# Contents

**Contents**

- **Preface** ................................................................. v
  - Getting Help ............................................................. v
  - Documentation Set .................................................... v
  - Documentation Conventions ....................................... vi

**Chapter 1 Preinstallation Procedures** ................................................. 1
  1.1 Procedures Related to Installing Linux .............................................. 1
  1.2 Procedures That Configure the Operating System ................................. 2
  1.3 Procedures That Set Up Networks and Clients ...................................... 3

**Chapter 2 Performing a Standard Installation** ........................................ 5
  2.1 Overview of the Standard Installation Procedure ................................. 5
  2.2 Installing the Fusion Manager Software ............................................... 6
  2.3 Installing the Segment Server Software .............................................. 6
  2.4 Installing the Linux Fusion Client Software .......................................... 7
  2.5 Installing and Registering the Windows Fusion Client ............................ 8
  2.6 Verifying Installation Success ........................................................... 8
  2.7 Troubleshooting Problems with a Standard Installation ......................... 9
    - **2.7.1 ibrixinit Hangs** ........................................................................... 9
    - **2.7.2 Cannot Install the Fusion Manager** ............................................. 9
    - **2.7.3 Fusion Manager or Segment Server Services Do Not Start** .......... 9
    - **2.7.4 Linux Fusion Client Services Do Not Start** ................................. 9
    - **2.7.5 Windows Fusion Client Driver Signing Error** ............................... 9

**Chapter 3 Installing the Fusion Manager High Availability Software** ................ 11
  3.1 Fusion Manager High Availability Prerequisites .................................... 11
  3.2 Basic and Extended Installations ....................................................... 12
  3.3 Fusion Manager High Availability Installation Scenarios ....................... 15

**Chapter 4 Performing an OCS Installation** ............................................. 17
  4.1 Installation Overview ........................................................................... 17
  4.2 Installing Required Software on the Front End ...................................... 17
  4.3 Adding the IBRIX Client Kit ............................................................. 18
  4.4 Client Installation .............................................................................. 19
    - **4.4.1 New Clients** ........................................................................... 19
    - **4.4.2 Re-Installing Clients** ............................................................. 20

**Chapter 5 Uninstalling IBRIX Fusion** ................................................... 21
  5.1 Uninstalling Linux Fusion Clients ....................................................... 21
  5.2 Uninstalling Windows Fusion Clients ............................................... 21
  5.3 Uninstalling Segment Servers in a SAN Environment ............................ 22
Preface

Getting Help

Contact IBRIX Customer Support with any questions or concerns about your IBRIX Fusion Server cluster:

- **Email:** support@ibrix.com
- **Telephone:** 1-800-92-IBRIX (1-800-924-2749)

Have the following information available:

- Your case number, if one is open.
- Your IBRIX Customer Support number.
- The Linux operating system and kernel version(s) used in your cluster.
- The software version number of all installed IBRIX Fusion software. To obtain software version numbers, run the `ibrix_version -l` command on the Fusion Manager.

Documentation Set

The documentation set for this version of IBRIX Fusion includes:

- *IBRIX Fusion Installation and Upgrade Guide* (PDF, this document)
- *IBRIX Fusion User's Guide* (PDF)
- *IBRIX Fusion Data Tiering Reference Guide* (PDF)
- *IBRIX Fusion Continuous Remote Replication Reference Guide* (PDF)
- *IBRIX Fusion File Cloning Reference Guide* (PDF)
- *IBRIX Fusion Snapshot Reference Guide* (PDF)
- *IBRIX Fusion Manager High Availability Reference Guide* (PDF)
- *IBRIX Fusion CLI Reference Guide* (PDF)
- Man pages for IBRIX Fusion commands (automatically installed)
- Online help for the Fusion Manager GUI and the Windows Fusion Client GUI
Documentation Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ibrixhome&gt;</code></td>
<td>Home directory for IBRIX Fusion.</td>
</tr>
<tr>
<td><strong>Italic text</strong></td>
<td>Files and directories; physical or logical volume names, mountpoints, or cluster entities.</td>
</tr>
<tr>
<td><strong>Fixed-width text</strong></td>
<td>Code, commands, keywords, command output</td>
</tr>
<tr>
<td><em>Italicized fixed-width text</em></td>
<td>Variables representing context-specific values.</td>
</tr>
<tr>
<td><strong>Bold fixed-width text</strong></td>
<td>Text that you enter as shown.</td>
</tr>
<tr>
<td>Square brackets: [-h HOSTLIST]</td>
<td>Enclose an optional command argument.</td>
</tr>
<tr>
<td>Braces: {tcp</td>
<td>udp}</td>
</tr>
</tbody>
</table>

The IBRIX Fusion software packages are installed into the directory `/usr/local/ibrix` by default. You can specify a different directory. Regardless of point of installation, the home directory is designated as `<ibrixhome>` in all IBRIX documents.
This section describes procedures that you must perform before installing the IBRIX Fusion software on any machines. The pre-installation procedures that are required for a given machine depend on the software that will be installed on it.

1.1 Procedures Related to Installing Linux

Perform these procedures if you will be installing the Linux operating system on a machine prior to installing any IBRIX Fusion software.

