AS3000 Installation and Configuration Guide

IMPAX 6.5.1

Installing and Configuring

the AS3000 Components of the IMPAX Cluster

AGFA

see more | do more

Copyright information

Trademark credits

Agfa and the Agfa rhombus are trademarks or registered trademarks of Agfa-Gevaert N.V., Belgium or its affiliates. IMPAX, Connectivity Manager, Audit Manager, WEB1000, Xero, TalkStation, Heartlab, and HeartStation are trademarks or registered trademarks of Agfa HealthCare N.V. or its affiliates. All other trademarks are held by their respective owners and are used in an editorial fashion with no intention of infringement.

Additional trademark credits

Sun, Sun Microsystems, the Sun Logo, and Solaris are trademarks or registered trademarks of Oracle America, Inc. in the United States and other countries.

CE
0413

Note: The IMPAX 6.5.1 software complies with the Council Directive 93/42/EEC Concerning Medical Devices, as amended by Directive 2007/47/EC.

Documentation warranty statement

Characteristics of the products described in this publication can be changed at any time without notice.

The information contained in this document is subject to change without notice. Agfa HealthCare N.V. and its affiliates make no warranties or representations, express, implied or statutory, with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Agfa HealthCare N.V. and its affiliates shall under no circumstances be liable for any damage arising from the use or inability to use any information, apparatus, method or process described in this document. Agfa HealthCare N.V. and its affiliates shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this manual.

The information in this publication is subject to change without notice.

2011 - 6 - 14

Manufacturer's responsibility

The manufacturer, installer, or importer will be responsible for the safety, reliability, and performance of the equipment only if:

- Installation, modifications, adjustments, changes, or repairs are performed by suitably qualified service personnel.

- The electrical installation of the site in which the equipment is used is according to an applicable safety standard (UL, CSA, or IEC/CDE).
- The equipment is used according to the instructions provided in the operation manuals.
- No software other than that which is distributed with this package or is sanctioned by Agfa will reside on the IMPAX 6.5.1 computers.

External software licenses

(Topic number: 7696)

Information about third-party software licenses and copyrights can be found in *External software licenses* (refer to page 104).

Giving feedback on the documentation

(Topic number: 122201)

Thank you for taking the time to provide feedback. Your comments will be forwarded to the group responsible for this product's documentation.

To give feedback on the documentation

1. In an email subject line or body, list which product, version, and publication you are commenting on.

   For example, "IMPAX 6.4 SU01 Client Knowledge Base: Extended". (You can find this information in the footer of the publications.)
2. Describe the incorrect, unclear, or insufficient information. Or, if you found any sections especially helpful, let us know.
3. Provide topic titles and topic numbers where applicable.

   Including your personal contact details is optional.
4. Send the email to doc_feedback@agfa.com.

Sorry, we cannot respond directly to every submission and we cannot accept requests for changes in the product; instead, contact your product sales representative or the product's technical support channel.

Contents

Getting started

1

Understanding certain key concepts and system requirements helps ensure a successful installation.

Attention: An archive is necessary to prevent permanent data loss

(Topic number: 98632)

Data archiving is an essential component of a PACS system. IMPAX Autopilot manages data in the cache and ensures that it does not run out of disk space. As the cache nears capacity, Autopilot deletes images to make space available for incoming images, usually on a first in, first out basis but ultimately governed by user-defined criteria. In addition to the automated cache management, users with the necessary permission can delete images from the cache.

For details about Autopilot configuration, refer to "Autopilot Management" (topic number 9129) in the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*. For details about permissions, refer to "Defining permissions" (topic number 9451) in the Administering IMPAX component of the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Under normal circumstances in which an archive is employed, any data that is deleted from the cache is stored on the archive and no permanent data loss occurs. If, however, an archive is not employed, data deletion results in a permanent loss of the record unless that data has been exported and/or stored elsewhere.

CAUTION!

Although IMPAX can be used without an archive, we highly recommend an archive be used to prevent data loss. It is the responsibility of any IMPAX customer to recognize and accept these conditions. In addition, granting the permission to delete an image or study from the

cache must be carried out with the understanding of the risk it can pose with regard to the permanent loss of patient data.

Prerequisite knowledge: IMPAX installations

(Topic number: 7633)

The installation procedures require that you have general knowledge of computer hardware and software concepts and proficiency in operating and troubleshooting computer software.

What is IMPAX?

(Topic number: 6910)

IMPAX is an image archiving and communications system that eliminates the need for film because it receives, distributes, archives, and displays images. IMPAX automates the flow of information to integrate the Radiology department with the rest of the hospital. IMPAX can also integrate remote locations such as clinics or home offices to the system for offsite viewing of images.

Additional IMPAX documentation

(Topic number: 6911)

This guide is intended for service and administrative personnel who are installing or upgrading, configuring, and maintaining the Server components of the IMPAX 6.5.1 system.

For information about using the IMPAX software once it is installed, refer to the *IMPAX 6.5.1 Server Knowledge Base*, *IMPAX 6.5.1 Application Server Knowledge Base*, and *IMPAX 6.5.1 Client Knowledge Base: Extended*. These Knowledge Bases are installed on the Application Server. Refer to "Installing the IMPAX documentation" (topic number 15523) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Opening the IMPAX 6.5.1 Server Knowledge Base

(Topic number: 58560)

Follow this procedure to open the IMPAX 6.5.1 Server Knowledge Base.

To open the IMPAX 6.5.1 Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed.
2. Launch the IMPAX Administration Tools and log in. Select **Help** > **Help URL**. On the IMPAX Documentation page, click the **IMPAX Server Knowledge Base** link.

or

From a browser on a connected computer, navigate to https://*app_server_name*/impax/documents/server/default.htm

Opening the IMPAX 6.5.1 Application Server Knowledge Base

(Topic number: 58563)

Follow this procedure to open the IMPAX 6.5.1 Application Server Knowledge Base.

To open the IMPAX 6.5.1 Application Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed.
2. On the Application Server, double-click the **AGFA IMPAX Knowledge Base** desktop shortcut. Select the **IMPAX Application Server Knowledge Base** link.

   or

   From a browser on a connected computer, navigate to https://*app_server_name*/impax/documents/appserver/default.htm

Opening the IMPAX 6.5.1 Client Knowledge Base: Extended

(Topic number: 58566)

Follow this procedure to open the IMPAX 6.5.1 Client Knowledge Base: Extended.

To open the IMPAX 6.5.1 Client Knowledge Base: Extended

1. Ensure that the IMPAX documentation has been installed.
2. Launch the IMPAX Client application and log in.
3. Press **F1**.

Components of the IMPAX cluster

(Topic number: 7091)

Every IMPAX 6.5.1 installation comprises the following main components:

- Database Server hosting the Oracle or SQL database

  The database used by the IMPAX 6.5.1 cluster. It collects, organizes, and manages all patient and study demographic data that is contained in DICOM header files. Installation of a Database Server is covered in this guide.

- Network Gateway

Workflow manager of the IMPAX 6.5.1 cluster. It receives studies from modalities and provides DICOM security and validation. Installation and configuration of a Network Gateway is covered in this guide.

- Archive Server

  DICOM archive used for permanent storage and retrieval of studies. Installation and configuration of an Archive Server is covered in this guide.

  Although IMPAX can be used without an archive, we highly recommend an archive be used to prevent data loss. For further information, see *Attention: An archive is necessary to prevent permanent data loss* (refer to page 7).

- Application Server

  Clients connect to one or more Application Server machines, which act much like a proxy machine to handle security, authentication, and communication with the IMPAX 6.5.1 Server components. Installation and configuration details are covered in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

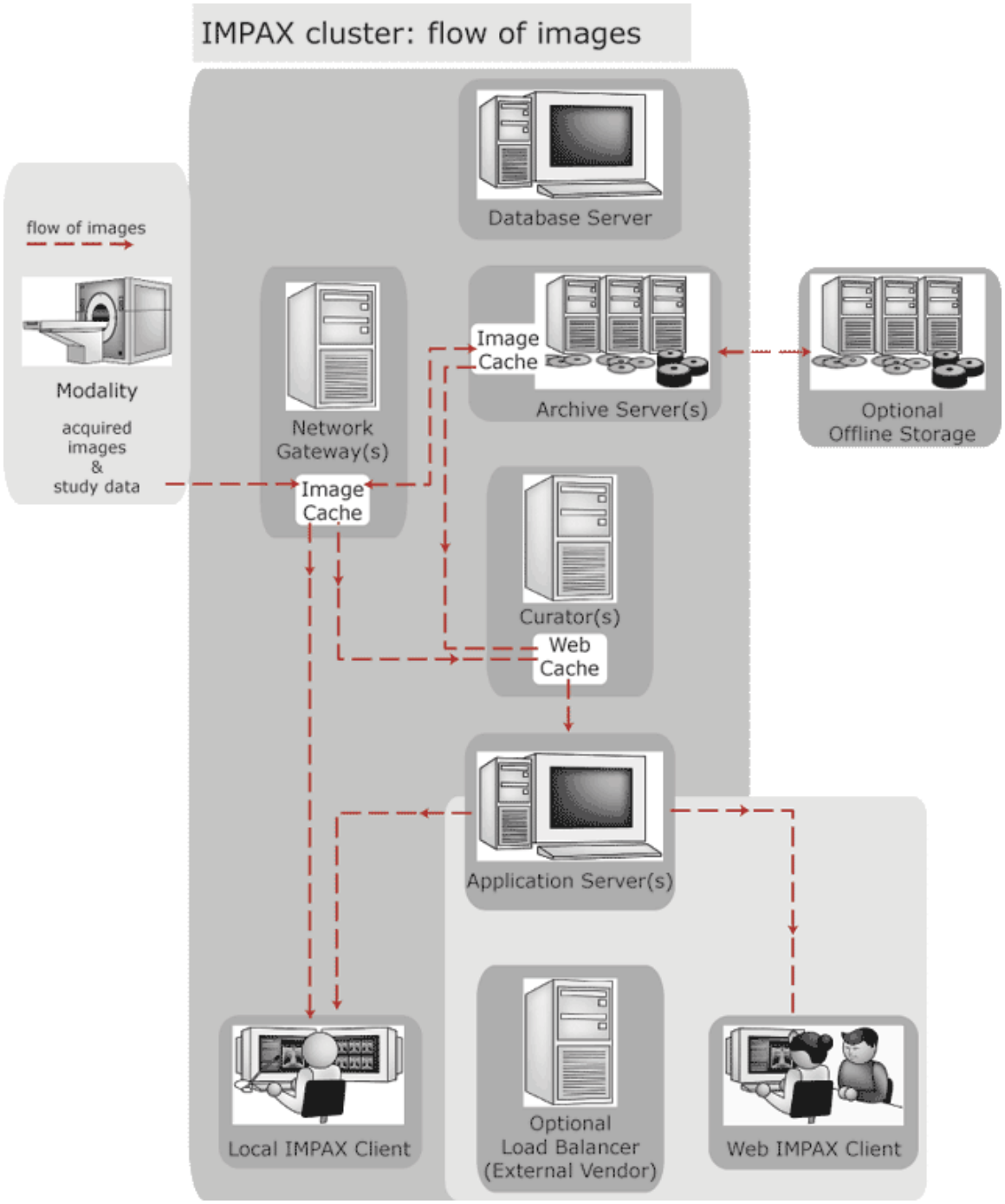
- Curator

  Clients can view JPEG compressed or wavelet compressed DICOM images generated by the Curator. Installation and configuration details are covered in the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*.

- Clients—Local and remote

  Multi-modality diagnostic or clinical display station for viewing images and diagnosing studies. Installation and configuration details are covered in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

The sum of these components is called the *cluster*. The IMPAX 6.5.1 cluster is the set of components that are controlled by one Oracle or SQL database. The Database Server must be installed first because the other stations must connect to the Oracle or SQL database.



IMPAX clusters also include a Connectivity Manager component. Connectivity Manager is a middleware component in the integration between hospital information systems and other hospital imaging departments. Connectivity Manager also provides connectivity to modalities and IMPAX. These systems often speak different languages, or protocols. PACS and modalities typically speak DICOM, while hospital information systems generally speak HL7.

Types of archives

(Topic number: 6917)

Supported archive configurations are:

- HSM (Hierarchical Storage Management)
- PACS Store and Remember

Tip:

For more details on archive functionality, refer to the Archive Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

HSM archives

(Topic number: 11577)

The HSM archive system provides long-term storage of data and access to data. Studies archived with HSM are stored to a file system. A mount point and subdirectory to store studies to is specified. The HSM system takes care of storing the data.

Before storing or retrieving data, ensure that the mounted location is set up properly and is ready for storage and retrieval of files.

PACS Store and Remember

(Topic number: 6941)

A PACS Store and Remember archive is an IMPAX Server computer that acts as an Archive Server, where the images are stored on a PACS archive external to the IMPAX system. Any IMPAX Server computer with a cache that is not currently an Archive Server can be set up as a Store and Remember archive. The PACS Store and Remember archive is aware of the studies that exist on the external archive, but is not aware of precisely where on the external archive these studies are stored. The external archive takes full responsibility for permanently archiving studies.

PACS Store and Remember archiving works the same way as other archiving. You configure the archiving based on the station, Autopilot creates STORE jobs based on the archiving settings, and studies can be retrieved via RETRIEVE jobs. A PACS Store and Remember queue is a DRIVE queue that is managed like any other DRIVE queue in the Administration Tools.

The difference between PACS Store and Remember archiving and media-based archiving is that the mvf-scu process handles the archiving, instead of a separate archive process. Also, a STORE job is done via DICOM C-STORE, and a RETRIEVE job is done via DICOM C-MOVE.

Single-cluster configurations

(Topic number: 6916)

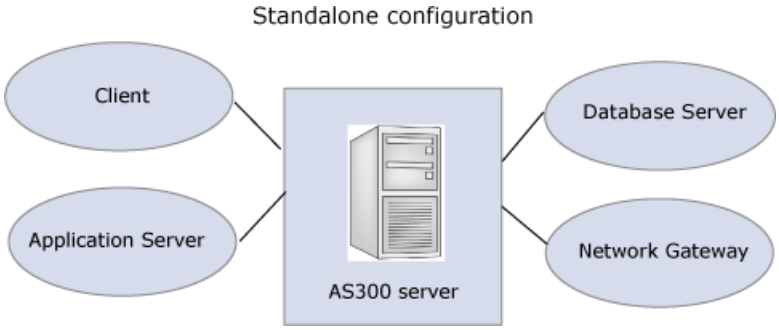
The components of a cluster can be distributed in various ways. A typical institution has a Database Server, one or more Archive Servers, one or more Network Gateways, one or more Curators, and one or more Application Servers. Clients are spread throughout the entire enterprise and through remote connection. A single IMPAX cluster can service one or more healthcare facilities and, in such an environment, IMPAX can HIS verify against and access reports from multiple Connectivity Managers for multiple RIS domains.

Note:

The Archive and Archive Server are the same thing. The archive station is the archive on its own machine. Both are part of the IMPAX cluster.

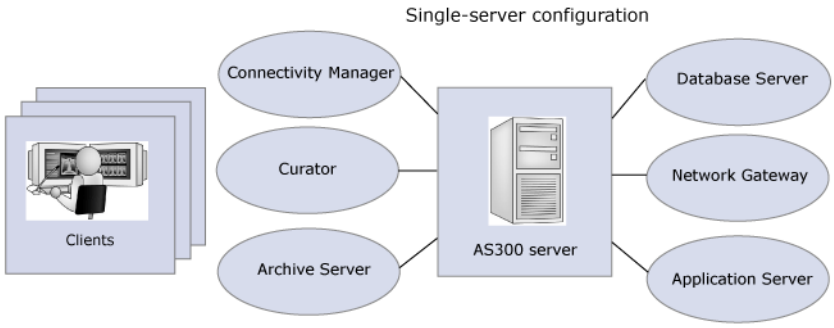
Standalone

In a standalone configuration, AS300 Server, Application Server, and Client components are installed on the same computer. The standalone station can be used for diagnostic or non-diagnostic purposes. New installations run under Windows 7 with an Oracle for Windows database. Using VMware Player, the AS300 Server and Application Server components run on Windows 2008 Server. Existing configurations can continue to run under Windows XP and with a SQL Server 2005 or 2008 database. Refer to the *IMPAX 6.5.1 Standalone Installation and Configuration Guide* or to the *IMPAX 6.5.1 Standalone Upgrade Guide*.



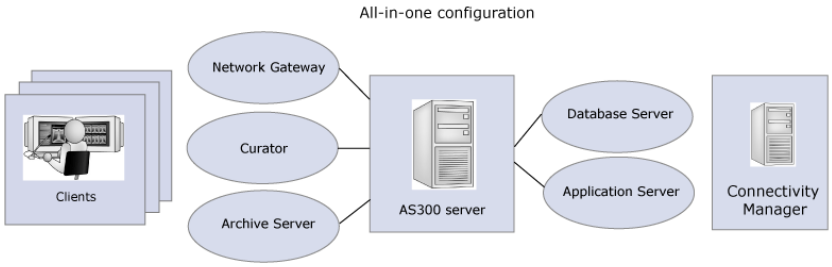
Single-server

In a single-server configuration, all AS300 Server, Application Server, and Connectivity Manager components are installed on the same Windows computer with an Oracle for Windows database using VMware; Clients are installed on other computers.



All-in-one

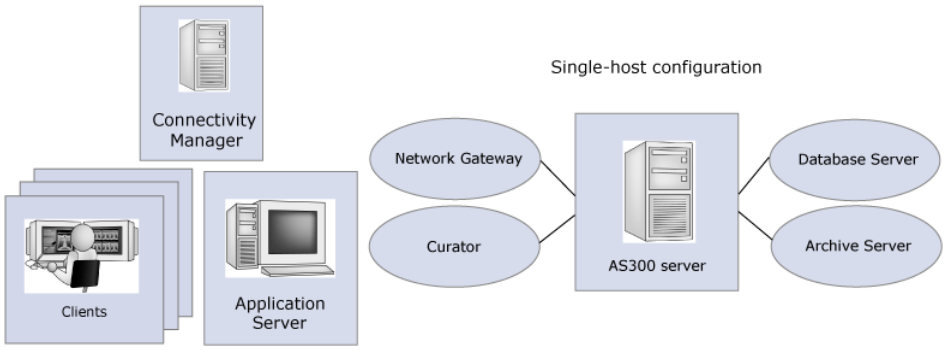
In an all-in-one server configuration, all AS300 Server and Application Server components are installed on the same Windows computer with an Oracle for Windows database.



