Opsware® SAS 6.61 Upgrade Guide

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Opsware SAS Version 6.61

Table of Contents

Preface

This guide describes how to upgrade Opsware SAS and is intended to be used by Opsware, Inc. Professional Services.

Conventions in this Guide

- For ease of readability, this document may use “6.x” to refer to the following Opsware SAS versions that you are upgrading from: SAS 6.51.x or 6.6.
- In Table 3-1, “Locating Parameter Values to Verify the Response File,” on page 10, 6.x refers to 6.5.1.x, and 6.6.

The table below describes the sections of this guide relevant to your installed SAS version:.

SAS Upgrade Guide Section	Contains Instructions For
“Upgrading a Standalone Core from 6.x to 6.61” on page 25	Upgrading an Opsware Core from Opsware SAS 6.5.1.x, or 6.6 to 6.61
“Upgrading a Multimaster Mesh from 6.x to 6.61” on page 27	Upgrading a multimaster mesh from Opsware SAS 6.5.1.x, or 6.6 to 6.61
“Upgrading an Opsware Satellite from 6.x to 6.61” on page 32	Upgrading an Opsware Satellite from Opsware SAS 6.5.1.x, or 6.6 to 6.61

Upgrading to Opsware SAS 6.61

IN THIS DOCUMENT

This document discusses the following topics:

Supported Upgrade Paths

The Opsware SAS 6.61 release supports the following types of upgrades:

- Upgrading a standalone core from Opsware SAS 6.5.1.x, and 6.6 to 6.61
- Upgrading a multimaster mesh from Opsware SAS 6.5.1.x and 6.6 to 6.61
- Upgrading an Opsware Satellite from Opsware SAS 6.5.1.x, and 6.6 to 6.61

For information about how to upgrade Opsware Agents to Opsware SAS 6.61, see the *Opsware® SAS User's Guide: Server Automation*.

Dual Layer DVD Requirements

The Product Software DVD and the Agent and Utilities DVD require a DVD drive that supports dual layer. See the *Opsware® SAS Planning and Installation Guide* for more information about the installation media for the Opsware Installer.

Rolling Mesh (Mesh Up) Upgrades

SAS 6.61 supports Rolling Mesh (mesh up) upgrades from SAS 6.6 only through the use of tunneled connections between Core Gateways and Agent and Satellite gateways that allow management of a core's servers to be taken over by other cores while it is down for upgrade. For more information about Rolling Mesh Upgrades, see "Rolling Mesh (Mesh Up) Upgrade (6.6 to 6.61Only)" on page 33.

Opsware Installer Upgrade Script

To upgrade components in a core, you run the Opsware Installer upgrade script using DVD media by entering the following command:

```
/<Opsware_SAS_6.61_distribution_path>/opsware_installer/
upgrade_opsware.sh -r <full_path_to_response_file>
```

Before running the upgrade script `upgrade_opsware.sh`, you must change directories to the root directory by entering the following command:

```
cd /
```

You must provide the full path to the response file.

Mount the Opsware SAS software on all core servers by mounting the DVD or NFS-mount a directory that contains the Opsware SAS software distribution contents.

The Opsware Installer must have root read access to the directories from where it installs Opsware components, even NFS-mounted network appliances.

The Opsware upgrade script displays a list of components that you can choose to upgrade. The list only contains components that have been installed on the server where you are running the script.

Configuration and Customizations

When running the Opsware SAS 6.61 Installer to upgrade a core to 6.61, the Installer preserves certain configuration files.

Backups of the configuration files are copied to the following location:

```
/var/opt/opsware/install_opsware/config_file_archive/
<config_file_original_path>/<filename>.<timestamp>
```

After the upgrade, you can use these backups to help you merge your customizations back into the correct Opsware SAS configuration files.

To use WinPE-based Windows OS Provisioning on an upgraded core, make sure that the `authoritative` keyword in the `/etc/opt/opsware/dhcpd/dhcpd.conf` file on the boot server is uncommented. If you modify the `dhcpd.conf` file, you must restart the dhcp server, by running `/etc/init.d/opsware-sas restart dhcpd`.

Preparation for Opsware SAS Upgrade

Preparation for All Upgrades to Opsware SAS 6.61

Before you upgrade an Opsware standalone core or multimaster core, perform the following tasks:

- Obtain the response files that were created when you deployed Opsware SAS.

  The Opsware Installer saves the response file in the following directory on the servers where you installed the Opsware SAS components:

  `/var/opt/opsware/install_opsware/resp/resp.<timestamp>`

  By looking at the timestamp, choose the latest version of the response file.

- The server running the Opsware Gateway component must be set up to resolve `wordcache` to the hostname for the server running the Opsware Software Repository
- The Opsware Gateway must be up and running for all Opsware SAS upgrades.
- The core servers with the Model Repository and the Software Repository must have the `en_US.UTF-8` locale installed. To display data from managed servers in various locales, the core server with the Opsware Global File System (OGFS) must have those locales installed.
- Verify the response file:

  Check that the values in your response file match the actual core configuration. If you have changed any of the values that are used in the response file, update the response file accordingly.

  See “Verify the Response File Before Upgrading” on page 10.

- Notify Opsware SAS users to cancel all scheduled Reconcile Patches jobs. After upgrading a standalone or multimaster core to 6.61, Opsware SAS users will not see their Reconcile Patches jobs in the Job Logs (SAS Client) or the My Jobs list (SAS Web Client) that ran or are scheduled to run. (By default, the data about a job is cleared from the Job Logs (SAS Client) and the My Jobs list (SAS Web Client) after 30 days.)

  After the upgrade, set up the scheduled reconcile patch jobs again by using the Remediate function in the Opsware SAS Client UI.

Preparation for All Multimaster Upgrades to Opsware SAS 6.61

Before you upgrade an Opsware multimaster core to SAS 6.61, perform the following task:

- Log in to the Opsware SAS Web Client as a member of the Opsware System Administrator group and check for and resolve multimaster conflicts by using the Multimaster Tools.

See the *Opsware® SAS Administration Guide* for information about running the Multimaster Tool.

See the *Opsware® SAS Administration Guide* for information about the types of Opsware administrators – the Opsware admin user and the Opsware System Administrators group.

You cannot proceed with an upgrade of a core in a multimaster mesh if multimaster conflicts are present in the mesh.

The Opsware Installer checks for conflicts right after you run the upgrade script. If conflicts are present, the Opsware Installer displays the a message similar to the following:

```
[root@yellow1 root]# /var/opsware/disk001/opsware_installer/
upgrade_opsware.sh -r /OPSW/yellow_mm_601.resp
Distribution version = opsware_32.a

Verifying no conflicts exist in DB "yellow_truth": FAILURE
(multiple rows selected)

Conflicts were detected in the Truth database. Please re-
start the core and resolve the conflicts before attempting to
perform this upgrade.

Upgrade aborted.
```

Where `yellow_truth` is the tnsname of the database.

