IBM FileNet Image Services
Version 4.2

High Availability Procedures and Guidelines

SC19-3303-0

Contents

Appendix C – VERITAS Volume Replicator 102

Notices 116

About this manual

This document outlines the procedures related to configuring an IBM FileNet Image Services system in a High Availability (HA) environment. This pertains to VERITAS Cluster Server software and also information for installing and updating software on a Microsoft® Cluster Server. There is an Appendix related to VERITAS Volume Replicator software.

Important This document is a supplement to the standard documentation that accompanies the VERITAS software. The VERITAS documentation should be your primary reference. Also, refer to the Microsoft Cluster Server Resource Center on the Microsoft Web site for a wide selection of Microsoft documentation.

Audience

This manual is written for Image Services System Administrators and support personnel. We assume that you are familiar with the Image Services Application Executive (Xapex), which includes Storage Library Control, Background Job Control, and Database Maintenance, as well as the Image Services System Configuration Editor. We also assume that you are familiar with your operating system environment and workstation operations.

Document revision history

Image Services version	Date	Comment
4.2	May 2011	Initial release.

Accessing IBM FileNet Documentation

To access documentation for IBM FileNet Image Services products:

1. On the **www.ibm.com** web site, enter “Image Services Documentation” in the search box on the menu bar.
2. Select **IBM - Product Documentation for FileNet Image Services** from the list of search results.

IBM FileNet Education

IBM FileNet provides various forms of education. Please visit Global Learning Services on IBM’s web site at (**www-306.ibm.com/software/sw-training/**).

Feedback

We value your opinion, experience, and use of our products. Please help us improve our products by providing feedback or by completing a consumability survey.

Documentation feedback

Send comments on this publication or other IBM FileNet Image Services documentation by email to **comments@us.ibm.com**. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a help topic, a chapter and section title, a table number, or a page number).

Product consumability feedback

Help is identify enhancements by taking a Consumability Survey (**http://www-306.ibm.com/software/data/info/consumability-survey/**). The results of this comprehensive survey are used by product development teams when planning future releases. Although we are especially interested in survey responses regarding the most recent product releases, we welcome your feedback on any of our products.

The survey will take approximately 30 minutes to complete and must be completed in a single session; there is no option to save a partially completed response.

1
Getting started

This document contains information for installing and updating software on a Microsoft® Cluster Server and configuring VERITAS.

Cluster Server Overview

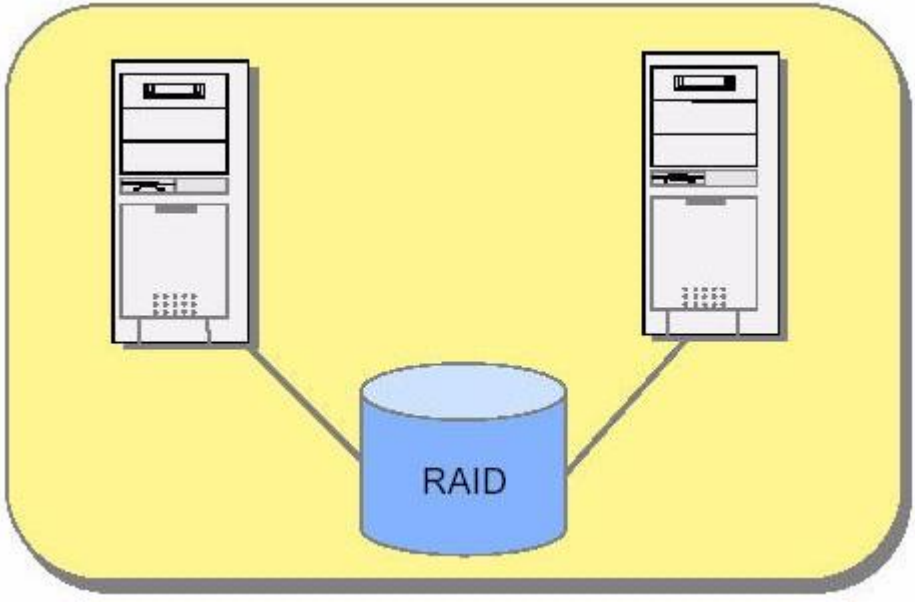
High availability is the ability to provide a service to an end-user with as little perceived downtime as possible. This does not mean that a service is guaranteed to always be available.

- Analysts such as META Group describe a range of high availability targets, from the so-called “five nines” availability, 99.999%, at the high end, to basic availability at 95%. This is a percentage of scheduled up time for a system, so five nines requires a system to be up 99.999% of that scheduled time. Five nines availability translates to five minutes or less downtime in a full year of 24 by 7 operations. By contrast, 99% availability allows up to 87 hours of downtime per year, and 95% allows up to 436 hours, or 18 days, of downtime.
- The Gartner Group notes that the cost of providing high availability increases exponentially as the target moves from 95% to 99% to 99.999%, so prudent system owners take into account the risk of downtime to their business when selecting their high availability targets.

Even a high availability system can still fail for a number of reasons, including people and process problems, in addition to hardware or software failures. Making the hardware and software high availability is a

necessary component in high availability, but professional and reliable system administration and well designed applications are equally necessary, if not more so. This document addresses just the hardware and software issues, but you need to consider all the components in providing high availability.

The goal of high availability is to continue to provide a user with a working system as seamlessly as possible in the event of a component failure. If a system component fails for any reason, the high availability solution ensures that another component takes over for the failed component, and that the newly composed system will maintain the same machine identifications (hostnames and IP addresses) as the system prior to failure, minimizing the disruption to the user.



Basic server cluster using RAID storage.

How does High Availability relate to Disaster Recovery?

High availability solutions provide business continuity in the face of localized failures, such as a single server failure or hard disk crash. Disaster recovery solutions, on the other hand, provide for business continuity in the face of natural or man-made disasters that cause the loss of an entire production system.

While the goal of both high availability and disaster recovery solutions is the same-keeping the Image Services system available for continued business operations-the solutions themselves are quite different. A disaster recovery solution must provide a complete alternate system, with current or near-current data, typically at a geographically remote site unaffected by the disaster. Disaster recovery solutions may also include an alternate working site for users of the system, if their primary work location is no longer available due to a disaster. In contrast, a high availability solution typically provides for an alternate system component that takes over for a failed component at the same site.

Server Clusters

Server clusters are based on the concept of shared data storage. Server hardware and software vendors offer vendor-specific server clustering products as their high availability offering for these kinds of data-centric servers. These products all have the following general characteristics:

- Two or more servers share a high availability disk array for data storage, shown in the figure below. The array incorporates redundant copies of the data, but appears as a single shared drive to the servers, thereby avoiding the need for data replication between servers. The servers may each have their own local disk for static storage of operating system, utilities, and other software.

- A common set of applications run on each server.
- Server clients see the cluster as a single virtual server.
- If one of the servers fails, the other server picks up the workload of the failed server (a so-called failover). When the failed server is repaired and ready to run again, the workload is shifted back over from the other server (a failback). In some configurations, the repaired server simply becomes the new backup server, and no failback is required.
- The failover feature can mask both planned and unplanned outages from users. For instance, an intentional failover can be done to allow one of the servers to be upgraded or backed up and then brought back online in a failback.
- In most server clusters, only one server is actively serving clients at a time. This is called an active/passive configuration. Some cluster server products also support another mode, called an active/active configuration. In this mode, all the servers in the cluster can be actively sharing part of the workload at the same time. It typically requires an application designed to partition data sets among the servers to avoid data integrity problems resulting from concurrent updates to the same data from multiple servers.

Server clusters typically communicate through a broadcast or share a central repository to keep track of cluster information and cluster node status.

Each server in the cluster is referred to as a node. Each node in the cluster monitors the local services it is running and broadcasts this information on a private network connection. This private network connection allows all nodes in the cluster to know the status of all clustered resources. In the event that a service on one node fails, another node receives this status through the private network connection and in response, can start the service locally to maintain high availability for the service.

These cluster server can be configured either as symmetric cluster systems or asymmetric cluster systems.

Symmetric Clustering

Microsoft Cluster Server software or VERITAS software in a symmetric cluster environment allows one server to run Image Services while the other runs the RDBMS software. If one of the servers fail, the remaining server runs both.

The database in a high availability configuration is set up separately from Image Services and separate resource groups are created for each. This configuration is known as a symmetric cluster. This is the preferred method of setting up a cluster server.

Because of the support of the database retry functionality, there is no longer a requirement that Image Services and the database be collocated and configured in the same high availability resource group. Now, if the database fails from one node to the other, Image Services automatically reconnects.

In a high availability symmetric cluster, the database behaves like a remote database. Even when one server fails and it becomes local, it still behaves like a remote database using the unique virtual RDBMS IP address.

When you configure your high availability system, we recommend that separate resource groups be created for the Image Services software and the RDBMS (each containing a drive and having a virtual IP address). This is required for symmetric clustering.

Attention The database can also still be completely separate (either HA or non-HA).

The two servers in the cluster, Nodes 1 and 2, must have an appropriate version of Windows or UNIX OS and the cluster server software installed on their local drives. Refer to the *IBM FileNet Image Services, Image Services Resource Adapter, and Print Hardware and Software Requirements* document for support information.

The FileNet Image Services and RDBMS software is also installed on the local drives. There are two shared drives. One shared drive contains the Image Services dataset files, while the other contains the RDBMS database files.

Asymmetric (Active/Passive) Clustering

An asymmetric cluster system includes both active (primary) and passive (back up) servers. As one server is working the other server is serving as its back up in case there is a problem with the primary server. Microsoft Cluster Server software in a local site-controlled environment allows you to set up two servers with the same configuration. They even have the same domain name and system serial number. Both servers are always running, but while one server is actually being used to run your FileNet and RDBMS software, the other server is standing by to automatically take over in the event of a problem or system failure. Only one server is active

A relational database (RDBMS) can be on a remote cluster server. In this case, the RDBMS client needs to be installed on the local drive of the FileNet Image Services system.

As with a symmetric cluster, the two servers in the cluster, Nodes 1 and 2, must each have APPROPRIATE, and the cluster server software installed on their local drives.

The FileNet Image Services and RDBMS software is also installed on the local drives. In an active/passive cluster, there is only one shared drive, and it contains all the datasets, logs, configuration files, and database files.

Microsoft Cluster Server

Microsoft Cluster Server is supported for both Symmetric and asymmetric systems.

Microsoft Cluster Server is supported for FileNet® Image Services Combined server (Root/Index/Storage Library) installations with a remote relational database or a local **Site-controlled** relational databases. These configurations can be run in either a **Native Mode** domain or in a **Mixed Mode** domain.

Dual server Systems (separate Root/Index and Storage Library servers), Remote Entry Systems, WorkFlo Management Systems, or Application Server Systems are **not** supported.

Attention Refer to the MS Cluster Server Resource Center on the Microsoft Web site for a wide selection of Microsoft documentation.

Before you can install the cluster server software, each server in the cluster (Node 1 and Node 2) must have the following prerequisites.

Verify Operating System Software

Verify that the servers you are setting up has the correct operating system software installed on each node. For servers that will be running Microsoft Cluster Server software, VERITAS Cluster Server software, or VERITAS Volume Replicator software, refer to the *IBM FileNet Image Services, Image Services Resource Adapter, and Print Hardware and Software Requirements* to verify supported operating system releases.

To download this document from the IBM Support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Cable Length Requirements

A very important aspect of setting up your cluster server system is determining the maximum allowable SCSI bus cable length.

The maximum length of the cable that connects the optical library to each node, including the terminators and the cable contained within the optical drive unit, cannot exceed the maximum length specified for the type of SCSI devices being used (Single Ended, Differential, Low Voltage Differential).

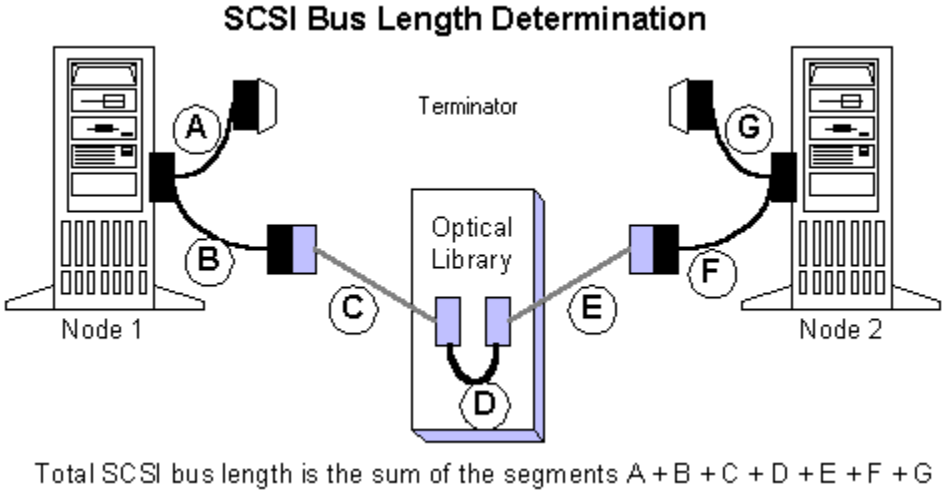
This is critical, because in a clustered environment the rules for cable length are very different than the rules for a non-clustered environment. It is very easy to exceed the maximum cable length in a cluster environment, and doing so would result in either intermittent errors or the system not working at all.