<table>
<thead>
<tr>
<th>Component</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Servers</td>
<td>(Recommended) Configure the base operating system with <code>kdump</code> enabled.</td>
</tr>
<tr>
<td>Fusion Manager Segment Servers</td>
<td>For machines that are connected to SAN storage: Physically disconnect the machines from their storage. This prevents loading the IBRIX Fusion software to SAN storage instead of to the machines’ local disks.</td>
</tr>
<tr>
<td>Fusion Manager Segment Servers</td>
<td>Check each machine’s boot order to verify that it seeks a boot from its hard drive before requesting a boot from its network connection. The default boot order on some machines is reversed, which will result in a loading loop.</td>
</tr>
<tr>
<td>Fusion Manager Segment Servers</td>
<td>Install the correct version of the operating system. Accept all packages for the installation. Do not add to or delete from the package list.</td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td><code>xinetd-2.3.14-10.el5</code> is required in IBRIX v4.3 for the Fusion Manager and the Segment Servers. Verify that the <code>xinetd</code> rpm is installed on each server. Use the command `rpm -qa</td>
</tr>
</tbody>
</table>
1.2 Procedures That Configure the Operating System

Table 1-2 Operating System Configuration

<table>
<thead>
<tr>
<th>Component</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fusion Manager</td>
<td>Disable Security-Enhanced Linux (SELinux). IBRIX Fusion services will not start if SELinux is enabled.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Disable DHCP. IBRIX Fusion requires static IP addresses to communicate.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Using hostname, check that the hostname returned is the expected name and that it can be resolved by its name and IP address.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Ensure that all machines’ clocks are synchronized (for example, via Network Time Protocol).</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>In the /etc/hosts file, change the name associated with the loopback address (typically, 127.0.0.1) to localhost. A correct /etc/hosts file should include this uncommented entry: 127.0.0.1 localhost.localdomain localhost</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Ensure that IBRIX Fusion is the only application on this machine that requires access to PostgreSQL. IBRIX Fusion requires exclusive use of PostgreSQL on the Fusion Manager. The IBRIX Fusion installer removes the PostgreSQL associations for other applications running on the designated machine.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Verify that the necessary PostgreSQL RPMs provided in the base operating system are installed. Run: rpm -qa</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Verify that the necessary SNMP RPMs provided in the base operating system are installed. Run: rpm -qa</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
</tbody>
</table>
### 1.3 Procedures That Set Up Networks and Clients

<table>
<thead>
<tr>
<th>Component</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fusion Manager</td>
<td>If you have created an IBRIX user and group, delete them. IBRIX Fusion requires exclusive use of the IBRIX user and group.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>In each machine’s base operating system, set up the network interface that will be used for Cluster network communications. Set up only one Cluster interface. If you will be bonding network interfaces for use as the Cluster interface, do it before installing IBRIX Fusion.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Fusion Manager</td>
<td>Make sure that all IBRIX Fusion machines can communicate with the Fusion Manager machine and with each other. IBRIX Fusion requires successful ping -s 16000 communications between all machines.</td>
</tr>
<tr>
<td>Segment Servers</td>
<td></td>
</tr>
<tr>
<td>Linux Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td></td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td>Verify that all Win clients have installed Microsoft .NET Framework Version 2.0. Verify that all Win clients are members of a security domain managed by Active Directory. The Active Directory server that executes Fusion Client queries requires Windows Services for UNIX (SFU) 3.5. If that server is running Windows Server 2003 SP2, install the SFU package. If running Windows Server 2003 R2, the SFU software is built-in.</td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td>On all Windows Fusion Client machines, install the Windows Fusion Client (contact IBRIX for the installer file if necessary).</td>
</tr>
<tr>
<td>Windows Fusion Clients</td>
<td>Configure firewalls to allow communication between the client and the cluster.</td>
</tr>
</tbody>
</table>
Chapter 2 Performing a Standard Installation

2.1 Overview of the Standard Installation Procedure

2.2 Installing the Fusion Manager Software

2.3 Installing the Segment Server Software

2.4 Installing the Linux Fusion Client Software

2.5 Installing and Registering the Windows Fusion Client

2.6 Verifying Installation Success

2.7 Troubleshooting Problems with a Standard Installation

A standard installation installs the IBRIX cluster components—the Fusion Manager (with or without the optional Fusion Manager High Availability), Segment Servers, and Fusion Clients.

2.1 Overview of the Standard Installation Procedure

The exact contents of the distribution package depends on the terms of your license. At a minimum, you will receive the IBRIX Fusion Manager and Segment Server software, an IBRIX Fusion license, and product documentation. The package will include Fusion Client software if they are licensed.

The software is delivered as one or more tar files or individual RPMs or on DVD, depending on your site requirements. Windows Fusion Client software is supplied as a Windows MSI file.

Installing IBRIX Fusion on a standard cluster involves the following steps:

1. Complete all required preinstallation procedures (refer to Chapter 1).
2. Install the Fusion Manager software on one Linux machine. The Fusion Manager monitors cluster status, maintains the configuration database, applies cluster topology changes, and administers such cluster operations as failover and statistics gathering.
   Optional: Install the Fusion Manager software on a second machine, and install Fusion Manager High Availability software on both machines. This extends failover protection to the Fusion Manager and its database.
3. Install the Segment Server software on one or more Linux machines.
4. If your cluster design includes Fusion Clients, install either the Linux or the Windows Fusion Client software on the client machines.
5. Verify that the installation was successful.
2.2 Installing the Fusion Manager Software

The Fusion Manager must be installed first. Other component installations request information about it. To install, follow these steps:

1. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an `ibrix` subdirectory containing the installer program. For example, if you expand the tarball in `/root`, the installer is in `/root/ibrix`.

2. Change to the installer directory.
   
   To install into the default IBRIX home directory (`/usr/local/ibrix`), enter:
   
   ```
   ./ibrixinit -tm -C INTERFACE
   ```

   where `INTERFACE` specifies the network interface to use for cluster communication, for example `eth1`. This interface must be set up prior to IBRIX Fusion installation.

   To install into a different directory:
   
   ```
   ./ibrixinit -tm -C INTERFACE -P PATHNAME
   ```

   Normally, the cluster name defaults to the Fusion Manager node name, but Fusion Manager High Availability users should assign a cluster name as part of the installation so that the Fusion Manager name resolves correctly, regardless of which Fusion Manager is active. The name should be unique in the cluster:

   ```
   ./ibrixinit -tm -C INTERFACE -c CLUSTER
   ```

3. Copy the IBRIX Fusion license file that you obtained from IBRIX (`license.rc`) to the `<ibrixhome>` directory. Overwrite the file placed there by the installation with your file.

