib/ext
   /runtime/lib
6. If you are running Thales NetHSM, you will need to reimport a security world. For more information, see "How to Manually Set Up the nCipher Card" in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

Acceptance Testing

Set up the load balancer and send test traffic to the new cluster to ensure that the cluster is behaving correctly.

Note: As the Layer 7 Gateway can serve a variety of needs and can be configured in many different ways, it is up to your organization to determine which tests are appropriate in determining whether the new cluster is functioning correctly.

Switch to Production

Once the new v8.0 cluster has passed acceptance testing, you can adjust the load balance so that production traffic is directed to the new cluster.

Layer 7 recommends keeping the v7.1 cluster running for a short period of time as a backup.

In Production

After the new cluster has been running for some time, you can decommission the old cluster.

- Simply shutting down and deleting the virtual machines for the v7.1 appliance will suffice in most instances.
- Some organizations may require suspending archiving of the old virtual machine files.

If in doubt, consult with your IT, management, or Legal teams to determine the correct course of action.

Collecting Log Files

All log files for the Upgrader are stored in the same directory where the *vm-migration.sh* script file is located.

The log files can be copied by connecting as the *ssgconfig* user and using a SFTP client

Tip: Include all files from the directory containing the *vm-migration.sh* script file when opening a ticket with Layer 7 Support.

Redirect Syslog Messages

You can send any messages, such as errors, info and debug, to any Syslog server. These messages usually are stored in */var/log/messages* or other */var/log* folders on the Gateway. To ensure that a record of the upgrade is preserved, it is recommended that you redirect to external Syslog servers. This allows you to centralize all logs and make backups easier to manage.

Post Upgrade Verification

To verify that the upgrade to version 8.0 (either standalone or clustered) is successful, you can perform the following checks:

Check #1

In MySQL, enter the following command:

```
mysql>select * from ssg_version
```

This should match the output of this command:

```
# rpm -qa | grep ssg
```

Check #2

In MySQL, enter the following command:

```
mysql>show tables; or SELECT COUNT(*) FROM information_schema.tables
WHERE table_schema = 'ssg1';
```

This should return 93 tables.

If your results differ, contact Layer 7 Technical Support for further assistance.

Chapter Four: Upgrading Software Gateways

Overview

The upgrade process differs slightly depending on the operating system of the host machine for the Software Gateway:

- **The host computer is still running RHEL 5 or Solaris:**

  Version 8.0 is compatible with RHEL 5 and Solaris. There is no specific requirement to upgrade to RHEL 6.

  Refer to the appropriate section below for details on upgrading to version 8.0:

  "RHEL/SUSE Linux Upgrade" on page 31

  "Solaris Upgrade" on page 35

  Documentation correction: For a list of the patch files to download, please consult the Layer 7 Technical Support Portal instead of the v8.0 Release Notes.

- **The host computer is on RHEL 6:**

  In this scenario, version 8.0 will be installed on a host computer that has been upgraded to RHEL 6. This Guide will provide instructions on migrating your v7.1 database to v8.0.

  Refer to "Migrating to Version 8.0 under RHEL 6" on page 38 for details.

RHEL/SUSE Linux Upgrade

Perform the appropriate section to upgrade a Gateway running on Red Hat Enterprise Linux (RHEL) or SUSE Linux.

If Using the MySQL Database

Ø *To upgrade the Gateway under RHEL or SUSE Linux with a MySQL database:*

1. *(Optional, but recommended)* Back up the database using the Backup Service. For details, see "Backing Up the Gateway" in the *Layer 7 Installation and Maintenance Manual (Software Edition)*.
2. Stop the Gateway with this command:

   ```
   /opt/SecureSpan/Gateway/runtime/bin/gateway.sh stop
   ```

3. Ensure that a Java SE Development Kit (JDK) has been installed.
4. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7 from the Sun web site. Unzip the files in UnlimitedJCEPolicyJDK7.zip[1] and then copy the extracted *jce_policy-7/**jce/****** files to the following JDK 1.7 *jre/lib/security* directory (based on the JDK 1.7 having been installed to the default directory */usr/j2se/*):

   ```
   cp jce_policy-7/jce/* /usr/j2se/jdk1.7.0_xx/jre/lib/security/
   ```

   Where *"xx"* represents the most recent update of JDK 1.7.
5. Stop the slave in MySQL on all nodes in the cluster.
6. Upload the version 8.0 patch files to the Gateway. These files are available from the Layer 7 Technical Support download site.