Preparation for Windows Patch Management for All Upgrades

For all upgrades, Opsware recommends that you download the latest version of all required Windows utilities.

See the *Opsware® SAS Planning and Installation Guide* for information about these required utilities which include:

- mbsaclie.exe
- qchain.exe
- wsusscn2.cab

- WindowsUpdateAgent20-x86.exe
- WindowsUpdateAgent20-x64.exe
- mbsacli20.exe
- wusscan.dll

Preparation for Visual Packager for Opsware SAS 6.0 and Later

If you are using Visual Packager 6.0.1 or later, you must use version 3.x of the IDK (Intelligent Software Module Development Kit). ISMs created with version 3.x of the IDK are compatible only with SAS 6.x versions. You cannot upload ISMs from IDK 1.x or 2.x into Opsware SAS 6.x. You cannot upload ISMs from IDK 3.x into Opsware SAS 5.x (or earlier). For more information about the IDK, see the *Opsware® SAS Content Utilities Guide*.

Verify the Response File Before Upgrading

The following table provides information about how to locate the values for the parameters in the response file that are in use in Opsware SAS. For ease of readability, 6.x in this table refers to Opsware SAS 6.5.1.x, and 6.6.

Table 3-1: Locating Parameter Values to Verify the Response File

PARAMETER	HOW TO FIND THE CURRENT VALUE
cast.admin_pwd	This parameter contains the password for the Opsware admin user. To verify that you have the correct value, log in to the Opsware SAS Web Client as the admin user.
decrypt_passwd	This parameter contains the password to decrypt the database of crypto material. The value for this parameter does not change after installing Opsware SAS. The value should be correct in the response file.
truth.authDom	Log in to the Opsware SAS Web Client, click System Configuration in the navigation panel, and then click Command Engine and look up the value for `auth_domain`.

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
truth.dcId	Log in to the Opsware SAS Web Client, click Facilities in the navigation panel and click the facility name for the facility you are upgrading to see its ID number.
truth.dcNm	Log in to the Opsware SAS Web Client, click Facilities in the navigation panel and click the facility name for the facility you are upgrading to see its short name.
truth.dcDispNm	Log in to the Opsware SAS Web Client, click Facilities in the navigation panel and click the facility name for the facility you are upgrading to see its display name.
truth.dcSubDom	Log in to the Opsware SAS Web Client, click System Configuration in the navigation panel, and then click the facility name for the facility you are upgrading; look up the value for opsware.core.domain.
truth.dest	This parameter is not required for upgrades.

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

truth.gcPwd	This parameter contains the password for the Oracle `gcadmin` user. To verify that you have the correct value, log in to the Model Repository (truth) database as the `gcadmin` user with this password. The Oracle gcadmin user does not have permission to log in to Oracle. If you have entered the correct password, the following message appears:
	`ORA-01045: user GCADMIN lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/ password; logon denied`

truth.lcrepPwd	This parameter contains the password for the Oracle lcrep user. To verify that you have the correct value, log in to the Model Repository (truth) database as lcrep with this password. The Oracle lcrep user does not have permission to log in to Oracle.
	If you have entered the correct password, the following message appears:
	`ORA-01045: user LCREP lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/ password; logon denied`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
truth.oaPwd	This parameter contains the password for the Oracle opsware_admin user. To verify that you have the correct value, log in to the Model Repository (truth) database as opsware_admin with this password.

truth.orahome	Log on to the server running the Model Repository (truth) component and enter the following command:
	`su - oracle`
	`echo $ORACLE_HOME`

truth.pubViewsPwd	The value for this parameter does not change after installing Opsware SAS. The value should be correct in the response file.
truth.servicename	This parameter contains the tnsname of the Model Repository (truth) database. Check `/var/opt/oracle/tnsnames.ora` on the server running the Model Repository (truth) component to find the value.
truth.sourcePath	This parameter is not required for upgrades.
truth.spinPwd	This parameter contains the password for the Oracle spin user. To verify that you have the correct value, log in to the Model Repository (truth) database as spin with this password
truth.tnsdir	This parameter contains the directory where the `tnsnames.ora` file is stored. Typically, this file is stored in the directory `/var/opt/oracle`.

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

truth.aaaPwd	This parameter contains the password for the Oracle aaa user. To verify that you have the correct value, log in to the Model Repository (truth) database as user aaa with this password. The Oracle aaa user does not have permission to log in to Oracle.
	
	If you have entered the correct password, the following message appears:
	
	`ORA-01045: user AAA lacks CREATE SESSION privilege; logon denied`
	
	If you have entered an incorrect password, the following message appears:
	
	`ORA-01017: invalid username/ password; logon denied`

truth.truthPwd	This parameter contains the password for the Oracle truth user. To verify that you have the correct value, log in to the Model Repository (truth) database as truth with this password. The Oracle truth user does not have permission to log in to Oracle.
	
	If you have entered the correct password, the following message appears:
	
	`ORA-01045: user TRUTH lacks CREATE SESSION privilege; logon denied`
	
	If you have entered an incorrect password, the following message appears:
	
	`ORA-01017: invalid username/ password; logon denied`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
truth.twistPwd	This parameter contains the password for the Oracle twist user. To verify that you have the correct value, log in to the Model Repository (truth) database as twist with this password.
truth.vaultPwd	This parameter contains the password for the Oracle vault user. To verify that you have the correct value, log in to the Model Repository (truth) database as vault with this password. This parameter is only relevant to Opsware multimaster cores.
twist.buildmgr.passwd	On the server where the Opsware OS Provisioning Build Manager component is installed, check the file `/var/opt/opsware/crypto/buildmgr/twist.passwd`
twist.integration.passwd	On the server where the Opsware SAS Web Client component is installed, check the file `/opt/opsware/twist/Defa...` In the file, locate the entry for the Integration password by searching for `uid=integration,ou=people` and reading the `userpassword` attribute.
media_server.linux_media	This parameter contains the location of your Linux OS media. Check the server where the Opsware OS Provisioning Media Server component is installed. Because this media is NFS exported, you can check the `/etc/exports` file (Linux) or the `/etc/dfs/dfstab` file (Solaris).