Single-host

In a single-host configuration, the AS300 or AS3000 Server Database, Archive Server, and Network Gateway components are all installed on one "box" or station, with the Application Servers, Clients, and Connectivity Manager each installed on separate stations.

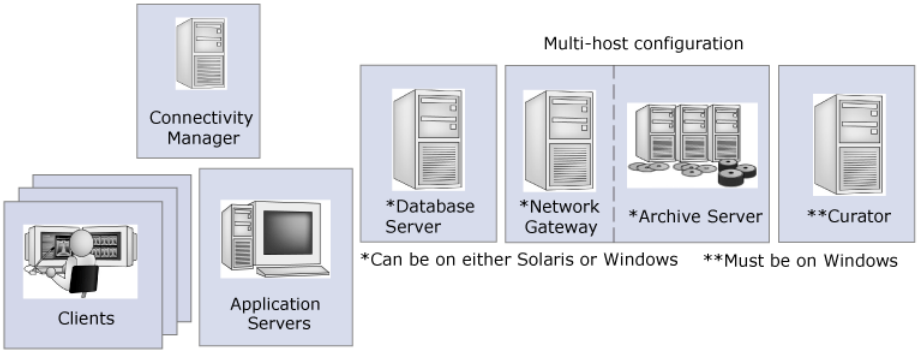
In an AS300 single-host configuration, Curator can also be installed on the same station as the Server components; however, in an AS3000 single-host configuration, Curator must be separately installed. The Curator component runs only on the Windows operating system.



Multi-host

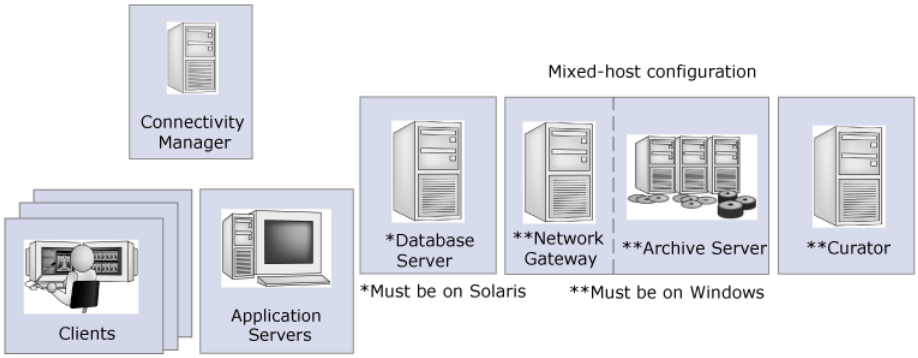
In a multi-host configuration, each Server component is installed on its own station: the Database Server is installed on a separate computer from the Archive Server. The Network Gateway component may either be installed on yet another server, or installed along with the Database Server or Archive Server.

By installing the Server components onto separate stations, workflow volume is better managed and system performance enhanced.



Mixed-host

In a mixed-host configuration, an AS3000 Database Server is combined with an AS300 (Windows-based) Archive Server, Network Gateway, and Curator server.



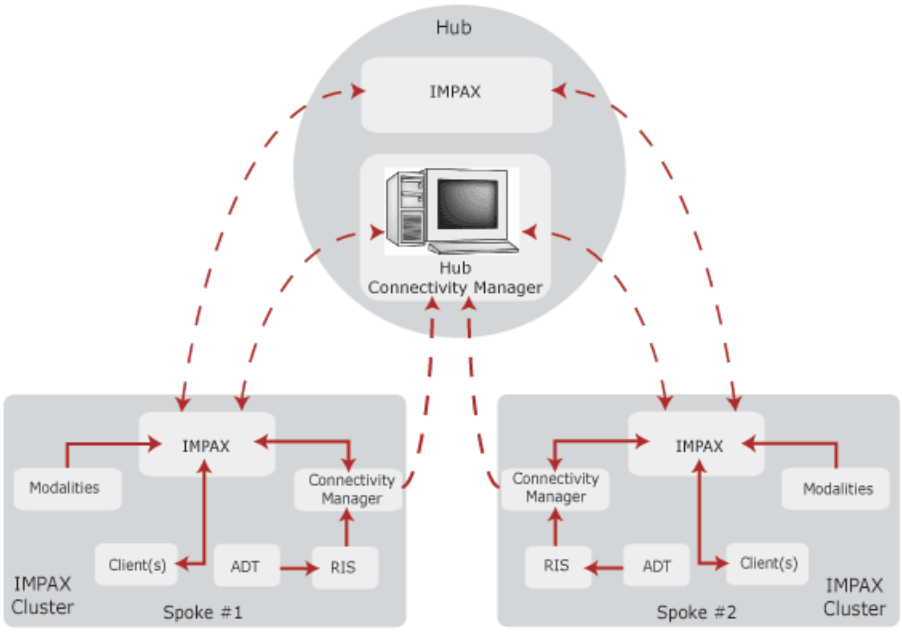
Multiple IMPAX cluster configurations

(Topic number: 10378)

IMPAX can optionally be run in a multiple IMPAX cluster configuration. This configuration provides a patient-centric view across hospitals within several sites. This view is delivered by extending the scope of study query, study retrieval, and data synchronization from a single hospital site to several hospital sites that have multiple patient domains (multiple RISs) in one or more IMPAX clusters.

Central to the multiple IMPAX cluster configuration is the MVF-based data center component. The data center provides storage for studies through the Archive Server, as well as retrieval of the study data. Connected to the data center are a collection of hospital groups known as *entities*, each with a local PACS infrastructure. Most entities use IMPAX as their PACS system.

The relationship between the data center and the various clusters is characterized as a *hub and spoke*. The data center (*hub*) serves or archives data from the entities, known as *spokes*.



Order of cluster installations

(Topic number: 7763)

The IMPAX cluster has many components and each depends on other components in the cluster. To correctly install and configure components in the cluster, follow this order of installation:

1. **Install the Database Server, Archive Server, and Network Gateway.**

   Install the core Server components and create the portable password file required to install other IMPAX components. Do not configure the AS300 Server components at this time; the Application Server must be installed before these Server components can be configured. Refer to the guide appropriate to your configuration.

   Required guide: One of *IMPAX 6.5.1 AS3000 Installation and Configuration Guide* or *IMPAX 6.5.1 AS300 Installation and Configuration Guide*

2. **Install the Application Server.**

   Install the Business Application services and IMPAX documentation on the Application Server.

   Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

3. **Begin configuration of the Application Server.**

   Create and import an SSL certificate, configure ADAM (Windows Server 2003) or AD LDS (Windows Server 2008), compress web services, set connections to the image and audit servers, and set logging levels.

   Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

4. **If you have installed a Windows-based Database Server, Archive Server, or Network Gateway, configure these components.**

   Configure database backups, image and web caches, and archives (if necessary). In clusters that include only Solaris-based systems, these configuration steps are done automatically during the installation.

   Required guide: *IMPAX 6.5.1 AS300 Installation and Configuration Guide*

5. **Install and configure Curator and the CD Export server.**

   If the site requires compressed web images, install and configure one or more Curator systems and set up the web cache. If you are installing multiple Curators, install and start the master Curator first, then install and start the slave Curators.

   If you will be using the CD Export feature in the IMPAX Client, install the CD Export server.

   Required guide: *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*

6. **Complete the configuration of the Application Server.**

   Complete the optional Application Server configuration tasks that are applicable to the site.

   Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

7. **Install and configure Clients.**

   Install and configure the IMPAX Client, the PACS system used to access images.

   Required guide: *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*

If installing a standalone station (single-host AS300 with Application Server and Client), refer to the *IMPAX 6.5.1 Standalone Installation and Configuration Guide*.

If installing a single-server (single-host AS300 with Connectivity Manager and Application Server), consult Installing an IMPAX AS300 single-server in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

All documentation is available on the IMPAX Documentation DVD.

IMPAX AS3000 Server: Supported hardware configurations

(Topic number: 6689)

The four general categories of servers are:

- Single-host server—Database Server/Archive Server/Network Gateway
- Database Server hosting the Oracle database
- Archive Server or combined Archive Server/Network Gateway
- Network Gateway

The hardware requirements for each of these are outlined in the sections that follow.

IMPAX AS3000 Server: Hardware requirements

(Topic number: 6622)

We recommend the following components for each AS3000 server:

Component	Requirements
Validated systems	The following Sun servers can be used in any combination as required: For new installations: • T5120, T5220, T5140, T5240 For upgrades: • V240/V440 or newer • T2000, T5120, T5220, T5140, T5240 **Solaris 10u8 or later only.** We do not recommend Sun T1000, V210, and V215 because of the single power supply limitation. When planning upgrades, note all end-of-sales and end-of-support dates published on MedNet. **Note:** These servers must have a DVD-ROM drive present for IMPAX installation purposes.
Number of CPUs	A minimum of two CPUs should be used in any of the server categories, after which the number of CPUs should be determined by server usage. General recommendations: • Database Server: Two to six CPUs • Archive Server/Network Gateway: Two to four CPUs • Network Gateway: Two CPUs • Single-host server: Two to eight CPUs Does not apply to the multi-core processors used in T-series Sun servers.
RAM	A minimum of 2 GB per CPU should be used in any of the server categories, after which the amount of RAM should be determined by server usage. General recommendations: • Database Server: 2GB per CPU • Archive Server/Network Gateway: 2GB to 4GB per CPU

Component	Requirements
	• Network Gateway: 2GB to 4GB per CPU • Single-host server: 2GB to 8GB per CPU
Hard drive	A minimum of two hard drives should be used in any of the server categories, after which the number of drives should be determined by server usage and configuration. We recommend having data available on an external disk subsystem and not an internal drive.
RAID	Required • RAID 1 + 0 is mandatory for the database (along with ForceDirectIO)—See the partitioning recommendations (refer to page 23) in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*. • RAID 5 or better for image cache.
Tape backup	Optional for Database Server but not recommended—not required if using file system backups.
Modem	Not required.
DVD-ROM	Required—One per cluster is required.
Floppy	No.
Network interface	Sun 10/100/1000 Mbps NICs. A 1 gigabit network should be considered the minimum for server interconnections. Consider segregating network traffic in order to improve overall throughput.
Jukebox	Direct attached archives are not supported.
Other	UPS that meets the region's safety approval standards and the power requirements of the machines it supports.

IMPAX AS3000 Server: Database backup requirements

(Topic number: 10319)

For file system backup, the following are supported:

- Back up to NFS or SAN

For tape backup (upgraded systems only, not new installations), the following are supported:

- SUN DAT-72
- Standalone DLT 8000
- Standalone LTO2
- Standalone SDLT

- Standalone L8 with LTO or LTO2 or SDLT

Important!

Oracle disk-to-tape backup requires significant disk space, as a minimum of two backups must be kept on disk. To accommodate disk-to-tape backups of the Oracle database, ensure that you define a Flashback partition that is at least 3 times the expected size of the database.

Operating systems disks should be configured as RAID 1, preferably with hardware mirroring; however, on platforms that do not support hardware mirroring, Solstice DiskSuite is acceptable. For more information regarding disk management strategies, see *Disk management strategies* (refer to page 23).

IMPAX AS3000 Server: External storage requirements

(Topic number: 10321)

When planning upgrades, note all end-of-sales and end-of-support dates published on MedNet. A comprehensive list of currently supported storage products is available through Agfa Professional Services.

For external storage, the following are supported:

EMC CX Series

EMC DMX series

EMC NS NAS

HP EVA series

HBAs supported by storage vendor and operating system

IMPAX AS3000 Server: Software requirements

(Topic number: 6620)

The following software is required for an IMPAX AS3000 cluster:

Component	Requirements
Operating system	Solaris™ 10u8 or later.
Database software	Oracle 10.2.0.4.0 Standard or Enterprise Editions (supplied with IMPAX)
Solaris patches	As recommended by Sun.
Other software	• Java Runtime (included with Solaris) • Apache Server (included with Solaris)

Component	Requirements
	• Adobe® Reader® for Solaris (for documentation)
Supported software	The following software is supported but not required: • SUN SAM-FS 4.5/4.6/5.0 on Solaris 10, NFS or local • IBM Tivoli Storage Manager—NFS only • QStar • EMC Centera

Setting up a Solaris server

2

Many of the same steps are required when deploying a Solaris server for IMPAX, regardless of whether it is to become a single-host server, a Database Server, an Archive Server, or a Network Gateway.

1. Physically setting up a Solaris server

(Topic number: 6931)

For details on setting up the hardware, or powering up a new Solaris station, refer to Sun's instructions.

2. Connecting the UPS

(Topic number: 6997)

Each component must be plugged into a UPS. In the event of system failure or power surge, the UPS protects your system from data corruption.

To connect the UPS

1. Follow the manufacturer's instructions on installing the UPS and associated software.
2. If using a whole-room UPS, you can also install a customer-provided shutdown agent. Follow the installation instructions provided with the shutdown agent to install it.

3. Installing Solaris 10

(Topic number: 13038)

If the Solaris 10 operating system is not already installed and configured, complete this procedure now, by following the Solaris instructions and using the recommended disk partitions (refer to page 23).

When selecting the Solaris Software Group, select **Entire Group Plus OEM** (SUNWCXall). This contains the packages for the Entire Solaris Software Group plus additional hardware drivers, including drivers for hardware that is not on the system at the time of installation.

Note:

Mirror the root disk using Sun's RAID hardware utility, *raidctl*. For information on how to use this utility, see the Sun Microsystems Documentation website (http://docs.sun.com/). For information on how to build volumes and mirror the root disk, consult the *Sun SPARC Enterprise T5140/T5240 Server Installation Guide* or http://www.sun.com/bigadmin/content/submitted/svm_mirroring.jsp (for systems such as sun490/890).

4. Disk management strategies

(Topic number: 103117)

Disk management strategies allow you to optimize performance by partitioning and configuring disks appropriately, or by separating the busy parts of the database from each other, assigning them to physically separate drives or volumes. Partition IMPAX disks and database drives as described in *Partitioning and configuring local disks* (refer to page 23) and *Partitioning recommendations for the database file systems* (refer to page 26).

Note:

In order to use Live Upgrade with older releases of Solaris 10, you must first patch the system as described in the document *Live Upgrade Software: Minimum Patch Requirements,* which can be downloaded from:
http://sunsolve.sun.com/search/document.do?assetkey=1-61-206844-1

5. Partitioning and configuring local disks

(Topic number: 6938)

This topic describes how to partition 146 GB disk arrays on IMPAX 6.5.1 AS3000 stations.

Note:

It is unusual to place database or cache volumes on local disk. Normally, to meet failover, migration and reliability considerations, these volumes are on external NAS or SAN storage.

To partition and configure local disks

1. When partitioning 146 GB disks in mirrored RAID arrays on IMPAX AS3000 servers, allocate the slices and create the partitions as follows on each disk, including one to accommodate Live Upgrade. (The temp database created during staging is rebuilt when the system is on-site and configured with the final RAID.)

Slice	Mount point	8 GB RAM	16 GB RAM	32 GB RAM	64 GB RAM
0	/	20480 MB	20480 MB	20480 MB	20480 MB
1	swap	32768 MB	32768 MB	32768 MB	65536 MB
2	Do not change				
3	Do not change				
4	Do not change				
5	/liveupgrade	20480 MB	20480 MB	20480 MB	20480 MB
6	/zoneroot	24576 MB	24576 MB	24576 MB	24576 MB
7	/agfa	15240 MB	15240 MB	15240 MB	15240 MB

6. Installing Solaris 10 patches

(Topic number: 58098)

To download and install Solaris 10 patches, you need a Solaris maintenance agreement and login details, which you can obtain from Oracle.

You must install the Solaris 10 patches recommended by Oracle on all IMPAX servers running Solaris 10.

To install Solaris 10 patches

1. Log into the Solaris support website using your maintenance agreement credentials.
2. Under Patches and Updates, select the **Solaris 10** patch set.
3. Review the Readme file associated with this patch set and make note of the password which is needed to run the installation script.

Note:

The latest, most complete patch installation information, including the password needed to run the installation script, is included in the Readme file provided. You must review it.

4. Download the patch file to a directory of your choice, such as the /agfa directory.

   The patch file is called 10_Recommended.zip.
5. Log in as root and change to the directory containing the patch file. (Mount the location, if necessary.)
6. Unzip the patches. Type

   unzip -q 10_Recommended.zip
7. Delete the 10_Recommended.zip file. Type

   rm 10_Recommended.zip
8. Change to the **10_Recommended/** directory.
9. Switch to single-user mode by typing **init s** and providing the root password.

Important!

Do not skip this step; doing so can create problems in Solaris.

10. Run the patch installation script. Type

    ./installcluster *password*

    where *password* is the password provided in the Readme file.
11. When the process is complete, reboot the server. Type

    shutdown -y -i6 -g0
12. When the server is restarted, in a browser, go to the Solaris support website again.
13. Under Patches and Updates, select the **J2SE Solaris 10** patch set.
14. Review the Readme file associated with this patch set.
15. Download the patch file to the same directory as the previous patch.

    The patch file is called J2SE_Solaris_10_Recommended.zip.
16. Change to the directory containing the patch file. (Mount the location, if necessary.)
17. Unzip the patches. Type

    unzip -q J2SE_Solaris_10_Recommended.zip
18. To delete the J2SE_Solaris_10_Recommended.zip file, type

    rm J2SE_Solaris_10_Recommended.zip
19. Change to the **J2SE_Solaris_10_Recommended/** directory.
20. Switch to system administrator mode by typing **init s** and providing the root password.

21. Execute the patch installation script. Type

    ./install_cluster

22. When the patch installation is complete, reboot the server. Type

    shutdown -y -i6 -g0

All the patches needed for IMPAX 6.5.1 are now installed.

7. Partitioning recommendations for the database file systems

(Topic number: 103140)

Optimize database performance by partitioning the disk arrays for the database file systems, separating the busy parts of the database from each other and assigning them to physically separate drives or volumes.

The Database Configurator tool is an Excel spreadsheet that can be used to determine the size of various Oracle database partitions, based on estimated or initial exam volume and anticipated growth for the next five years.

The Database Configurator tool is available on Mednet at the following location: http://ftp.agfa.be/HE/software/PACS/3rd_Party_Solutions/Oracle/Software/database_configurator/.