When measuring the cable be sure to consider all sections, including:

- The length of each end of the special Y-Connector at each node.

- The length from each node to the optical drive.
- The length of the cable contained within the optical drive. (For larger optical libraries, the length of cabling inside the unit is especially important.)

The diagram below explains how to determine the total cable bus length.



where A, B, F, and G are the lengths of the cable segments of the special “Y” cables, C and E are the lengths of SCSI cabling connecting the “Y” cable ends to the optical library, and D is the length of the SCSI cabling used inside the optical library.

Other Configuration Requirements

- Only optical libraries with SCSI robotic arms are supported.
- Microsoft requires dual Ethernet cards, dual SCSI cards, special RAID controllers, and specifically listed RAID drives.

- All hardware used in the Cluster System **must** be on the Microsoft Hardware Compatibility list (HCL).

Important Do not use any use any hardware components that are not Cluster compatible.

- To view the Microsoft Hardware Compatibility list (HCL) go to the Microsoft Web site and search for “HCL”. This list identifies certified products tested for the Cluster Server environment.

Installation Worksheet

Identify the two machines that will be used in the Cluster as Node 1 and Node 2. This worksheet will be used when installing your cluster server software, as well as when installing Image Services in your Cluster Server environment.

Obtain the following information before you begin your installation:

Cluster and Machine Names	Public IP Address
Image Services DNS Name:	
RDBMS DNS Name:	
Node 1: Machine Name:	
Node 2: Machine Name:	

Attention For a symmetric cluster, two virtual IP addresses are required: one for the Image Services cluster group and one for the RDBMS cluster group.

Identify a network name for your FileNet cluster resource. This will be the same name that you use for your SQL Server or Oracle network name.

Image Services Network Name: _____

Public IP Address: _____

System Serial Number: _____

RDBMS Network Name: _____

Public IP Address: _____

Attention The System Serial Number will be the same for both nodes.

The Windows drive letter or UNIX path for the Shared drive where Image Services shared files will reside: _____

The Windows drive letter or UNIX path for the RDBMS database files: _____

Important **Do Not** use the same drive letter for the quorum drive and the shared drive. The quorum drive, which is used to store cluster configuration database checkpoints and log files, should be a separate drive from the Shared drive where Image Services shared files will reside. **The examples shown in this document, use Z or S as the shared drive**.

Attention The Shared drive should also be a separate logical drive from the application drive which will hold the relational database.

For SQL Server

SQL Server database Name: _____

SQL Server table filegroup Name: _____

SQL Server index filegroup Name: _____

For Oracle

Oracle Service Name:
(siteDB.world, for example) _____

Oracle Database Name:
(siteDB, for example) _____

Oracle Parameter File:
(Z:\siteDB\init_siteDB.ora, for example) _____

Oracle table tablespace Name: _____

Oracle index tablespace Name: _____

For DB2

DB2 Database Name: _____

DB2 table tablespace Name: _____

DB2 index tablespace Name: _____

Verify That System Names Can Be Resolved to IP Addresses

Verify that you can resolve the system names to IP Addresses for this system and any servers you want to communicate with remotely. **Do not** proceed with the cluster installation procedure if you are unable to verify.

VERITAS Cluster Server

Image Services supports VERITAS Cluster Server, VERITAS Volume Manager, and VERITAS Volume Replicator. Refer to the *IBM FileNet Image Services, Image Services Resource Adapter, and Print Hardware and Software Requirements* to verify supported software releases.

To download this document from the IBM Support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Image Services supports two-node clusters.

Attention Image Service Storage Library servers with SCSI optical libraries are not supported with VERITAS Cluster Server in this release.

It's very important that the servers in a cluster environment and the servers in a replication environment be configured identically. Refer list of supported software versions for this release starting at **"Verify Operating System Software" on page 21**.

VERITAS Cluster Server (VCS) provides a network of servers that are capable of running applications in a high availability cluster environment with shared storage.

VCS works by monitoring resources and applications associated with a provided service (for example a Root/Index or Combined server with a remote RDBMS server). When a provided service goes offline on one server in the cluster, it is automatically started on another node in the cluster.

VERITAS provides, for purchase, several Agents for popular products such as Oracle and Microsoft SQL Server. VCS Agents monitor, start,

and stop services in a cluster. Agents are a middle layer between the user interface, and the services running in a cluster. Commands are given to the Agents and the Agents are responsible for fulfilling the command and verifying that everything executed without error. When you execute a command in VCS to bring a resource offline this is in effect telling the Agent to go and take the resource offline.

VCS also provides a highly configurable framework for creating your own Agents to control services in a cluster.

Software

VERITAS Cluster Server (VCS) provides high availability management for both hardware and software resources in clustered server configurations using RAID redundancy techniques.

VERITAS Volume Manager (VxVM) provides storage management for enterprise computing and emerging Storage Area Network (SAN) environments. VERITAS Volume Manager provides a logical volume management layer which overcomes the physical restrictions of hardware disk devices by spanning logical volumes across multiple physical volumes.

Hardware

VCS requires duplicate servers for each node in the cluster. Since Image Services supports two node clusters, you'll need two identical, but separate servers for Image Services and, if Oracle RDBMS software and databases reside on a remote server, two identical but separate servers for the Oracle software and data.

Installation

VCS requires that the Image Services software and Oracle software be installed and configured exactly the same on both servers in their respective clusters. Each cluster contains at least one shared disk for data storage.

Cluster Server Setup Sequence

The following outlines the installation path sequence that can be taken to setup your Cluster Server system. Nine steps are required.

1. Make sure the applicable operating system is installed on each node and the applicable cluster software (VERITAS or Microsoft SQL Server) is installed on each node.

2. Install the RDBMS and create a unique database resource group in the applicable cluster software. Add the database virtual IP address and the database shared drive to this resource group and test the failover.

3. Configure the Image Services failover resource group, including the the virtual IP and disk or mount resources.

Attention The Image Services virtual IP address and disk resources are unique from the RDBMS virtual IP address and disk resources.

You may want two disks or mount points, one for /fnsw/local (fnsw_loc on a Windows Server system) and the other for the datasets. Test that these mount points can fail over.

Attention The Image Services application will be added to this group later in the procedure.

4. Install and configure the Image Services software on Node 1. Point to the database created in Step 2 above, create the datasets and start Image Services.

5. Manually fail over the Image Services resource group to Node 2.

6. Install Image Services on Node 2, point to the existing configuration located in /fnsw/local (fnsw_loc on a Windows Server system), and start Image Services. This directory structure was created when Image Services is installed in Step 4 above.

7. Manually fail back over to Node 1. Make sure Image Services comes up on both nodes by manually starting Images Services.

8. Add your application resource to the Image Services resource group and configure Image Services for autostart.

9. Make sure Image Services starts automatically on both nodes after a failover.

Modify the hosts file

The /etc/hosts file on both hosts must contain the four-part NCH service name of the local server. If an entry for your local server does not exist, you can add one now.

The general format of a hosts file entry is:

```
<IP_address_of_IS_Domain> <IS_cluster_DNS_name> <NCH_four_part_service_
name> <hostname>
```

For example:

Image Services Root/Index server cluster IP address: **9.42.31.3**

Image Services Root/Index server cluster DNS name: **titian**

Image Services Root/Index server1 name: **titian1**

Image Services Root/Index server2 name: **titian2**

Image Services Domain name: Titian:**Yourco**

The hosts file entry on server 1 looks like this:

```
9.42.31.3 titian titian-yourco-nch-server titian1
```

The hosts file entry on server 2 looks like this:

```
9.42.31.3 titian titian-yourco-nch-server titian2
```

Important Your hosts file might contain a combination of the familiar IPv4 network addresses and the more recent IPv6 network addresses. The IPv6 addresses contain up to eight groups of hexadecimal numbers separated by colons (for example, FE80::2C0:FE35:9FFF:D28).

Install and Update Cluster Server Software

Depending on the type of Cluster server you are installing or updating, refer to one of the following chapters to configure your cluster server system:

- For servers running Microsoft Cluster Server (MSCS) software, go to **Chapter 2, "Installing Image Services on a MS Cluster Server System," on page 32**.
- For servers running VERITAS software, go to **Chapter 3, "Installing Image Services on a VERITAS Cluster Server System," on page 59**.
- For servers updating Image Services on their Cluster Server system, go to **Chapter 5, "Updating Image Services on a Cluster Server," on page 88**.

2

Installing Image Services on a MS Cluster Server System

This chapter contains information for installing Image Services software and configuring a Microsoft Cluster Server (MSCS) system.

Remote Database Support

A remote database can be supported on a MS Cluster Server. Refer to one of the following guidelines documents for setting up a remote database, depending on the type of RDBMS you are using:

- *Guidelines for Installing and Configuring IBM DB2 Software*
- *Guidelines for Installing and Configuring Oracle 10g Software on UNIX Servers (FileNet-Controlled)*
- *Guidelines for Installing and Configuring Oracle 11g Software on UNIX Servers (FileNet-Controlled)*
- *Guidelines for Installing and Configuring Oracle Software on UNIX Servers (Site-Controlled)*
- *Guidelines for Installing and Updating Site-Controlled Oracle and MS SQL Software fir Windows Server*

To download these guidelines from the IBM Support page, see **“Accessing IBM FileNet Documentation” on page 12**.

The following sections only describe the installation and configuration of RDBMS and Image Services software on a local system.

Setup Cluster Server Domain

Your cluster server can be configured on either a Native Mode domain or a Mixed Mode domain using Windows 2003 or Windows 2008 or Windows 2012 servers. Using a Native Mode domain is the preferred network configu- ration for Cluster Server. See **“Appendix A – User and Group Secu- rity Configuration for Cluster” on page 93** and **“Appendix B – Setting up a Secure Native Mode Domain Installation” on page 94** for more information.

Install Relational Database Software

Refer to the *Guidelines for Installing and Updating Site-Controlled Oracle and MS SQL Software for Windows Server* for information on either your Oracle or SQL RDBMS software or *Guidelines for Installing and Configuring IBM DB2 Software* for more information on your IBM DB2 software.

- If you are installing MS SQL, skip to the next section.
- If you are installing Oracle, skip to **“Install Oracle Software” on page 36**.
- If you are installing DB2, skip to **“Install FileNet Software” on page 39**.

Install Microsoft SQL Server Software

Refer to the Microsoft installation instructions to install the SQL software. Perform this procedure on the Node 1 server first and then on Node 2. You can find these instructions on the Microsoft Web site.

The Microsoft installation procedure automatically installs the SQL software on both nodes and creates all appropriate resources in a dedicated cluster group.

Important You must choose Custom setup type for the installation of SQL Server and enter the following information. In the Authentication Mode dialog box, choose Mixed Mode.

Attention For local databases on symmetric clusters, all resources (Oracle and Image Services) must reside in two separate groups. For local databases on asymmetric clusters, all resources must reside in only one group. Use the Cluster Administrator to check that all resources have been added to the same group.

Create the Site Database

Perform this procedure on the Node 1 server.

Refer to the SQL Server installation documentation (found on the Microsoft Web site) and Chapter 3 of the *Guidelines for Installing/Updating Site-Controlled RDBMS Software for Windows* document for Local SQL Server RDBMS Guidelines. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Attention Make sure to put the database on the shared drive in the database group.

Set SQL Environment Variable (SQL Server 2000 only)

If you are using SQL Server 2005, skip to **"Test RDBMS Cluster Failover" on page 38**.

Before starting the installation of FileNet software, set the following environment variable on both nodes. Set the environment variable on the Node 1 server first.