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
media_server.sunos_media	This parameter contains the location of your Solaris OS media. Check the server where the Opsware OS Provisioning Media Server component is installed. Because this media is NFS exported, you can check the `/etc/exports` file (Linux) or the `/etc/dfs/dfstab` file (Solaris).
word.remove_files	This parameter is not required for upgrades.
media_server.windows_media	This parameter contains the location of your Windows OS media. Check the server where the Opsware OS Provisioning Media Server component is installed. Check the file to see what this value is set to. `/etc/opt/opsware/samba/smb.conf`
media_server.windows_share_name	On the server where the Opsware OS Provisioning Media Server component is installed, see the file `/opt/OPSWsamba/etc/smb.conf` for the value.
media_server.windows_share_password	This password is only used when importing Windows OS media; it is not used internally by Opsware SAS. You cannot recover or validate the current Windows share password; however, you can set it or reset it during the upgrade.
boot_server.buildmgr_host	Log in to the Opsware SAS Web Client, click Service Levels in the navigation panel, click Opsware, click **buildmgr**, and then click the Members tab.

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
boot_server.speed_duplex	On the server running the OS Provisioning Boot Server, check the file `/opt/OPSWboot/jumpstart/Boot /etc/.speed_duplex.state`
truth.uninstall.needdata	This parameter is not required for upgrades. (It is only relevant when uninstalling Opsware SAS.)
truth.uninstall.aresure	This parameter is not required for upgrades. (It is only relevant when uninstalling Opsware SAS.)
bootagent.host	This parameter contains the hostname of the OS Provisioning Boot Server. Log in to the Opsware SAS Web Client, click Service Levels in the navigation panel, click Opsware, click boot_server, and then click the Members tab.
truth.sid	On the server running the Model Repository (truth) component, check the `tnsnames.ora` file; for example, if the file contains an entry similar to this: `devtruthac03 = (DESCRIPTION=(ADDRESS= (HOST=truth.XXX.dev.example.com)(PO RT=1521) (PROTOCOL=tcp))(CONNECT_DATA= (SERVICE_NAME=truth)))` Then, the SID for the Model Repository is `truth`.
save_crypto	This parameter is not required for upgrades. (It is only relevant when uninstalling Opsware SAS.)

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE
agent_gw_list_args	This value is required only when upgrading an Opsware Satellite. Obtain this value from the Gateway Properties file on the server running the Opsware Gateway component. In the properties file, locate the values for the following parameters: `opswgw.GWAddress` -> contains the value for the IP address of the server running the Opsware Gateway component. `opswgw.ProxyPort` -> contains the value for the port number that the Opsware Agents use to communicate with the Opsware Gateway (port 3001 by default).
default_locale	Log in to the Opsware SAS Web Client to determine which locale is being used by Opsware SAS (the locale value is apparent from the SAS Web Client UI).

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

ogfs.store.host	`Linux`: on the server running the OGFS component, check the value in the `/etc/fstab` file. The entry is specified as follows:
	`# Begin Opsware Global Filesystem mounts`
	`<ogfs.store.host>``:<ogfs.store.path> /var/opt/OPSWmnt/store nfs <ogfs.audit.host>:<ogfs.audit.path> /var/opt/OPSWmnt/audit nfs`
	`# End Opsware Global Filesystem mounts`
	Solaris: on the server running the OGFS component, check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<`**`ogfs.store.host`**`>:<ogfs.store.path> /var/opt/opsware/ogfs/mnt/store nfs intr,bg,xattr,dev=43c0003 1167864831`
	`<ogfs.audit.host>:<ogfs.audit.path> /var/opt/opsware/ogfs/mnt/audit nfs rw,xattr,dev=43c0004 1167864831`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

ogfs.store.path	**Linux**: on the server running the OGFS component, check the value in the file `/etc/fstab`. The entry is specified as follows:
	`# Begin Opsware Global Filesystem mounts`
	`<ogfs.store.host>:`**`<ogfs.store.path>`**
	`/var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host>:<ogfs.audit.path>`
	`/var/opt/OPSWmnt/audit nfs`
	`# End Opsware Global Filesystem mounts`
	`Solaris`: on the server running the OGFS component, check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<ogfs.store.host>:<`**`ogfs.store.path`**`>`
	`/var/opt/opsware/ogfs/mnt/storenfs intr,bg,xattr,dev=43c0003 1167864831`
	`<ogfs.audit.host>:<ogfs.audit.path>`
	`/var/opt/opsware/ogfs/mnt/auditnfs rw,xattr,dev=43c0004 1167864831`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

ogfs.audit.host	**Linux**: on the server running the OGFS component, check the value in the file `/etc/fstab` (Linux). The entry is specified as follows:
	
	`# Begin Opsware Global Filesystem mounts`
	`<ogfs.store.host>:<ogfs.store.path> /var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host>:<ogfs.audit.path> /var/opt/OPSWmnt/audit nfs`
	`# End Opsware Global Filesystem mounts`
	
	Solaris: on the server running the OGFS component, check the value in the `/etc/mnttab` file. The entry is specified as follows:
	
	`<ogfs.store.host>:<ogfs.store.path> /var/opt/opsware/ogfs/mnt/storenfs intr,bg,xattr,dev=43c0003 1167864831`
	
	`<ogfs.audit.host>:<ogfs.audit.path> /var/opt/opsware/ogfs/mnt/auditnfs rw,xattr,dev=43c0004 1167864831`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

ogfs.audit.path	**Linux**: on the server running the OGFS component, check the value in the file `/etc/fstab`. The entry is specified as follows:
	`# Begin Opsware Global Filesystem mounts`
	`<ogfs.store.host>:<ogfs.store.path> /var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host>:`**`<ogfs.audit.path>`**
	`/var/opt/OPSWmnt/audit nfs`
	`# End Opsware Global Filesystem mounts`
	Solaris: on the server running the OGFS component, check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<ogfs.store.host>:<ogfs.store.path> /var/opt/opsware/ogfs/mnt/storenfs intr,bg,xattr,dev=43c0003 1167864831`
	`<ogfs.audit.host>:<`**`ogfs.audit.path`**`> /var/opt/opsware/ogfs/mnt/auditnfs rw,xattr,dev=43c0004 1167864831`

truth.detuserpwd	On the server running the Opsware SAS Web Client component, check the value in the file `/var/opt/opsware/crypto/twist/detuserpwd`
windows_util_loc	This parameter contains the directory where the seven Patch Management utilities are located. See “Preparation for Windows Patch Management for All Upgrades” on page 9.