For information on installing the disk arrays, refer to these Sun Microsystems documents:

- *SunFire T2000 Installation Guide*
- *Sun SPARC Enterprise T5140/T5240 Server Installation Guide*
- *Sun SPARC Enterprise T5120/T5220 Server Installation Guide*

We recommend partitioning the IMPAX database drives as follows:

Disk partitions or volumes	Recommended requirements (no fault tolerance or redundancy)	Strategy for fault tolerance or performance
/dbase/system • system tablespace • temp tablespace • control file 1	Use Database Configurator tool	Mirror and stripe RAID 10 on separate volume/mount on FC (fibre channel) or SAS (serial attached SCSI) drives
/dbase/redo (optional for four-volume configuration—in four-volume configuration this would be in /dbase/system)	Use Database Configurator tool	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives

Disk partitions or volumes	Recommended requirements (no fault tolerance or redundancy)	Strategy for fault tolerance or performance
• redo logs		
/dbase/rbs (optional for four-volume configuration—in four-volume configuration this would be in /dbase/system) • undo tablespace	Use Database Configurator tool	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives
/dbase/data1 • data1 (volatile data) • data2 (static data) • control file 3	Use Database Configurator tool	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives
/dbase/index1 • index 1 (volatile indexes) • index 2 (static indexes) • tools • control file 2	Use Database Configurator tool Indexes use about 50% more than data tables	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives
/dbase/arch or in /flashback area in /flashback/db_recovery_area /MVF1/archivelog (if installing Oracle Data Guard) • transaction logs • Database Configurator tool	Use Database Configurator tool Need enough to hold a week's worth of logs	RAID 5 or better—minimum of three disks is required
/flashback (for IMPAX sites using Oracle Data Guard or RMAN) • Contains many different log files but notably the transaction logs, arch logs, flashback logs as well as a		Separate the logs and backup areas which have very different performance requirements and sizing needs; this minimizes the total space of RAID 10 FC or SAS disks, and provides the option of backup sets being placed on more economical RAID 5 SATA (serial

Disk partitions or volumes	Recommended requirements (no fault tolerance or redundancy)	Strategy for fault tolerance or performance
location for the backup sets from RMAN		advanced technology attachment) disks
/flashback/db_recovery_area/MVF1/flashback • Required only for four-volume configuration for /flashback • In two-volume configuration this is included in the /flashback mount but separate from the backup area in /flashback/db_recovery_area/MVF1/backupset	Use Database Configurator tool Normally twice the size of the sum of the database (/data1, /index1, /system)	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives
/flashback/db_recovery_area/MVF1/backupset • Area where RMAN places and maintains the backups • Normally a minimum of one full backup of the database is required (Three is recommended)	Use Database Configurator tool Normally one to three times the size of the sum of the database (/data1, /index1, /system)	RAID 5 on SATA drives or better (minimum three drives) Normally much lower performance requirements than remaining file systems in /flashback For performance and reliability, place on a separate mount from remaining flashback file systems
/flashback/db_recovery_area/MVF1/autobackup • Optional for two-volume configuration for /flashback • In two-volume configuration this would be included in the /flashback mount	Use Database Configurator tool	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives
/flashback/db_recovery_area/MVF1/archivelog • Optional for two-volume configuration for /flashback • In two-volume configuration, this would be	Use Database Configurator tool Need enough to hold a week's worth of logs	Mirror and stripe RAID 10 on separate volume/mount on FC or SAS drives

Disk partitions or volumes	Recommended requirements (no fault tolerance or redundancy)	Strategy for fault tolerance or performance
included in the /flashback mount		
Hot spares	One or two drives per array	One or two drives per array

Note:

To ensure component compatibility, follow the support matrix provided by the SAN vendor. This compatibility should include HBAs (host bus adapters), HBA Firmware, HBA Fcode, SAN Switch firmware, and storage enclosure operating system level.

Flash Recovery Area

After installing Solaris, lay out the file systems for /flashback and /dbase and plan for the various mounts.

The flashback directory in an Oracle Data Guard implementation houses all of the database recovery information. (The /dbase mounts contain the actual database datafiles.) Contained in the /flashback/db_recovery_area/MVF1 Flash Recovery Area is a unified storage location for all recovery-related files and activities in an Oracle database. All RMAN backups, transaction logs, flashback logs, archive logs, control file autobackups, and datafile copies are automatically written to the specified file system.

In addition to the unified storage location of the recovery-related files, the Flash Recovery Area also manages the disk space allocated for recovery files. This management has two components:

1. RMAN configuration that manages the number of complete backups retained within the Flash Recovery Area: in IMPAX with Oracle Data Guard, these backups are retained in /flashback/db_recovery_area/MVF1/backupset.
2. Oracle flashback management of the amount of disk space used by all the recovery-related files in the mount: to use this component, the Flash Recovery Area has to be defined as an operating system directory. A number of server parameters control the Flash Recovery Area, including:
    - db_recovery_file_dest—Defines the directory to store the flashback data to (but can be used for archived redo logs and backups as well).
    - db_recovery_file_dest_size—Defines the maximum size of the directory. The Oracle kernel manages the deletion of files no longer required (for example, due to a retention policy).

Laying out /flashback (two-volume configuration)

(Topic number: 119984)

Note:

If using a four-volume configuration, skip this procedure and see *Laying out /flashback (four-volume configuration)* (refer to page 33).

This configuration includes two specific mounted file systems:

1. /flashback

   Approximately twice the database size and on RAID 10 FC or SAS disk systems

2. /ora_backups

   Approximately one to three times the database size, to retain one or three backups respectively, and can be on less expensive and lower performing disks (RAID 5 SAS drives)

Two options exist for configuring the backup set:

1. Mount the file system directly at /ora_backups

   or

2. Mount the file system directly at /flashback/db_recovery_area/MVF1/backupset

To mount the file system directly at /ora_backups

1. Set up the file systems as described in *Partitioning recommendations for the database file systems* (refer to page 26) and mount /flashback and /ora_backups.
2. Add entries into /etc/vfstab for both /flashback and /ora_backups.

   For example:

```
# sample /etc/vfstab extract (for attached SAN Storage)
#The database Data files mounts (RAID 10 FC or SAS)
/dev/dsk/emcpower5h          /dev/rdsk/emcpower5h        /dbase/data1
  ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower0h          /dev/rdsk/emcpower0h        /dbase/index1
 ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower3h          /dev/rdsk/emcpower3h        /dbase/system
 ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower4h          /dev/rdsk/emcpower4h        /dbase/redo
   ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower1h          /dev/rdsk/emcpower1h        /dbase/rbs
    ufs 2 yes nologging,forcedirectio
#
# Two mount option for flashback – version 1.
#   /flashback on RAID 10 FC or SAS – same type as all of the /dbase above.
/dev/dsk/c7t6001604d0s7    /dev/rdsk/c7t6001604d0s7    /flashback
 ufs 2 yes nologging,forcedirectio
#
#   /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
/dev/dsk/c7t6003000d0s0    /dev/rdsk/c7t6003000d0s0   / ora_backups
```

```
ufs2 yes nologging,forcedirectio


# sample /etc/vfstab extract (for NFS to NAS Storage)
#The database Data files mounts (RAID 10 FC or SAS)
10.101.44.7:/vol/Ora_data/data1   -  /dbase/data1   nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.39:/vol/Ora_data/index1 -  /dbase/index1  nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/system  -  /dbase/system  nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/rbs     -  /dbase/rbs     nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/redo    -  /dbase/redo    nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#
# Two mount option for flashback – version 1.
#  /flashback on RAID 10 FC or SAS – same type as all of the /dbase above.
#
10.101.44.71:/vol/Ora_Flash/flashback  -   / flashback   nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#
#   /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
10.101.44.72:/vol/Ora_backup/backup   -   /ora_backups   nfs - yes
rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp
```

3. To mount /flashback, type

   mount /flashback

4. To mount /ora_backups, type

   mount /ora_backups

5. Confirm that the directory /flashback/db_recovery_area/MVF1 exists in /flashback.
6. Create a symbolic link from /flashback/db_recovery_area/MVF1/backupset to /backup. Type

   In –s /ora_backups /flashback/db_recovery_area/MVF1/backupset

7. During the database installation, set the following parameters for the space in /flashback:

   `db_recovery_file_dest` = **/flashback**

   `db_recovery_file_dest_size` = ***size_of_/flashback_file_system*** (do not include the size of /ora_backups in this value)

   For more details, see *Installing the IMPAX 6.5.1 AS3000 database packages* (refer to page 40).

Note:

The space in /flashback/db_recovery_area/MVF1/backupset is managed by RMAN.

To mount the file system directly at /flashback/db_recovery_area/MVF1/backupset

1. Set up the file systems as described in *Partitioning recommendations for the database file systems* (refer to page 26).
2. Add entries into /etc/vfstab for both /flashback and for /flashback/db_recovery_area/MVF1/backupset.

   For example:

```
# sample /etc/vfstab extract (for attached SAN Storage)
#The database Data files mounts (RAID 10 FC or SAS)
/dev/dsk/emcpower5h          /dev/rdsk/emcpower5h        /dbase/data1
 ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower0h          /dev/rdsk/emcpower0h        /dbase/index1
ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower3h          /dev/rdsk/emcpower3h        /dbase/system
ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower4h          /dev/rdsk/emcpower4h        /dbase/redo
  ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower1h          /dev/rdsk/emcpower1h        /dbase/rbs
   ufs 2 yes nologging,forcedirectio
#
# Two mount option for flashback – version 2.
#  /flashback on RAID 10 FC – same as all of the /dbase above.
/dev/dsk/c7t6001604d0s7    /dev/rdsk/c7t6001604d0s7    /flashback
 ufs 2 yes nologging,forcedirectio
#
#  /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
/dev/dsk/c7t6003000d0s0    /dev/rdsk/c7t6003000d0s0
/flashback/db_recovery_area/MVF1/backupset ufs3 yes nologging,forcedirectio



# sample /etc/vfstab extract (for NFS to NAS Storage)
#The database Data files mounts (RAID 10 FC or SAS)
10.101.44.7:/vol/Ora_data/data1            -    /dbase/data1   nfs - yes

forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.39:/vol/Ora_data/index1        -    /dbase/index1  nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/system         -    /dbase/system nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/rbs               -    /dbase/rbs        nfs -
 yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/redo             -    /dbase/redo      nfs -
yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#
# Two mount option for flashback – version 1.
#   /flashback on RAID 10 FC or SAS – same type as all of the /dbase above.
10.101.44.71:/vol/Ora_Flash/flashback  -   / flashback        nfs - yes
```

```
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#   /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
10.101.44.72:/vol/Ora_backup/backup   -
/flashback/db_recovery_area/MVF1/backupset nfs - yes

rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp
```

3. Mount /flashback first. Type

   mount /flashback

4. Once the /flashbackfile system is mounted, ensure that the directory /flashback/db_recovery_area/MVF1/backupset exists and is empty.
5. Mount /flashback/db_recovery_area/MVF1/backupset. Type

   mount /flashback/db_recovery_area/MVF1/backupset

6. During the database installation, set the following parameters for the space in /flashback:

   `db_recovery_file_dest` = **/flashback**

   `db_recovery_file_dest_size` = ***size_of_/flashback_file_system*** (do not include the size of /ora_backups in this value)

   For more details, see *Installing the IMPAX 6.5.1 AS3000 database packages* (refer to page 40).

Note:

The space in /flashback/db_recovery_area/MVF1/backupset is managed by RMAN.

Laying out /flashback (four-volume configuration)

(Topic number: 119997)

This configuration includes four specific mounted file systems. They are mounted directly at /flashback/db_recovery_area/MVF1:

File system	Size	Disk system
/flashback/db_recovery_area/MVF1/flashback	Approximately twice the database size	On RAID 10 FC or SAS disk systems
/flashback/db_recovery_area/MVF1/archivelog	Sized to hold at least a week's worth of archive logs	On RAID 10 FC or SAS disk systems
/flashback/db_recovery_area/MVF1/autobackup		On RAID 10 FC or SAS disk systems
/flashback/db_recovery_area/MVF1/backupset	Approximately one to three times the database size, to retain one or three backups respectively	Can be on less expensive and lower performing disks (RAID 5 SAS drives)

To mount the file systems directly at /flashback/db_recovery_area/MVF1

1. Set up the file systems as described in *Partitioning recommendations for the database file systems* (refer to page 26) and mount all four of the flashback file systems noted previously.
2. Add entries into /etc/vfstab for all four of the file systems.

   For example:

```
# sample /etc/vfstab extract (for attached SAN Storage)
#The database Data files mounts (RAID 10 FC or SAS)
/dev/dsk/emcpower5h          /dev/rdsk/emcpower5h        /dbase/data1
  ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower0h          /dev/rdsk/emcpower0h        /dbase/index1
 ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower3h          /dev/rdsk/emcpower3h        /dbase/system
 ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower4h          /dev/rdsk/emcpower4h        /dbase/redo
   ufs 2 yes nologging,forcedirectio
/dev/dsk/emcpower1h          /dev/rdsk/emcpower1h        /dbase/rbs
    ufs 2 yes nologging,forcedirectio
#
# Two mount option for flashback – version 1.
#   /flashback on RAID 10 FC or SAS – same type as all of the /dbase above.
/dev/dsk/c7t6001604d0s7    /dev/rdsk/c7t6001604d0s7
/flashback/db_recovery_area/MVF1/flashback        ufs 2 yes
nologging,forcedirectio
/dev/dsk/c5t6007604d0s7    /dev/rdsk/c5t6007604d0s7
/flashback/db_recovery_area/MVF1/autobackup        ufs 2 yes
nologging,forcedirectio
/dev/dsk/c2t6003604d0s7    /dev/rdsk/c2t6003604d0s7
/flashback/db_recovery_area/MVF1/archivelog        ufs 2 yes
nologging,forcedirectio
#
#   /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
/dev/dsk/c7t6003000d0s0    /dev/rdsk/c7t6003000d0s0
/flashback/db_recovery_area/MVF1/backupset       ufs2 yes
nologging,forcedirectio


# sample /etc/vfstab extract (for NFS to NAS Storage)
#The database Data files mounts (RAID 10 FC or SAS)
10.101.44.7:/vol/Ora_data/data1            -    /dbase/data1   nfs - yes

forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.39:/vol/Ora_data/index1        -    /dbase/index1  nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/system         -    /dbase/system nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/rbs               -    /dbase/rbs        nfs -
 yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.7:/vol/Ora_data/redo             -    /dbase/redo      nfs -
yes
```

```
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#
# Two mount option for flashback – version 1.
#  /flashback on RAID 10 FC or SAS – same type as all of the /dbase above.
10.101.44.71:/vol/Ora_Flash/flashback     -
/flashback/db_recovery_area/MVF1/ flashback             nfs – yes

forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

10.101.44.71:/vol/Ora_Flash/archive         -
/flashback/db_recovery_area/MVF1/ archivelog             nfs - yes
forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp
10.101.44.71:/vol/Ora_Flash/autobackup  -
/flashback/db_recovery_area/MVF1/autobackup            nfs – yes

forcedirectio,rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp

#   /flashback/db_recovery_area/MVF1/backupset  on RAID 5 SATA
#
10.101.44.72:/vol/Ora_backup/backup   -
/flashback/db_recovery_area/MVF1/backupset   nfs – yes
 rsize=32768,wsize=32768,hard,intr,largefiles,vers=3,proto=tcp
```

3. To mount the flashback file systems, type

   mount /flashback/db_recovery_area/MVF1/flashback

   mount /flashback/db_recovery_area/MVF1/archivelog

   mount /flashback/db_recovery_area/MVF1/autobackup

   mount /flashback/db_recovery_area/MVF1/backupset

4. During the database installation, set the following parameters for the space in /flashback:

   `db_recovery_file_dest` = **/flashback**

   `db_recovery_file_dest_size` = ***size_of_/flashback_file_system*** (do not include the size of /ora_backups in this value)

   For more details, see *Installing the IMPAX 6.5.1 AS3000 database packages* (refer to page 40).

Note:

The space in /flashback/db_recovery_area/MVF1/backupset is managed by RMAN.

8. Obtaining Server license keys

(Topic number: 7637)

IMPAX uses software license keys that are unique to the station on which the software is installed. One license key is required for the Network Gateway and a separate license key must be obtained for the Archive Server (even if using PACS Store and Remember archiving).

Obtaining Server licenses for Solaris stations

(Topic number: 10701)

To obtain new license keys, if this is required, email licensekey@agfa.com. To generate the license keys, Agfa must know the Ethernet MAC (Media Access Control) address of the server.

To obtain Server licenses for Solaris stations

1. On a Solaris station, confirm that the Ethernet is connected.
2. Log in as the **root** user and open a terminal window.
3. Type

   arp `uname -n`

   or

   arp $(uname -n)

   The MAC addresses for all connections are returned, which is the information Agfa requires to issue a license.
4. To obtain a license key for the server, copy and send the returned information to licensekey@agfa.com, along with a description of the type of component being installed on that server.

Creating the Database Server

3

You must install IMPAX 6.5.1 AS3000 on the Database Server or single-host AS3000 Server, then configure the IMPAX 6.5.1 AS3000 cluster to connect to Client stations through the Application Server. Ensure that you have first completed all relevant procedures in *Setting up a Solaris server* (refer to page 22).

1. Creating the AS3000 software repository

(Topic number: 9936)

You can optionally install the IMPAX 6.5.1 AS3000 and Oracle for Solaris software from a software repository created on the AS3000 Database Server.

Note:

Installing IMPAX 6.5.1 AS3000 from a software repository is **much** faster, and much less prone to error, than installing it from DVD.

The AS3000 software repository can be created using ISO files or DVDs.

To create the AS3000 software repository using ISO files

1. On the AS3000 Database Server, create a directory for the repository by typing **mkdir /agfa/*repository***

   where *repository* is your choice of directory name.
2. Copy the IMPAX 6.5.1 AS3000 Server ISO file to this repository.
3. As the **root** user, type:

   # lofiadm –a /agfa/*repository*/IMPAX 6.5 AS3000 Server.iso

   /dev/lofi/1

 # mount –F hsfs /dev/lofi/1 /mnt

 # cd /mnt

 # cp -r . /agfa/*repository*

where *repository* is the directory you created in step 1.

The files are unpacked onto the Database Server into the *repository* directory.

4. Unmount /mnt and optionally remove the IMPAX 6.5.1 AS3000 Server ISO file.
5. Copy the Oracle for Solaris ISO file to the repository.
6. Repeat the process to extract and copy the Oracle software to the repository.