4. Activate the IBRIX Fusion license:

   ```
   <ibrixhome>/bin/ibrix_license -a
   ```

   License activation starts the Fusion Manager.

5. Make sure that the correct license is installed:

   ```
   <ibrixhome>/bin/ibrix_license -i
   ```

   Check the configuration details, your IBRIX Customer Support number, and the support start and stop dates. If you installed the wrong license, copy the correct license to `<ibrixhome>`, activate the license, and verify that it is correct.

6. Verify that the Fusion Manager is operational:

   ```
   /etc/init.d/ibrix_fusionmanager status
   ```

   The status command will confirm if the correct services (Quota Monitor, postmaster, and Fusion Manager Daemon) are running.

7. If you plan to implement Fusion Manager High Availability in this cluster, repeat these instructions to install the Fusion Manager on a second machine.

2.3 Installing the Segment Server Software

Perform this installation procedure on each machine that you want to be a cluster Segment Server, up to the limit allowed by your license.

Before performing this procedure, make sure that the IBRIX Fusion license has been activated and that the Fusion Manager is running.

To verify that the license has been activated, run `ibrix_license -i` on the Fusion Manager and check the output to make sure that `Active : Yes` appears in it.

```
<ibrixhome>/bin/ibrix_license -i
``` 

To determine whether the Fusion Manager is running, execute:

```
/etc/init.d/ibrix_fusionmanager status
```

If the Fusion Manager is stopped, run:

```
/etc/init.d/ibrix_fusionmanager start
```
Note!  
NFS services are disabled by default on all newly installed Segment Servers. 
IBRIX Fusion manages NFS services, turning them on or off as needed.

On each Segment Server machine:

1. Expand the distribution tarball or mount the distribution DVD in a directory of your 
   choice. This creates an ibrix subdirectory containing the installer program. For example, if 
you expand the tarball in /root, the installer is in /root/ibrix.

2. Change to the installer directory.
   To install into the default IBRIX home directory (/usr/local/ibrix) enter:
   ```
   ./ibrixinit -ts -C CLUSTER_INTERFACE -i CLUSTER_IP_ADDRESS
   ```
   Where CLUSTER_INTERFACE specifies the interface to be used for cluster 
   communication, and CLUSTER_IP_ADDRESS is either the name or IP address of your 
   Fusion Manager. To install into a different directory:
   ```
   ./ibrixinit -ts -C CLUSTER_INTERFACE -i CLUSTER_IP_ADDRESS -P PATHNAME
   ```

3. Verify that the Segment Server is operational:
   ```
   /etc/init.d/ibrix_server status
   ```
   The status command will confirm if IBRIX services are running.

2.4 Installing the Linux Fusion Client Software

Perform this installation procedure on each machine that you want to be a Fusion Client, up to 
the limit allowed by your license.

Complete all required preinstallation procedures before installing the Linux Fusion Client 
software on any machines (refer to Chapter 1).

1. Expand the distribution tarball or mount the distribution DVD in a directory of your 
   choice. This creates an ibrix subdirectory containing the installer program. For example, if 
you expand the tarball in /root, the installer is in /root/ibrix.

2. Change to the installer directory.
   To install into the default IBRIX home directory (/usr/local/ibrix), enter:
   ```
   ./ibrixinit -tc -C CLUSTER_INTERFACE -i CLUSTER_IP_ADDRESS
   ```
   where CLUSTER_INTERFACE specifies the interface to be used for cluster 
   communication, and CLUSTER_IP_ADDRESS is either the name or IP address of your 
   Fusion Manager. To install into a different directory:
   ```
   ./ibrixinit -tc -C CLUSTER_INTERFACE -i CLUSTER_IP_ADDRESS 
   -P PATHNAME
   ```

3. Verify that the Fusion Client is operational:
   ```
   /etc/init.d/ibrix_client status
   ```
   The status command will confirm if IBRIX services are running.

4. If you installed from the distribution CD, unmount it.
2.5 Installing and Registering the Windows Fusion Client

Complete all required preinstallation procedures before installing the Windows Fusion Client software (refer to Chapter 1).

Copy the Windows Installer’s MSI file to each Windows Fusion Client machine, up to the license limit. Launch the installer and follow the instructions to complete installation.

Included in the installation is an IBRIX Virtual Bus Enumerator, which creates a Virtual IBRIX Disk Device on the bus and registers a plug-and-play driver to service it. This virtual partition provides the mountpoint for the IBRIX file system.

To verify the installation of the virtual bus and driver, check:

- In Control Panel > System > Hardware Tab > Device Manager, in the devices tree under System Devices, look for the IBRIX Virtual Bus Enumerator.
- In Control Panel > System > Hardware Tab > Device Manager, look for the IBRIX Virtual Disk Device.
- In Control Panel > Administrative Tools > Computer Management, in the hierarchy under Computer Management (Local) /Storage/Disk Management, look for the volume Virtual IBRIX Disk.

**Note!** This volume is shown with a capacity of 2T, the maximum size of a disk in a 32-bit Windows system. Your actual volume may be bigger or smaller, but because of synchronization issues, the disk appears as 2T regardless of actual size.

The installed files are `c:\windows\system32\drivers\idef.sys` and `virtbd.sys`.

1. Launch the Windows Fusion Client GUI and navigate to the Registration tab.
2. Select the client’s IP address from the drop-down list.
3. Enter the Fusion Manager name into the FM Host Name field.
4. Check Recover Registration to avoid having to re-register this client if you reinstall it. This option automatically retrieves the Fusion Client’s ID from the Fusion Manager.
5. To start the Windows Fusion Client service, check Start Service After Registration. It is not mandatory to start the Fusion Client service following registration. To start the client service at a later time, use the Windows Services Manager.
6. Click Register.
7. On the Active Directory Settings tab, click Verify to validate that the proxy user has access to Active Directory for query mapping.
8. On the client’s Mount tab, select the Fusion Manager in the drop-down list if necessary and enter the file system name. To mount the IBRIX file system to a Windows drive letter, click Mount.
9. If you are using Remote Desktop to access the client and the drive letter does not display, log out and log back in. This is a known limitation of Windows Terminal Services when exposing new drives.