   Tip: The upload is performed using the "upload" command. See "Managing Gateway Patches" in the *Layer 7 Installation and Maintenance Manual (Software Edition)* for more information.
7. Install each uploaded patch file. Unless noted otherwise, the patch files may be installed in any order.

   Tip: The installation is performed using the "install" command. See "Managing Gateway Patches" in the *Layer 7 Installation and Maintenance Manual (Software Edition)* for more information.
8. Open *my.cnf* for editing:

   ```
   # edit my.cnf
   ```
9. Add the following property to *my.cnf*:

   ```
   log_bin_trust_function_creators=1
   ```

   The following property may also need to be added; please contact Layer 7 Support if it is required for your installation:

   ```
   slave_exec_mode=IDEMPOTENT
   ```

   The properties should be added to this section:

[1] can be obtained from: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

```
# Uncommment log-bin and log-slave-update if a clustered
# db server
log-bin=/var/lib/mysql/ssgbin-log
log_bin_trust_function_creators=1
log-slave-update
# uncomment the next item on 1st db master server
server-id=1
# uncomment the next item on 2nd db master servers
#server-id=2
relay-log = /var/lib/mysql/ssgrelay-bin
relay-log-index = /var/lib/mysql/ssgrelay-bin.index
relay-log-info-file = /var/lib/mysql/ssgrelay-bin.info

# Slave reliability items:
slave-skip-errors=126,1053,1105,1129,1158,1159,1160,1161
slave_compressed_protocol=1
slave-net-timeout=30
slave_exec_mode=IDEMPOTENT
```

Figure 1: Editing my.cnf

10. Restart the MySQL service on all nodes in the cluster.
11. Restart the Gateway.
12. Upgrade the Gateway database on one node. To do this:
    a. Access the Gateway main menu.
    b. Select option **1** (Upgrade the Layer 7 Gateway database).
13. Start the Gateway with this command:

    # /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start

    The databases on the other nodes will be replicated from the primary database.

The upgrade is now complete.

If Using the Embedded Database

Ø *To upgrade the Gateway under RHEL or SUSE Linux with the embedded database:*

1. Stop the Gateway with this command:

   # /opt/SecureSpan/Gateway/runtime/bin/gateway.sh stop

2. Back up the previous embedded database by copying this directory to your local directory:

   /opt/SecureSpan/Gateway/node/default/var/db

3. Remove this directory:

   /opt/SecureSpan

4. Reboot the computer.
5. Install the Gateway software with this command:

   # rpm -Uvh ssg-*<version>*.noarch.rpm

   where *"<version>"* is the version number of the new Gateway.

6. Run the following to configure the Gateway:

   ```
   # /opt/SecureSpan/Gateway/runtime/bin/setup.sh
   ```

   The Layer 7 Gateway main menu appears.

7. Select option **2** (Configure the Gateway).
8. Select option **1** (Java VM) and verify that the Java VM settings are correct.
9. Select option **2** (Database Connection) and then configure the Gateway to use the embedded database.
10. Exit the Gateway main menu and reboot the computer.
11. Restore the database by copying the backup made in step 2 on page 36 back to this directory:

    /opt/SecureSpan/Gateway/node/default/var/

12. Change the ownership and permissions back for the database directory and all of its subdirectories/files:
    - Change the owner of database directory (in step 11) from **root** to **gateway**.
    - Change the permissions of database directory to **rwxrwxr-x**
    - Change the permissions of the following directory and all its subdirectories to **rwxrwxr-x**

      /opt/SecureSpan/Gateway/node/default/var/db/ssgdb

    - Change the permissions of all files within the “ssgdb” directory (from above) to **rw-rw-r- -**
    - Change the permissions of the subdirectories within the “ssgdb” directory (from above) to **rwxrwxr-x**
    - Change the permissions of the following log file to **rw-rw-r- -**

      /opt/SecureSpan/Gateway/node/default/var/db/derby.log

13. Start the Gateway with this command:

    ```
    # /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start
    ```

The upgrade is now complete.

Solaris Upgrade

Perform the appropriate section to upgrade the Gateway running on Solaris.

If Using the MySQL Database

Ø *To upgrade the Solaris 10 version of the Gateway using MySQL database:*

1. On the Solaris Gateway server, install the JDK for Solaris and note the installation path. This JDK is available from *java.sun.com/javase/downloads/index.jsp*.
2. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7 from the Oracle web site. Unzip the files in **UnlimitedJCEPolicyJDK7.zip**[2] and then copy the extracted *jce_policy-7/**jce/****** files to the following JDK 1.7 *jre/lib/security* directory (based on the JDK 1.7 having been installed to the default directory */usr/j2se/*):

   cp jce_policy-7/jce/* /usr/j2se/jdk1.7.0_*xx*/jre/lib/security/

   Where *"xx"* represents the most recent update of JDK 1.7.