To create the AS3000 software repository using DVDs

1. On the AS3000 Database Server, log in as the root user and create a directory for the repository by typing **mkdir /agfa/*repository***

   where *repository* is your choice of directory name.
2. Insert the IMPAX 6.5.1 AS3000 Server DVD.
3. Change to the **/cdrom/cdrom0** directory.
4. Copy and unpack the files from the DVD by typing

   tar cvf - . | (cd /agfa/*repository*; tar xf -)

   where *repository* is the directory you created.
5. Remove the IMPAX AS3000 DVD and insert the Oracle for Solaris DVD.
6. Still in the /cdrom/cdrom0 directory, copy and unpack the files from this DVD as well.

   tar cvf - . | (cd /agfa/*repository*; tar xf -)

The files are unpacked onto the Database Server into the *repository* directory.

2. Determining a password for the AgfaService account

(Topic number: 7705)

During the IMPAX Server software installation, you are prompted to create a password for the AgfaService account. The password must conform to the following requirements:

- Be at least eight characters long
- Not contain three or more characters from the user's account name
- Contain characters from at least three of the following five categories:
  - Uppercase (A to Z)
  - Lowercase (a to z)

- Digits (0 to 9)
- Non-alphanumeric (for example, !, $, #, or %); avoid commas
- Unicode

3. What is Oracle Data Guard?

(Topic number: 65374)

Oracle Data Guard enables and automates the management of a disaster recovery solution for Oracle databases.

In an Oracle Data Guard configuration, two database servers run at the same time. The active one is called the *primary database*. The second one is called the *standby database*. As transactions occur in the primary database, redo data is generated and is written to the local redo logs. Data Guard automatically transfers this redo data to the standby sites and applies it to the standby databases, synchronizing them with the primary database. If a problem occurs with the primary database, the standby database can take over as the active database, so the problem on the primary database can be resolved without the site losing access to data.

Oracle Data Guard can be used only with Oracle Enterprise Edition, and not with Oracle Standard Edition. Data Guard can be configured such that backups do not take place, yet the system does not issue an error message. Agfa provides tools to make the configuration and maintenance easier:

1. A set of scripts to automate the configuration of the Data Guard portion of the Oracle database.
2. Implementation of Oracle RMAN (Recovery Manager) to perform a daily backup of the existing database once the configuration has been completed. (Note that RMAN can also be used for backup and recovery exclusive of Oracle Data Guard.)

   We recommend three times the database size for backup allocation.
3. A set of tools to monitor the configuration (refer to page 87).

To use Oracle Data Guard, the IMPAXoradg package (AS3000) or MVForadg package (AS300) must be installed; see *Installing the Oracle Data Guard package on a Database Server* (refer to page 65).

4. Installing Oracle Server for Solaris

(Topic number: 65304)

Oracle is installed separately from the IMPAX 6.5.1 AS3000 Server software. The Oracle software appears on the Oracle for Solaris DVD.

To install Oracle Server for Solaris

1. Log into the Database Server machine as the **root** user.
2. Change to the directory containing the Oracle install script, mounting the drive first if necessary.

This could be the DVD drive or a software repository.

3. Type

   ./install-Oracle server

4. At the `Standard or enterprise install [standard] ?` prompt, if using Oracle Standard Edition, press **Enter**.

   If using Oracle Enterprise Edition, type **enterprise** and press **Enter**.

   If intending to use Oracle Data Guard, you must install Oracle Enterprise Edition. Otherwise we recommend Oracle Standard Edition.

5. At the `What machine is the repository host [localhost] ?` prompt, if it is the localhost, press **Enter**; otherwise, specify the appropriate IP address.

6. At the `Where is the software repository [/cdrom/cdrom0] ?` prompt, if installing from the DVD drive, press **Enter**; otherwise, type the software repository directory.

7. At the `Temporary work directory [/tmp] ?` prompt, to use the /tmp directory, press **Enter**; otherwise, type the directory to use.

   A series of messages appear as Oracle is installed and configured.

8. After the `Oracle installation complete` message appears, type the following to clear volatile memory (RAM) to disk and reboot:

   init 6

5. Installing the IMPAX 6.5.1 AS3000 database packages

(Topic number: 6963)

After you have installed Solaris and Oracle Server, you can install the IMPAX AS3000 Database Server software. You must install the Database Server before other servers can connect remotely for installing the Network Gateway or Archive Server.

To install the IMPAX 6.5.1 AS3000 database packages

1. Log into the Database Server machine as the **root** user.

   You can log into the Database Server machine remotely through ssh.

2. Change to the DVD drive or the software repository directory—whichever of these contains the IMPAX install script.

3. Type

   ./impax_install

4. When prompted, type your name.

5. At the `Please enter the fully qualified hostname of the login server` prompt, type the hostname of the Application Server.

Tip:

If necessary, you can change this hostname after installation, as described in *Configuring the connection to the Application Server* (refer to page 60). For details on installing the Application Server, refer to the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

6. At the `Do you wish to enable Lossy JPEG compression in cache?` prompt, type **y** if you want to enable lossy JPEG compression in the cache. Type **n** if you do not want to enable lossy JPEG compression in the cache.

   This prompt appears only when installing the Database Server. The IMPAXcmpr package contains the Compressor Scheduler process, which is used for scheduling Compressor jobs. The Compressor process is installed on other systems when the IMPAXmvfc package is selected during installation. Both processes are installed and started on each server when lossy compression is enabled at IMPAX 6.5.1 AS3000 installation. We recommend having lossy compression distributed on multiple servers, as described in *Installing Compressor Scheduler manually on Solaris* (refer to page 46).

7. At the `Please enter a password that conforms to the above rules` prompt, create a password for the AgfaService user that conforms to the rules displayed.

   The characters you type are not displayed. Ensure that you type your password carefully. If you are having difficulty in this step and are unsure of what password you have typed, break out of the install script (**Ctrl** + **C**) and return to step 3.

Note:

In a cluster where the database is running on Solaris, we recommend setting the same AgfaService password on all Windows boxes when installing IMPAX; however, the portable password file which is created by default does not contain an entry for the AgfaService user. To address this, see *Generating the AS3000 portable password file for the AgfaService user* (refer to page 48).

8. Confirm the password.
9. Answer the `Please enter flashback location` prompt appropriately.
   - If this server is not using Oracle Data Guard and /flashback is not enabled, and even if RMAN is configured for backups, type **/dbase/flashback**.
   - If this server is using Oracle Data Guard or /flashback is enabled, and RMAN is configured for backups using /flashback (two-volume configuration), type **/flashback**.
   - If this server is using Oracle Data Guard or /flashback is enabled, and RMAN is configured for backups using /flashback (four-volume configuration), type **/flashback/db_recovery_area/MVF1/flashback**.
10. Answer the `Please enter flashback recovery location size in gigabytes` prompt appropriately. See *Partitioning recommendations for the database file systems* (refer to page 26) for more information.

- If this server is not using Oracle Data Guard and /flashback is not enabled, and even if RMAN is configured for backups, use the default of 10 GB (The volume is retained under /dbase but not used.).
- If this server to using Oracle Data Guard or /flashback is enabled, and RMAN is configured for backups using /flashback (two-volume configuration), enter the size of the /flashback volume (excluding the backup area).
- If this server to using Oracle Data Guard or /flashback is enabled, and RMAN is configured for backups using /flashback (four-volume configuration), enter the size of /flashback/db_recovery_area/MVF1/flashback.

In the four-volume configuration of /flashback, the /flashback/db_recovery_area/MVF1/archivelogs directory must be large enough to retain at least a week's worth of archive logs. In the two-volume configuration, this directory and its files are retained in the /flashback volume.

11. If the prompt `NOTE: Archive, Gateway and PACS Archive Provider (PAP) servers require an image cache: Does this station require an image cache?` appears, then, if installing a dedicated Database Server, type **n**.

    or

    If installing a single-host server, type **y**.

    This prompt is bypassed if the script finds a /cache directory already on the system.

12. At the `Install Gateway packages?` prompt, if installing a dedicated Database Server, type **n** to prevent installing the Gateway package.

    or

    If installing a single-host server, type **y** to install the Gateway package.

13. At the `Install OCR package?` prompt, if installing a dedicated Database Server, type **n** to prevent installing the OCR package.

    or

    If installing a single-host station, optionally type **y** to install the OCR package. Otherwise type **n**.

14. At the `Install an Archive?` prompt, if installing a dedicated Database Server, type **n** to prevent installing the Archive package.

    or

    If installing a single-host server, to install the Archive package, type **y**.

15. If installing a single-host server, when prompted, specify the type of archiving.

Archive	Type
Hierarchical Storage Management	hsm
PACS Archiving	PACS

If you are using PACS Archiving, it must be configured and registered separately (refer to page 96).

16. At the `Install PACS Archive Provider (PAP) package?` prompt, if installing a PACS Archive Provider, optionally type **y** to install the PAP package. Otherwise type **n**. Press **Enter**.

    Note:

    A PACS Archive Provider (PAP) allows sites to have their studies mirrored at another site through PACS Store and Remember archiving. This mirroring protects against loss of data and allows studies at one PACS to be viewed at another.

17. When prompted, type any additional system configuration information.
18. When prompted, type any additional comments about the installation process.

    The database is constructed.
19. To reboot the machine to initiate startup of Oracle and all services, type the following to clear volatile memory (RAM) to disk and reboot:

    init 6

After the system has restarted, you must wait a few minutes while the system is initialized before logging in.

6. Configuring the Enterprise Management console for Oracle 10.2.0.4

(Topic number: 120815)

The Oracle Enterprise Manager is a browser-based GUI through which administrators can perform all monitoring, administration, and configuration tasks for the enterprise. The IMPAX installation scripts install the necessary components to run the Enterprise Management Console on the Oracle 10g server. However, you must configure the service manually.

Note:

If you have problems configuring the Enterprise Management console, refer to the *IMPAX 6.5.1 Server Knowledge Base* topic "Troubleshooting: Cannot configure the Oracle 10.2.0.4 Enterprise Management console" (Topic number 120817).

To configure the Enterprise Management Console for Oracle 10.2.0.4

1. If the Database Server is running on a Solaris system, log into the database server as the **oracle** user.

   or

   Log into the Database Server as the **Administrator** user.
2. Open a sqlplus session.

3. Set the database parameter job queue processes by typing

   alter system set job_queue_processes = 10 scope = BOTH;

4. If Oracle is running on a Windows system, skip ahead to step 8.
5. If Oracle is running on a Solaris system, at the Solaris prompt, change to the /opt/oracle/current/network/admin directory.
6. Create a link for the listener.ora file. If the listener.ora file already exists, remove it prior to creating the link. To create the link, type:

   ln -s /var/opt/oracle/listener.ora listener.ora

7. At the Solaris prompt, verify that the link was created by typing

   lrt

   To the right of the date field, the listener.ora file is listed as:

   `listener.ora -> /var/opt/oracle/listener.ora`

8. Start the configuration assistant by typing

   emca -config dbcontrol db -repos create

   or

   If you are attempting to start the configuration assistant a second time, type

   emca -config dbcontrol db -repos recreate

9. When prompted for the Database SID, type

   MVF

10. When prompted for the listener port number, type

    1521

11. When prompted for the SYS user password, type

    stayout

12. When prompted for the DBSNMP user password, type:

    long2figureout

13. When prompted for the SYSMAN user password, type

    sysman

14. Respond to other prompts appropriately.

Note:

The Email address for notifications and Outgoing Mail (SMTP) server for notifications fields are optional.

15. When the system displays the message `Do you wish to continue? [yes(Y)/no(N)]:`, type

    y

16. Log on to the Enterprise Manager, open a web browser and, in the address bar, type the following address:

    https://*Database_Server name*:1158/em

7. Configuring disk arrays for the database filesystems

(Topic number: 103135)

For logistical reasons, a pre-staged IMPAX Database Server is typically not built with the proper disk arrays. Instead, it is shipped with a dummy database with a single mount point that is too small for live use and performs poorly; this should be replaced once the host is on-site and the proper disk arrays are available. Normally, separate arrays are used for the database LUNs and the cache and/or HSM LUNs to reduce disk contention. To utilize the new database LUNs, follow this procedure.

After installing IMPAX, configure the disk arrays for the database filesystems to optimize database performance.

Note:

Ensure that all hardware and firmware are matched appropriately. (Mismatches are a common problem for SAN arrays.)

To configure disk arrays for the database filesystems

1. Check the current firmware version, and update to the latest firmware version, if necessary.
2. To prevent IMPAX from restarting, type

   disable_impax
3. Build volumes on the disk arrays as recommended by the appropriate vendor installation guide.

   For partitioning recommendations, see *Partitioning recommendations for the database file systems* (refer to page 26).
4. After the station has rebooted, login as the **root** user.
5. Instead of deleting the existing /dbase content, you may want to move the shipped database to a suitable free area of disk and retain it for reference purposes. (If required, move the dummy cache and archive volumes that were shipped by staging as well.)

   Important!

   UNIX experience is highly recommended. Follow these instructions carefully or you may render the machine unbootable. If necessary, contact Agfa Professional Services for assistance before proceeding any further.

   Type

   dbshutmvf

umount /dbase

mkdir /export/dbase.orig

sed 's% /dbase% /dbase.orig%' /etc/vfstab >/tmp/$$

cp /etc/vfstab /etc/vfstab.orig

cp /tmp/$$ /etc/vfstab

mount /dbase.orig

6. Create appropriate RAID volumes for cache volumes, if applicable.
7. To change privileges on dbase directories, type

   chmod 777 /dbase /dbase/*

   where the directories are system, index1, rbs, data2, redo, arch, and so on.
8. We recommend that you rebuild the database to take advantage of the new, larger volumes that have been created.
9. To enable IMPAX and reboot, type

   enable_impax

   init 6

After the system has restarted, wait a few minutes while the system is initialized before logging in.

8. Installing Compressor Scheduler manually on Solaris

(Topic number: 6969)

Note:

Compressor Scheduler must run on only one host in the IMPAX cluster.

The IMPAXcmpr package installs Compressor Scheduler (mvf-compressor-scheduler), which is used for scheduling Compressor jobs. If lossy compression was not enabled when IMPAX was installed, and you want to enable it now, you must manually install and start the package on the selected server.

To install Compressor Scheduler manually on Solaris

1. Log into the Database Server as the **root** user.
2. Insert the IMPAX AS3000 Server DVD.
3. If the Compressor Scheduler is required to run at startup, open the /install_info file in a text editor such as vi, and ensure that it has a `LOSSY_JPEG='y'` line.

   Editing the install_info file causes step 5 to run enable_compression automatically (step 6).
4. Change to the **/cdrom/cdrom0/IMPAX_R6.5-*impax_build_label*/`arch -k` directory.**

5. To install the Compressor Scheduler package, type

   pkgadd -d . IMPAXcmpr

6. If step 3 was not performed prior to the installation of the IMPAX cmpr package, you can run it now by typing

   /usr/mvf/bin/enable_compression

   Startup and shutdown files are installed and the mvf-compressor-scheduler service is set up.

9. Recommended frequency of database backups

(Topic number: 6935)

Backups of the database are mandatory. Among other information, the database contains the following information:

- Clinical data such as image markups
- Configuration information for printers, acquisition stations, routing patterns, and preferences, and so on

To guard against information loss due to equipment failure, you must make backup copies of the database and configuration files. Oracle maintains a record of all database transactions in transaction log files. If you fail to make database backups on a non-Oracle Data Guard server, the /dbase/arch directory fills up. On a Data Guard server, the flashbackup directory fills up.

Make a backup once each working day. A backup is not necessary for idle days (for example, weekends). For IMPAX AS3000, the best time of day to make the backup is when the system is least busy.

Performing a warm backup of the database

(Topic number: 15588)

After the IMPAX Database Server is installed, perform a warm backup of the database.

To perform a warm backup of the database

1. Log into the Database Server as the **oracle** user.
2. If backing up to tape, record the date on the tape jacket and insert the tape into the tape drive.
3. Change to the **/usr/mvf** directory.
4. To reconfigure the database, type

   configure_backup

Note:

You must rerun this command after upgrading from all versions of IMPAX. For more details on using this command, refer to “Configuring backups to disk” (topic number

8904) or “Configuring backups using Flashbackup on Solaris” (topic number 66399) in the *IMPAX 6.5.1 Server Knowledge Base*.

5. Type **runbackup**

The backup may take a significant amount of time.

If you ever need to restore the database from a backup, follow the instructions in the Oracle Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

10. Collecting database statistics

(Topic number: 7004)

System statistics allow Oracle 10g to efficiently control a system’s CPU performance and utilization. These statistics should be collected during a period of typical workload.

To collect database statistics

1. Use the *gather_stats_job* and *gather_and_lock_stats_job* utilities.

For details about these utilities, refer to “Collecting database statistics” (topic number 113178) in the Oracle Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

11. Generating the AS3000 portable password file for the AgfaService user

(Topic number: 131115)

In an AS3000 cluster, we recommend setting the same AgfaService password on all Windows boxes when installing IMPAX; however, the portable password file that is created by default does not contain an entry for the AgfaService user. To create this entry, you must delete the mvf.portable.psd file, set the passkey password for the AgfaService user, then use the export mode to re-create the portable password file.

To generate the AS3000 portable password file for the AgfaService user

1. Log into the AS3000 Database Server as the **root** user.
2. Change to the **/usr/mvf** directory.
3. Delete the mvf.portable.psd file from the Database Server.
4. To set the passkey password for the AgfaService user, type

   ./bin/passkey -M SET -u AgfaService -P *password*

   where *password* is the AgfaService user password. See *Determining a password for the AgfaService account* (refer to page 38).

5. To export the passkey for installing IMPAX on remote machines, type

   ./bin/passkey -M EXPORT -k *temporary_password*

   where *temporary_password* is a password to be used to import the portable password file later.

   This re-creates the /usr/mvf/mvf.portable.psd password file.

6. To copy the portable password file from the Database Server to the target server, type

   scp /usr/mvf/mvf.portable.psd service@[*target_host_name*]:/usr/mvf/mvf.portable.psd

   where *target_host_name* is the host name of the target server.

   The mvf.portable.psd file is copied from the Database Server to the target server.

Delete /usr/mvf/mvf.portable.psd from the Database Server when you are finished copying it to the target servers or servers.

For more details, see *Understanding the passkey utility* (refer to page 100).