2.6 Verifying Installation Success

To verify that the entire installation was successful, on the Fusion Manager run:

```
<ibrixhome>/bin/ibrix_host -l
<ibrixhome>/bin/ibrix_version -l
```

The `ibrix_host` output lists all Segment Servers and Fusion Clients that are installed.

The `ibrix_version` output displays the same version number in the FILE SYSTEM field and the IAD/FS field for each host.

If the output for either of these commands is not correct, contact IBRIX Customer Support.
2.7 Troubleshooting Problems with a Standard Installation

2.7.1 ibrixinit Hangs

The RPM database is corrupted, a problem caused by bugs in the Redhat Package Manager. Rebuild the RPM database using the following commands and then attempt the install/upgrade again. Note that `rm` is followed by a space and then two underscores, and `rpm` is followed by a space and then two dashes:

```
cd /var/lib/rpm
rm __*
rpm --rebuilddb
```

2.7.2 Cannot Install the Fusion Manager

The name associated with the loopback address (typically, 127.0.0.1) is not set correctly on the Fusion Manager. In the `/etc/hosts` file, change the name associated with the loopback address to `localhost`, as shown:

```
# more /etc/hosts
# Do not remove the following line, or various
# programs that require network functionality
# will fail.
127.0.0.1 localhost.localdomain localhost
```

2.7.3 Fusion Manager or Segment Server Services Do Not Start

SELinux may be enabled. To determine the current state of SELinux, execute `getenforce`. If it returns `enforcing`, disable SELinux with either of these commands:

```
setenforce Permissive
setenforce 0
```
To permanently disable SELinux, edit its configuration file (`/etc/selinux/config`) to set `SELINUX=parameter` to either `permissive` or `disabled`. SELinux will be stopped at the next boot.

2.7.4 Linux Fusion Client Services Do Not Start

There are two possible causes:

1. SELinux is enabled. See the preceding section for the fix.
2. You used method 2 to install the Fusion Client, but you did not perform the final step of the procedure, which registers the machine with the Fusion Manager. Follow the instructions on page 7 for registering the Fusion Client.

2.7.5 Windows Fusion Client Driver Signing Error

The IBRIX plug-and-play driver must be signed and certified by a recognized Certification Authority to guarantee Windows operability. If your installation reports a driver signing problem, navigate to Control Panel > System > Hardware tab > Driver Signing.

On the Driver Signing window, select **Ignore - Install the software anyway and don’t ask for my approval**, or **Warn - Prompt me each time to choose an action**. You will be able to install with the IBRIX test certificate but this certificate may limit your ability to perform automated installations.

The installed files are `C:\Windows\System32\drivers\idef.sys` and `virtbd.sys`. 
Chapter 3 Installing the Fusion Manager High Availability Software

3.1 Fusion Manager High Availability Prerequisites .......................................................... 11
3.2 Basic and Extended Installations .................................................................................. 12
3.3 Fusion Manager High Availability Installation Scenarios .............................................. 15

The Fusion Manager High Availability option extends automated failover protection to the Fusion Manager and its database. It utilizes two hosts on which Fusion Manager is installed, assigning to one the primary High Availability role and the second the standby role. Follow the installation scenario in Section 3.3, Fusion Manager High Availability Installation Scenarios, appropriate to your situation.

Fusion Manager High Availability is based on the Linux-HA Heartbeat service and IPMI. Communication between nodes uses SSH over a private interface; backup files are copied from active node to standby node with SCP. These components must be in place before you can run this installation script.

Note! IBRIX recommends that you install Fusion Manager High Availability using a bonded interface for IPMI. If you do not and the IPMI interface encounters a problem, Fusion Manager High Availability will not function because the standby Fusion Manager cannot power manage the primary Fusion Manager.

3.1 Fusion Manager High Availability Prerequisites

<table>
<thead>
<tr>
<th>Table 3-1 Fusion Manager High Availability Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPMI or ILO power management</td>
</tr>
<tr>
<td>Clock synchronization</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td>Linux-HA</td>
</tr>
</tbody>
</table>
3.2 Basic and Extended Installations

The Fusion Manager High Availability software is installed by the `install_fmha` script. This interactive script can be run to configure a minimal set of installation options (basic), or the full set of options (extended). The basic set configures what your site needs to run Fusion Manager High Availability. The extended set prompts for additional addresses and backup options.

Select the node you want to use as the primary node, and run `install_fmha` on that machine.

To start the installation script for basic installation, enter:

```
<ibrixhome>/fm-ha/install_fmha
```

To start the installation script for extended installation, enter:

```
<ibrixhome>/fm-ha/install_fmha -x
```

Default values within the script, if any, are shown in square brackets. If this script has been run previously, the last value entered is shown in the brackets and used as the default, and pressing Enter accepts that value.

The sample configuration in Figure 3-1 and the example script following it are based on the same set of NICs and addresses. In the example script that follows, what the user types is shown in **bold**, and refers to addresses in Figure 3-1. Note that some fixed addresses are not used by the script.

<table>
<thead>
<tr>
<th>Networks</th>
<th>Network interfaces must be configured and operating before you begin this installation. Refer to Figure 3-1 for an example of the cluster network fixed addresses that must be predefined. Neither the user network nor the secondary cluster network are required for Fusion Manager High Availability operation, but they are also included. The shared addresses are system-assigned.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fusion Manager</td>
<td>The Fusion Manager must be installed on both hosts and running on one, with failover enabled. Its license must be active.</td>
</tr>
</tbody>
</table>

---

**Table 3-1  Fusion Manager High Availability Prerequisites**

<table>
<thead>
<tr>
<th>Network</th>
<th>Cluster Network</th>
<th>User Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>192.168.17.172</td>
<td>192.168.12.40</td>
</tr>
<tr>
<td>eth0:1</td>
<td>10.1.1.40</td>
<td>10.1.1.50</td>
</tr>
<tr>
<td>eth1</td>
<td>192.168.17.173</td>
<td>192.168.12.41</td>
</tr>
</tbody>
</table>

---

**Figure 3-1  Fusion Manager High Availability installation and configuration overview**
Note! IBRIX recommends that you assign the heartbeat and IPMI functions to addresses on different interfaces. Assigning both to the same interface can result in network errors.