   Note: Ensure that the copied policy files are readable by other than the owner. They may not be, depending on the umask of the user used to copy the files.

3. If you have previously upgraded the MySQL software but not yet run "mysql_upgrade", navigate to the MySQL directory and run:

   # mysql_upgrade --skip-write-binlog

Next, do the following to upgrade the Gateway software:

4. Stop the slave in MySQL on all nodes in the cluster.
5. Run the following command to remove the old installation:

   # pkgrm L7TECHssg-*<version>*

6. Copy the new Gateway software package **L7TECHssg**-<*version*>**.pkg** to the host machine.
7. Run the following command to install the Gateway software:

   # pkgadd -d L7TECHssg-*<version>***.pkg**

8. Enter **Y** when prompted whether to install the conflicting files, and then enter **Y** to confirm installing <L7TECHssg>.
9. Open *my.cnf* for editing:

   # edit my.cnf

[2] can be obtained from: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

10. Add the following properties to *my.cnf*:

    ```
    log_bin_trust_function_creators=1
    slave_exec_mode=IDEMPOTENT
    ```

    See Figure 1 on page 33 for an example.

11. Restart the MySQL service on all nodes in the cluster.
12. Run the following to configure the Gateway:

    ```
    # /opt/SecureSpan/Gateway/runtime/bin/setup.sh
    ```

    The Layer 7 Gateway main menu appears.

13. Select option **2** (Configure the Gateway).
14. Select option **1** (Java VM) and verify that the Java VM settings are correct.
15. Select option **2** (Database Connection) and then verify that the database connection settings are correct. The settings from the previous version of the Gateway should be displayed as the default for each setting. Press [**Enter**] to use the existing value from the previous installation. You will need to enter the password of the database from the previous installation.
16. Select option **1** (Upgrade the Gateway database) and follow the prompts to upgrade the database.
17. Start the Gateway:

    ```
    /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start
    ```

The upgrade is now complete.

If Using the Embedded Database

Ø *To upgrade the Solaris 10 version of the Gateway using the embedded database:*

1. Stop the Gateway service with this command:

   ```
   /opt/SecureSpan/Gateway/runtime/bin/gateway.sh stop
   ```

2. Back up the previous embedded database by copying this directory to your local directory:

   /opt/SecureSpan/Gateway/node/default/var/db

3. Remove the old installation with this command:

   ```
   # pkgrm L7TECHssg-<version>
   ```

4. Remove this directory:

   /opt/SecureSpan

5. Reboot the computer.
6. Copy the new Gateway software package **L7TECHssg**-<*version*>**.pkg** to the host machine.

7. Install the Gateway software with this command:

   # pkgadd -d L7TECHssg-*<version>*.pkg

8. Enter **Y** when prompted whether to install the conflicting files, then enter **Y** to confirm installing <L7TECHssg>.

9. Run the following to configure the Gateway:

   # /opt/SecureSpan/Gateway/runtime/bin/setup.sh

   The Layer 7 Gateway main menu appears.

10. Select option **2** (Configure the Gateway).

11. Select option **1** (Java VM) and verify that the Java VM settings are correct.

12. Select option **2** (Database Connection) and then configure the Gateway to use the embedded database.

13. Exit the Gateway main menu and reboot the computer.

14. Restore the database by copying the backup made in step 2 on page 36 back to this directory:

    /opt/SecureSpan/Gateway/node/default/var/

15. Change the ownership and permissions back for the database directory and all of its subdirectories/files:

    - Change the owner of database directory (in step 14) from **root** to **gateway**.
    - Change the permissions of database directory to **rwxrwxr-x**
    - Change the permissions of the following directory and all its subdirectories to **rwxrwxr-x**

      /opt/SecureSpan/Gateway/node/default/var/db/ssgdb

    - Change the permissions of all files within the “ssgdb” directory (from above) to **rw-rw-r- -**
    - Change the permissions of the subdirectories within the “ssgdb” directory (from above) to **rwxrwxr-x**
    - Change the permissions of the following log file to **rw-rw-r- -**

      /opt/SecureSpan/Gateway/node/default/var/db/derby.log

16. Start the Gateway with this command:

    /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start

The upgrade is now complete.

Migrating to Version 8.0 under RHEL 6

This section describes how to migrate your v7.1 Gateway database to a host computer running RHEL 6 (either same machine or different machine).