1. Create a new System Environment Variable.
2. Enter **ISQLServer** in the Variable Name: box.
3. In the Variable Value: box, enter the SQL Network Name of your cluster system.
4. After you set the variable, the new variable will be added to the list of System Variables.
5. Repeat this entire procedure for the second node of your cluster system. After both nodes have set the SQL environment variables, skip to **"Test RDBMS Cluster Failover" on page 38**.

Install Oracle Software

This section describes installing and configuring Oracle database.

Install Oracle RDBMS Software

Attention Refer to the *IBM FileNet Image Services, Image Services Resource Adapter, and Print Hardware and Software Requirements* for the supported versions of Oracle.

Perform this procedure on the Node 1 server first and then on Node 2.

To install the Oracle database software, refer to the Oracle installation documentation (found on the Oracle CD-ROM) and the Oracle guidelines in the *Guidelines for Installing/Updating Site-Controlled RDBMS Software for Windows* document. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

After the Oracle database installation is completed, all Oracle resources must reside in only one group. Use the Cluster Administrator to check that all resources have been added to the same group.

Install Oracle Fail Safe Software (Optional)

Attention Install the database software first and then Oracle Fail Safe Manager.

Perform this procedure on the Node 1 server first and then on Node 2.

Refer to the Oracle installation documentation found on the Oracle CD-ROM to install the Fail Safe Manager. You can download Oracle Fail Safe software from Oracle's Web site.

Create the Site Database

Perform this procedure on the Node 1 server.

Refer to the Oracle installation documentation (found on the Oracle CD-ROM) and the Oracle guidelines in the *Guidelines for Installing/ Updating Site-Controlled RDBMS Software for Windows* document. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Attention Make sure to put the database on the shared drive in the database group.

Create the Oracle Resource Group

Use the MS Cluster Administrator or Oracle Fail Safe Manager to create an Oracle Resource Group.

Install IBM DB2 Software

Refer to the IBM DB2 installation instructions to install the DB2 software. Perform this procedure on the Node 1 server first and then on Node 2. You can find these instructions on the IBM Web site.

Attention For local databases on symmetric clusters, all resources (DB2 and Image Services) must reside in two separate groups. For local databases on asymmetric clusters, all resources must reside in only one group. Use the Cluster Administrator to check that all resources have been added to the same group.

Create the Site Database

Perform this procedure on the Node 1 server.

Refer to the DB2 installation documentation (found on the IBM Web site) and the *Guidelines for Installing and Configuring IBM DB2 Software* document for Local DB2 Guidelines. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Create the DB2 Resource Group

Use the MS Cluster Administrator to create an DB2 Resource Group.

Test RDBMS Cluster Failover

Before you install the FileNet software, it is important that you test your RDBMS resource group to make sure that it will failover successfully from node 1 to 2, and then back to node 1.

Move Control of the RDBMS Resource Group to Node 2

1. If you are using Oracle, open the Oracle Fail Safe Manager.
   If you are using DB2 or MS SQL, open MC Cluster Administrator.
2. Right-click on the RDBMS resource group and move it to Node 2.
3. Verify that RDBMS comes up on Node 2.
4. Check the RDBMS logs on Node 2 to verify that it started without error.

Move Control of RDBMS Resource Group to Node 1

1. After all the resources in the group are online at Node 2, *Reboot* the Node 1 server.
2. After Node 1 has rebooted, right-click the group and move the resource group back to Node 1.
3. Verify that RDBMS comes up on Node 1.
4. Check the RDBMS logs on Node 1 to verify that it started without error.

Install FileNet Software

Attention

Refer to the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system to install your Image Services software. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Install the FileNet software on the primary server local drive (Node 1) first. Install the FileNet software on the Shared drive and the local drives of each server as follows:

- FNSW (Image Services executables) will be installed on the local drive of each node using the same drive letter on each node.

Important

It is crucial that the same drive letter or directory path be used on each node when installing Image Services executables on the local drive. If different drive letters or paths are used, the system will not be able to failover.

- FNSW_LOC (Image Services Shared Files) will be installed on the shared drive.

Important **Do Not** use the same drive letter for the quorum drive and the shared drive. The quorum drive, which is used to store cluster configuration database checkpoints and log files, should be a separate drive from the Shared drive where Image Services shared files will reside. **The examples shown in this document, use Z or S for the shared drive**.

Attention The shared drive can only be accessed by one node at a time. If this is an symmetric cluster system and the Image Services and RDBMS resources are in separate resource groups, be sure to use the drive in the Image Services group for FNSW_LOC.

Important The domain name and SSN (system serial number) used during the installation procedure **must** be the same for both servers.

This installation procedure can be complicated. To prevent errors, follow the steps in this procedure **exactly** as they are written.

1. Refer to **"Getting started" on page 14** to ensure that all Hardware and Software requirements and other prerequisites are met for each server node. After ensuring that all requirements have been met, return to this page.
2. IF the RDBMS software is running on Node 2, fail it to Node 1 now.
3. Shut down Node 2.

Attention Because Cluster Service has already been installed on both nodes, it is important to **keep Node 2 off** so that the rebooting of Node 1 during setup does not cause the cluster supported components, including the shared drive, to failover to Node 2.

Installing FileNet software on Node 1 and Node 2

1 Turn on power to the Node 1 server **only**. If you aren't already, logon as Windows **Administrator** for the domain.

Attention If you are installing software as a user **without** Full Domain Administrator Rights, logon with the user name and password that was created during the installation of Image Services.

2 Access the **Image Services for Windows Server** software on Node 1.

3 Follow the instructions in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system to launch the Image Services installer. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

4 On the End User License Agreement screen, click **Yes** to accept the agreement.

5 On the Image Services Configuration Information screen, locate the check box for Cluster Server. Make sure it is checked **Yes,** and continue the installation.

6 When the Enter Network Name screen displays, enter the network name from your **"Installation Worksheet" on page 23**. The Network Name must match the Image Services Cluster DNS Name.

7 Continue the Image Services software installation.

8 When the installation is complete, reboot the Node 1 server and logon as the FileNet software user, such as **fnsw**.

9 Check the Windows Event Viewer for any errors. Resolve any errors before continuing.

10 Power on Node 2 and shutdown Node 1. This will automatically move control of resource groups to Node 2.

11 Repeat Steps 1 - 9 on Node 2 and then reboot Node 2.

Stop Image Services ControlService

Perform this procedure on the Node 1 and Node 2 servers.

1. Open Administrative Tools and double-click the *Services* icon.

   The Services dialog box displays.

2. Double-click the Image Services ControlService, in the Services window. The FileNet IS Service Properties dialog box opens.

3. Click the *Stop* button to stop the FileNet IS Service. In a few seconds the service status in the FileNet IS Service Properties window will indicate that the service has stopped.

4. Click the Startup type drop-down arrow and set the Startup type to **Manual**.

5. Click **OK** to exit the IS ControlService Properties window.

6. Close the Services window.

Create Configuration Database

Make sure the Image Services resource group is running on Node 1. Perform the following procedure on the Node 1 server.

1. Open the FileNet System Configuration Editor.

   The New Configuration Database window opens.

2. Click **OK** to continue.

   The Initialize Combined Server Template window opens.

3. In the Initialize Combined Server Template window, change the drive letter to the Image Services resource group's shared drive, and click **Next**.

4. A series of dialog boxes and prompts for the Combined Server Template appears next. Answer each prompt as appropriate for your site to configure your system.

Attention **Do not** configure a Storage Library at this time.

5. When your configuration is complete, the "Configuration is Complete..." message appears. Click **Next** to continue.

   The *FileNet Image Services System - Configuration Editor* window displays.

Tip When you are finished configuring the database, you can select tabs in the Configuration Editor to verify that you entered the information correctly.

Define RDB Object Locations

Use the procedure in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system to define IDB object locations for your RDBMS on the Relational Databases tab, RDB Object subtab. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Attention Enter the virtual hostname for the RDBMS. This is the Virtual IP resource form the RDBMS group.

The table space names specified in the RDB Objects list must exist before you initialize the FileNet Image Services databases.

Exit from the *FileNet Image Services - System Configuration Editor* and save the configuration changes you just made.

Initialize the Database

As the FileNet software user such as **fnsw**, initialize the index database and all the MKF databases (includes permanent, transient, and security databases)

1 Do this by entering the following commands on the Image Services server (the Node 1 server):

fn_setup_rdb -f

fn_util init > \fnsw_loc\local\logs\init.log

This process may take a while (sometimes up to 30 minutes without any feedback to the user); the larger the datasets, the longer the wait. After the initialization process finishes, the prompt returns.

Tip You can monitor the progress of the initialization by viewing the fn_util.log and oracle.log (or init.log) files in a command prompt window. These files are located in the following directories:

\fnsw_loc\logs\fn_util\fn_util.log
\fnsw_loc\logs\fn_util\oracle.log (for Oracle)
\fnsw_loc\logs\fn_util\FileNet.log (for SQL Server)
\fnsw_loc\logs\fn_util\init.log (does not always display)

The file size increases each time you view the log files, indicating the progress of the initialization.

2 After the initialization is finished, view the contents of the \fnsw_loc\logs\fn_util\init.log and oracle.log files to make sure that there were no errors in the database initialization process.

Verify/Set FileNet Dataset Permissions

Perform the following procedure on the Node 1 server.

Because the FileNet datasets reside on a different drive than the FileNet Image Services software, you must set the group permissions.

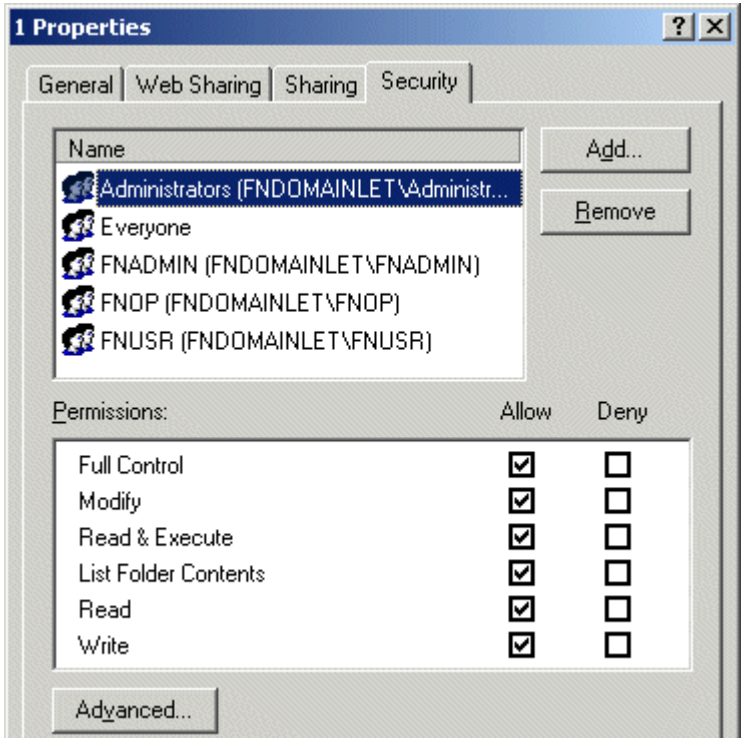
1 If you aren't already, logon as Domain user **fnsw**.

2 Open Windows Explorer, and select the directory containing the FileNet datasets, such as Z:\fnsw\dev\1

3 From the File menu, select the Properties menu option.

4 In the Properties window, select the Security tab.

The Security Properties for \fnsw\dev\1 display on this tab.



5 For each group in the table below, set the following permissions in the Security tab dialog box:

Group	Permissions
Administrators*	Full Control
fnadmin	Full Control

***** The Administrators group can be listed on the Owners tab which is accessed by clicking the Advanced button on the Security Properties window.

Group	Permissions
fnop	Read & Execute, List Folder Contents, Read, and Write
fnusr	Read & Execute, List Folder Contents, Read, and Write

***** The Administrators group can be listed on the Owners tab which is accessed by clicking the Advanced button on the Security Properties window.

6 Click **OK** to set the permissions and close the Properties dialog box.

Enable Autostart Image Services Processes Option

Perform this procedure on the Node 1 server. Use the **fn_setup** tool to enable the Autostart Image Services processes.

1 Logon as the FileNet software user with **root** privileges and run the fn_setup utility as follows:

\fnsw\bin\fn_setup

2 Answer all the prompts with information related to your system. Reply to the prompts with the requested information. Answer **y** at the following prompt:

```
Autostart IS Processes (y=yes, n=no) [y]:
```

Add NCHBroadcast Value to Registry Editor

Add the NCHBroadcast value to the registry on both nodes as shown in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system. To download this document from the IBM support page, see **“Accessing IBM FileNet Documentation” on page 12**.