Note! This example documents an installation for systems using IPMI power management. The questions are the same for ILO systems.

--- System Network Configuration ---

Enter the IP address of this node: **192.168.17.172**

The pre-existing IP address of the host where the script is run, the de facto primary Fusion Manager node. This node can be on either the user or cluster network, and here we use the cluster network. It must be accessible to all Fusion Manager machines. In Figure 3-1, this is eth0 address on Fusion Manager 1.

Enter the IP address of the other node: **192.168.17.173**

The pre-existing IP address of the second host. This node must be on the same network as the primary and it must be accessible to all cluster machines. In Figure 3-1, this is eth0 address on Fusion Manager 2.

Enter the heartbeat IP address of this node [192.168.17.172] : **192.168.17.172**

The pre-existing IP address on the primary node that Fusion Manager High Availability will use to send heartbeat messages. The heartbeat address must be on a physical interface and not on a virtual interface. In Figure 3-1, this is the eth0 address on Fusion Manager 1. The IP address supplied in question 1 is used as the default here. Appears in extended installations only. In the basic installation, the host’s IP address doubles as the heartbeat address.

Enter the heartbeat IP address of the other node [192.168.17.173] : **192.168.17.173**

The pre-existing IP address on the standby node that Fusion Manager High Availability will use to send heartbeat messages. The heartbeat address must be on a physical interface and not on a virtual interface. In Figure 3-1, this is the eth0 address on Fusion Manager 2. The IP address supplied in question 2 is used as the default here. Appears in extended installations only. In the basic installation, the host’s IP address doubles as the heartbeat address.

Enter the power source used by 192.168.17.172 (ilo or ipmi): **ipmi**

Fusion Manager High Availability is compatible with two server management technologies, Integrated Lights-Out (ILO) and the Intelligent Platform Management Interface (IPMI).

Enter the power source BMC username for 192.168.17.172 [ibrix]: **ipmi-username**

A user-defined name for the IPMI administrator. If the user name already exists, this value overwrites it.

Note! If you are installing Fusion Manager High Availability on a system using ILO power management, do not accept the default user name and password (ibrix/ ibrix) presented by the installation script. Use your ILO user name and password instead.

Enter the power source BMC password for 192.168.17.172 [ibrix]: **ipmi-password**

A user-defined password. If a password already exists, this value overwrites it.

Enter the IP address assigned to the power source BMC of 192.168.17.172: **10.1.1.40**
The pre-existing IP address used by the primary to communicate with the IPMI/ILO controller. It must be on the same subnet as that controller. In Figure 3-1, this is the address assigned to eth0:1 on Fusion Manager 1; this NIC name indicates a virtual interface, one having an actual IP address but using the physical facilities of eth0.

Enter the power source used by 192.168.17.173 (ilo or ipmi): ipmi

This must be the same as the power source technology specified on the primary.

Enter the power source BMC username for 192.168.17.173 [ibrix]: ipmi-username

A user-defined name. If the user name already exists, this value overwrites it.

Enter the power source BMC password for 192.168.17.173 [ibrix]: ipmi-password

A user-defined password. If a password already exists, this value overwrites it.

Enter the IP address assigned to the power source BMC of 192.168.17.173: 10.1.1.50

The pre-existing IP address used by the standby to communicate with the IPMI/ILO controller. It must be on the same subnet as that controller. In Figure 3-1, this is the address assigned to eth0:1 on Fusion Manager 2.

=== High-Availability Network Configuration ===

Enter the interface name for the cluster network: eth0

The shared NIC name that is used to establish the High Availability network. In Figure 3-1, this is eth0:n. The actual name is system-assigned. This NIC name indicates a virtual interface, one having an actual IP address but using the physical facilities of eth0.

Enter the IP address of the cluster network: 192.168.17.175

The shared, or floating, IP address that will always represent the active node in the High Availability pair on the primary cluster network. This must be an unassigned address. In Figure 3-1, this is the shared address on the eth0:n interface.

Enter the netmask of the cluster network: 255.255.255.0

The cluster network’s subnet mask.

Will this installation use a dedicated user network? [y/n] : y

If this network supports a user network, enter yes. In Figure 3-1, this is represented by the User Network and the eth1 NICs on the FusionManagers.

Enter the interface name for the user network: eth1

The NIC name used by the user network. In Figure 3-1, this is eth1.

Enter the IP address of the user network: 192.168.12.45

The IP address that identifies the user network. In Figure 3-1, this is 192.168.45. This address is an unassigned address on the user network. This NIC name indicates a virtual interface, one having an actual IP address but using the physical facilities of eth1.

Enter the netmask of the user network: 255.255.255.0

The user network’s subnet mask.

Enter the Fusion Manager backup path: [/var/lib/ibrix/backup]

Enter a pathname for Fusion Manager backups only if you want to change from the default backup path of /var/lib/ibrix/backup. The path must be on the local system (the installation enforces this requirement) and cannot be an NFS mount point. The installation sets up the same path on both nodes, and the backup files are copied from
the backup directory on the active Fusion Manager to the backup directory on the inactive Fusion Manager. Appears in extended installations only.

Enter the Fusion Manager backup keep number: [10]

Enter the maximum number of Fusion Manager backups to keep. The default is 10 backup files. The most recent is used when restoring. Appears in extended installations only.