Creating the Network Gateway

4

Before installing a dedicated AS3000 Network Gateway, ensure that you have completed all relevant procedures in *Setting up a Solaris server* (refer to page 22). Also ensure that you have installed the Database Server hosting the Oracle database, as described in *Creating the Database Server* (refer to page 37).

If installing the Network Gateway on the same Solaris station as the Archive Server, follow the procedures in *Creating the Archive Server* (refer to page 54) instead. If setting up an AS300 (Windows-based) Network Gateway, refer to the Network Gateway installation instructions in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

1. Generating the password file from the Database Server

(Topic number: 6978)

When installing IMPAX 6.5.1 AS3000 Network Gateway software, the IMPAX 6.5.1 AS3000 installation script requires a portable password file, mvf.portable.psd. This file is automatically generated when you first install the Oracle Database Server. Prudent security management recommends this file be deleted once all Network Gateway, Archive Server, Application Server, and Curator machines are installed.

If you know the mvf.portable.psd file has not yet been deleted, you can now proceed with the Network Gateway installation.

But if you are now installing another new Network Gateway after the mvf.portable.psd file has been deleted, you must first follow the instructions in *Generating and importing mvf.portable.psd* (refer to page 98).

2. Installing Oracle Client for Solaris

(Topic number: 66700)

Oracle is installed separately from the IMPAX AS3000 Server software. The Oracle software appears on the Oracle for Solaris DVD. The Oracle Client software is required to communicate with the IMPAX AS3000 Oracle Database Server.

To install Oracle Client for Solaris

1. Log into the Solaris server machine as the **root** user.
2. Change to the directory containing the Oracle install script, mounting the drive first if necessary.

   This could be the DVD drive or a software repository.
3. Type **./install-Oracle client**.
4. At the `Hostname of the Oracle server [] ?` prompt, type the name of the Oracle Database Server and press **Enter**.
5. At the `What machine is the repository host [localhost] ?` prompt, if it is the localhost, press **Enter**; otherwise, specify the appropriate IP address.
6. At the `Where is the software repository [/cdrom/cdrom0] ?` prompt, if installing from the DVD drive, press **Enter**; otherwise, type the software repository directory.
7. At the `Temporary work directory [/tmp] ?` prompt, to use the /tmp directory, press **Enter**; otherwise, type the directory to use.

   A series of messages appear as Oracle is installed and configured.
8. After the `Oracle installation complete` message appears, type the following to clear volatile memory (RAM) to disk and reboot:

   init 6

3. Installing IMPAX 6.5.1 AS3000 Network Gateway software

(Topic number: 58050)

The Network Gateway is the workflow manager of the IMPAX 6.5.1 AS3000 cluster. It receives studies from modalities and provides DICOM security and validation.

Note:

If installing the Network Gateway on the same Solaris server as the Archive Server, follow the instructions in *Installing IMPAX 6.5.1 AS3000 Archive Server software* (refer to page 55).

To install IMPAX 6.5.1 AS3000 Network Gateway software

1. Log into the target server machine as the **root** user.
2. Insert the IMPAX 6.5.1 AS3000 Server DVD-ROM and change to the **/cdrom/cdrom0** directory.

   or

   Change to the IMPAX software repository location.
3. To run the IMPAX 6.5.1 AS3000 install script, type

   ./impax_install
4. When prompted for your name, type your name.
5. When prompted, type the password for the AgfaService user.

   This is the password you created when installing the Database Server (refer to page 40).
6. Confirm the password.
7. At the Gateway package prompt, type **y** to install the Network Gateway package.
8. At the OCR package prompt, if installing the OCR station, type **y**. Otherwise, type **n**.
9. At the Archive package prompt, type **n** to prevent installing the Archive Server package.
10. At the Install PACS Archive Provider (PAP) package prompt, type **n**.
11. When prompted, type any additional system configuration information and comments about the installation process.

    This information is saved in /install_info.

    Note:

    The compressor package is installed as part of the IMPAXmvfc package and it is automatically started when the system is rebooted. But you must manually start the compressor scheduler (refer to page 59).
12. After the installation is completed, you must reboot the machine. Type the following to clear volatile memory (RAM) to disk and reboot at the -bash-3.00# prompt:

    init 6
13. Manually import the mvf.portable.psd file (refer to page 99).

4. Installing the mvf license key on a Solaris server

(Topic number: 58053)

MVF license keys must be installed on each single-host, Archive Server/Network Gateway, and Network Gateway station.

To install the mvf license key on a Solaris server

1. Match up the correct license key with the machine's MAC address.

The license key name is the MAC address with a .lic file extension.

2. Change to the **/usr/mvf** directory.
3. Copy the license key file to the mvf directory on the hard drive.
4. Rename the license key file to:

   mvf.lic

Creating the Archive Server

5

Before installing a dedicated AS3000 Archive Server or a Network Gateway/Archive Server, ensure that you have completed all relevant procedures in *Setting up a Solaris server* (refer to page 22). Also ensure that you have installed the Database Server hosting the Oracle database, as described in *Creating the Database Server* (refer to page 37).

If setting up an AS300 (Windows-based) Archive Server instead, refer to the Archive Server installation instructions in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

1. Generating the password file from the Database Server

(Topic number: 6979)

When installing IMPAX 6.5.1 AS3000 Archive Server software, the IMPAX 6.5.1 AS3000 installation script requires a portable password file, mvf.portable.psd. This file is automatically generated when you first install the Oracle Database Server. Prudent security management recommends this file be deleted once all Network Gateway, Archive Server, Application Server, and Curator machines are installed.

If you know the mvf.portable.psd file has not yet been deleted, you can now proceed with installing the Archive Server software.

But if you are now installing a new Archive Server after the mvf.portable.psd file has been deleted, you must first follow the instructions in *Generating and importing mvf.portable.psd* (refer to page 98).

2. Installing Oracle Client for Solaris

(Topic number: 66700)

Oracle is installed separately from the IMPAX AS3000 Server software. The Oracle software appears on the Oracle for Solaris DVD. The Oracle Client software is required to communicate with the IMPAX AS3000 Oracle Database Server.

To install Oracle Client for Solaris

1. Log into the Solaris server machine as the **root** user.
2. Change to the directory containing the Oracle install script, mounting the drive first if necessary.

   This could be the DVD drive or a software repository.
3. Type **./install-Oracle client**.
4. At the `Hostname of the Oracle server [] ?` prompt, type the name of the Oracle Database Server and press **Enter**.
5. At the `What machine is the repository host [localhost] ?` prompt, if it is the localhost, press **Enter**; otherwise, specify the appropriate IP address.
6. At the `Where is the software repository [/cdrom/cdrom0] ?` prompt, if installing from the DVD drive, press **Enter**; otherwise, type the software repository directory.
7. At the `Temporary work directory [/tmp] ?` prompt, to use the /tmp directory, press **Enter**; otherwise, type the directory to use.

   A series of messages appear as Oracle is installed and configured.
8. After the `Oracle installation complete` message appears, type the following to clear volatile memory (RAM) to disk and reboot:

   init 6

3. Installing IMPAX 6.5.1 AS3000 Archive Server software

(Topic number: 58065)

The Archive Server is the DICOM archive used for permanent storage and retrieval of studies.

To install IMPAX 6.5.1 AS3000

1. Log into the target server machine as the **root** user.

   or

   From the server hosting the repository, log into the remote Archive Server station as the **root** user.

2. Insert the IMPAX 6.0 AS3000 Server DVD-ROM and change to the **/cdrom/cdrom0** directory.

   or

   Change to the IMPAX software repository location.
3. To run the installation script, type

   ./impax_install
4. When prompted for your name, type your name.
5. Type the password for the AgfaService user.

   This is the password you created when installing the Database Server (refer to page 40).
6. Confirm the password.
7. At the Gateway package prompt, to install an Archive Server only, type **n**.

   To install a combined Archive Server and Network Gateway, type **y**.
8. When prompted about installing the Archive Server, type **y**.
9. To install an Archive Server, specify the type of archiving.

Archive	Type
Hierarchical Storage Management	hsm
PACS Archiving	PACS

   If you are using PACS Archiving, it must be configured and registered separately (refer to page 96).
10. At the Install PACS Archive Provider (PAP) package prompt, type **n**.
11. When prompted, type any additional system configuration information.

    This information is saved in /install_info.
12. When prompted, type any additional comments about the installation process.

    This information is saved in /install_info.
13. After the installation is completed, you must reboot the machine. Type the following to clear volatile memory (RAM) to disk and reboot at the -bash-3.00# prompt:

    -init 6

4. Configuring the mounted location for HSM

(Topic number: 6999)

The Hierarchical Storage Management (HSM) archive system provides long-term storage of data and access to data. Studies archived with HSM are stored to a file system. HSM is an archive storage option and is not installed by default.

Note:

Before configuring the mounted location, you must set up the subdirectory within the mount point and set the appropriate permissions.

After the HSM package is installed, a few additional configuration steps are required. Ensure that the mounted location is set up and is ready for storage/retrieval of files before the HSM starts to store/retrieve data to/from the mounted location.

To configure the mounted location for HSM

1. Log in as a **service** user.
2. To get information about the tool, type

   mvf-hsm-archive-add-mp -?
3. To check the mounted location, type

   mvf-hsm-archive-add-mp -S
4. To set the mounted location, type

   mvf-hsm-archive-add-mp -M *mount_point* -D *dir*

5. Installing Server license keys on a new server

(Topic number: 40455)

If you have not already installed the appropriate license keys on the servers, do so now. MVF license keys must be installed on each single-host and Network Gateway station. Archive license keys must be installed on each single-host and Archive Server station.

If you do not have license keys, you must obtain them from the Agfa Account Manager. More information, including details about obtaining the MAC address, is available in *Obtaining Server license keys* (refer to page 35).

Installing the mvf license key on a Solaris server

(Topic number: 58053)

MVF license keys must be installed on each single-host, Archive Server/Network Gateway, and Network Gateway station.

To install the mvf license key on a Solaris server

1. Match up the correct license key with the machine's MAC address.

   The license key name is the MAC address with a .lic file extension.
2. Change to the **/usr/mvf** directory.
3. Copy the license key file to the mvf directory on the hard drive.

4. Rename the license key file to:

   mvf.lic

Installing the archive license key on a Solaris server

(Topic number: 58056)

Archive license keys must be installed on each single-host, Archive Server/Network Gateway, and Archive Server station.

To install the archive license key on a Solaris server

1. Match up the correct license key with the machine's MAC address.

   The license key name is the MAC address with a .lic file extension.
2. Change to the **/usr/mvf** directory.
3. Copy the license key file to the mvf directory on the hard drive.
4. Rename the license key file to:

   mvfarch.lic

Completing the installation of an IMPAX AS3000 cluster

6

After the installation and preliminary setup of the IMPAX AS3000 servers, additional tasks are required to complete the installation.

1. Starting Compressor manually on Solaris

(Topic number: 6925)

The Compressor files are already installed on those systems with the IMPAXmvfc package (such as Network Gateways and Archives); however, Compressor is not actively running and must be manually started.

To start Compressor manually on Solaris

1. Log into the server as **root**.
2. To start the Compressor, at the terminal window prompt, type

   /etc/init.d/IMPAXcomp start

   This command installs the startup and shutdown files, and starts the Compressor process, which creates a Compressor Job queue.
3. To ensure that the Compressor is running, type

   ps -ef | grep comp
4. Verify that the IMPAXcomp.boot and mvf-compressor processes are running.

   If the Compressor Scheduler is installed and running on this system, the IMPAXcompressor.boot and mvf-compressor-scheduler processes may be listed.

5. From **Administration Tools** > **Job Manager**, verify that a new MVF_COMPRESSOR queue exists.

2. Installing the IMPAX Server documentation

(Topic number: 6962)

The IMPAX Server documentation is located on the IMPAX Documentation DVD. You install it on an IMPAX Application Server, not on any of the AS300 or AS3000 servers. Refer to "Installing the IMPAX documentation" (topic number 15523) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

3. Installing the Application Server

(Topic number: 40165)

Before configuring IMPAX Server, install the Application Server software. Refer to the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Note:

If installing a single-host AS300 (Windows) server, you can optionally install the Application Server software on that same server, creating what is called an *all-in-one* server.

4. Configuring the connection to the Application Server

(Topic number: 7000)

When installing IMPAX AS3000 on the Database Server, you are prompted to type the host name of the login server, which is known as the Application Server. This location is stored in the database and hosts file, which you can configure manually if necessary.

To configure the connection to the Application Server

1. Log into the Database Server as the **root** user.
2. To stop the Administration Tools server, type

   /etc/init.d/IMPAXjsgw stop
3. Change to the**/usr/mvf/bin** directory.
4. Launch CLUI.
5. At the $ prompt, type

update map_ini set ini_value = 'https://*Application_Server_FQDN*/AgfaHC.User.Security.Web.Services/Login.asmx' where ini_key = 'ws.authenticate.uri' and ini_section = 'SERVICE_TOOLS'

where *Application_Server_FQDN* is the fully qualified domain name of the Application Server; for example, **server1.domain.com**.

6. Update the host file with the IP address, FQDN and, optionally, any aliases of the Application Server.
7. To start the Administration Tools server, type

   /etc/init.d/IMPAXjsgw start

5. Installing and configuring Curator

(Topic number: 7152)

After installing the Application Server and performing its initial configuration, install and configure the Curator server, as per the instructions in the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*.

6. Configuring the Audit Record Repository database connection

(Topic number: 32237)

After installing or upgrading the database and adding an Audit Record Repository, you must update certain entries in the database to ensure that auditing functions correctly.

To configure the Audit Record Repository database connection

1. On the IMPAX Database Server, open a command prompt or terminal window.
2. Change to the **C:\mvf\bin** (AS300) or **/usr/mvf/bin** (AS3000, logged in as mvf user) directory.
3. Type **clui**.
4. To check if the entry already exists in the database, type

   ```
   select * from map_ini where ini_key='ARR_INSTALLED' and
   ini_section='MAP_EVENT'
   ```

5. If the entry exists, to update the entry, type

   ```
   update map_ini set ini_value='T' where ini_key='ARR_INSTALLED' and
   ini_section='MAP_EVENT'
   ```

   or if the key does not exist, to insert it, type

   ```
   insert into map_ini (ini_section,ini_key,ini_value) values
   ('MAP_EVENT','ARR_INSTALLED','T')
   ```

The Application Server must also be connected to the Audit Record Repository. For details, refer to "Connecting IMPAX Application Server to Audit Manager" (topic number 11444) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

7. Configuring IMPAX 6.5.1 stations

(Topic number: 7002)

After all cluster components are installed, you must configure the capabilities for each station in the IMPAX 6.5.1 Administration Tools. For details and instructions, refer to the Network Management section (topic number 8988) of the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*. For instructions on installing IMPAX Client, refer to the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

Oracle Data Guard: Disaster recovery solution

A

Oracle Data Guard enables and automates the management of a disaster recovery solution for Oracle databases.

What is Oracle Data Guard?

(Topic number: 65374)

Oracle Data Guard enables and automates the management of a disaster recovery solution for Oracle databases.

In an Oracle Data Guard configuration, two database servers run at the same time. The active one is called the *primary database*. The second one is called the *standby database*. As transactions occur in the primary database, redo data is generated and is written to the local redo logs. Data Guard automatically transfers this redo data to the standby sites and applies it to the standby databases, synchronizing them with the primary database. If a problem occurs with the primary database, the standby database can take over as the active database, so the problem on the primary database can be resolved without the site losing access to data.

Oracle Data Guard can be used only with Oracle Enterprise Edition, and not with Oracle Standard Edition. Data Guard can be configured such that backups do not take place, yet the system does not issue an error message. Agfa provides tools to make the configuration and maintenance easier:

1. A set of scripts to automate the configuration of the Data Guard portion of the Oracle database.
2. Implementation of Oracle RMAN (Recovery Manager) to perform a daily backup of the existing database once the configuration has been completed. (Note that RMAN can also be used for backup and recovery exclusive of Oracle Data Guard.)

   We recommend three times the database size for backup allocation.

3. A set of tools to monitor the configuration (refer to page 87).

To use Oracle Data Guard, the IMPAXoradg package (AS3000) or MVForadg package (AS300) must be installed; see *Installing the Oracle Data Guard package on a Database Server* (refer to page 65).

Configuring Oracle Data Guard

(Topic number: 65856)

Data Guard is Oracle's high-availability solution, using primary and standby database servers. For this solution to work, you must configure it correctly.

Oracle Data Guard configuration overview

(Topic number: 66674)

Oracle Data Guard is Oracle's high-availability solution. In an Oracle Data Guard configuration, two database servers run at the same time. The active one is called the primary database. The second one is called the standby database.

The main tasks in setting up an Oracle Data Guard configuration are as follows.

1. Install the IMPAX Database Server following the procedures in the appropriate installation guide: *IMPAX 6.5.1 AS300 Installation and Configuration Guide* or *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

   This will be the primary database.

2. On AS3000 machines, install the IMPAXoradg package as described in *Installing the Oracle Data Guard package on a Database Server* (refer to page 65). When installing an AS300, select the optional MVForadg component.

3. Back up the database on the primary database, then restore it onto the standby server, using one of the following methods:

   - RMAN backup and restore (refer to page 65)

     or

   - Cold backup and restore (refer to page 69)

   This initially configures the standby server.

4. To ensure that the database servers are backed up and that any archive logs no longer required are cleaned up, configure RMAN backups (refer to page 76) on the primary and standby servers.

Installing the Oracle Data Guard package on a Database Server

(Topic number: 66583)

To use Oracle Data Guard, the IMPAXoradg package (AS3000), or the MVForadg package (AS300) must be installed. On the IMPAX AS3000, you must install the IMPAXoradg package separately.

To install the IMPAXoradg package on an AS3000 Database Server

1. Log into the Database Server as the **root** user.
2. Change to the IMPAX software repository directory.
3. Change to the **IMPAX_R6.5-*impax_build_label*** directory.
4. Run the following command:

   pkgadd -d ./IMPAXoradg.pkg

To install the MVForadg package on an AS300 Database Server

1. When installing the AS300, select the MVForadg as one of the optional packages.

Note:

If you did not install MVForadg at installation time, re-run the IMPAX software installer and select the MVForadg package. Installation instructions are available in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide.*

Configuring Oracle Data Guard using RMAN

(Topic number: 125069)

To configure Oracle Data Guard, you must back up the primary database and restore it onto the standby database server. You can do this either by using RMAN, as described in this topic, or through a cold backup and restore (refer to page 69). Large sites may find the cold backup and restore approach is faster than using RMAN.