Add Registry Keys for Replication to Image Services Resource Group

1. From the Cluster Administrator window, right-click the IS Resource Group and click **Bring Online**.
2. From the Cluster Administrator, double-click the FileNet IS resource to display the FileNet IS Properties window.
3. Click the Registry Replication tab. The FileNet IS Properties dialog box displays.
4. Click the **Add** button.
5. In the Registry Key box enter the following text:

   software\filenet\ims\currentversion
6. Click **OK** to add the Registry Key.
7. Click the **Add** button again and enter the following text,

   system\CurrentControlSet\Services\IMSService
8. Click **OK** to add the Registry Key.
9. Click **Apply** to have the changes you made take effect.
10. Click **OK** to close the FileNet IS Properties window.

Connect/Configure Optical Storage Library Devices

This procedure is used to connect and configure your SCSI Optical Storage Devices.

Connect Storage Library Device

1. Logoff both Windows server nodes and turn them off.
2. Connect the storage library device to each node, and power the device on.

   Wait until the storage library device is ready before you continue to the next procedure.

Attention The storage library device must have its own separate SCSI controller.

Configure SCSI Host Adapter Utility Settings

Use this procedure to configure the SCSI Host Adapter Utility Settings.

Attention The settings in this procedure are for configuring an Adaptec AHA-2944UW SCSI Adapter. Other SCSI adapters can have different settings. Refer to the Microsoft Web site for a list of other supported SCSI adapters.

1. Turn on power to the Node 1 server and watch the screen as the storage device initializes.

   A message will display that tells you what keystroke to enter to access the SCSI Adapter Utility.

   For example, if you see the following message, you would press CTRL+A:

   <<<Press <CTRL><A> for SCSISelect(TM) Utility!>>>

Attention The manufacturer of the SCSI adapter determines what keystroke you need to enter to access the SCSI Adapter Utility. For example, the Adaptec 2944 uses the keystroke, **CTRL+A**.

2 While the SCSI adapter for the optical library is initializing, type **CTRL+A** (or other keystroke) to access the SCSI Adapter Utility.

The SCSI Adapter Utility opens.

3 Select the option to configure the Host Adapter Settings.

4 Verify the Host Adapter SCSI ID is 7.

Attention The setting for each node must be different and Node 1 should already be set to 7.

5 Change the Host Adapter SCSI Termination to, “Low OFF/High OFF”

6 Select Advanced Configuration Options and make the following changes:

a Verify that the Host Adapter BIOS is set to, “Enabled”

b Change the Support removable disks under BIOS as fixed disks to “Disabled”

7 Save the changes and exit the SCSI Adapter Utility. The Node 1 server will automatically reboot.

8 After the server automatically reboots, logon as the FileNet user, such as **fnsw**.

9 Open a Command Prompt window, and enter the following command:

fnddcfg

When the command is finished, you will receive a message instructing you to reboot the server to make the changes effective.

10 Reboot the Node 1 server, and logon again as the FileNet user, such as **fnsw**.

11 Open a Command Prompt window, and enter the following command:

fndev

12 The physical addresses of all attached storage library devices should appear.

13 Turn off power to the Node 1 server.

Attention Since the Host Adapter Settings have been changed, Node 1 must be off to prevent Node 2 from hanging as it starts up.

14 Turn on power to the Node 2 server and watch the screen as the storage device initializes.

A message will display that tells you what keystroke to enter to access the SCSI Adapter Utility.

For example, if you see the following message, you would press CTRL+A:

<<<Press <CTRL><A> for SCSISelect(TM) Utility!>>>

Attention The manufacturer of the SCSI adapter determines what keystroke you need to enter to access the SCSI Adapter Utility. For example, the Adaptec 2944 uses the keystroke, **CTRL+A**.

15 While the SCSI adapter for the optical library is initializing, type **CTRL+A** (or other keystroke) to access the SCSI Adapter Utility.

The SCSI Adapter Utility opens.

16 Select the option to configure the Host Adapter Settings.

17 Change the Host Adapter SCSI ID to 6.

Attention The setting for each node must be different and Node 1 should already be set to 7.

18 Change the Host Adapter SCSI Termination to, “Low OFF/High OFF”

19 Select Advanced Configuration Options and make the following changes:

a Verify that the Host Adapter BIOS is set to, “Enabled”

b Change the Support removable disks under BIOS as fixed disks to “Disabled”

20 Save the changes and exit the SCSI Adapter Utility. The Node 2 server will automatically reboot.

21 After the server automatically reboots, logon as the FileNet software user, such as **fnsw**.

22 Open a Command Prompt window, and enter the following command:

fnddcfg

After the command is finished, you will receive a message instructing you to reboot the server to make the changes effective.

23 Reboot the Node 2 server, and logon again as the FileNet software user, such as **fnsw**.

24 Open a Command Prompt window, and enter the following command:

fndev

25 The physical addresses of all attached storage library devices should appear.

26 Turn-off power to the Node 2 server.

Attention Node 2 is turned off to prevent it from starting-up before Node 1 in the next procedure.

Automatically Configure Storage Library

1 Turn-on power to the Node 1 server.

2 When Node 1 is ready, logon as the FileNet software user, such as **fnsw**, or Windows **Administrator** for the domain**.**

3 Take the Image Services resource group off line.

4 Open the *FileNet Image Services System Configuration Editor*.

5 Verify that the two-part domain information is correct, and click **OK**.

The FileNet Image Services System Configuration Editor window opens with the Procedures tab displayed.

6 From the Procedures tab, select Automatically Configure a Storage Library from the list of available procedures.

7 Click **Run**.

8 After you have completed configuring the storage library, exit the System Configuration Editor and save your changes.

9 At a Command Prompt, run the following command to initialize the configuration database:

fn_build -a

10 Bring the Image Services resource group back on line.

11 Check the following logs for any errors that would indicate that the Image Services did not start correctly.

a Open the Windows Event Viewer and check the Application and System Logs.

b Open the FileNet Task Manager and check the Event Logs.

c Resolve any errors before continuing.

Attention The Images Services software now gives you the ability, through a TXT file, to disable the automatically configure utility that runs each time a node gets control and starts Image Services. Because there are cases where you can have certain optical libraries that cannot be automatically configured, the automatically configure utility can be disabled by

creating a blank trigger file named no_autoconfig.txt in the \fnsw_loc\sd directory on each node (\fnsw_loc\sd\no_autoconfig.txt).

Move Control of Image Services Resource Group to Node 2

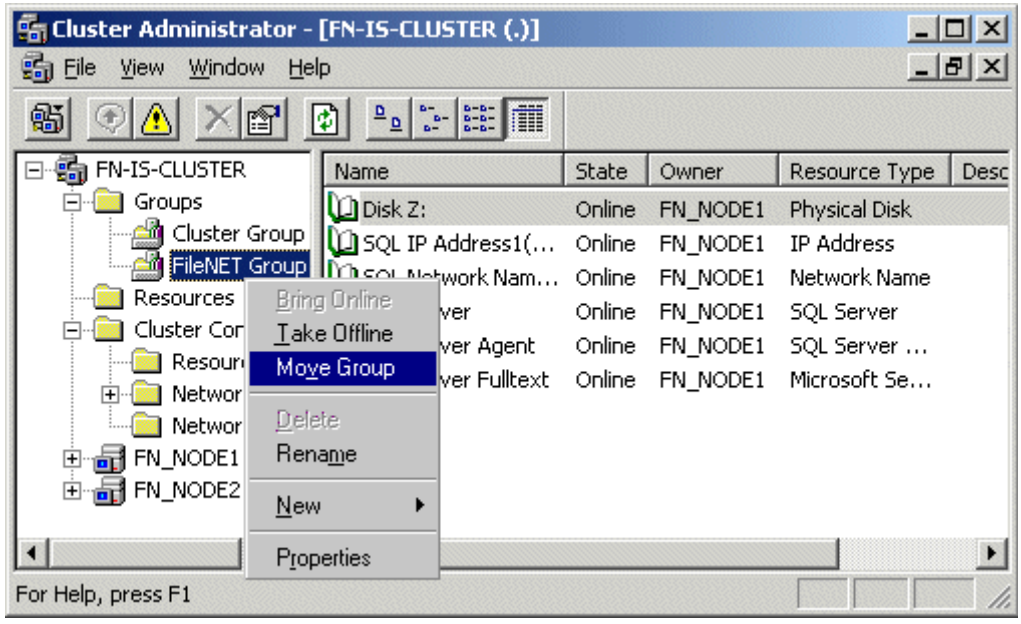
This procedure will test that control of the cluster server and the Storage Library Device can be moved from one node to another.

1 If Node 2 is off, turn on power to the Node 2 server and logon as **fnsw** or Windows **Administrator** for the domain**.**

2 When Node 2 is ready, move control of the FileNet group to Node 2.

a From the **Taskbar** at either node, click the **Start** button, point to **Programs**, point to the **Administrative Tools (Common)**, and click **Cluster Administrator**.

The Cluster Administrator window opens.



b Right-click on FileNet (IS) Group and click *Move Group.* In a few minutes the Owner of the FileNet Group will switch from Node 1 to Node 2.

c Verify that the owner of the FileNet Group is now Node 2.

3 Use FileNet Task Manager (or other means) to verify that the Image Services software processes started successfully.

4 This procedure is completed. If you want to move control of the cluster back to node 1, you can do so now.

Cluster Server Installation Completed

You have successfully installed and configured Image Services on your Cluster system.

3

Installing Image Services on a VERITAS Cluster Server System

This chapter contains information for installing a VERITAS Cluster Server system.

Setup Cluster Server Domain (Microsoft only)

Your cluster server can be configured on either a Native Mode domain or a Mixed Mode domain using Windows 2003 or Windows 2008 servers. Using a Native Mode domain is the preferred network configuration for Cluster Server. See **“Appendix A – User and Group Security Configuration for Cluster” on page 93** and **“Appendix B – Setting up a Secure Native Mode Domain Installation” on page 94** for more information.

Install VERITAS Cluster Server

Attention On all servers, VERITAS uses "Service Groups" of resources to provide high availability services to users. The following instructions specify how to add resources to a service group to provide a high availability Image Services service.

Installation Overview

The following high-level steps are necessary to make Image Services highly available in a cluster environment on UNIX platforms. These steps are described in more detail in the later sections:

- Install the appropriate RDBMS software. This can be a remote install or it can be installed on the same cluster as the Image Services software. If RDBMS and Image Services are installed on the same cluster, a separate service group must be set up for both Image Services and the relational database.
- Install the appropriate VERITAS software prior to installing or configuring any FileNet services for high availability.
- Configure the cluster groups
- Verify cluster failover.
- Create cluster resources for Image Services partitions.
- Install Image Services software on all nodes in the cluster.
- Configure the Image Services ControlService (Windows Server only).
- Enable event triggering for the Image Services Cluster (Windows Server only).
- Verify the installation
- Verify Cluster fail over

Remote Database Support

A remote database is supported. Refer to one of the following guidelines documents for setting up a remote database, depending on the type of RDBMS you are using:

- *Guidelines for Installing and Configuring IBM DB2 Software*
- *Guidelines for Installing and Configuring Oracle 10g Software on UNIX Servers (FileNet-Controlled)*
- *Guidelines for Installing and Configuring Oracle 11g Software on UNIX Servers (FileNet-Controlled)*
- *Guidelines for Installing and Configuring Oracle Software on UNIX Servers (Site-Controlled)*
- *Guidelines for Installing and Updating Site-Controlled Oracle and MS SQL Software fir Windows Server*

To download these guidelines from the IBM Support page, see **"Accessing IBM FileNet Documentation" on page 12**.

The following sections only describe the installation and configuration of RDBMS and Image Services software.

Installing VERITAS Software

1. Install the appropriate VERITAS software prior to installing or configuring any FileNet services for high availability. In addition to the VERITAS Volume Manager (VxVM), you can install either Cluster Server software, the Volume Replicator software, or both:
   - VERITAS Volume Manager
   - VERITAS Cluster Server - required for high availability
   - VERITAS Volume Replicator - optional for disaster recovery
2. For VERITAS Cluster Server, verify that two cluster service groups already exist with the following minimum resource:

- Shared storage resources (can include VERITAS Volume Group [VMDg] and MountV, or Mount for a basic disk [includes /fnsw/local, MSAR, Image Services datasets]).
- Clustered IP resources
- Application resource (Start and stop Image Services). This will be added after Image Services is installed.

Attention Image Services uses the GenericService or Application resource and does not have a custom agent.