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

cgw_admin_port	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware Gateway component, check the files:
	`/etc/opt/opsware/opswgw-cgw0-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgw0-<truth.dcNm>/opswgw.pem`

cgw_address	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware Gateway component, check the files:
	`/etc/opt/opsware/opswgw-cgw0-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgw0-<truth.dcNm>/opswgw.pem`

cgw_proxy_port	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware Gateway component, check the files:
	`/etc/opt/opsware/opswgw-cgw0-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgw0-<truth.dcNm>/opswgw.pem`

Table 3-1: Locating Parameter Values to Verify the Response File (continued)

PARAMETER	HOW TO FIND THE CURRENT VALUE

agw_proxy_port	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware Gateway component, check the files:
	`/etc/opt/opsware/opswgw-agw0-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-agw0-<truth.dcNm>/opswgw.pem`

cgw_tunnel_listener_port	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware Gateway component, check the files:
	`/etc/opt/opsware/opswgw-cgw0-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgw0-<truth.dcNm>/opswgw.pem`
	NOTE: The file might contain two entries for `opswgw.TunnelDst`. Use the value from the line that specifies `opswgw.pem`.

hub.ip	To verify whether the value for this parameter is correct in the response file, on the server running the Opsware SAS Web Client component, check the file:
	`/etc/opt/opsware/opswgw-lb/opswgw.properties`
	`opswgw.LoadBalanceRule=tcp:hub:ssh:STICKY:<hub.ip>:2222`

Upgrading a Standalone Core from 6.x to 6.61

The following procedure describes how to upgrade an Opsware SAS standalone core.

To upgrade the Opsware components, perform the following steps:

1. From the *Opsware SAS 6.61 Product Software* DVD, invoke the Opsware Installer upgrade script by entering the following command. You must have the response file used to install Opsware SAS.

   ```
   /<Opsware_SAS_6.61_distribution_path>/opsware_installer
   /upgrade_opsware.sh -r <full_path_to_response_file>
   ```

   If you are not sure where the response file is, use the latest file from `/var/opt/opsware/install_opsware/resp`.

2. Select 1: Standalone Installation: Standalone Opsware Core.

3. Select the simple or advanced interview mode. The Opsware Installer starts the interview mode.

4. Save the response file and copy it to all the servers in the core running an Opsware component.

5. Stop all installed Core Components including the Core Gateway with the command:

   ```
   /etc/init.d/opsware-sas stop <component>
   ```

6. Start the Core Gateway:

   ```
   /etc/init.d/opsware-sas start opswgw-cgw0
   ```

7. Invoke the upgrade script on each of the core servers. You must upgrade the SAS Components in the following order:

   1. Model Repository
   2. Data Access Engine (spin)
   3. Command Engine (way)
   4. Software Repository (word)
   5. Opsware Global Filesystem Server (OGFS)
   6. Opsware Command Center (OCC)
   7. OS Provisioning Media Server

8. OS Provisioning Build Manager
9. Opsware Gateway
10. OS Provisioning Boot Server

You can select multiple components at a time if they are installed on the same host as long as you preserve the overall ordering.

8 Install the Opsware SAS 6.61 content by performing the following steps:

1. From the Software Repository server, mount the "Agent and Utilities" DVD and invoke `upgrade_opsware.sh` script with the response file that you generated for the core installation.

   ```
   /<Opsware_SAS_6.61_content_upload_path>/opsware_
   installer/upgrade_opsware.sh -r /<full_path_to_response_
   file>
   ```

   The following prompt appears:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.
   1 ( ) Software Repository - Content (install once per mesh)
   2 ( ) Add OS Provisioning Stage2 Images to Software
   Repository
   Enter a component number to toggle ('a' for all, 'n' for
   none).
   When ready, press 'c' to continue, or 'q' to quit.
   ```

2. Select 1 to install the Software Repository – Content component.
3. If you encounter communication timeout errors when installing the content, restart the Multimaster Software Repository component by entering the following commands; then repeat sub-step 1 and sub-step 2 in this step:

   ```
   /etc/init.d/opsware-sas restart mm_wordbot
   ```

   If restarting the Multimaster Software Repository component does not solve the problem, restart all the Opsware SAS components on the Software Repository server by entering the following command; then repeat sub-step 1 and sub-step 2 in this step:

   ```
   /etc/init.d/opsware-sas restart
   ```


9 Verify that the Opsware core upgraded successfully. Log in to the Opsware SAS Web Client as a member of the Opsware System Administrator group and run the System Diagnosis tool on the core. See the *Opsware® SAS Administration Guide* for information about running the System Diagnosis tool.

After you upgrade Opsware SAS, you need to upgrade the Opsware Agent on each managed server in the facility. The latest version of the Opsware Agent enables you to use new SAS features in the Opsware core. See the *Opsware® SAS User's Guide: Server Automation* for information about the Opsware Agent Upgrade Tool.

Upgrading a Multimaster Mesh from 6.x to 6.61

1 From the Model Repository server, mount the Opsware SAS 6.61 "Product Software" DVD and invoke the Opsware Installer upgrade script by entering the following command. You must have the response file used to install Opsware SAS 6.5.1.x.

```
/<Opsware_SAS_6.61_distribution_path>/opsware_installer/
upgrade_opsware.sh -r <full_path_to_response_file>
```

2 On the **source** core, perform the following steps to complete the interview process:

1. Select 2 - Multimaster Installation: First Core (convert from standalone).
2. Select the simple or advanced interview mode. The Opsware Installer starts the interview mode.
3. Save the response file and copy it to all servers in the source core running an Opsware component.

3 For each **destination** core in the mesh, perform the following steps to complete the interview process:

1. Invoke the Opsware Installer upgrade script.
2. Select 4 - Multimaster Installation: Additional Core.
3. Select the simple or advanced interview mode. The Opsware Installer starts the interview mode.
4. Save the response file and copy it to all servers in each **destination** core running an Opsware component.

4 In all Opsware cores, stop all Opsware components except the Opsware core-side Gateway. Do not stop the Oracle database.

1. On each core server in each core, run the following command:

```
/etc/init.d/opsware-sas stop
```

2. On the server running the Opsware Gateway component, run the following command:

```
/etc/init.d/opsware-sas start opswgw-cgw0
```

5 After all Opsware components have been stopped, if necessary, unmount the Global Shell audit file system (if this file system is NFS mounted).

1. To determine whether the audit file system is NFS mounted, enter the following command (*the path for your system may be different, see the value for ogfs.audit.path and/or ogfs.audit.store*):

```
% df -k /var/opt/opsware/ogfs/mnt/audit.
```

2. To unmount the file system, enter the following command (*the path for your system may be different, see the value for ogfs.audit.path and/or ogfs.audit.store*):

```
% umount /var/opt/opsware/ogfs/mnt/audit.
```

   Because the file system is remounted by the Opsware Installer, there is no requirement to manually remount it.

6 On all **destination** cores, upgrade the Model Repository (truth). Invoke `upgrade_opsware.sh -r <resp_file>`.

1. Select Model Repository Multimaster Component from the menu then press `c` to continue.

   While you upgrade the Model Repository, you might be prompted to confirm the Opsware SAS configuration values.

2. Start the `rvrdscript` and the `vaultdaemon`:

```
/etc/init.d/opsware-sas start rvrdscript vaultdaemon
```

3. Stop the Data Access Engine (spin) on all destination cores.

7 In the **source** core, upgrade all components in the following order. Make sure to invoke the `upgrade_opsware.sh` script with the `-r <response_file>` option.

1. On the server running the Model Repository (truth), select Model Repository (truth), Multimaster Additions.

   While you upgrade the Model Repository, you might be prompted to confirm the Opsware SAS configuration values.

2. On the server running the Data Access Engine (spin), select Data Access Engine (spin), Multimaster Component.
3. On the server running the Model Repository Multimaster Component (vault), select Model Repository Multimaster Component (vault). The Model Repository Multimaster Component (vault) is often installed on the server running the Model Repository.
4. On the server running the Command Engine (way), select Command Engine (way), Multimaster Component.
5. On the server running the Software Repository (word), select Software Repository (word), Multimaster Component.
6. On each server running an Opsware Global Filesystem Server (OGFS), select Opsware Global Filesystem Server (OGFS), multimaster component.
7. On the server running an Opsware Command Center (OCC), select Opsware Command Center (OCC), Multimaster Component.
8. On each server running an Opsware Media Server, select OS Provisioning Media Server.
9. On each server running an Opsware Build Manager, select OS Provisioning Build Scripts.
10. On each server running an Opsware Gateway, select Opsware Gateway.
11. On each server running an OS Provisioning Boot Server component, select OS Provisioning Boot Server.

If the upgrade takes more than an hour from the time spin starts up, some managed devices may be marked unreachable. Run the communications test to resolve this.

8 Let the multimaster traffic propagate to all cores in the multimaster mesh.

Log in to the spin UI in the source core (`https://<hostname or IP address of the spin>:1004`), click Administration ➤ Mesh State to see the status of transactions. The transaction should all appear in black (not yellow, red, or green). To access the spin UI, you need either the browser certificate `browser.p12` or `spin-developer.p12`.

It is essential to wait for all transactions to be received and published at all cores. Upgrading the source core, for example, can generate 5000 transactions that need to be sent to all destination cores in the mesh. If you do not wait long enough for all of these transactions to be published, you can generate many multimaster conflicts.

9 In each **destination** core, upgrade the remaining components in the following order. Make sure to invoke the `upgrade_opsware.sh` script with the `-r <response_file>` option.

1. On the server running the Data Access Engine (spin), select Data Access Engine (spin), Multimaster Component.
2. On the server running the vault, select vault, Multimaster Component.
3. On the server running the Command Engine (way), select Command Engine (way), Multimaster Component.
4. On the server running the Software Repository (word), select Software Repository (word), Multimaster Component.
5. On each server running an Opsware Global Filesystem Server (OGFS), select Opsware Global Filesystem Server (OGFS), multimaster component.
6. On the server running an Opsware Command Center (OCC), select Opsware Command Center (OCC), Multimaster Component.
7. On each server running an Opsware Media Server, select OS Provisioning Media Server.
8. On each server running an Opsware Build Manager, select OS Provisioning Build Scripts.
9. On each server running an Opsware Gateway, select Opsware Gateway.
10. On each server running an OS Provisioning Boot Server component, select OS Provisioning Boot Server.

You can perform sub-step 3 through sub-step 10 in step 9 in parallel in each destination core. However, you must upgrade the Gateway separately.

10 Install the Opsware SAS 6.61 content on the **source** core by performing the following steps:

1. From the Software Repository server, mount the "Agent and Utilities" DVD and invoke `upgrade_opsware.sh` script with the response file that you generated for the core installation.

   ```
   /<Opsware_SAS_6.61_content_upload_path>/opsware_installer/
   upgrade_opsware.sh -r /<full_path_to_response_file>
   ```

   The following prompt appears:

   Welcome to the Opsware Installer.

   Please select the components to install.

   1 ( ) Software Repository – Content (install once per mesh)

   2 ( ) Add OS Provisioning Stage2 Images to Software Repository

   Enter a component number to toggle ('a' for all, 'n' for none).

   When ready, press 'c' to continue, or 'q' to quit.

2. Select 1 to install the Software Repository – Content component.
3. If you encounter communication timeout errors when installing the content, restart the Multimaster Software Repository component by entering the following commands; then repeat sub-step 1 and sub-step 2 in this step:

   ```
   /etc/init.d/opsware-sas restart mm_wordbot
   ```

   If restarting the Multimaster Software Repository component does not solve the problem, restart all the Opsware SAS components on the Software Repository server by entering the following command; then repeat sub-step 1 and sub-step 2 in this step:

   ```
   /etc/init.d/opsware-sas restart
   ```

You need to perform this step only once when upgrading the cores in a multimaster mesh; for example, if you installed the content component in the source core, you do *not* need to install the content in each destination core.

11 On the **Source** Core, select 2 to add OS Provisioning Stage2 Images to the Software Repository. The Stage2 Images must be added to each server with an installed Software Repository.

12 On the **Destination** Cores, select 1 to add OS Provisioning Stage2 Images to the Software Repository. The Stage2 Images must be added to each server with an installed Software Repository.

13 Verify that the Opsware core upgraded successfully. Log in to the Opsware SAS Web Client as a member of the Opsware System Administrator and run the System Diagnosis tool on the core.

See the *Opsware® SAS Administration Guide* for information about running the System Diagnosis tool.

See the *Opsware SAS Configuration Guide* for information about the types of Opsware administrators – the Opsware admin user and the Opsware System Administrators group.

14 Verify that the multimaster mesh is functioning properly after the upgrade. Log in to the Opsware SAS Web Client as the a member of the Opsware System Administrators group, open the Multimaster Tools page (click Administration ➤ Multimaster Tools in the navigation panel).

See the *Opsware® SAS Administration Guide* for information about running the Multimaster Tools.

Upgrading an Opsware Satellite from 6.x to 6.61

You are not required to upgrade your Satellites immediately after a SAS Core upgrade. Satellite upgrades can be delayed and the mesh will function properly.

1. Mount the Opsware SAS 6.61 “Satellite Base” DVD (or “Satellite Base Including OS Provisioning” DVD if you have the OS Provisioning feature installed in the Satellite) and invoke the Opsware Installer upgrade script by entering the following command. You must have the response file used to install Opsware SAS 6.5.1.x or 6.6.