Note:

We recommend three times the database size for backup allocation.

The following tasks must be performed:

1. Stop IMPAX and the Application Server.
2. Run the Oracle Data Guard configuration on the primary server and start the public listener (refer to page 66).
3. For Solaris servers only: Share the Flashback area (refer to page 67).

4. Run the Oracle Data Guard configuration on the standby server (refer to page 68).
5. Complete the Data Guard configuration on the primary server (refer to page 69).
6. Start IMPAX and the Application Server.

Running the Oracle Data Guard configuration on the primary server

(Topic number: 125049)

When backing up and restoring the primary database using RMAN, you must first run the Oracle Data Guard configuration on the primary server.

To run the Oracle Data Guard configuration on the primary server

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.
2. If on Solaris, log in as the **root** user.
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
5. Enter the following information when prompted:
   a. The location of the Flashback partition.

      The location is typically **/flashback** (Solaris) or **E:\data\flashback** (Windows).
   b. Whether the current server is the primary or standby server.
   c. The host names of both the primary and standby server.
   d. The size of the Flash Recovery Area in GB.

      Use a value as prescribed for the /flashback area by the Database Configurator tool. Do *not* include the space for the backups in this amount if backups are on their own file system. Normally, no more than two times the database size is required if backups are separated.
6. When asked if you want to continue with the RMAN backup, type **"y"**.
7. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory.
8. On Solaris, log in as the **oracle** user and type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

mv PWDMVF.ora PWDMVF.ora.pre_dg

orapwd file=PWDMVF.ora password=stayout entries=40

This creates an Oracle password file.

9. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, in a command prompt, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

After the Data Guard configuration is run on the primary server, the public listener needs to be started.

To start the public listener

1. Log in as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Type **lsnrctl start listener_public**.

Next, if using Solaris servers, share the Flashback area (refer to page 67); otherwise go directly to restoring the database on the standby server (refer to page 68).

Sharing the Flashback Recovery Area and the primary /dbase partition on a Solaris Server

(Topic number: 125477)

Important!

This task is **not** required on Windows servers.

If the database volumes are mounted using NFS, complete this procedure from the NAS hosting the NFS share to the primary server.

To share the primary Flashback Recovery Area and the primary /dbase partition on a Solaris server

1. Copy the contents of the Flashback directory from the primary to the standby server.
2. Open the file **/etc/dfs/dfstab** in a text editor.
3. Add the following line:

   share –F nfs -o rw,anon=0 *path_to_Flashback_recovery_area*
4. Save and close the file.
5. If the system is armored, type

   svcadm enable network/nfs/server
6. Type **shareall**.
7. Log in as the **mvf** user.

8. To confirm that the directory was shared, type **dfshares**.

Next, restore the database on the standby server (refer to page 68).

Restoring the database on the standby server

(Topic number: 125059)

Restoring the database on the standby server is required for both Solaris and Windows servers.

To restore the database on the standby server

1. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory
3. On Solaris, type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

   orapwd file=PWDMVF.ora password=stayout entries=40

   This creates an Oracle password file.
4. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;
5. On Solaris, to mount the partition locally, log in as the **root** user and type

   mount ***primary_server_name:path_to_flashback_recovery_area_on_primary_server*** **/mnt1**

   Note:

   If the database volumes are mounted using NFS, complete this procedure from the NAS hosting the NFS share to the primary server.
6. Copy all flashback recovery files from the primary server to the standby server.

   On Solaris, change to the mnt1 directory and use the **cp -rp** * **/complete_path_to_standby_database_flashback_area/** command.

   On Windows, use standard file copy and paste functionality.
7. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
8. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

On Windows, type **bash setup_dg**.

9. Enter the Flashback and host name information as prompted.
10. When asked if you want to do the RMAN restore, type **"y"**.

Finally, to link the two servers, complete the Data Guard configuration (refer to page 69).

Completing the Data Guard configuration

(Topic number: 125469)

Linking the two servers, a final Oracle Data Guard configuration task is necessary.

To complete the Data Guard configuration

1. Log into the primary server as the **root** (Solaris) or **AgfaService** (Windows) user.
2. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
3. To continue the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
4. At the prompt, `About to enable log_archive_dest_1 on Primary. Has Data Guard been configured on the Standby?`, type **yes**.
5. When prompted, manually copy the **tnsnames.ora.client** file to the Oracle Client stations.
6. For AS3000 Oracle Clients, also copy the **/usr/mvf/odbc32v52/odbc.ini** file.
7. To free up disk space, clean up the RMAN backup created by the Data Guard configuration by typing:

   rman target /

   delete backup;

Next you must configure RMAN backups (refer to page 76) on the primary and standby servers.

Configuring Oracle Data Guard using cold backup

(Topic number: 124225)

In configuring Oracle Data Guard, the second task is to back up and restore the primary database. You can do this either by using RMAN (refer to page 65) or through a cold backup and restore, as described in the following topics. Large sites may find the cold backup and restore approach is faster than using RMAN.

Note:

We recommend three times the database size for backup allocation.

The following tasks must be performed:

1. Run the Oracle Data Guard configuration on the primary server (refer to page 70).
2. Start the public listener (refer to page 71).
3. Run the Oracle Data Guard configuration on the standby server (refer to page 71).
4. For Solaris servers only: Share the primary Flashback and database areas (refer to page 72).
5. Restore the database on the standby server (refer to page 72).
6. Complete the Data Guard configuration by linking the two servers (refer to page 75).

Running the Oracle Data Guard configuration on the primary server

(Topic number: 124026)

When backing up and restoring the primary database through a cold backup and restore, you must first run the Oracle Data Guard configuration on the primary server.

To run the Oracle Data Guard configuration on the primary server

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.
2. If on Solaris, log in as the **root** user.
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
5. Enter the following information when prompted:
   a. The location of the Flashback partition.

      The location is typically **/flashback** (Solaris) or **E:\data\flashback** (Windows).
   b. Whether the current server is the primary or standby server.
   c. The host names of both the primary and standby server.
   d. The size of the Flash Recovery Area in GB.

      Use a value as prescribed for the /flashback area by the Database Configurator tool. Do *not* include the space for the backups in this amount if backups are on their own file system. Normally, no more than two times the database size is required if backups are separated.

6. When asked if you want to continue with the RMAN backup, type **"n"**.
7. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory.
8. On Solaris, log in as the **oracle** user and type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

   orapwd file=PWDMVF.ora password=stayout entries=40

   This creates an Oracle password file.
9. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, in a command prompt, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

Next, you must run the Oracle Data Guard configuration on the standby server (refer to page 71).

Running the Oracle Data Guard configuration on the standby server

(Topic number: 123967)

After the Data Guard configuration is run on the primary server and before running the configuration on the standby server, the listener needs to be started.

To start the public listener

1. Log in as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Type **lsnrctl start listener_public**.

After the listener service is started, run the Oracle Data Guard configuration on the standby server.

To run the Oracle Data Guard configuration on the standby server

1. On the standby server, log in as user **root** (Solaris) or **AgfaService** (Windows).
2. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
3. On Solaris, type **./setup_dg**.

   or

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt by selecting **Start**, then right-clicking **Command Prompt**, then selecting **Run as administrator**. Then, type **bash setup_dg**
4. When prompted, provide the Flashback area and host name information requested.
5. When asked if you want to do the RMAN restore, type **"n"**.

6. When asked about the manual restore, start up a separate prompt on the standby server and perform the procedures that follow to restore the database on the standby server in the new command prompt.

   For the time being, leave the existing prompt alone.

Next, if using Solaris servers, share the primary Flashback Recovery Area and primary /dbase partition (refer to page 72); otherwise, if using Windows servers, restore the database on the standby server (refer to page 72).

Sharing the primary Flashback Recovery Area and primary /dbase partition on a Solaris Server

(Topic number: 123990)

Important!

This task is **not** required on Windows servers or on the standby database server. It requires a root user login.

If the database volumes are mounted using NFS then this procedure must be completed from the NAS hosting the NFS share to the primary server.

To share the primary Flashback Recovery Area and primary /dbase partition on a Solaris server

1. Type **shareall**.
2. Open the file **/etc/dfs/dfstab** in a text editor.
3. Add the following line:

   share –F nfs -o rw,anon=0 *path_to_Flashback_recovery_area*

   share –F nfs -o rw,anon=0 /dbase
4. Save and close the file.
5. If the system is **not** armored, type **shareall**.

   or

   If the system is armored, type

   svcadm enable network/nfs/server

   shareall
6. Log in as the **mvf** user.
7. To confirm that the directory was shared, type **dfshares**

Next, restore the database on the standby server (refer to page 72).

Restoring the database on the standby server

(Topic number: 124004)

Restoring the database on the standby server is required for both Solaris and Windows servers.

To restore the database on the standby server

1. Log into the primary server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Shut down the primary server by typing

   sqlplus / as sysdba

   shutdown immediate;

   exit;
3. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
4. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory
5. On Solaris, type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

   orapwd file=PWDMVF.ora password=stayout entries=40

   This creates an Oracle password file.
6. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;
7. To shut down the standby database, type

   sqlplus / as sysdba

   shutdown immediate;

   exit;
8. On Solaris, to mount the partition locally, log in as the **root** user and type

   mount *primary_server_name*:*path_to_flashback_recovery_area_on_primary_server* /mnt1

   mount *primary_server_name*:/dbase /mnt2
9. Clean up the existing data files and redo log files from the standby server by deleting (or move) these files. In doing so, ensure that the /dbase directory structure and any symlinks remain untouched.

/dbase/system/*.ctl	/dbase/redo/*.dbf	/dbase/data1/*.ctl
/dbase/system/*.dbf	/dbase/index1/*.ctl	/dbase/data1/*.dbf
/dbase/rbs/*.ctl	/dbase/index1/*.dbf	/dbase/data2/*.ctl
/dbase/rbs/*.dbf	/dbase/index2/*.ctl	/dbase/data2/*.dbf

/dbase/redo/*.ctl /dbase/index2/*.dbf /dbase/arch/*.dbf

10. Copy the necessary data files and redo log files from the primary server to the standby server:

Note:

On Solaris, use the **cp -rp** command for each. On Windows, use standard file copy and paste functionality.

Source directory	Source files	Target directory	Additionally
flashback/ db_recovery_area	standby_control.ctl	flashback/*db_recovery_area*	–
/mnt2/data1	All files with *.dbf extensions	/dbase/data1 (Solaris) or D:\data\dbase\data1 (Windows)	If you have data2/data3/data4 directories that are not symlinks of data1, also copy to those directories.
/mnt2/index1	All files with *.dbf extensions	/dbase/index1 (Solaris) or D:\data\dbase\index1 (Windows)	If you have index2/index3/index4 directories that are not symlinks of index1, also copy to those directories.
/mnt2/system	All files with *.dbf extensions	/dbase/system (Solaris) or D:\data\dbase\system (Windows)	If you have rbs/redo directories that are not symlinks of system, also copy to those directories.
/mnt2/system	All redo0*.log files	/dbase/system (Solaris) or D:\data\dbase\system (Windows)	Make sure the redo_standby*.log files are not copied. Note that the redo log files could be in the redo directory.

11. Copy any additional data or index files from the primary to the standby server, but do **not** copy the control files or the standby redo log files.
12. On the standby server, restore the standby control file in RMAN.
    a. Log in as user **oracle** (Solaris) or **AgfaService** (Windows).
    b. Type

       rman target /

       startup nomount;

restore standby controlfile from *'flashback/db_recovery_area directory*/standby_control_file.ctl';

shutdown abort;

startup mount;

exit

13. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
14. On the standby server, switch back to the command prompt where setup_dg was running. At the manual restore prompt, type **"y"** to continue with Data Guard configuration.

Finally, to link the two servers, complete the Data Guard configuration (refer to page 75).

Completing the Data Guard configuration

(Topic number: 124015)

Linking the two servers, a final Oracle Data Guard configuration task is necessary.

To complete the Data Guard configuration

1. Log into the primary server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. If the primary database is not started, start it up by typing

   sqlplus / as sysdba

   startup;

   exit;
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To continue the Oracle Data Guard configuration, log in as **root** (Solaris) or **AgfaService** user (Windows).
5. On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
6. At the prompt, `About to enable log_archive_dest_1 on Primary. Has Data Guard been configured on the Standby?`, type **"y"**.
7. When prompted, manually copy the **tnsnames.ora.client** file to the Oracle Client stations.
8. On Solaris systems, manually copy the **/export/mvf/odbc32v52/odbc.ini** file to the same location on the Network Gateway servers.

Next you must configure RMAN backups (refer to page 76) on the primary and standby servers.

Configuring RMAN backups after the Oracle Data Guard configuration

(Topic number: 66586)

Perform this task after you have backed up the database on the primary server and restored it on the standby server as part of the Oracle Guard configuration.

Configuring RMAN to perform a disk backup at this point cleans up the archive logs.

To configure RMAN backups after the Oracle Data Guard configuration

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.

2. In a command prompt, change to the **/usr/mvf/bin** (Solaris) or the **C:\mvf\bin** (Windows) directory.

3. Run the **configure_backup** command.

4. To create a standby control file on the primary server, type

   sqlplus / as sysdba

   alter database create standby controlfile as '/opt/oracle/standby_control_file.ctl';

5. Copy the control file, **standby_control_file.ctl**, from the primary to the standby server.

   On Solaris, you can use the following command to do so:

   scp /opt/oracle/standby_control_file.ctl service@*host_name_of_standby_server*/usr/mvf

   On Windows, use standard copy and paste functionality to copy the file over.

6. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.

7. Run the **configure_backup** command on this server as well.

8. To shut down the standby server, type the following:

   sqlplus / as sysdba

   shutdown immediate;

9. To import the standby control files from the primary server to the standby server, first rename them with a **.orig** extension on the standby server; for example, change **control03.ctl** to **control03.ctl.orig**. The files to rename are:

   a. **/usr/mvf/data/dbase/data2/control03.ctl** (Solaris) or **E:\data\dbase\data2\control03.ctl** (Windows)

   b. **/usr/mvf/data/dbase/index2/control02.ctl** (Solaris) or **E:\data\dbase\index2\control02.ctl** (Windows)

   c. **/usr/mvf/data/dbase/system/control01.ctl** (Solaris) or **E:\data\dbase\system\control01.ctl** (Windows)

10. Now copy the standby control files from the primary server to the standby server. The files to copy are the same as those listed in the previous step.

11. To start and mount the standby server, type

sqlplus / as sysdba

startup mount

Maintaining Oracle Data Guard

(Topic number: 67248)

Data Guard is Oracle's high-availability solution, using primary and standby database servers. Once this solution is configured, ongoing maintenance is required to ensure system availability.

Synchronizing redo changes from the primary database to the standby database

(Topic number: 67142)

Changing the size and number of the online redo log files is sometimes done to tune the database. You can add or drop online redo log file groups or members to the primary database without affecting the standby database. Similarly, you can drop log file groups or members from the primary database without affecting the standby database. However, these changes can affect the performance of the standby database after switchover.

For example, the primary database has 10 redo log files and the standby database has two online redo log files. When you switch over to the standby database so that it functions as the new primary database, the new primary database is forced to archive more frequently than the original primary database.

We strongly recommend that if you add or drop online redo log files from the primary database, you synchronize the changes on the standby database.

To synchronize redo changes from the primary database to the standby database

1. If Redo Apply is running, you must cancel it before you can change the log files. In sqlplus on the standby server, execute the command:

   alter database recover managed standby database cancel;

2. If the STANDBY_FILE_MANAGEMENT initialization parameter is set to AUTO, to change the value to MANUAL, execute the command:

   alter system set standby_file_management = manual;

3. To add or drop an online redo log file, execute the commands:

   connect internal

4. To check the existing redo log groups, execute the command

   select * from v$log;

5. To determine the location and the file names of the current redo log files, execute the command

   select * from v$logfile;

6. To add a new online redo log file, execute the command

alter database add logfile 'usr/mvf/data/dbase/redo/redo#.log' size 25000K; (Solaris) or **alter database add logfile 'd:\data\dbase\redo\redo#.log' size 25000K;** (Windows)

Where # is the number of the next redo log group. For example, if the **select * from v$logfile;** command returns redo03, you would create redo04.

7. To add more redo log files, repeat steps 5 and 6.
8. To switch to the current log file, execute the command:

   alter system switch logfile;
9. If the redo log needs to be dropped, execute the commands:

   alter database drop logfile group #;

   select * from v$log;

   Where # specifies the log group to drop, for example, **alter database drop logfile group 1;** drops the redo01.log file
10. To restore the STANDBY_FILE_MANAGEMENT initialization parameter and the Redo Apply options to their original states, execute the commands:

    alter database recover managed standby database using current logfile disconnect from session;

    alter system set standby_file_management = auto;

Rebooting the standby database server

(Topic number: 67099)

If you have to do any type of servicing of the standby server, you can reboot the server after the servicing.

To reboot the standby database server

1. Log into the standby server.

   On Solaris, log in as the **root** user. On Windows, log in as the **AgfaService** user.
2. To prevent IMPAX from starting after a reboot, in a command prompt, type

   # disable_impax
3. If running on Windows, ensure all the IMPAX services are set to **Manual** startup.
4. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
5. To reboot the standby server, type

   $ sqlplus / as sysbda

   alter database recover managed standby database cancel;

   shutdown immediate;
6. Change to the root directory.
7. Reboot the Windows server or on Solaris, type **# init 6**.

8. After the standby server reboots, change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
9. To start the Oracle Managed Recovery Process, type

   $ sqlplus / as sysbda

   startup mount;

   alter database recover managed standby database using current logfile disconnect from session;

   exit;
10. To start the private listener, type

    lsnrctl start listener

Rebooting the primary database server

(Topic number: 67102)

If you have to do any type of servicing of the primary server, you can reboot the server after the servicing.

To reboot the primary database server

1. Reboot the primary server.

   On Solaris, log in as the **root** user and type **init 6**. On Windows, reboot the server.
2. After the reboot, verify that the public listener is started.

   On Solaris type **psg tns.** On Windows check that the **OracleohomeTNSListener_listener_public** service is started.
3. Start the public listener if not already started.

   On Solaris type**lsnrctl start listener_public**. On Windows, start the **OracleohomeTNSListener_listener_public** service.

Resizing Oracle data files

(Topic number: 67133)

You must run the **monitor_add** or **monitor_resize** command to increase or resize the Oracle data files before propagating the file changes to the standby database.