Required resource dependencies for VCS Clusters

Dependencies determine the order VCS brings resources and service groups online and takes them offline. They also define whether a resource or service group failure impacts other resources or service groups configured in the cluster.

In VCS terminology, a parent resource is dependent upon a child resource. For example Mount resource (parent) depends on the Disk resource (child). The Mount agent mounts a block device on a directory. The file system cannot be mounted without the physical disk partition being available.

Please note that cyclical dependencies are not allowed for either resources or service groups.

Create Cluster Resources

Create cluster resources for the Image Services partitions on the shared storage using the permission and size settings as documented

in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system.

- Create the /fnsw partition on local storage for each node.
- Create the /fnsw/local partition on the shared drive.
- Create the datasets on the shared drive.

Configure the Cluster Groups for Image Services

Configure the cluster groups with the minimum resources listed above.

UNIX Examples of Image Services VCS Cluster

The following example is a sample Resource Dependency Tree for an Image Services group named **isgrp** in a non-replication environment:

```
group isgrp
{
Application is_app
    {
    IP isip
        {
        NIC isnic
        }
    Mount ismount
        {
        DiskGroup isdatadg
        }
    Mount msarmount
        {
        DiskGroup isdatadg
        }
    }
 }
```

The example below illustrates the cluster configuration for a highly available Image Service cluster:

```
include "types.cf"

cluster iscluster (
        UserNames = { admin = dijBidIfjEjjHrjDig }
        Administrators = { admin }
        CounterInterval = 5
        )
(continued on next page)
```

```
(continued from previous page)

system hq-cfgaix5 (
        )

system hq-cfgaix6 (
        )

group isgrp (
        SystemList = { hq-cfgaix5 = 1, hq-cfgaix6 = 2 }
        AutoStartList = { hq-cfgaix5 }
        )

        Application is_app (
                User = fnsw
                StartProgram = "/fnsw/bin/initfnsw start"
                StopProgram = "/fnsw/bin/initfnsw stop"
                MonitorProcesses = { "TM_daemon -s" }
                )

        DiskGroup isdatadg (
                DiskGroup = isdatadg
                )

        IP isip (
                Device = en0
                Address = "10.15.16.171"
                NetMask = "255.255.252.0"
                )

(continued on next page)
```

```
(continued from previous page)

        Mount ismount (
                MountPoint = "/fnsw/local"
                BlockDevice = "/dev/vx/dsk/isdatadg/v_isdata"
                FSType = vxfs
                MountOpt = rw
                FsckOpt = "-y"
                )

        Mount msarmount (
                MountPoint = "/fnsw/msar"
                BlockDevice = "/dev/vx/dsk/isdatadg/msar"
                FSType = vxfs
                MountOpt = rw
                FsckOpt = "-y"
                )

        NIC isnic (
                Device = en0
                )

        is_app requires isip
        is_app requires ismount
        is_app requires msarmount
        isip requires isnic
        ismount requires isdatadg
        msarmount requires isdatadg
```

Windows Server Examples of Image Services VCS Cluster

The following example is a sample Resource Dependency Tree for the built-in **ClusterService** group in a non-replication environment:

```
group ClusterService
{
VRTSWebApp VCSweb
    {
    IP csg_ip
        {
        NIC csg_nic
        }
    }
}
```

ClusterService group example:

```
include "types.cf"

cluster vcs-win-cluster (
        UserNames = { admin = iHIeHCgEHp }
        ClusterAddress = "10.14.101.102"
        Administrators = { admin }
        CredRenewFrequency = 0
        CounterInterval = 5
        )

system FONTANA (
        )

system NTNINER (
        )

(continued on next page)
```

```
(continued from previous page)

group ClusterService (
        SystemList = { FONTANA = 0, NTNINER = 1 }
        UserStrGlobal = "LocalCluster@https://10.14.100.90:8443;"
        Authority = 1
        AutoStartList = { FONTANA, NTNINER }
        )

        IP csg_ip (
                Address = "10.14.101.102"
                SubNetMask = "255.255.252.0"
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )

        NIC csg_nic (
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )

        VRTSWebApp VCSweb (
                AppName = vcs
                InstallDir @FONTANA = "C:\\\\\\\\Program
Files\\\\\\\\VERITAS\\\\\\\\VRTSweb\\\\\\\\VERITAS"
                InstallDir @NTNINER = "C:\\\\\\\\Program
Files\\\\\\\\VERITAS\\\\\\\\VRTSweb\\\\\\\\VERITAS"
                )

        csg_ip requires csg_nic
        VCSweb requires csg_ip
```

The following is a sample Resource Dependency Tree for an Image Services **fn_sg** group in a non-replication environment:

```
group fn_sg
{
GenericService IS_ControlService
IP is_ip_1
NIC ISNic
MountV Mount
}
```

fn_sg group example:

```
group fn_sg (
        SystemList = { FONTANA = 0, NTNINER = 1 }
        )

        GenericService IS_ControlService (
                ServiceName = "IS ControlService"
                UserAccount = fnsw
                Password = hvlTitKtw
                Domain = "vcs.net"
                )

        IP is_ip_1_1 (
                Address = "10.14.101.106"
                SubNetMask = "255.255.252.0"
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )

(continued on next page)
```

```
(coninued from previous page)

        MountV mount (
                MountPath = I
                VolumeName = FileNetVol
                VMDGResName = VVRDg
                )

        NIC ISNic (
                MACAddress @FONTANA = "00-C0-9F-27-14-e3"
                MACAddress @NTNINER = "00-C0-9F-35-0D-28"
                )

        requires group VVRGrp online local hard
```

Verify Cluster Failover

Test the RDBMS service group to verify the the service group can failover to all nodes in the cluster, and verify that the shared storage can be accessed from all nodes.

Install Image Services Software

Install Image Services on each node in the cluster. Refer to the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system. To download this document from the IBM Support page, see **“Accessing IBM FileNet Documentation” on page 12**.

Attention The steps in this section apply only to servers requiring Image Services software. This section does **not** apply to servers that do not require Image Services, such as remote relational database servers.

Attention On Windows Servers only, run the Image Services installer as a domain user who has at least Account Operator privileges. This is required as the **fnsw** user created by the installer needs to be a domain user so that both nodes recognize security over the shared fnsw_loc directory.

1. Make sure the cluster group is online on the node you are currently installing.

2. On the active node in the cluster, Install Image Services.

   - Image Services software (binary files) must be installed on the local drives of both nodes of the VCS Cluster. (If VERITAS Volume Replicator is installed, the Image Services software must also be installed on both nodes of the standby Image Services System.) See **"Appendix C – VERITAS Volume Replicator"** for VVR information.
   - Image Services configuration and data files (including MSAR and MKF); that is, everything in /fnsw/local on UNIX servers or \fnsw_loc on Windows servers, must be installed on the shared drive.
   - /fnsw/local (UNIX) or \fnsw_loc (Windows) must be a VERITAS Volume and file system.
   - Image Services datasets must be created on the shared drive in VERITAS raw partitions (UNIX only).
   - Image Services datasets under the /fnsw/dev/1 folder are actually links pointing to the real datasets on the shared drive. (These were

created in the last bullet of **"Install Image Services Software" on page 70**.) (UNIX only)

- Use **fn_util init** to initialize the datasets on the shared drive.

3 On Windows Server servers, when the installation is finished, verify the domain user **fnsw** has been added to the local server's Administrators group. This allows the system to start and stop services using the **fnsw** user account.

4 After you have installed and configured the Image Services software, shutdown the Image Services software manually and failover the cluster to the other node.

5 Install Image Services on the next node, specifying the same information entered during the installation on the first node. Image Services software must be installed on the local drive on each node.

6 After you have installed and configured the Image Services software on this node, shutdown the Image Services software manually.

Configure the IS ControlService (Windows Server only)

1 Modify the following service through the Windows Service Control Manager:

- IS ControlService
  - Change 'startup type' to 'manual ' for Image Services in Window 'Services'.
  - Set the Logon information to be the domain user **fnsw** (use the new password that was reset for this user earlier).

- Set the Logon format to (domain_name\fnsw), not (fnsw@domain.name.com).
- Start ISControlService.

Create the Image Services Service Group in VERITAS

1 Complete one of the following sub-steps, depending upon your platform:

a On a Windows Server, add a resource for the IS ControlService:

- Resource Type: **GenericService**
- Set the ServiceName to: **IS_ControlService**
- Set the Domain parameter to the fully qualified domain name of the Active Directory domain.
- Set the UserAccount parameter to the domain user **fnsw** and supply a password.
- Make the resource dependent on the following resources:
  - Clustered IP resource
  - Shared disk resource

b On a UNIX server, add a resource for Image Services with the following parameters:

- User = fnsw
- StartProgram = /fnsw/bin/initfnsw start
- StopProgram = /fnsw/bin/initfnsw stop

- MonitorProcesses = TM_daemon -s
- Make the resource dependent on the following resources:
  - Clustered IP resource
  - Shared disk resource

2 Bring the current node in the cluster online.

Enable Autostart IS Processes Option (Windows only)

Perform this procedure on the Node 1 server. Use the **fn_setup** tool to enable the Autostart IS Processes option.

1 Logon as the FileNet software user with **root** privileges and run the fn_setup utility as follows:

\fnsw\bin\fn_setup

2 Answer all the prompts with information related to your system. Reply to the prompts with the requested information. Answer **y** at the following prompt:

```
Autostart IS Processes (y=yes, n=no) [y]:
```

Verify the Installation

1 Make sure the current node owns the shared drive.

2 The virtual IP address of the Image Services system must be resolvable, either by the Domain Name Service (DNS) or by an entry in the local **hosts** file.

3 Use the FileNet Image Services System Configuration Editor, **fn_edit** to make sure the **Network Addresses** tab has the DNS network name and the virtual IP address of the cluster.

- In the Network Name field, enter the DNS name that resolves to the NCH network name of the system. This name may or may not be the same as the Server Name; however, it must be unique, less than 256 characters, and be composed only of alpha, digits, dot, dash, and underline characters. Spaces are not allowed.
- In the Network Address field, enter the virtual IP address of the VCS cluster.
- Make sure the IP address in the Image Services resource group in the cluster has the same virtual IP address.

4 Start Image Services by entering:

```
initfnsw -y start
```

5 Check the status by entering:

```
initfnsw status
```

6 Image Services should start successfully.

Attention If Image Services does not start successfully at this point, enter:

```
initfnsw -y stop
killfnsw -D -A -y
initfnsw start
```

7 Failover to the second node in the cluster.

8 Repeat steps 1 through 7 on the second node.

Verify Cluster Failover

After the entire cluster has been successfully configured, use VERITAS documentation procedures to verify that the cluster group can failover to all nodes in the cluster, and that the shared storage can be accessed from the active node.

- Start Node 1
- Verify Image Services runs with no problems on Node 1
- Failover to Node 2 and verify Image Services runs with no problems on Node 2.

Cluster Server Installation Completed

You have successfully installed and configured Image Services on your Cluster system.

4

Installing Image Services on an IBM PowerHA Cluster Server System

This chapter contains information for installing and configuring an AIX PowerHA Cluster Server system.

Install IBM PowerHA Cluster Server

The following high-level steps are necessary to make Image Services highly available in a cluster environment on UNIX platforms. These steps are described in more detail in the later sections of this chapter:

- Plan the system layout and parameters.
- Verify the prerequisites and create cluster resources.
- Install the appropriate AIX version software which supports PowerHA prior to installing or configuring any FileNet services for high availability.
- Configure the cluster groups.
- Install the appropriate RDBMS software on node1. This can be a remote install or it can be installed on the same cluster as the Image Services software. If RDBMS and Image Services are installed on the same cluster, a separate service group must be set up for both Image Services and the relational database.
- Install the FileNet Image Services software and the latest available Fix Pack on node 1.

- Switch cluster resources over to cluster node 2.
- Install the FileNet Image Services software and the latest available Fix Pack on node 2.
- Test the Image Services installation and cluster takeover behavior.

Image Services installation planning

An active/passive HA cluster with Image Services requires the following components:

- Two cluster nodes running IBM PowerHA
- Shared Storage for Image Services or Magnetic Storage and Retrieval (MSAR)
- A common local or remote database
- An Image Services license

HA limitations for Image Services:

- Maximum number of cluster modes is 2
- Combined and dual-server configurations are supported

The preferred way to install Image Services in an HA environment is to set up the HA cluster first and then install Image Services on the cluster, providing all of the resources that are necessary to run Image Services. The cluster controls the following resources that are required by Image Services:

- Virtual IP address (service address)
- Access to local and shared disks, including:

- Volume groups
- Logical volumes
- File systems

HACMP resource group

Before the Image Services installation starts, you must configure the cluster resources and make them available. The HACMP Resource Group (RG) controls the service address and the shared volume group with the raw logical volumes and file systems. The Image Services installation also requires common users and groups and a local /fnsw file system on each of the cluster nodes.