Enter the FM start timeout (in seconds): [300]

Enter the number of seconds that Linux-HA waits for a Fusion Manager migration to start before considering the migration to have failed and starting its failover. The default is 300 seconds, which should be adequate even on heavily loaded systems. Appears in extended installations only.

Enter the FM stop timeout (in seconds): [300]

Enter the number of seconds that Linux-HA waits for a Fusion Manager migration to complete before considering the migration to have failed and starting its failover. The default is 300 seconds, which should be adequate even on heavily loaded systems. Appears in extended installations only.

At this point, the installation program tests the SSH connection to the heartbeat IP address. If the test fails and you are prompted for a password, SSH is not properly configured. Exit this script, reconfigure SSH, and rerun this installation procedure.

If the test is successful, the installation program displays your configuration for review.

Enter n to cancel the configuration and rerun at a later time, or enter y to complete the installation procedure using the information shown.

When the script completes, allow a few minutes for all services to start up. To verify operation, enter:

<ibrixhome>/bin/ibrix_fmha -i

This command displays Fusion Manager High Availability status information. If the command does not run, check the log (/usr/local/ibrix/log/install_fmha.log) for error information.

As a post-installation step, IBRIX recommends that you enable all Fusion Manager High Availability events (those starting with ha.) to aid in troubleshooting. Set this up on the Fusion Manager with the ibrix_event command.

### 3.3 Fusion Manager High Availability Installation Scenarios

In these scenarios, Fusion Manager 1 designates the primary and Fusion Manager 2 the backup Fusion Manager. NICs and addresses should be pre-configured. In these descriptions, ethn represents some actual interface, for example eth0. The sample addresses used in these procedures match those used in Figure 3-1.

**New installation, no Fusion Managers or existing Segment Servers**

This is the vanilla installation, starting from scratch, with no High Availability IPs assigned.

1. Install Fusion Manager on both Fusion Manager hosts, following the instructions in Section 2.2, *Installing the Fusion Manager Software*.
2. Install Fusion Manager High Availability on Fusion Manager 1, following the instructions in Section 3.2, *Basic and Extended Installations*.
3. Install the Segment Servers.

The cluster is ready to use.

**On an existing cluster, keep the same cluster IP address**
Fusion Manager1 is the existing Fusion Manager and the primary, and Fusion Manager2 is the new backup server. This procedure entails updating the network configuration on Fusion Manager1, then completing installations for Fusion Manager and Fusion Manager High Availability.

1. Remove the existing static IP for Fusion Manager1 by editing the file 
   `/etc/sysconfig/network-scripts/ifcfg-ethn` (where `ifcfg-ethn` is the configuration file for NIC being reassigned) and assigning the new cluster address, for example 
   `IPADDR=192.168.17.172`.

2. Restart network service. Change directory and run:
   `/etc/init.d/network restart`

3. Assign a new cluster IP to the Fusion Manager 1 node:
   `ifconfig ethn add 192.168.17.272`

4. Assign the cluster address to Fusion Manager 1:
   `<ibrixhome>/bin/ibrix_fm -t -I 192.168.17.272`

5. Log on to the Fusion Manager 2 host and install Fusion Manager, following the instructions in Section 2.2, Installing the Fusion Manager Software.

6. Switch back to the Fusion Manager 1 host and install Fusion Manager High Availability, following the instructions in Section 3.2, Basic and Extended Installations.

The cluster is ready to use.

On an existing cluster, create a new cluster IP address

1. Update the cluster network on Fusion Manager 1 by temporarily adding a cluster IP as a VIF on Fusion Manager 1:
   `ifconfig ethn add 192.168.17.272`

2. Assign the cluster IP to Fusion Manager 1:
   `<ibrixhome>/bin/ibrix_fm -t -I 192.168.17.272`

3. Update Segment Servers to pick up new cluster IP address. On each Segment Server, run:
   `<ibrixhome>/init/ibrix_iad restart`

4. Log on to the Fusion Manager 2 host and install Fusion Manager, following the instructions in Section 2.2, Installing the Fusion Manager Software.

5. Switch back to the Fusion Manager 1 host and install Fusion Manager High Availability, following the instructions in Section 3.2, Basic and Extended Installations.

The cluster is ready to use.
Chapter 4  Performing an OCS Installation

4.1 Installation Overview

In an Open Cluster Stack (OCS) installation, the IBRIX kit is first installed on a front end machine (installer node), and from there on each of the Fusion Clients (compute nodes). When the installation completes, IBRIX services start automatically on bootup. This chapter covers this installation process.

Before beginning the installation activities in this chapter:

- Review the Kusu release information for installation requirements and information on known issues.
- Install and verify the operation of an IBRIX Fusion Manager and at least one Segment Server and file system. These IBRIX components are not described in this section.

Installing IBRIX Fusion Clients in a Kusu OCS environment involves three high-level steps:

1. Install the IBRIX kit on the front end and write the IBRIX configuration file.
2. Set up the client kit on the front end.
3. Install the Fusion Client software on the compute nodes via the front end. If your cluster has existing compute nodes, use Platform OCS to reinstall the operating system and other needed software first. If you are adding new compute nodes, install the Fusion Client software on the new nodes.

Note! An OCS cluster must use the eth0 network interface for the Cluster interface, as shown in the sample configuration file. Verify that all compute nodes are connected to eth0 before beginning installation.

Caution! When installing on an OCS cluster, any previously configured software on the boot drive of servers and compute nodes is lost during reformatting.

4.2 Installing Required Software on the Front End

1. Insert the Kusu OCS disk (CD or DVD) and reboot to start from the ISO. When prompted for additional kits, insert the RHEL 5 kit (RHEL 5.1 DVD). Refer to the Kusu documentation for details on this procedure.
2. If you did not add it during front end installation, copy the IBRIX ISO kit (kit-ibrix_client_node-0.2-0.x86_64.iso) to the front end.
3. Log on to the front end and create a text file named /var/www/html/ibrix.conf. Change the values of FUSION_MANAGER_IP, CLUSTER_IFC and FILESYSTEMS to match your config-
Adding the IBRIX Client Kit

Run these installation procedures on the front end.