To resize Oracle data files

1. Log into the primary server, log into sqlplus as the **sys** user.
2. Execute the command

   alter system switch log file;

Removing the Oracle Data Guard configuration on the primary and standby servers

(Topic number: 67105)

If you want to uninstall Oracle Data Guard or completely reconfigure it, you can remove the Oracle Data Guard configuration on the primary and standby servers.

To remove the Oracle Data Guard configuration on the primary and standby servers

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.

2. In a command prompt, to run Data Guard manager, type

   dgmgrl sys/stayout@MVF1

3. In Data Guard manager, to remove the Data Guard configuration, type

   remove configuration

4. Remove the Data Guard configuration files from the primary server.

   On Solaris, type

   cd /opt/oracle/current/dbs

   rm dr*.dat

   On Windows, delete the **dr*.dat** file from C:\oracle\product\10.2.0\db_1\database.

5. Save all the edited Data Guard files such as initMVF.ora, spfileMVF.ora, tnsnames.ora, and listener.ora. To make a copy of these files, type

   On Solaris:

   cd /opt/oracle/current/dbs

   cp initMVF.ora initMVF.ora.dg_save

   cp spfileMVF.ora spfileMVF.ora.dg_save

   cd /var/opt/oracle

   cp tnsnames.ora tnsnames.ora.dg_save

   cp listener.ora listener.ora.dg_save

   On Windows:

   cd C:\oracle\product\10.2.0\db_1\database

   cp initMVF.ora initMVF.ora.dg_save

   cp spfileMVF.ora spfileMVF.ora.dg_save

   cd C:\oracle\product\10.2.0\db_1\network\ADMIN

   cp tnsnames.ora tnsnames.ora.dg_save

   cp listener.ora listener.ora.dg_save

6. To turn off flashback, type

   sqlplus / as sysdba

   alter database flashback off;

7. To turn off force logging, type

   alter database no force logging;

8. Halt all the job queues.
9. Stop IMPAX and IIS on the core servers.
10. To shut down the database, type

    sqlplus / as sysdba

    shutdown immediate;

11. Revert the edited files (listener.ora, tnsnames.ora, spfile.ora) to the original files. To copy the original initMVF.ora, tnsnames.ora and listener.ora files back to their respective locations, type

    On Solaris:

    cd /opt/oracle/current/dbs

    cp –rp initMVF.ora.pre_dg initMVF.ora

    cd /var/opt/oracle

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

    On Windows:

    cd C:\oracle\product\10.2.0\db_1\database

    cp –rp initMVF.ora.pre_dg initMVF.ora

    cd C:\oracle\product\10.2.0\db_1\network\ADMIN

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

12. To create the spfile from the pfile, type

    sqlplus / as sysdba

    create spfile from pfile;

13. To start the database, type

    startup;

14. Modify crontab (Solaris) or Task Scheduler (Windows) and remove references to Oracle Data Guard.

    On Solaris:

    Comment the **15 20 * * * /usr/mvf/bin/check_if_primary_db && /usr/mvf/bin/check_standby** crontab entry out by adding a **#** at the beginning of the line.

    On Windows:

Disable or delete the **CheckStandby** task in Task Scheduler.

15. Repeat the previous steps on the standby server.
16. On the core servers, restart IMPAX and IIS.
17. Restart all the job queues.
18. To ensure that IMPAX starts successfully, test the primary database server.
19. Test the IMPAX Client connectivity.

Switching over to the standby server

(Topic number: 67114)

If you want to service the primary server, you can switchover to the standby server.

The public listener on the current standby server has not been set. To avoid IMPAX Client connectivity problems, you must stop listener_public on the primary server when the primary database goes down. You can then switchover to the standby server, run the standby database, and reinstate the former primary server. During this time, the IMPAX Client can still connect to the database, which is running on the standby Oracle Data Guard host.

To switch over to the standby server

1. Stop the public listener on the primary server.

   On Solaris, as the oracle user, type **lsnrctl stop listener_public**. On Windows stop the **public_listener** service.

2. To stop IMPAX on the primary server, as the root user, type

   stop_impax (Solaris) or **stopall** (Windows)

3. To launch the Data Guard manager on the primary server and perform the switchover, as the Oracle user, type

   dgmgrl sys/stayout@mvf1

   show configuration

   switchover to 'MVF2'

   show configuration

   exit

4. Start the public listener on the standby server, which has been promoted to the primary server.

   On Solaris, as the oracle user, type **lsnrctl start listener_public**.

   On Windows, start the **public_listener** service.

5. To query for the ae_ref and the ae_title, in CLUI, type

   ae query

6. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref =

map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='*AE_title_of_failed_primary_server*'

Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete *service_ref*

8. To set the new primary Task Scheduler, in CLUI, type

   update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

   update mvf_ts_config set ae_ref='*AE_title_of_new_primary_server*' where ae_ref='*AE_title_of_failed_server*'

9. To start IMPAX on the new primary server, as the root user, type

   start_impax (Solaris) or **startall** (Windows)

10. As the root user, restart the MVF Task Scheduler on the remaining IMPAX servers such as the Archives, Network Gateways, and Curators.

    On Solaris, restart the MVF Task Scheduler by killing the process or restarting IMPAX. On Windows, restart the Mitra System Task Scheduler service.

Note:

If this is the first time that the standby database is opened after a switchover, re-create the temporary file on the standby server (refer to page 85).

The IMPAX Clients can now connect to the new primary database. After the switchover, the Client may continue to experience connectivity problems, specifically in the Image area, but should be resolved on its own a few minutes after switchover as IMPAX re-establishes the connection to the newly promoted database server.

Failing over to the standby server

(Topic number: 67117)

If the primary server is unavailable, you can fail over to the standby server to ensure maximum availability.

To fail over to the standby server

1. If you can connect to the primary server, stop the public listener.

   On Solaris, as the oracle user, type**lsnrctl stop listener_public**.

   On Windows, stop the **public_listener** service.

   If you cannot connect to the primary server, skip to step 3.

2. To stop IMPAX, as the root user on the primary server, type

stop_impax (Solaris) or **stopall** (Windows)

3. To launch the Data Guard manager on the standby server and perform the failover, as the oracle user on Solaris or the AgfaService user on Windows, type

   dgmgrl sys/stayout@mvf2

   show configuration

   failover to 'MVF2'

   show configuration

   MVF2 is now the primary server.

4. Start the public listener on the standby server, which has been promoted to the primary server.

   On Solaris, as the oracle user, type **lsnrctl start listener_public**. On Windows, start the public_listener service.

5. To query for the ae_ref and the ae_title, in CLUI, type

   ae query

6. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref = map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='<AE Title of the failed primary server>'

   Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete <*service ref*>

8. To set the new primary Task Scheduler, in CLUI, type

   update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

   update mvf_ts_config set ae_ref='*AE_title_of_new_primary_server*' where ae_ref='*AE_title_of_failed_server*'

9. To start IMPAX on the new primary server, as the root user, type

   start_impax (Solaris) or **startall** (Windows)

10. As the root user, restart the MVF Task Scheduler on the remaining IMPAX servers such as the Archives, Network Gateways, and Curators.

    On Solaris, restart the MVF Task Scheduler by killing the process or restarting IMPAX. On Windows, restart the Mitra System Task Scheduler service.

Note:

If this is the first time that the standby database is opened after a failover, you must re-create the temporary file on the standby server (refer to page 85).

The IMPAX Clients can now connect to the new primary database. After the switchover, the Client may continue to experience connectivity problems, specifically in the Image area, but should be resolved on its own a few minutes after switchover as IMPAX re-establishes the connection to the newly promoted database server.

Re-creating the temporary file on the standby server

(Topic number: 67286)

If this is the first time that the standby database is opened after a switchover or failover, you must re-create the temporary file on the standby server.

To re-create the temporary file on the standby server on Windows

1. To log into sqlplus, from the command line, type

   sqlplus sys/stayout as sysdba

2. To add a new temp file to F:\DATA\DBASE\SYSTEM, type

   alter tablespace TEMP add tempfile 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' SIZE 500M REUSE;

3. To bring the original temp file offline and bring the new one online, type

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' OFFLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' ONLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' DROP;

4. To recreate TEMP01.DBF, type

   alter tablespace TEMP add tempfile 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' SIZE 500M REUSE;

5. To bring TEMP01.DBF online and to drop TEMP02.DBF, type

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' OFFLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' ONLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' DROP;

To re-create the temporary file on the standby server on Solaris

1. To log into sqlplus, from the command line, type

   sqlplus sys/stayout as sysdba

2. To add a new temp file to F:\DATA\DBASE\SYSTEM, type

   alter tablespace TEMP add tempfile '/usr/mvf/data/dbase/system/temp02.dbf' SIZE 500M REUSE;

3. To bring the original temp file offline and bring the new one online, type

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' OFFLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' ONLINE;

alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' DROP;

4. To recreate TEMP01.DBF, type

   alter tablespace TEMP add tempfile '/usr/mvf/data/dbase/system/temp01.dbf' SIZE 500M REUSE;

5. To bring TEMP01.DBF online and to drop TEMP02.DBF, type

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' OFFLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' ONLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' DROP;

Reinstating the failed primary database

(Topic number: 67120)

Once the failed primary server has been repaired, you can reinstate it as the primary database.

To reinstate the failed primary database

1. After the primary database has been repaired, to restart the database, as the oracle user on Solaris or the AgfaService user on Windows, type

   sqlplus / as sysdba

   startup mount;

   quit

2. To launch the Data Guard manager, on the primary server as the oracle user on Solaris or the AgfaService user on Windows, type

   dgmgrl sys/stayout@mvf2

3. To perform the switchover type

   show configuration

   reinstate database 'MVF1'

   show configuration

   exit

4. To launch the Data Guard manager on the repaired primary, as the Oracle user, type

   dgmgrl sys/stayout@mvf2

5. To make MVF1 the primary server type

   switchover to 'MVF1'

   exit

6. Stop the public listener on the new standby server.

   On Solaris, as the oracle user, type**lsnrctl stop listener_public**. On Windows, stop the **public_listener** service.

7. To stop IMPAX on the new standby server, type

stop_impax (Solaris) or **stopall** (Windows)

8. To query for the ae_ref and the ae_title, in CLUI, type

   ae query

9. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref = map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='*AE_Title_of_ failed_primary_server*'

   Two service refs are returned.

10. For each service ref, in CLUI, type

    service delete <*service ref*>

11. To set the new primary Task Scheduler, in CLUI, type

    update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

    update mvf_ts_config set ae_ref='*AE_reference_of_new_primary_server*' where ae_ref='*AE_reference_of_old_primary_server*'

12. Start the public listener on the new primary server.

    On Solaris, as the oracle user, type **lsnrctl start listener_public**. On Windows, start the **public_listener** service.

13. To start IMPAX on the new primary server, as the root user, type

    start_impax (Solaris) or **startall** (Windows)

Tools for monitoring Oracle Data Guard

(Topic number: 66589)

Oracle Data Guard is a high-availability solution that uses two database servers—the active, primary server, and a standby server that can take over should any problems occur on the primary server. The following tools are available for monitoring an Oracle Data Guard configuration.

Script	Description
check_dg_configuration	Used to sanity check an existing Data Guard configuration to see if the init parameters are set as expected. Run this script manually, as necessary. It works only on the primary server. **Note:** On Windows 2008, run check_dg_configuration from an elevated command prompt.

Script	Description
check_standby	Configured through crontab (AS3000) or Scheduled Tasks (AS300) to run daily at 3:45 and 20:15 to detect any archive gaps between the primary and standby servers. If the gap exceeds 20, an exception is sent. This script works only on the primary server.

Tip:

To run these scripts on Windows, precede them with **bash**; for example **bash check_dg_configuration**.

Troubleshooting: The application encountered a problem with the standby database

(Topic number: 66656)

Issue

The following error message appears in the Exception Viewer:

```
The application encountered a problem with the Standby database
```

Details

This message applies only when using an Oracle Data Guard configuration, with a primary and standby database. It indicates that the archive gap between the primary and standby databases exceeds 20.

Solution

Perform diagnostics such as the following.

1. To verify that the listener.ora files on both the primary and standby servers are correct, log into the primary server as the oracle user on Solaris and the AgfaService user on Windows.

   Change to the **/usr/mvf** (Solaris) or **C:\mvf\bin** (Windows) directory and type the following

   tnsping MVF

   tnsping MVF1

   tnsping MVF2
2. Ensure that the standby server is up and running.
3. Ensure that the private listener is running on the standby by typing:

   lsnrctl status
4. Look for errors in the following logs, on both the primary and standby servers:

   /usr/mvf/data/logs/oracle/bdump/alert_MVF.log and arcMVF.log (Solaris)

   C:\mvf\data\logs\oracle\bdump (Windows)

5. Ensure that Oracle is running on the standby server by typing **psg ora**.
6. To confirm that the redo log has been set on both the primary and standby server, execute the following command in sqlplus on the primary server, then repeat it on the standby server. Ensure that the list matches between the two servers.

   select * from v$logfile
7. Ensure that the last line of the redo log contains the standby log files; for example, /usr/mvf/data/dbase/redo/redo_stdby07.log (Solaris) or d:\data\dbase\redo\redo_stdby07.log (Windows).
8. To check that the log files are being received and applied on the standby server, in sqlplus, execute the command

   select sequence#,applied from v$archived_log order by sequence#;
9. To force a log switch on the primary server, execute the command

   alter system switch logfile;
10. Check again to ensure that the log files are being received and applied on the standby server. Execute the command

    select sequence#,applied from v$archived_log order by sequence#;

    Ensure that one additional entry appears in the list.
11. To check the configuration, on the primary server, open the Data Guard manager:

    dgmgrl sys/stayout@mvf1

    show configuration;

Troubleshooting: Reducing the time needed for a Solaris client to connect to the Oracle standby server

(Topic number: 111472)

Issue

After Oracle Data Guard has failed over to the standby server, there is a long delay before Solaris clients such as Network Gateways can connect to the standby database. This delay can be up to 3 minutes long. During this time, IMPAX essentially ceases to function.

Details

The delay is caused by the TCP/IP settings. You can significantly reduce this time interval by changing the TCP/IP values on the Oracle database's Solaris clients.

Solution

Important!

This solution applies to Solaris servers only. This procedure is not necessary on Windows clients in a mixed-host cluster.

On each of the Oracle database's Solaris clients, change the TCP/IP values as follows:

1. Log in to one of the Oracle database's Solaris clients and open a command prompt.
2. View the current TCP settings by typing:

   ndd -get /dev/tcp tcp_ip_abort_cinterval

   ndd -get /dev/tcp tcp_ip_abort_interval

   ndd -get /dev/tcp tcp_keepalive_interval
3. Record these values in case you have to reset them.
4. Change the current TCP settings by typing:

   ndd -set /dev/tcp tcp_ip_abort_cinterval 10000

   ndd -set /dev/tcp tcp_ip_abort_interval 60000

   ndd -set /dev/tcp tcp_keepalive_interval 240000

After modifying the TCP/IP values, the client will connect to the standby Oracle database much faster than before.

Integrating the IMPAX Enterprise Solution

B

The IMPAX Enterprise Solution offers a fully integrated RIS, PACS, and Reporting solution.

What is the IMPAX Enterprise Solution?

(Topic number: 56712)

The IMPAX Enterprise Solution is an integrated offering designed to meet the needs of large healthcare organizations. The IMPAX Enterprise Solution:

- Leverages the diversity and depth of the Agfa IMPAX product portfolio
- Forms an integrated solution for large-scale healthcare institutions with multi-disciplinary and multi-departmental needs
- Delivers consistent and predictable workflow and outcomes, employing workflow-aware adaptability and scalability

Key modules in the IMPAX Enterprise Solution

The foundations of the IMPAX Enterprise Solution are the key modules in a fully integrated offering:

- PACS
- RIS
- Reporting

Integrating into the IMPAX Enterprise Solution

(Topic number: 56715)

As part of the IMPAX Enterprise Solution, this product must be configured to fully support an integrated RIS-PACS-Reporting solution. For details about planning and implementing a RIS-PACS-Reporting integration, contact your local Agfa representative.

Reference material: Solaris

C

Various reference materials may be useful during the installation procedure.

For more information about Solaris zones, also refer to the *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones* (http://download.oracle.com/docs/cd/E18752_01/pdf/817-1592.pdf).

CAUTION!

Solaris zones should not be modified without sufficient understanding of the consequences. If necessary, consult your Agfa Professional Services representative for assistance.

Solaris Live Upgrade: Key concepts

(Topic number: 97408)

Solaris Live Upgrade provides a method of upgrading an operating system that substantially reduces the downtime usually associated with this type of upgrade. This procedure involves creating a duplicate of your current boot environment, then upgrading the duplicate while the original boot environment continues to run.

Note:

To enable upgrades, Solaris Live Upgrade has specific partitioning requirements. From IMPAX 6.5 on Solaris 10 onward, these partitioning requirements have been met, facilitating upgrades with Live Upgrade to subsequent versions or updates; however, because of these partitioning requirements, Live Upgrades of any previous IMPAX systems on Solaris are not supported.

Key Benefits

- Minimal system downtime—Solaris Live Upgrade enables system administrators to upgrade or patch the Solaris operating system with minimal system downtime and therefore minimal impact on those who rely on IMPAX. Administrators can upgrade the operating system, install patches, and perform routine system maintenance without shutting down the system for any significant amount of time.
- Minimal risk when upgrading—The system administrator can revert to the former boot environment if the new boot environment does not work as expected. Reverting to the old boot environment is accomplished by simply rebooting the system.
- Solaris Live Upgrade 2.0 integration with Web Start Flash technology enables system administrators to install a complete pre-tested, pre-configured system image rapidly on a new inactive boot environment while the production boot environment is fully operational.

Separate boot environment

The system administrator installs the latest release of the operating system in a separate, inactive boot environment which is located on a separate partition on the local disk. See *Disk management strategies* (refer to page 23) for details on how to partition disks. When the upgrade process is complete, the administrator reboots the system to run the updated operating system using the new boot environment. If the new boot environment does not work as expected, the administrator can revert to the previous boot environment by rebooting the system.

For more information on upgrading Solaris for IMPAX 6.5 onward, refer to the *Agfa Solaris Live Upgrade Guide* which can be found on the Main IMPAX Knowledge Base Page in the "Additional documents" section, or contact Agfa Professional Services.