Prior to installing Image Services, you must disable all application server (AS) scripts on both nodes, if they exist.

Users and groups

The ID of the Image Services groups (GID) and users (UID) must be identical on each cluster nodes. You can create the users and groups by using Cluster-Single Point Of Control (C-SPOC) to achieve the uniqueness of the IDs on both cluster nodes. It is a good practice to choose one of the cluster nodes for all HACMP-related changes and to synchronize the cluster "one way" only, each time a change is made.

1 To add the group and user ID, using smitty, enter the following command:

 # smitty hacmp

2 Select System Management (C-SPOC) > HACMP Security and Users Management > Groups in an HACMP cluster > Add a Group to the Cluster.

You must leave the Group ID field blank to have C-SPOC generate the ID.

3 Select System Management (C-SPOC) > HACMP Security and Users Management > Users in an HACMP cluster > Add a User to the Cluster.

You must leave the User ID field blank to have C-SPOC generate the ID.

4 Make the user root (UID 0) part of the newly created fnusr and fnadmin groups.

Image Services Service Address

The Image Services service address is configured as an IP alias, which HACMP IP address takeover (IPAT) moves together with the Image Services resource group. IPAT using IP aliases is the default when HACMP networks are configured in SMIT.

1 For example, to configure the public network that is shared with the clients, using smitty, enter the following command:

 # smitty hacmp

2 Select Extended Configuration > Extended Topology Configuration > Configure HACMP Networks > Change/Show a Network in the HACMP Cluster.

3 For example, you can enter values similar to the following values:

```
Network Name: net_pub_1
Network Type: ether
Netmask: 255.255.255.0
Enable IP Address Takeover via IP Aliases: Yes
Network attribute: Public
```

IPAT using IP aliasing is faster and more reliable with cluster takeovers than IPAT using IP address replacement. However, IPAT using IP address replacement is required with certain types of networks that cannot process Address Resolution Protocol (ARP) cache updates and that require a Hardware Address Takeover (HWAT) of the NIC's hardware or Media Access Control (MAC) address. HWAT was often used with the old Image Services client, WorkForce Desktop (WFD). For descriptions of the two types of IPAT, refer to HACMP for AIX, Planning Guide, Version 5.4.1, SC23-4861-10. With IPAT using IP aliasing, the Image Services service address alias (9.30.188.78) can be brought up on any of the boot interfaces that are defined for the cluster. If the current network interface card (NIC) fails, HACMP will move the alias with an adapter swap to another interface. If the whole node fails, HACMP will move the alias as part of the resource group to the standby node.

AIX prerequisites for Image Services

In order for clients to properly communicate with clients, the ephemeral port setting must be set as shown in the following example:

```
# no -po tcp_ephemeral_high=65535
# no -po tcp_ephemeral_low=42767
# no -po udp_ephemeral_high=65535
# no -po udp_ephemeral_low=42767
```

Before the Image Services installation, add the Image Services domain name to /etc/hosts. This entry points to the (virtual) Image Services service address, which the PowerHA Resource Group provides. By using the highly available service address for Image Services, clients will connect to the correct (active) node of the cluster.

See the *IBM FileNet Image Services System Administrator's Companion for UNIX* for details about how to convert the NCH domain name to a host name. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Create cluster resources

Create cluster resources for the Image Services partitions on the shared storage using the permission and size settings as documented in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

- Create the /fnsw partition on local storage for each node.
- Create the /fnsw/local partition on the shared drive.
- Create the datasets on the shared drive.

Database Installation

Local and remote databases are supported. Refer to one of the following guidelines documents for setting up a remote database, depending on the type of RDBMS you are using:

- *Guidelines for Installing and Configuring IBM DB2 Software*

- *Guidelines for Installing and Configuring Oracle Software on UNIX Servers (Site-Controlled)*

To download these documents from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Verify Cluster Failover

Test the RDBMS service group to verify that the service group can failover to all nodes in the cluster, and verify that the shared storage can be accessed from all nodes.

Restriction The steps in this section apply only to servers requiring Image Services or RDBMS software.

Install Image Services Software

Install Image Services on each node in the cluster. Refer to the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system.

To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.

Restriction The steps in this section apply only to servers requiring Image Services software. This section does not apply to servers that do not require Image Services, such as remote relational database servers.

1 Enter the following series of commands to ready the volume group and user.

```
# mount -t fnvg
# mount | grep fnsw
# export DISPLAY=
```

2. Make sure the cluster group is online on the node you are currently installing.

3. On the active node in the cluster, install Image Services.

   - Image Services software (binary files) must be installed on the local drives of both nodes of the VCS Cluster.
   - Image Services configuration and data files (including MSAR and MKF); everything in /fnsw/local must be installed on the shared drive.
   - Image Services datasets under the /fnsw/dev/1 folder are actually links pointing to the real datasets on the shared drive.
   - Use fn_util init to initialize the datasets on the shared drive.

4. After you have installed and configured the Image Services software, shutdown the Image Services software manually and failover the cluster to the other node.

5. Install Image Services on the next node, specifying the same information entered during the installation on the first node. Image Services software must be installed on the local drive on each node.

6. After you have installed and configured the Image Services software on this node, shutdown the Image Services software manually.

Verify the Installation

Complete the following steps to verify the Image Services software installation:

1. Make sure the current node owns the shared drive.

2. The virtual IP address of the Image Services system must be resolvable, either by the Domain Name Service (DNS) or by an entry in the local hosts file.

3. Use the FileNet Image Services System Configuration Editor, fn_edit to make sure the Network Addresses tab has the DNS network name and the virtual IP address of the cluster.

   - In the Network Name field, enter the DNS name that resolves to the NCH network name of the system. This name may or may not be the same as the Server Name; however, it must be unique, less than 256 characters, and be composed only of alpha, digits, dot, dash, hyphens and underline characters. Spaces are not allowed.

   - Make sure the IP address in the Image Services resource group in the cluster has the same virtual IP address.

4. Start Image Services by entering the following command:

   initfnsw -y start

5. Check the status by entering the following command:

   initfnsw status

   Image Services should start successfully.

Attention If Image Services does not start successfully at this point, enter the following series of commands:

```
initfnsw -y stop
killfnsw -D -A -y
initfnsw start
```

6. Failover to the second node in the cluster.

7. Repeat steps 1 through 6 on the second node.

Verify Cluster Failover

After the entire cluster has been successfully configured, use PowerHA documentation procedures to verify that the cluster group can failover to each node in the cluster, and that the shared storage can be accessed from the active node.

- Start Node 1.
- Verify Image Services runs with no problems on Node 1.
- Failover to Node 2 and verify Image Services runs with no problems on Node 2.

Cluster Server Installation Completed

You have successfully installed and configured Image Services on your Cluster system.

5

Updating Image Services on a Cluster Server

This chapter contains information for updating Images Services on a Microsoft Cluster Server system or a VERITAS Cluster Server system.

Before you Begin

Before you can update the Image Services software, each server in the cluster (Node 1 and Node 2) must have the following software installed.

RDBMS Support Issues

Update RDBMS Software to a Supported Release

Refer to the *IBM FileNet Image Services, Image Services Resource Adapter, and Print Hardware and Software Requirements* for supported RDBMS versions. To download IBM FileNet documentation from the IBM support page, see **“Accessing IBM FileNet Documentation” on page 12**.

Verify Resources Added to Same Group

After the RDBMS update is completed, all RDBMS resources must reside in only one group. Check that all resources have been added to the same group.

Update Oracle Fail Safe Software (Optional/MSCS only)

Refer to the Oracle installation documentation found on the Oracle CD-ROM to install the Fail Safe software. You can download Oracle Fail Safe from Oracle's Web site.

Update FileNet Image Services Software

Update the FileNet software on the primary server local drive (Node 1) first.

Install the FileNet Image Services software on the Shared Drive and the local drives of each server as follows:

- FNSW (Image Services executables) will be installed on the local drive for each node.
- FNSW_LOC (Image Services Local Files) will be installed on the shared drive.

Important

Do Not use the same drive letter for the quorum drive and the shared drive. The quorum drive, which is used to store cluster configuration database checkpoints and log files, should be a separate drive from the Shared drive where Image Services shared files will reside. **The examples shown in this document, use Z or S for the shared drive**.

Attention

The shared drive can only be accessed by one node at a time.

Shut down Node 2.

Attention Because Cluster Service is installed on both nodes, it is important to **keep Node 2 off** so that the rebooting of Node 1 during setup does not cause the cluster supported components, including the shared drive, to failover to Node 2.

Updating FileNet Image Services Software on Nodes 1 and 2

1. If the RDBMS software is running on Node 2, fail it to Node 1 now.
2. Turn on power to the Node 1 server **only**. If you aren't already, logon as **Windows Administrator** or **Account Operator** for the domain.
3. Take the RDBMS resource offline, which shuts down the RDBMS.
4. Access the **Image Services for Windows Server** software on Node 1.
5. Follow the instructions in the *IBM FileNet Image Services Installation and Configuration Procedures* for your operating system to launch the Image Services installer. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 12**.
6. When the End User License Agreement screen displays, click **Yes** to accept the agreement.
7. When the Enter Network Name screen displays, enter the network name from your **"Installation Worksheet" on page 23**, if it is not already there.
8. Continue the Image Services software upgrade.

9 When the installation is complete, logon as the FileNet software user, such as **fnsw** configure the relational databases by entering the following command:

fn_setup_rdb -u

10 Reboot the Node 1 server and logon as the FileNet software user, such as **fnsw**.

11 Check the error logs for any errors. Resolve any errors before continuing.

12 Start the RDBMS.

13 Start FileNet Image Services.

14 Make sure that the RDBMS software and Image Services software is running successfully before you continue.

15 After you've verified that Node 1 has been successfully updated, take the Image Services resource group off line. This will shut down the Image Services software.

16 Power off Node 1.

17 Turn-on power to the Node 2 server.

18 After the Node 2 server comes up, logon as **Administrator** or **Account Operator**.

19 Verify that the Image Services resource group is on line.

20 Repeat Steps 4 - 14 on Node 2.

Restart Node 1

1. Turn-on power to the Node 1 server.
2. After the Node 1 server comes up, logon as **Administrator**.
3. Depending on which Node is the primary and which is the standby server, you might want to move system resources at this time. Use the Microsoft Cluster Administrator, VERITAS, or Oracle Fail Safe Manager to move the Image Services or RDBMS resource group to the preferred server.

Cluster Server Update Completed

You have successfully updated the Cluster Service on your system.

Appendix A – User and Group Security Configuration for Cluster

The Users and Groups should be set up on the Domain Controller according to this schema:

On the Domain Controller:

fnsw (User)
Member of Domain Users, FNADMIN, FNOP, FNUSR.

oracle (User)
Member of Domain Users, FNUSR.

FNADMIN (Security Group - Domain Local)
Members should be Domain/Administrator, Domain/fnsw.

FNOP (Security Group - Domain Local)
Members should be Domain/fnsw.

FNUSR (Security Group - Domain Local)
Members should be Domain/fnsw, Domain/oracle.

On the Image Services server:

ORA_DBA (Local Group)
Members should be Domain/fnsw, Domain/oracle, Domain/Administrator, Administrators.

Appendix B – Setting up a Secure Native Mode Domain Installation

Currently, Image Services requires that the person who installs cluster server must have Full Domain Administrator Rights in order to perform a normal installation. However, if you **do not** want the user who installs the Cluster Server system to have Full Domain Administrator Rights, you can use this appendix to create the **Installer** user (with limited rights), setup other required FileNet users and groups, and configure the node 1 and node 2 cluster servers.

Add Domain Users to Local Admin Group

In this procedure you will add the **Installer** and **fnsw** users to the Local Admin Group on each node.