1. Change to the directory where you copied the IBRIX Client kit.
2. Install the kit. Run:
   ```
   kitops -a -m kit-ibrix_client_node-0.2-0.x86_64.iso
   ```
3. Verify that the kit was successfully installed. Run:
   ```
   kitops -l
   ```
4. Get the name of the main repository, for example, `Repo for rhel-5-x86_64`. Run:
   ```
   repoman -l
   ```
5. Add the IBRIX kit to the repository. Run:
   ```
   repoman -r "repository_name" -a --kit ibrix_client_node
   ```
6. Rebuild the repository. Run:
   ```
   repoman -r "repository_name" -u
   ```

Next associate the kit to the node groups that will use the IBRIX Fusion Client. On the front end, run the node group editor, `nget`.

1. Run `nget` and select `compute-rhel-5-x86_64` for editing.
2. There are various editing screens in `nget`. Many are not needed for IBRIX Fusion, but you may wish to change them to meet the needs of your own configuration, for example the Boot Time screen. Do not change the Repository Name. Click through the setup windows by pressing `Next` until you reach the Components window:
3. On the Components window, scroll to the ibrix_client_node item and press ENTER.
4. Press the space bar to select component-Ibrix-compute. Verify that component-Ibrix-compute is checked and select Next.
5. Click through the Network, Optional Packages, Custom Scripts, and Partition Schema screens by clicking Next.
6. When you reach the Summary of Changes screen, select Accept. Click OK to update the nodes in the node group.
7. Accept the remaining choices until you can select Exit.

The final setup task is to run addhost. Prepare any hardware before running addhost.

1. Run: addhost
2. Select compute-rhel-5-x86_64
3. Click through the Network Interface screen by clicking Next. On the Rack Number screen, enter a rack number (enter 0 instead of leaving the field blank) and press Ok.
4. Leave the Installing Node Status screen open until all client nodes have finished installation.

Do not exit addhost until clients are installed.

4.4 Client Installation

With the kit added to the front end, there are three installation options: installing a new client as part of a new compute node installation, installing a new client on an existing compute node, and reinstalling a client.

4.4.1 New Clients

To install a new client as part of a new compute node installation:

1. Reboot the compute nodes, setting system to PXE boot (F12). This installs the Fusion Client and automatically reboots the node.
2. The client gets its configuration from the front end, registers with the Fusion Manager, starts, and mounts the specified file systems.

When this process is complete, exit the addhost program.
3. On the Fusion Manager, list hosts to verify that all compute nodes installed successfully:
   
   `<ibrixhome>/bin/ibrix_host -l`

   If compute nodes are installed before the new Fusion Client, run the `cfmsync` command to install the client on the existing compute node, and run step 3 as shown to verify.

### 4.4.2 Re-Installing Clients

To reinstall a client, first uninstall the current client from the configuration. Complete this procedure while the client (`nodename`) is running.

1. On the Fusion Manager, run:
   
   `<ibrixhome>/bin/ibrix_host -d -l nodename`

2. On the front end, run:
   
   `addhost -e nodename`

3. Reboot the client and follow the instructions in Section 4.4.1, “New Clients”.


Chapter 5  Uninstalling IBRIX Fusion

5.1 Uninstalling Linux Fusion Clients

Note! Be sure to unmount the IBRIX file system from Fusion Clients before uninstalling them.

1. On each Fusion Client to unmount the IBRIX file system, run:
   `<ibrixhome>/bin/ibrix_lwumount -f fsname`
   You can also use the Fusion Manager GUI to perform the unmount.
2. On the Fusion Manager, delete the Fusion Clients from the configuration database:
   `<ibrixhome>/bin/ibrix_client -d -h CLIENTLIST`
3. On each Fusion Client, change to the installer directory and run:
   `./ibrixinit -tc -U`

5.2 Uninstalling Windows Fusion Clients

It is not necessary to unmount the IBRIX file system prior to uninstalling the Windows Fusion Client software.

1. On the Fusion Manager, delete the Windows Fusion Clients from the configuration database:
   `<ibrixhome>/bin/ibrix_client -d -h CLIENTLIST`
2. Locally uninstall the Windows Fusion Client software from each Fusion Client via the Add or Remove Programs utility in the Control Panel.
5.3 Uninstalling Segment Servers in a SAN Environment

Before uninstalling the Segment Server software, make sure that the Segment Server does not own any segments, does not mount any IBRIX file systems, and has no IBRIX Fusion High Availability failover responsibilities. This section describes how to clear these cluster responsibilities from a machine. Refer to the IBRIX Fusion CLI Reference Guide for information on the commands used in this procedure.

Transferring segment ownership from one Segment Server to another is known as segment migration. Migration transfers only segment ownership in the configuration database. It does not move segments from their physical locations. If owned segments are not migrated, the Segment Server cannot be uninstalled.

Uninstall Procedure

1. For each Segment Server, run one of the migration commands on the Fusion Manager as appropriate.
   - To migrate specific segments in LVLIST to the named host:
     `<ibrixhome>/bin/ibrix_fs -m -f FSNAME -s LVLIST -h HOSTNAME [-M]`
   - To migrate all segments from host 1 to host 2:
     `<ibrixhome>/bin/ibrix_fs -m -f FSNAME -H HOSTNAME1,HOSTNAME2 [-M]`
   Include the -M argument to force the migration:

2. Verify that no Segment Servers are serving as failover standbys (check with `ibrix_server -l`) or monitoring network interfaces (check with `ibrix_nic -l`).