   ```
   /<Opsware_SAS_6.61_satellite_distribution_path>
   /opsware_installer/upgrade_opsware.sh -r
   <full_path_to_response_file>
   ```

2. Select the simple or advanced interview mode. The Opsware Installer starts the interview mode.

3. Go through the interview and save the response file.

   The component menu presents the following components:

   - Opsware Gateway (Interactive Install)
   - Software Repository Cache (wordcache)

4. Select Opsware Gateway (Interactive Install).

   This selection will take you through the interactive Gateway Installer to upgrade the Opsware Gateway.

5. Invoke the `upgrade_opsware.sh` script with the response file you generated and from the component menu, and select Software Repository Cache (wordcache).

6. Using the “Satellite Base Including OS Provisioning” DVD, invoke the `upgrade_opsware.sh` script with the response file you generated and from the component menu, and select OS Provisioning Boot Sever.

7. Using the “Satellite Base Including OS Provisioning” DVD, invoke the `upgrade_opsware.sh` script with the response file you generated and from the component menu, and select OS Provisioning Media Server.

Rolling Mesh (Mesh Up) Upgrade (6.6 to 6.61 Only)

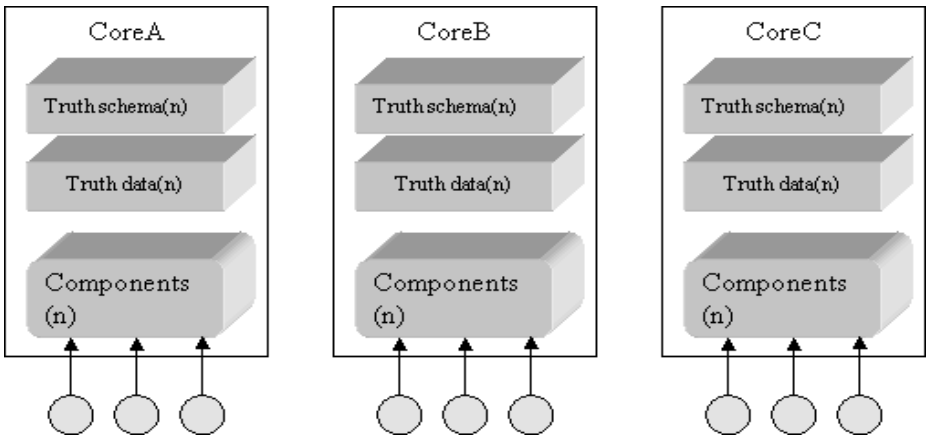
New in SAS 6.61 is the ability to perform *rolling mesh* (mesh up vs. mesh down) upgrades of cores in a Multimaster Mesh. A rolling mesh upgrade is one in which it is not necessary to stop all cores and their components in the mesh before performing the upgrade.

The ability to perform a rolling upgrade allows you to shut down one core at a time, perform the upgrade on that core while the other cores in the mesh takeover management of the mesh's agents and satellites.

Rolling upgrades are ideal where the upgrade is limited in scope and includes no schema changes.

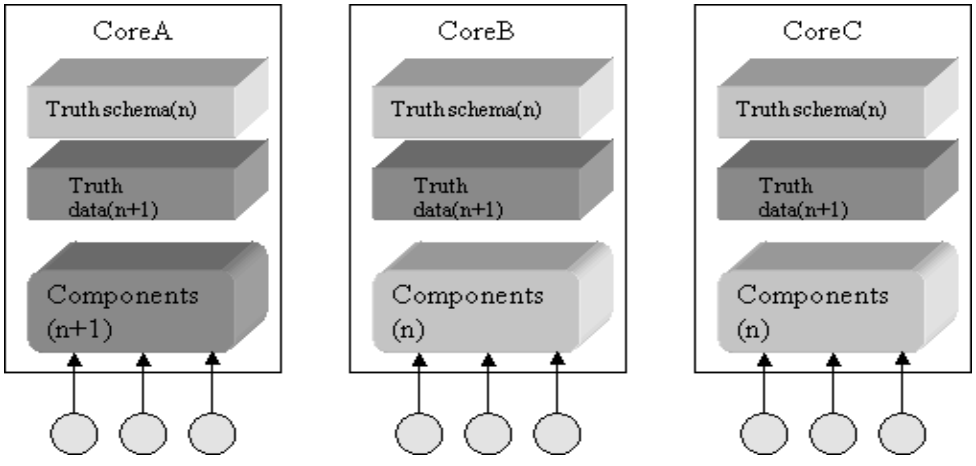
Figure 3-1 illustrates a Multimaster Mesh with three SAS Cores before a rolling upgrade.

Figure 3-1: Multimaster Mesh Cores before a Rolling Mesh Upgrade.



In Figure 3-2, Core A has been shut down and upgraded while Cores B and C continue managing servers. Core A is then brought back up.

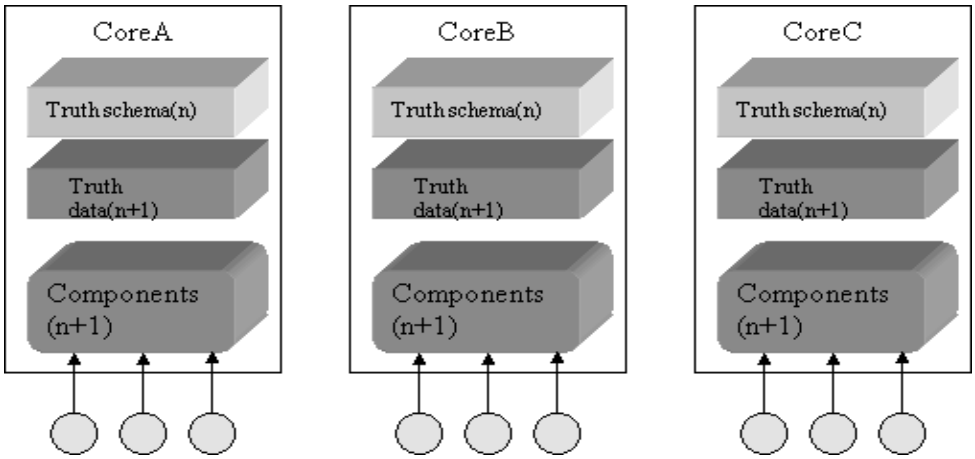
Figure 3-2: Multimaster Mesh Cores after Core A has been Upgraded



At this point, Core A's Model Repository, core components, and data are at a newer version than that of Cores B and C. Therefore, there are mixed-version components running in the same Multimaster Mesh.

In the next phase, Core B is shut down, upgraded, then brought back up followed by Core C (and, one-by-one, all other Cores in the mesh). Figure 3-3 shows the Multimaster Mesh status after the rolling mesh upgrade is complete.

Figure 3-3: Multimaster Mesh Cores after a Complete Rolling Mesh Upgrade



Managing Servers During a Rolling Mesh Upgrade

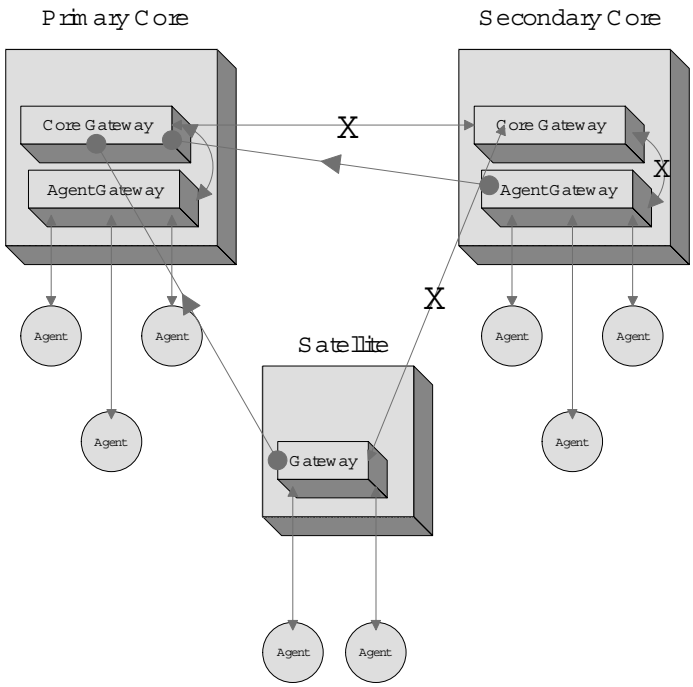
During a rolling mesh upgrade, one core at a time is shut down and upgraded. The existing gateway infrastructure is used to keep that core's agents and satellites manageable by the other cores in the mesh.

This is achieved through the use of *backup gateway tunnels* between all the other cores in the mesh. While a core is down, communication with its agents and satellites continues through these backup gateway tunnels to the other, still active, cores. These backup gateway tunnels must be assigned a higher cost than the tunnel to the Core Gateway on the core being upgraded. When the upgraded core's Core Gateway comes back online, communication will revert to that gateway and the backup gateway tunnels will no longer be used

The cores that are not being upgraded must handle the extra load of managing the agents/satellites of the core that is being upgraded. However, the upgrade itself should not take long, so hopefully the load increase should not be all that significant.

Figure 3-4 shows how communication is maintained between the Satellites and Agents in a mesh through tunneled connections when the Primary Core has been shutdown for upgrade.

Figure 3-4: Agent and Satellite Communication Paths during a Rolling Mesh Upgrade



Rolling Mesh Upgrade Procedure

Use a rolling upgrade only when you must continue to maintain Satellites and Agents in a Multimaster Mesh manageable for the duration of the upgrade.

A Rolling Mesh Upgrade impacts the performance of the mesh when one core is taken down for upgrade. For example, in a three-core mesh, one core handles 10,000 Agents, while the other cores typically handle 500 Agents each. After you create backup tunnels and bring down the larger core for the upgrade, the two smaller cores must temporarily

manage 5500 agents each, 11 times their normal load. This spike in the load could render a core unusable during the course of the Rolling Mesh Upgrade.

A Rolling Mesh Upgrade consists of three phases:

- **Phase 1, Prepare for the Upgrade**: During this phase you will create the backup tunnels for communication between the Satellites and Agents and the cores that will manage them.
- **Phase 2, Upgrade the First Core**: During this phase you will shut down the mesh's First Core, apply the upgrade, and bring the core back up.
- **Phase 3, Upgrade the Secondary Core**: During this phase you will shut down one-by-one the secondary cores, apply the upgrade, and bring the cores back up.

Phase 1: Prepare for the Upgrade

Step 1: Create backup tunnels for the Agents

For the First Core and all other cores in the mesh, create backup tunnels from the Agent Gateway (AGW) to the Core Gateways (CGWs) for all other cores in the mesh.

1. Edit the file

   `/etc/opt/opsware/opswgw-agw0-<dcname>/opswgw.properties`

   to define the backup tunnels.

   For each core in the mesh (other than the core you're working on) add this line:

   `opswgw.TunnelSrc=<IP of CGW in another core>:200:0:<cert_location>`

   where `<cert_location>` can be one of:

   `/etc/opt/opsware/opswgw-agw0-<dcname>/opswgw.pem`

   `/var/opt/opsware/opswgw-agw0-<dcname>/opswgw.pem`

   This configuration assigns a relatively high cost to the tunnel so it acts as a backup until needed.

2. Restart the Agent Gateway:

   `/etc/init.d/opsware-sas restart opswgw-agw0`

3 Verify that the tunnels have been established. For each of the core gateways that you've added tunnels to:

1. Go to *https://<IP of the Core Gateway>:8085* and click on **Status**.
2. Verify that the table of connected gateways (shown on the right) lists the Agent Gateway you just restarted.

Step 2: Create backup tunnels for the Satellites

For each Satellite in the mesh, create backup tunnels from the Satellite Gateway to the Core Gateways (CGWs) for all other cores in the mesh.

1 Edit the file

`/etc/opt/opsware/opswgw/opswgw.properties`

to define tunnels to the core gateways in other cores.

For each core you are creating a backup tunnel to, add this line:

`opswgw.TunnelSrc=<IP of CGW>:200:0:<cert_location>`

where `<cert_location>` is

`/var/opt/opsware/crypto/opswgw-<gwname>/opswgw.pem`

There should already be a `TunnelSrc` line pointing to the Core Gateway in your core, that you can use as an example.

This configuration assigns a relatively high cost to the tunnel so it acts as a backup until needed.

2 restart the Satellite Gateway:

```
/etc/init.d/opsware-sas restart opswgw
```

3 Verify that the tunnels have been established. For each of the Core Gateways that you've added tunnels to:

1. Go to *https://<IP of the Core Gateway>:8085* and click on **Status**.
2. Verify that the table of connected gateways (shown on the right) lists the Satellite Gateway you just restarted.

Phase 2: Upgrade the First Core

In this phase, you will shutdown the mesh's First Core, allowing the tunneled connections between the Agent and Satellites and the other cores in the mesh to take over core communication, upgrade the First Core, then restart it.

1 Shut down all of the First Core's components except the Agent Gateway

1. On each First Core server, run:

   `/etc/init.d/opsware-sas stop`

2. On the server running the Core/Agent Gateway pair, edit the Core Gateway configuration file (`/etc/opt/opsware/opswgw-cgw0-<dcname>/opswgw.properties`) and comment out the line that starts with `TunnelDst` and specifies a listener for connections from the local Agent Gateway (by default the listener listens on port 2002). For example:

   `opswgw.TunnelDst=127.0.0.1:2002`

   This forces the Agent Gateway to connect to a Core Gateway in another facility while the connection to its *local* Core Gateway is unavailable during the upgrade of the First Core.

3. On the server where the First Core's Core and Agent Gateways are installed, run:

   `/etc/init.d/opsware-sas start opswgw-agw0`

2 Verify that the backup tunnels you set up prior to upgrade have taken effect. Go to:

`https://<IP of CGW in another core>:8085/`

click on **Status** and verify that the Agent Gateway in the First Core is listed.

3 Mount SAS 6.61 **Primary** distribution media on each First Core server.

4 Enter the following to start the upgrade:

`<distro_loc>/disk001/opsware_installer/upgrade_opsware.sh -r <resp_file>`

You must upgrade components in the First Core in the following order:

1. Model Repository
2. Data Access Engine
3. Model Repository Multimaster Component

Note: At this point, SAS 6.61 data changes will begin flowing to the rest of the cores in the mesh.

4. Command Engine
5. Software Repository
6. OGFS

7. OCC
8. OS Provisioning Build Manager
9. OS Provisioning Media Server
10. First Core Gateway
11. OS Provisioning Boot Server

Note: At this point, your mesh is running in the configuration described in Figure 3-2.

5 Revert the change to the `opswgw.properties` file in step 1, substep 2 of this phase.

1. Run `/etc/init.d/opsware-sas stop opswgw-cgw0`
2. Edit the `/etc/opt/opsware/opswgw-cgw0-<dcname>/opswgw.properties` file and uncomment the `TunnelDst` line that you commented out in step 1 of this phase.
3. Run `/etc/init.d/opsware-sas start opswgw-cgw0`

6 Upload the new content:

1. Mount the SAS 6.61 **Upload** distribution media on the core server hosting the Software Repository.
2. Run the command:

```
<upload_distro_loc>/disk001/opsware_installer/
upgrade_opsware.sh -r <resp_file>
```

3. From the displayed menu, select both components:

```
Welcome to the Opsware Installer.
Please select the components to upgrade.
1 ( ) Software Repository - Content (install once per mesh)
2 ( ) Add OS Provisioning Stage2 Images to Software
Repository
Enter a component number to toggle ('a' for all, 'n' for
none.
```

Phase 3: Upgrade the Secondary Cores

The Secondary Core upgrade is similar to the First Core upgrade, with these exceptions:

- A Secondary Core Model Repository upgrade does not result in any database changes.

- Only the OS Provisioning Stage2 Images must be uploaded.

You can upgrade multiple Secondary Cores in parallel, but if you have set up backup tunnels, each core you shut down will increase the load on the remaining cores.

Perform these tasks on each Secondary Core in the mesh:

1 Shut down all of the Secondary Core's components except the Agent Gateway

1. On each Secondary Core server, run:

   ```
   /etc/init.d/opsware-sas stop
   ```

2. On the server where the Secondary Core's Core and Agent Gateways are installed, run:

   ```
   /etc/init.d/opsware-sas start opswgw-agw0
   ```

2 Verify that the backup tunnels you set up prior to upgrade have taken effect. Go to:

```
https://<IP of CGW in another core>:8085/
```

click on **Status** and verify that the Agent Gateway in the Secondary Core is listed.

3 Mount SAS 6.61 **Primary** distribution media on each Secondary Core server.

4 Enter the following to start the upgrade:

```
<distro_loc>/disk001/opsware_installer/upgrade_opsware.sh -r
<resp_file>
```

You must upgrade components in the Secondary Core in the following order:

1. Model Repository
2. Data Access Engine
3. Model Repository Multimaster Component

Note: At this point, SAS 6.61 data changes will begin flowing to the rest of the cores in the mesh.

4. Command Engine
5. Software Repository
6. OGFS
7. OCC
8. OS Provisioning Build Manager
9. OS Provisioning Media Server

10. First Core Gateway
11. OS Provisioning Boot Server

Note: At this point, your mesh is running in the configuration described in Figure 3-3

5 Upload the new content:

1. Mount the SAS 6.61 **Upload** distribution media on the core server hosting the Software Repository.
2. Run the command:

```
<upload_distro_loc>/disk001/opsware_installer/
upgrade_opsware.sh -r <resp_file>
```

3. From the displayed menu, select:

```
OS Provisioning Stage2 Images
```

Post-Upgrade Tasks (6.5.x to 6.6.1 Upgrades Only)

Apply Fix Scripts

The following scripts will apply several fixes for specific problems:

Bug ID: 152990

Description: Remediate preview is missing Windows patches that need to be installed.
Platform: Independent
Subsystem: Patch Management
Symptom: Although certain patches appear as Needed Patches, they do not appear under Preview Remediate as Pending Installation.
Apply the Fix Script:
On any server in the Multimaster Mesh that has a Data Access Engine installed:
1 After logging in, enter:

```
export LD_LIBRARY_PATH=/opt/opsware/lib
```

2 Run the bz152990.pyc script to preview any data that may need to be fixed:

```
/opt/opsware/bin/python /opt/opsware/spin/util/fix_6.5.1_
data/bz152990.pyc -p | tee /usr/tmp/bz152990.preview
```


3 After previewing the data that needs to be fixed, this script will perform a trial fix of the data without committing the changes to ensure that no constraints are violated. If any constraints are violated, contact Opsware, Inc. Support.

```
/opt/opsware/bin/python /opt/opsware/spin/util/fix_6.5.1_
data/bz152990.pyc -n | tee /usr/tmp/bz152990.trial
```

4 If no constraints have been violated, run this script to fix the data and commit.

```
/opt/opsware/bin/python /opt/opsware/spin/util/fix_6.5.1_
data/bz152990.pyc | tee /usr/tmp/bz152990.real
```

Bug ID: 153784

Description: Errors parsing the MBSA patch database result in invalid patch unit records being created and missing patch unit records.

Platform: Windows

Subsystem: Patch Management

Symptom: The MBSA parser does not create unit records for Windows 2000, Windows Server 2003, Windows Server 2003 x64, and Windows XP.

Apply the Fix Script:

On any server in the Multimaster Mesh that has a Data Access Engine installed:

1 After logging in, enter:

```
export LD_LIBRARY_PATH=/opt/opsware/lib
```

2 Run this script to apply and commit the fixes necessary to prevent invalid MBSA patch database results:

```
/opt/opsware/bin/python /opt/opsware/spin/util/fix_6.5.1_
data/bz153784.pyc
```