1 At the Computer Management window, click **Groups**.

2 Double-click on the Administrators group icon. The Administrators Properties dialog box appears.

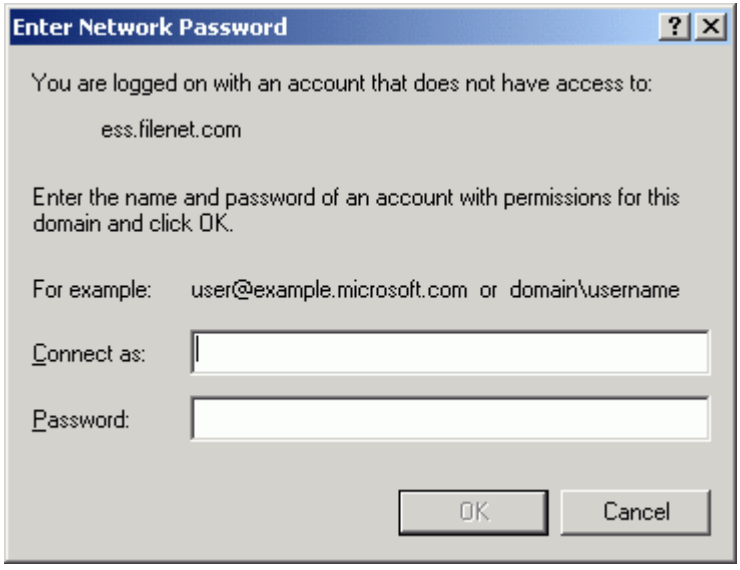
3 Click the **Add** button.

The Select Users and Groups dialog box appears.

4 In the Look in box, select **Domain Controller** from the pulldown menu. The Enter Network Password dialog box **might** appear.

5 a If the Enter Network Password dialog box appears, continue to **step 6**.

b If the Enter Network Password dialog box does not appear, skip to **step 7**.



6 Enter the Domain Windows Administrator ID and password, and click **OK**. The Select Users or Groups window displays.

7 Select the **Installer** user name from the Name list; then click **Add**.

8 Click **OK**. The Administrators Properties dialog box appears.

9 Click **Apply** to complete the procedure.

10 Repeat **step 3** through **step 9** to add the **fnsw** user.

After both the installer and fnsw users have been added to the Local Admin group, close the Computer Management window and continue to the next section.

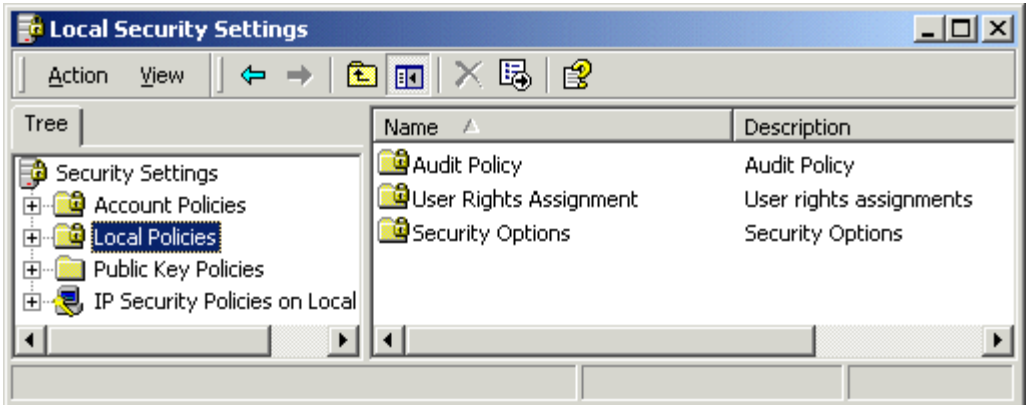
Modify Local Security Policy for the Domain Account (fnsw)

Modify the local security policy on both nodes to give the domain account permissions for the following policies:

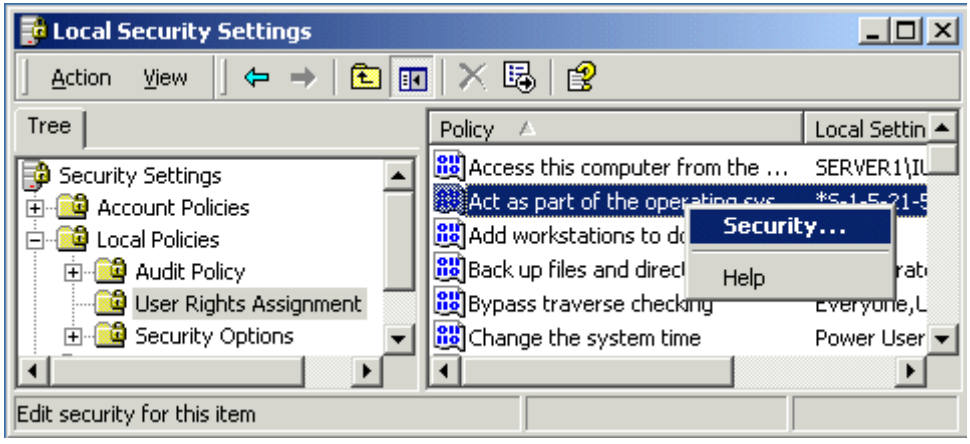
- Act as part of the operating System
- Log on as a service
- Increase quotas
- Replace a process token

1 From the Taskbar, click Start, point to Programs, point to the **Administrative Tools**, and click **Local Security Policy**.

The Local Security Settings screen opens.



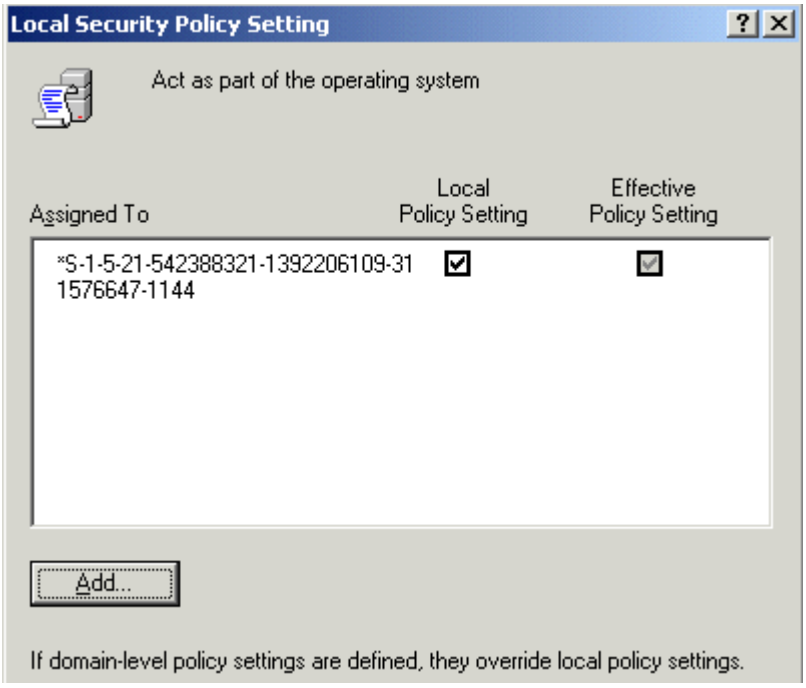
2 Expand the Local Policies folder and select the **User Rights Assignment** folder.



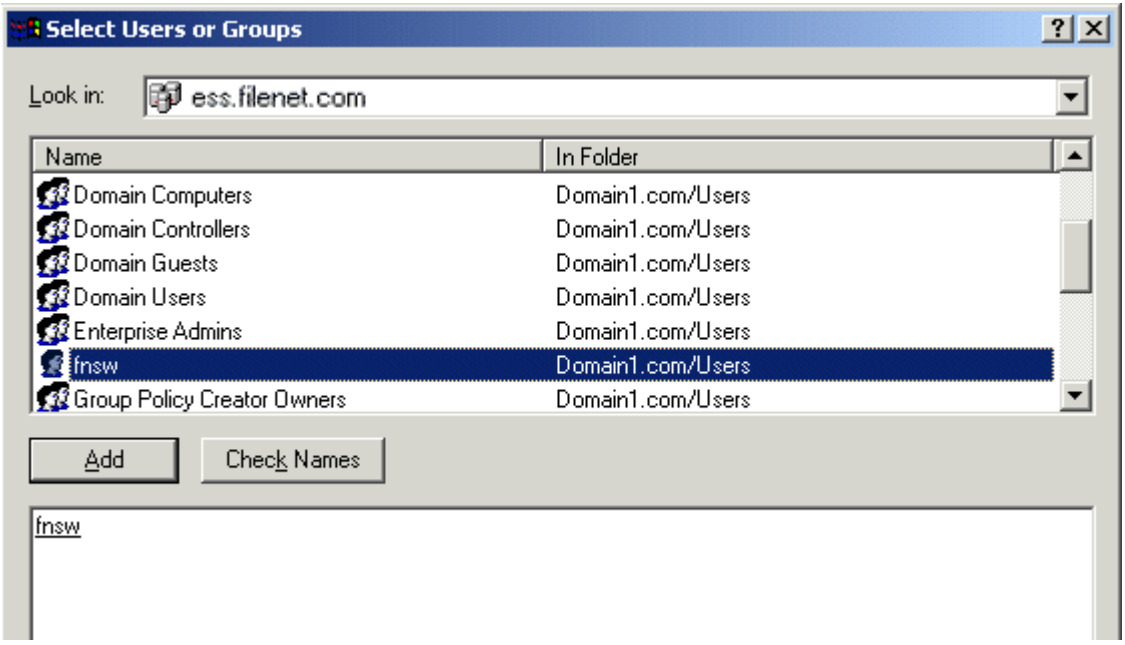
3 Right-click on the policy selection you want to add, and select **Security**.

Attention There are four policy selections that you will be adding. The first one, Act as part of the operating system, is shown in the following example screens.

The Local Security Policy Setting window opens.



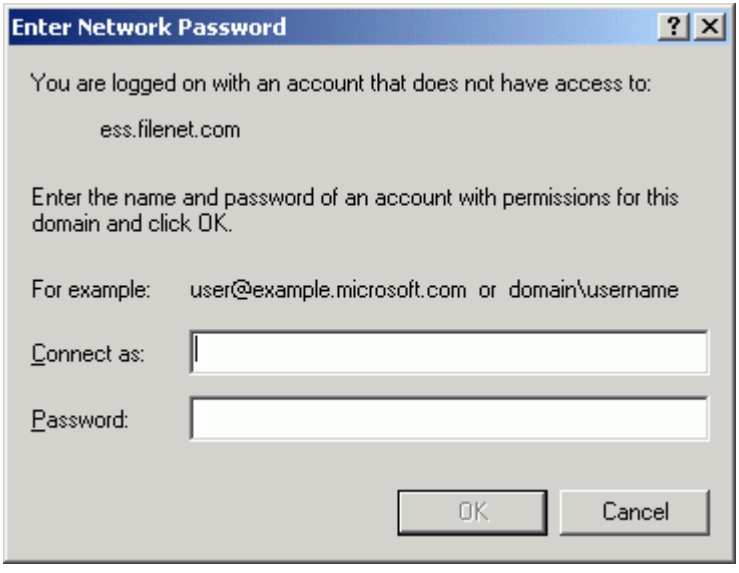
4 Click the **Add** button to open the Select Users or Groups window.



5 In the Look in box, select **Domain Controller** from the pulldown menu. The Enter Network Password dialog box **might** appear.

6 a If the Enter Network Password dialog box appears, continue to **step 7**.

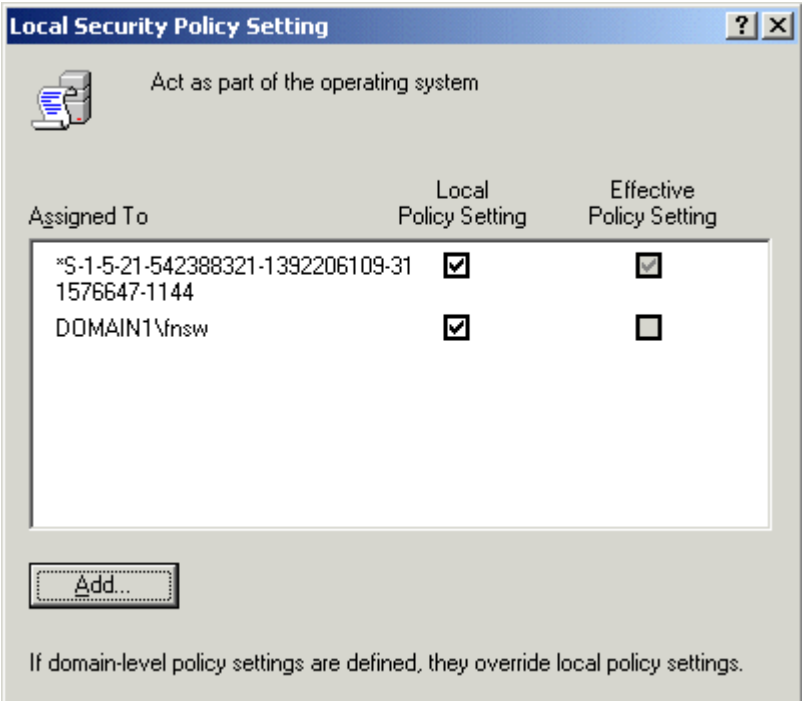
b If the Enter Network Password dialog box does not appear, skip to **step 8**.