Modifications made automatically by the Solaris armoring installation

(Topic number: 6954)

Solaris armoring installation makes the following modifications to a standard Solaris install:

- Removes all unnecessary services from /etc/inetd.conf.
- Disables ftp, telnet rsh access (to be replaced by scp and ssh).
- Turns off a number of unnecessary services in the rc scripts.
- Locks down .rhosts, .netrc, and hosts.equiv files (rsh no longer functions, replaced by ssh).
- Enables sulogging, tcpdlogging, inetlogging, and login log, which improve the system's IDS capabilities.
- Modifies the /etc/default/inetinit sets TCP_STRONG_ISS = 2.
- Randomizes all initial sequence number for all TCP connections, guarding against IP spoofing and hijacking.

- Secures the kernel parameters for /dev/ip by restricting IP querying.
- Modifies /etc/system to help protect against buffer overflow attacks.

Understanding Solaris armoring

(Topic number: 6915)

Solaris armoring disables non-essential system services and modifies system parameters to improve the security of the system. Solaris armoring is installed automatically as part of the Solaris 10 installation.

For systems that must connect to an external Network File System (NFS), such as Netapp Hierarchical Storage Management (HSM), the nfs.client must be re-enabled and started on all systems that mount the NFS storage subsystem. This must be done after armoring is installed by typing the following:

svcadm -v enable -r network/nfs/client

svcadm -v restart svc:/network/nfs/client:default

Groups and accounts created for IMPAX

(Topic number: 6976)

Certain operating system groups and accounts are created for IMPAX when it is installed.

Operating system groups created for IMPAX

During the IMPAX installation, the following operating system groups are created:

Group	Description
dba	Group created for database activities
mitra	Created for IMPAX activities

Operating system account created for IMPAX

During the IMPAX installation, the following operating system account is created, with a secure password:

Account	Description
mvf	Account for administrative IMPAX access

Accounts created for IMPAX

Account	Description
oracle	Administrator account for the Oracle database, with a secure password
ocr_train	User account created when optional MVFocr package is installed

PACS Store and Remember archiving

(Topic number: 6939)

If you do not have a physical archive, or want to use PACS Store and Remember archiving in addition to your media archive, you can set up the PACS Store and Remember archive in the Administration Tools and register the services with IMPAX.

Adding a PACS Store and Remember archive

(Topic number: 9215)

To configure an external PACS archive as a PACS Store and Remember archive, set up the external PACS archive in Network Management in the IMPAX Administration Tools.

To add a PACS Store and Remember archive

1. Launch and log into the IMPAX Administration Tools.
2. On the Setup tab, click **Network Management**. 
3. To set up a new destination, click **New**. 
4. Type the AE title of the external PACS archive.
5. Type an alias for the archive.
6. Type the host name or IP address of the archive.
7. Click **Save**. 
8. Switch to the **Capabilities** tab.
9. From the list at the bottom of the manager, select the added external PACS archive.
10. Under Station Type, select **PACS**.
11. Under Server is Allowed to, select **Query/Retrieve from Station**.
12. If using different AE titles on the external PACS archive for store and retrieve jobs, repeat steps 3 to 11 for the retrieve AE title.
13. Click **Save**. 

Next you must register the PACS Store and Remember archive services.

Registering PACS Store and Remember archive services in Solaris

(Topic number: 9214)

Designate the server that will perform the PACS Store and Remember archiving.

Often this is the server running the Network Gateway software.

To register PACS Store and Remember archive services in Solaris

1. Log into the IMPAX server as the **mvf** user.
2. To register the server as a PACS Store and Remember archive, in a terminal window, type

   install_pacs -a *AE_title_PACS_Store_and_Remember_archive* -p *AE_title_external_PACS_archive* [-r *AE_title_external_PACS_archive_retrieval*]

   The AE title used here must match the AE title used when defining the external PACS archive in Network Management (refer to page 96). The AE title is case-sensitive.

   If the AE title for store jobs is the same as the AE title for retrieve jobs on the external PACS archive, the -r *AE_title_external_PACS_archive_retrieval* parameter is optional.
3. To restart the mvf-scu processes, launch CLUI and type

   signal kill 0 MVF_SCU
4. Test the PACS Store and Remember archive functionality (refer to page 97).

Testing PACS Store and Remember archiving

(Topic number: 9213)

Test the PACS Store and Remember archive to ensure that the services were registered properly.

To test that the archive was set up correctly

1. On Solaris, check that the external archive is listed in the /etc/hosts file.
2. To confirm that the external archive can be accessed, ping the external archive using the host name or IP address.

To test store and retrieve functionality

1. Launch and log into the IMPAX Administration Tools.
2. On the Daily tab, click **Job Manager**.
3. Ensure that a PACS Archive queue exists.
4. On the Daily tab, click **Study Manager**. 
5. Search for and select a study to store to the PACS Store and Remember archive.
6. To test the store functionality, click **Store to Archive**. 
7. If you are using more than one archive, from the Archive list, select the PACS Store and Remember archive and click **OK**.
8. Ensure that the study is stored to the PACS Store and Remember archive.
9. To delete the study from the local cache so that you can test the retrieve functionality, from the Location list, select **Cached**.
10. Search for and select the study you stored to the PACS Store and Remember archive.
11. Click **Delete from Cache**. 

12. Confirm that you want to delete the selected study from cache.
13. To test the retrieve functionality, from the Location list, select **Archived**.
14. Search for and select the study in the PACS Store and Remember archive.

    If the study is stored in more than one location, ensure that you select the copy in the PACS Store and Remember archive.
15. Click **Retrieve**.

Generating and importing mvf.portable.psd

(Topic number: 6980)

System security is enforced by having credentials for IMPAX internal processes contained within encrypted password files that must be distributed to all machines in the cluster.

When installing IMPAX on the Database Server, the impax_install script uses a passkey utility to save the AgfaService password to a password file at /usr/mvf/mvf.psd. Next the utility creates a portable version of this password file at /usr/mvf/mvf.portable.psd.

When installing IMPAX Network Gateway or Archive Server software, the IMPAX installation script imports mvf.portable.psd, re-encrypts it using a machine specific key, and creates the file /usr/mvf/mvf.psd on the target server.

In some cases the mvf.portable.psd file is not available on the Database Server. This does not prevent any of the initial Network Gateway or Archive Server installs, but you must manually generate and import the password key to the target server.

In other cases following initial installations, prudent security management recommends that the mvf.portable.psd file be deleted from the Database Server once all Network Gateway and Archive Server machines are installed. Therefore, if at some later point you install a new Network Gateway or Archive Server, you must manually generate and import the password key to the target server.

Whenever the import of mvf.portable.psd to the target server fails during an AS3000 installation, you see the following log message indicating the required password file is not on the Database Server:

```
The AgfaService ID password file failed to import properly. You will need to
import the password file manually.
```

The AS3000 Network Gateway or Archive Server installation completed successfully (unless other log messages indicate otherwise), but you must manually generate and import the password key to the target server.

Generating the AS3000 portable password file

(Topic number: 58083)

You may need to generate the portable password file to install new servers or to troubleshoot when password file import fails during installation.

To generate the AS3000 portable password file

1. Log into the AS3000 Database Server machine as the **root** user.
2. Change to the **/usr/mvf** directory.
3. To export the passkey for installing IMPAX on remote machines, type

   ./bin/passkey -M EXPORT -k *temporary_password*

   where *temporary_password* is a password to be used to import the portable password file later.

   This creates the /usr/mvf/mvf.portable.psd password file.
4. On the target server, open a Cygwin command window to download the portable password file from the Database Server.
   a. Ensure the C:\temp directory exists on the target server. If the C:\temp directory does not exist, create one.
   b. Double-click the Cygwin.bat file located in the C:\cygwin\ directory.
   c. On the Cygwin command window, type

      scp service@<Database server hostname>:/usr/mvf/mvf.portable.psd /cygdrive/c/temp
   d. If prompted to add the Database Server's RSA key fingerprint to the list of known hosts, click **Yes**.

      The portable password file is downloaded to the C:\temp directory on the target server.

      Important!

      You should know the service user's password on the Database Server before downloading the portable password file.

Delete /usr/mvf/mvf.portable.psd from the Database Server when you are finished downloading it to the target servers or servers.

Importing the portable password file locally to the target server

(Topic number: 58086)

Once generated, you can import the password file onto the server that needs it.

To import the portable password file locally to the target server

1. Log into the target Network Gateway or Archive Server as the **root** user.
2. To import the portable password file, type

   /usr/mvf/bin/passkey -M IMPORT -k *temporary_password*

   where *temporary_password* is the password you gave when exporting the portable password file.

   This reads the mvf.portable.psd file, re-encrypts it using a machine specific key, and creates the local /usr/mvf/mvf.psd file.

3. To restrict permissions on the newly created mvf.psd file, type

   chmod 640 /usr/mvf/mvf.psd

4. Delete /usr/mvf/mvf.portable.psd from the target server.

CAUTION!

The mvf.portable.psd file contains sensitive information. To maintain the security of the system, the portable password file should be deleted both the Database Server and the target servers.

Understanding the passkey utility

(Topic number: 9302)

System security is enforced by having credentials for IMPAX internal processes contained within encrypted password files that must be distributed to all server machines in the cluster.

IMPAX 6.5.1 sets up various user accounts for the IMPAX services. These accounts are set up with a random alphanumeric password, different for each installation. The passwords are encrypted with a key specific to the machine, and stored locally in a password file. The file cannot be copied to another system and decrypted.

To facilitate sharing information among servers, a passkey utility is used to export the password key into a portable format that can then be copied to another machine and imported. This portable file is encrypted during the export and secured with a password; the portable file is imported into another system by using the same password.

Differences between system and portable password files

(Topic number: 6936)

Two files contain IMPAX password information:

- System password file

  This file is encrypted with a key specific to the machine and unknown to the user, called the *system key*. This file is not transferable between machines and can be decrypted only on the system where it was created. It is located under the mvf directory and is named mvf.psd by default.

Note:

If the mvf.psd file already exists, do not remove it; otherwise, IMPAX services cannot start.

- Portable password file

This file is encrypted with a key specified by the user, thus having a much weaker type of encryption. It is created upon user request, and should be deleted when no longer required. This key can be used to transfer passwords between systems during the installation of IMPAX.

Passkey utility reference

(Topic number: 6937)

To facilitate sharing information among servers, a passkey utility is used to export the password key into a portable format that can then be copied to another machine and imported. This portable file is encrypted during the export and secured with a password; the portable file is imported into another system by using the same password.

The passkey utility is in the /usr/mvf/bin directory on Solaris and the C:\mvf\bin directory on Windows. The command can be used in various modes, specified by the -M option. The -p and -r options allow you to specify non-default file names for the system password file and portable password file.

The command syntax is as follows:

passkey -M *mode, arguments* [**-p *file_name***] [**-r *file_name***]

where:

-M *mode*	**Arguments**	**Description**
CHECKKEY	**-k *user_key*** specifies the user key to check	This mode validates the user key against a portable password file.
CREATE	**-u *username*** specifies which user to associate with the new password in the password file	This mode creates random, machine-specific passwords for users. Specify the user name for whom the password will be created, and optionally specify the name of the file to store the password in with the -p option.
DEC	**-S *source_string*** string to decrypt **-k *user_key*** key to use to decrypt machine	This mode is used for base64 decoding and decrypting a string. The encryption/decryption mechanism uses a system-specific key, meaning that the string cannot be decrypted on another machine. It can be decrypted only on the system where it was originally encrypted.
ENC	**-S *source_string*** string to encrypt **-k *user_key*** key to use to encrypt machine	This mode is used for base64 encoding and encrypting a string. The base64 encoding ensures the encrypted string is in ASCII format so that it can be stored in a text format. The encryption/decryption mechanism uses a system-specific key, meaning that the string cannot be decrypted on another machine. It can be decrypted only on the system where it was originally encrypted.

-M *mode*	Arguments	Description
EXPORT	**-k *user_key*** specifies the key to use when creating the portable password file	This mode decodes the password file using the machine-specific key, and re-encodes it into a portable password file using the specified password (user key). This portable password file can then be copied to a new system and imported (see IMPORT) using the same specified user key.
IMPORT	**-k *user_key*** specifies the key used to create the portable password file	This mode decodes the portable password file using the user key, and re-encodes it into a password file with a machine-specific key. Creates an encrypted password file.
QUERY	**-u *username*** specifies which user to query for	This mode queries for a password associated with a given user name. The passkey utility writes the password to stdout (standard output). Typically, this function determines what password to set up for an account on a NAS server, which will allow the IMPAX components to connect.
SET	**-u *username*** specifies user to associate the password with **-P *password*** specifies password to associate with user	This mode sets the password for a given user to the password specified. This is used in cases where a random password is not suitable.

VALIDATE	**-u *username*** username to use in strong password validation **-P *password*** validates password against strong password encryption rules (used by Solaris installer)	This mode can be used to test a specific password against strong password rules. A strong password must:
		• Be at least eight characters long
		• Not contain three or more characters from the user's account name
		• Contain characters from at least three of the following five categories:
		  • Uppercase (A to Z)
		  • Lowercase (a to z)
		  • Digits (0 to 9)
		  • Non-alphanumeric (for example, !, $, #, or %); avoid commas
		  • Unicode

-p *file_name*

optionally specifies a system password file name other than the default C:\mvf\mvf.psd (AS300) or usr/mvf/mvf.psd (AS3000)

-r *file_name*

optionally specifies a portable password file name other than the default C:\mvf\mvf.portable.psd (AS300) or usr/mvf/mvf.portable.psd (AS3000)

CAUTION!

The mvf.portable.psd file contains sensitive information. To maintain the security of the system, the portable password file should be deleted from both the Database Server and the target server locations after all new Network Gateway, Archive Server, Application Server, and Curator components are installed.

External software licenses

D

Some of the software provided utilizes or includes software components licensed by third parties, who require disclosure of the following information about their copyright interests and/or licensing terms.

Cygwin

(Topic number: 121758)

Copyright 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010 Red Hat, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly

through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Editline 1.2-cstr

(Topic number: 121768)

Copyright 1992 Simmule Turner and Rich Salz. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California. Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it freely, subject to the following restrictions: 1. The authors are not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it. 2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation. 3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation. 4. This notice may not be removed or altered.

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995-2003 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL

DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

OpenSSL

(Topic number: 121771)

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*

==========

* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

*

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THEIMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*

==========

*

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

*

*This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

*

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

*THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

*/

Xerces C++ Parser, version 1.2

(Topic number: 121761)

This product includes software developed by The Apache Software Foundation (http://www.apache.org/). Please read the LICENSE files present in the Help > About dialog of the IMPAX Client.

Zlib

(Topic number: 7595)

zlib.h -- interface of the 'zlib' general purpose compression library Version 1.2.1, November 17th, 2003

Copyright (C) 1995-2003 Jean-loup Gailly and Mark Adler

This software is provided “as-is”, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Glossary

A

all-in-one configuration

A configuration in which the Database, Archive Server, Network Gateway, and Curator Server components are all installed on a single Windows server, along with the Application Server software.

Application Server

Intermediary server between IMPAX Client and IMPAX Server machines. LDAP, Documentation, and other Business Services reside on the Application Server.

C

C-MOVE

An operation that allows an application entity to instruct another application entity to transfer stored SOP Instances to the original application entity or to a third application entity, using the C-STORE operation.

Connectivity Manager

A middleware component in the integration between hospital information systems and other hospital imaging departments. Connectivity Manager also provides connectivity to each modality and the PACS.

C-STORE

The mechanism used to transfer SOP Instances between application entities.

D

DICOM

Digital Imaging and Communications in Medicine. The standard communication protocol used by a PACS, HIS, or modality to exchange information or images with other systems.

F

fully qualified domain name (FQDN)

The full name of a system, consisting of its local host name and its domain name, including a top-level domain. For example, venera is a host name and venera.isi.edu is a fully qualified domain name. A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called name resolution, uses the Domain Name System (DNS).

H

high availability

With a high-availability solution, a site is protected against system downtimes, either planned or unplanned. Redundant servers are put in place that can take over functionality should the primary server become unavailable.

HIS verification

An option that forces the PACS to verify all incoming images from an acquisition station or modality against specific criteria, such as the patient ID and accession number. The

PACS sends a message through the RIS Gateway to verify the criteria against what is contained in the HIS. If the criteria match, then the images can be stored permanently.

M

master Curator

When using multiple Curators, the first Curator that runs, which owns the job queue.

multiple IMPAX cluster configuration

In a multiple IMPAX cluster configuration, an IMPAX cluster is linked to one or more other IMPAX or external PACS clusters, such that patient and study data can be shared and synchronized between them.

N

NAS

Network Attached Storage. A storage device attached directly to a Storage Area Network (SAN) or other direct network connection.

P

PACS

A Picture Archive and Communication Systems (PACS) makes it possible to electronically store, manage, distribute, and view images.

PACS Store and Remember archive

An IMPAX server computer set up with the PACS Store and Remember archiving functionality. This server usually has Network Gateway functionality.

R

RIS

Radiology Information System. Responsible for scheduling exams and for report management in the Radiology department.

S

SCU

Service Class User. Primarily sends DICOM requests to an SCP.

single-host configuration

A configuration in which the Database, Archive Server, and Network Gateway server components are all installed on a single server.

single-server configuration

An IMPAX single server is a Windows server that runs the AS300 Server software in a single-host configuration along with the Application Server and Connectivity Manager software.

slave Curator

When using multiple Curators, the secondary Curators. Though the master Curator owns the job queue, PREPARE jobs are associated with the Curator that started the job.

SSL

Secure Sockets Layer. A protocol from Netscape Communications Corporation, which is designed to provide secure communications on the Internet.

standalone station

Windows server on which the IMPAX Client, AS300, and Application Server software are installed. Runs under Windows XP SP3. The standalone does not have its own installation program. To create a standalone , the AS300, Application Server, and Client installation programs are each run separately.

Store and Remember archiving

Also called *PACS Store and Remember archiving*. A configuration in which an IMPAX system is set up as a PACS Store and

Remember Archive, and used for archiving studies to an archive external to the IMPAX system.

V

volume

A volume refers to the division of data on the media. For example, if a tape has two sides, each side is referred to as a separate volume.

W

warm backup

Descriptive of a backup process in which the database does not have to be shut down. Compared with cold backups, warm backups are faster and keep the database accessible while the backup is being performed.

web cache

Images that have been compressed by Curator are stored in the web cache. These images are compressed using Mitra Wavelet compression to reduce their size for access over low bandwidth.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z