Ø *To migrate Gateway information to version 8.0:*

1. On the version 7.1 Gateway, log in to MySQL and use the following command to back up the database to a file named "ssgbackup.sql":

   mysql> mysqldump --add-drop-table --routines ssg > ssgbackup.sql

   Be sure to store *ssgbackup.sql* in a safe place.

2. If your Gateway includes the OAuth Toolkit (OTK), use this command to back up the OTK database to a file named "otkbackup.sql":

   mysql> mysqldump --add-drop-table otk_db > otkbackup.sql

   Be sure to store *otkbackup.sql* in a safe place.

3. Enter the following command and make a note of the *mysql.users* grants:

   mysql -e 'select user,host,password from mysql.user;'

4. Install version 8.0 of the Gateway:

   - **On same machine:** Follow the steps under "RHEL/SUSE Linux Upgrade" on page 31.
   - **On different machine:** Install version 8.0 as a new system and configure it as necessary. Detailed instructions for doing this are provided in Chapter 3, "Installing and Configuring the Gateway" in the *Layer 7 Installation and Maintenance Manual (Software Edition)*.

5. On the version 8.0 Gateway, log in to MySQL and enter the following command to drop the database:

   mysql> mysqladmin drop ssg

   Enter **Y** to confirm the drop.

6. Create a new Gateway database with this command:

   mysql> mysqladmin create ssg

7. Apply the necessary grants with these commands:

   # mysql ssg

   mysql> grant all on ssg.* to gateway@localhost identified by '7layer';

   mysql> grant all on ssg.* to gateway@localhost.localdomain identified by '7layer';

8. Restore the backup file(s) created in steps 2 and 3 above:

   mysql> mysql ssg < ssgbackup.sql

   mysql> mysql ssg < otkbackup.sql *(only if OAuth Toolkit is present)*

   Your version 7.1 database is now migrated to version 8.0.

9. Return to the command prompt and access the Gateway main menu with this command:

   ```
   # /opt/SecureSpan/Gateway/runtime/bin/setup.sh
   ```

10. Select option **1** (Upgrade the Layer 7 Gateway database). It may take a moment for the upgrade to complete.

11. Select **X** (Exit) to return to the command prompt.

12. Start the Gateway with this command:

    ```
    # /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start
    ```

This completes the upgrade process. Connect to the v8.0 Gateway using the Layer 7 Policy Manager and install the new license file. Tip: Be sure to use the new v8.0 license file provided; your old v7.1 license will no longer work.

Appendix A: Cluster Configuration Worksheet

Use the following worksheet to record configuration information for upgrading clusters.

Table 1: Upgrade cluster configuration worksheet

Description	Example Value	MY VALUE
Gateway cluster Fully-Qualified Domain Name (FQDN)	clusterhostname.mycompany.com	
IP address for clusterhostname (load balancer)	10.0.0.10	
Gateway node host names	ssg1.mycompany.com, ssg2.mycompany.com	
IP addresses for nodes	10.0.0.11, 10.0.0.12	
MySQL database nodes	ssg1.mycompany.com, ssg2.mycompany.com	
MySQL root user name	root	
MySQL root user password	password	
MySQL database replication username	repluser	
MySQL database replication password	replpass	
Gateway database name	ssg	
Gateway database user	gateway	
Gateway database password	7layer	
Keystore password	7layer	
Cluster Configuration passphrase	7layer	

Appendix B: Default Manifest

When upgrading a virtual appliance, you can create a custom manifest to specify which OS-level files to include in a custom backup. For more information, see "Custom Backup" on page 22.

A custom manifest is created based on the default manifest, which contains the following files:

/etc/hosts
/etc/iproute2/rt_tables
/etc/ldap.conf
/etc/localtime
/etc/motd
/etc/nsswitch.conf
/etc/ntp.conf
/etc/ntp/keys
/etc/ntp/step-tickers
/etc/openldap/ldap.conf
/etc/pam.d/login
/etc/pam.d/sshd
/etc/pam.d/system-auth-ac
/etc/pam_radius.conf
/etc/rc.local
/etc/resolv.conf
/etc/rsyslog.conf
/etc/skel_ssg/.bash_logout
/etc/skel_ssg/.bash_profile
/etc/skel_ssg/.bashrc
/etc/snmp/snmpd.conf
/etc/ssh/ssh_allowed_users
/etc/ssh/sshd_config
/etc/sysconfig/authconfig
/etc/sysconfig/clock
/etc/sysconfig/i18n
/etc/sysconfig/iptables
/etc/sysconfig/keyboard