7 Enter the Domain Windows Administrator ID and password, and click **OK**. The Select Users or Groups window displays.

8 Select the **fnsw** user, click the **Add** button, and click **OK**.

The Local Security Policy Setting window is updated (as shown below) to show that the domain user has been added to the security settings for the policy selected.



9 Click **OK** to close the Local Security Policy Setting window.

10 Repeat **step 3** through **step 9** for the remaining Policy selections.

After all Policy selections have been modified, close the Local Security Settings window.

Return to Main Body of this Document

After you have performed these procedures on both nodes, return to Chapter one and the section, **"Install Relational Database Software" on page 33** to continue with your cluster server system installation.

Appendix C – VERITAS Volume Replicator

Overview

VERITAS Volume Replicator (VVR) is the core of the disaster recovery environment. VVR manages the replicated volume group or RVG at each site and sends block level updates to the replicated sites.

VVR replicates volumes by intercepting block level writes to volumes in the RVG and duplicating the same write on the peer cluster or system at the secondary site. The caveat to VVR replication is the difference in I/O throughput between local volumes and the remote replicated volumes. Two replication modes exist to address this deficiency: Symmetric I/O and Asymmetric I/O.

- **Symmetric I/O** suspends write operations until all of the blocks on the primary site have been replicated to the secondary. This slows down I/O throughput.
- **Asymmetric I/O** allows the write operation to return as soon as it has been queued for replication and thus the impact to I/O is minimal. The downside to this mode is the propensity for the secondary site to be a number of I/O operations behind the primary.

  This solution then assumes the risk of losing the newest transactions that have not yet replicated when site failure occurs. This is the unfortunate reality of any disaster recovery solution.

Software

VERITAS Volume Replicator (VVR) provides the foundation for wide area availability, site migration, and disaster recovery. Based on VER-

ITAS Volume Manager, the VERITAS Volume Replicator mirrors data to remote locations over any IP network.

VERITAS Volume Manager (VxVM) provides storage management for enterprise computing and emerging Storage Area Network (SAN) environments. VERITAS Volume Manager provides a logical volume management layer which overcomes the physical restrictions of hardware disk devices by spanning logical volumes across multiple physical volumes.

Hardware

VVR does not require any additional hardware not outlined in the initial disaster recovery plan. It is important that WAN connectivity to the remote site should be redundant. This will greatly improve the reliability of the disaster recovery environment.

Installation

VVR does not interact directly with Image Services, so little needs to be configured to operate VVR. In general, a VVR secondary replication log (SRL) should use the same performance tuning as the application. For instance, if a file system with a logical volume spans six physical volumes, so should the SRL. This is critical to maintaining optimal performance of Image Services components.

Install VERITAS Volume Replicator

Follow the instructions in the VERITAS Volume Replicator documentation (*VERITAS Volume Replicator Administrator's Guide*) to install the appropriate software on all servers in the volume replication environment.

Complete the following steps after VERITAS Volume Replicator has been installed and replication has started.

Configure the Cluster Groups for Image Services

Configure the cluster groups with the following minimum resources:

- Shared storage resources (can include VERITAS Volume Group (VMDg) and MountV, or Mount for a basic disk)
- Clustered IP resource

UNIX Image Services VCS Cluster with VVR Replication

The following example is a sample Resource Dependency Tree for an Image Services group named **isvvrgrp** in a replication environment:

```
group isvvrgrp
{
RVG is_rvg
    {
    DiskGroup isdatadg
    IP isvvrip
        {
        NIC isvvrnic
        }
    }
}
```

UNIX example:

```
include "types.cf"
include "VVRTypes.cf"

cluster iscluster (
        UserNames = { admin = dijBidIfjEjjHrjDig }
        Administrators = { admin }
        CounterInterval = 5
        )

system hq-cfgaix5 (
        )

system hq-cfgaix6 (
        )

(continued on next page)
```

```
group isgrp (
        SystemList = { hq-cfgaix5 = 1, hq-cfgaix6 = 2 }
        AutoStartList = { hq-cfgaix5 }
        )

        Application is_app (
                User = fnsw
                StartProgram = "/fnsw/bin/initfnsw start"
                StopProgram = "/fnsw/bin/initfnsw stop"
                MonitorProcesses = { "TM_daemon -s" }
                )

        IP isip (
                Device = en0
                Address = "10.15.16.171"
                NetMask = "255.255.252.0"
                )

        Mount ismount (
                MountPoint = "/fnsw/local"
                BlockDevice = "/dev/vx/dsk/isdatadg/v_isdata"
                FSType = vxfs
                MountOpt = rw
                FsckOpt = "-y"
                )

        Mount msarmount (
                MountPoint = "/fnsw/msar"
                BlockDevice = "/dev/vx/dsk/isdatadg/msar"
                FSType = vxfs
                MountOpt = rw
                FsckOpt = "-y"
                )

(continued on next page)
```

```
(continued from previous page)

        NIC isnic (
                Device = en0
                )

        RVGPrimary rvg-pri (
                RvgResourceName = is_rvg
                AutoResync = 1
                )

        requires group isvvrgrp online local hard
        is_app requires isip
        is_app requires ismount
        is_app requires msarmount
        isip requires isnic
        ismount requires rvg-pri
        msarmount requires rvg-pri

group isvvrgrp (
        SystemList = { hq-cfgaix5 = 1, hq-cfgaix6 = 2 }
        AutoStartList = { hq-cfgaix5 }
        )

        DiskGroup isdatadg (
                DiskGroup = isdatadg
                )

        IP isvvrip (
                Device = en0
                Address = "10.15.16.126"
                NetMask = "255.255.252.0"
                )

(continued on next page)
```

```
(continued from previous page)

        NIC isvvrnic (
                Device = en0
                )

        RVG is_rvg (
                RVG = rvg_isdatadg
                DiskGroup = isdatadg
                SRL = srl_oradata
                )

        is_rvg requires isdatadg
        is_rvg requires isvvrip
        isvvrip requires isvvrnic
```

Windows Server Image Services VCS Cluster with VVR Replication

The following example is a sample Resource Dependency Tree for an Image Services group named **VVRGrp** in a replication environment:

```
group VVRGrp
{
VvrRvg rvg
     {
     IP VVRip
          {
          NIC VVRNic
          }
     VMDg VVRDg
     }
}
```

Windows Server Example:

```
include "types.cf"

cluster vcs-win-cluster (
        UserNames = { admin = iHIeHCgEHp }
        ClusterAddress = "10.14.101.102"
        Administrators = { admin }
        CredRenewFrequency = 0
        CounterInterval = 5
        )

system FONTANA (
        )

system NTNINER (
        )

group ClusterService (
        SystemList = { FONTANA = 0, NTNINER = 1 }
        UserStrGlobal = "LocalCluster@https://10.14.100.90:8443;"
        Authority = 1
        AutoStartList = { FONTANA, NTNINER }
        )

        IP csg_ip (
                Address = "10.14.101.102"
                SubNetMask = "255.255.252.0"
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )

(continued on next page)
```

```
(continued from previous page)

        NIC csg_nic (
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )

        VRTSWebApp VCSweb (
                AppName = vcs
                InstallDir @FONTANA = "C:\\\\\\\\Program
Files\\\\\\\\VERITAS\\\\\\\\VRTSweb\\\\\\\\VERITAS"
                InstallDir @NTNINER = "C:\\\\\\\\Program
Files\\\\\\\\VERITAS\\\\\\\\VRTSweb\\\\\\\\VERITAS"
                )

        csg_ip requires csg_nic
        VCSweb requires csg_ip


group VVRGrp (
        SystemList = { FONTANA = 0, NTNINER = 1 }
        )

        IP VVRip (
                Address = "10.14.101.110"
                SubNetMask = "255.255.252.0"
                MACAddress @FONTANA = "00-C0-9F-27-14-E3"
                MACAddress @NTNINER = "00-C0-9F-35-0D-28"
                )

        NIC VVRNic (
                MACAddress @FONTANA = "00-C0-9F-27-14-e3"
                MACAddress @NTNINER = "00-C0-9F-35-0D-28"
                )

(continued on next page)
```

```
(continued from previous page)

        VMDg VVRDg (
                DiskGroupName = winvcs
                DGGuid = ebc05a43-11d4-4d2a-9177-f4e638817954
                )

        VvrRvg rvg (
                RVG = rvg_winvcs
                VMDgResName = VVRDg
                IPResName = VVRip
                SRL = rep_log
                RLinks = { "" }
                )

        VVRip requires VVRNic
        rvg requires VVRip
        rvg requires VVRDg

group fn_sg (
        SystemList = { FONTANA = 0, NTNINER = 1 }
        )

        GenericService IS_ControlService (
                ServiceName = "IS ControlService"
                UserAccount = fnsw
                Password = hvlTitKtw
                Domain = "vcs.net"
                )

        IP is_ip_1_1 (
                Address = "10.14.101.106"
                SubNetMask = "255.255.252.0"
                MACAddress @FONTANA = "00:C0:9F:27:14:E3"
                MACAddress @NTNINER = "00:C0:9F:35:0D:28"
                )
 (continued on next page)
```

```
(continued from previous page)

        MountV mount (
                MountPath = I
                VolumeName = FileNetVol
                VMDGResName = VVRDg
                )

        NIC ISNic (
                MACAddress @FONTANA = "00-C0-9F-27-14-e3"
                MACAddress @NTNINER = "00-C0-9F-35-0D-28"
                )

        requires group VVRGrp online local hard
```

Install Image Services Software

The steps in this section apply only to servers requiring Image Services software.

Attention This section does **not** apply to servers that do not require Image Services, such as remote relational database servers.

1. Install Image Services software on the servers in the cluster that will be replicated. Follow the steps in the section, **"Install FileNet Software" on page 39**.
2. Use VVR to failover the cluster servers and datasets on the shared disk.
3. Repeat the installation of Image Services software on the standby system as though it were a cluster node.

Switching to the Standby (Replicated) System

When the time comes to switch to the standby (replicated) system, VVR reassigns the datasets and file systems from the production system to the standby system. See the VERITAS documentation for complete details.

By Domain Name Services (DNS)

You must modify the DNS server to change the network addresses either manually or using VERITAS Cluster Server.

By Adding or Changing IP Addresses in Image Services

If DNS is not being used, the Image Services System Administrator needs to log onto the standby Image Services root/index server and modify the network addresses appropriately using the Image Services Configuration Editor, **fn_edit**.

To change network addresses in Image Services:

1. Launch the Image Services Configuration Editor on the standby system.

Attention You may receive some error messages resulting from the mismatched network addresses, but you can ignore them.

2. Click the **Network Addresses** tab.
3. In Network Address column modify the address to the IP address of the standby Image Services system.
   - In the Network Name field, enter the DNS name that resolves to the NCH network name of the system. This name may or may not

be the same as the Server Name; however, it must be unique, less than 256 characters, and be composed only of alpha, digits, dot, dash, and underline characters. Spaces are not allowed.

The NCH network name resolves to either the production system when in production mode or the standby system in standby mode. It is recommended that this name be an alias to the virtual cluster name when in production mode and then switched to be an alias to the standby system when in standby mode. For example, DNS would look like this:

- In production mode:
  10.15.17.54 iscluster isnchname
  77.41.41.04 isstandby

- In standby mode:
  10.15.17.54 iscluster
  77.41.41.04 isstandby isnchname

- The first Network Address is the IP address of the VCS cluster.
- The second Network Address is the IP address of the VVR standby system.

4 Click **File** then click **Exit**.

5 When asked if you would like to save your changes, select **yes**.

6 Rebuild the system configuration files by entering:

fn_build -a

7 Restart Image Services:

initfnsw restart

8 If necessary, clear any Image Services resource faults.

9 After Image Services has successfully restarted, it will be using the standby system.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14 Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims

related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **www.ibm.com/legal/copytrade.shtml**.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names might be trademarks of IBM or other companies.

U.S. Patents Disclosure

This product incorporates technology covered by one or more of the following patents: U.S. Patent Numbers: 6,094,505; 5,768,416; 5,625,465; 5,369,508; 5,258,855.

Product Number: 5724-R95

Printed in USA

SC19-3303-00