3. We recommend that any exported file systems be unexported before unmounting them:
   `ibrix_exportfs -f FSNAME -U -h HOSTNAME -p CLIENT:PATHNAME`

4. Unmount all IBRIX file systems from all Segment Servers. To unmount a named file system from all Segment Servers, enter:
   `<ibrixhome>/bin/ibrix_umount -f FSNAME`

5. Delete all Segment Servers from the configuration database:
   `<ibrixhome>/bin/ibrix_server -d -h HOSTLIST`

6. Finally, on the Segment Server, change to the installer directory and run:
   `./ibrixinit -ts -U`

5.4 Uninstalling Segment Servers in a DAS Environment

A Segment Server cannot be uninstalled if it owns segments, but in a direct attached storage environment, migration is not an option. This means that it is your responsibility to back up any data before proceeding with an uninstall, or that data will be lost. It also means that the IBRIX environment must be deleted in the reverse order it was created, and only then can the server be uninstalled. In some cases, for example when upgrading system software, a better option might be to back up the data and skip this uninstall procedure completely.

Refer to the IBRIX Fusion CLI Reference Guide for information on the commands used in this procedure.

Uninstall Procedure

1. Back up the segment data.

2. Verify that the Segment Server is not serving as failover standby (check with `ibrix_server -l`) or monitoring network interfaces (check with `ibrix_nic -l`).

3. Unexport and unmouted file system before unmounting:
   `ibrix_exportfs -f FSNAME -U -h HOSTNAME -p CLIENT:PATHNAME`

4. Unmount all IBRIX file systems from the Segment Server:
   `<ibrixhome>/bin/ibrix_umount -f FSNAME`
5. Delete the file system from the configuration database:
   `ibrix_fs -d -f FSLIST`

6. Delete logical volumes (segments):
   `ibrix_lv -d -s LVLIST`

7. Delete volume groups:
   `<ibrixhome>/bin/ibrix_vg -d -g VGLIST`

8. Delete physical volumes:
   `<ibrixhome>/bin/ibrix_pv -d -p PVLIST`

9. Delete the Segment Server from the configuration database:
   `<ibrixhome>/bin/ibrix_server -d -h HOSTNAME`

10. Finally, on the Segment Server, change to the installer directory and run:
    `./ibrixinit -ts -U`

### 5.5 Uninstalling Fusion Manager High Availability

**Caution!** Before you uninstall the Fusion Manager High Availability software, make sure to reassign the Fusion Manager IP address to a fixed address on the Fusion Manager machine, and to reassign the Segment Server cluster interface to the Fusion Manager’s fixed IP address. Do not leave the IP set to the shared IP address used by Fusion Manager High Availability. If the shared address is still assigned when the software is uninstalled, it is the same as the Fusion Manager being down. Segment Servers will continue to serve data, but there will be no communication with the Fusion Manager.

To uninstall, on the Fusion Manager node where you installed Fusion Manager High Availability, enter:

```
<ibrixhome>/fm-ha/install_fmha -u
```

This command shuts off the Heartbeat service and removes the Fusion Manager High Availability components.

### 5.6 Uninstalling the Fusion Manager

On the Fusion Manager, change to the installer directory and run:

```
./ibrixinit -tm -U
```
Chapter 6 Upgrading IBRIX Fusion

6.1 Overview of the Upgrade Process

Follow the procedures in this chapter to install any IBRIX Fusion software upgrades that you receive. In all cases, upgrade the Fusion Manager first, followed by Segment Servers and Fusion Clients in any order.

The Fusion Manager and all Segment Servers must be upgraded to a new version at the same time. However, Fusion Clients are supported for one version beyond their release. For example, a Fusion V2.2 client can run with a Fusion V3.1 server, but not with a Fusion 4.x server.

**Note!** Be sure to read all instructions *before* initiating any upgrade procedure.

**Online Upgrades**

If the cluster implements IBRIX Fusion High Availability, you can avoid service interruption by manually failing over Segment Servers, upgrading, and manually failing back each Segment Server. This method cannot be used for major upgrades (as in v3.x to v4.x). For detailed information, see Section 6.2.

**Offline Upgrades**

During this upgrade procedure, the file system is unmounted, services are stopped, each Segment Server is rebooted to ensure that all existing modules unload from the kernel, and the upgrade software executes. Clients will experience a short interruption to IBRIX file system access when each Segment Server is upgraded. For detailed information, see Section 6.3.

**Fast Reboot Option**

The fast reboot option for upgrading requires minimal down time for each Segment Server and Fusion Client. It is recommended for installations where the client applications can withstand momentary interruptions in service. Note that all Segment Servers must reboot simultaneously for this procedure to complete properly. For detailed information, see Section 6.4.
6.2 Online Upgrade for a Standard Cluster

This online (failover) upgrade method cannot be used for major upgrades (as in v3.x to v4.x). For major upgrades, use the Offline Upgrade (see Section 6.3) or the Fast Reboot Upgrade (see Section 6.4) procedures.

- **Prerequisite:** `xinetd-2.3.14-10.el5` is required in IBRIX v4.3 for the Fusion Manager and the Segment Servers. Verify that the `xinetd` rpm is installed on each server.

```
rpm -qa | grep xinetd
```

Upgrade the Fusion Manager before upgrading any Segment Servers or Linux Fusion Clients.

**Note!** Be sure to read all instructions before initiating any upgrade procedure.

### Preparing for the upgrade

1. From the Fusion Manager, disable automated failover on all Segment Servers:
   ```
   <ibrixhome>/bin/ibrix_host -m -U
   ```
2. From the Fusion Manager, verify that automated failover is off:
   ```
   <ibrixhome>/bin/ibrix_host -l -S (Failover will display no.)
   ```

### Upgrading the Fusion Manager

**Note!** Fusion Manager High Availability users should refer to the next section before proceeding with a Fusion Manager upgrade. Fusion Manager High Availability must be put into administrative mode before upgrading the individual Fusion Managers.

1. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an `ibrix` subdirectory containing the installer program. For example, if you expand the tarball in `/root`, the installer is in `/root/ibrix`.
2. Change to the installer directory and execute the following command:
   ```
   ./ibrixupgrade -f
   ```
   The upgrade automatically stops services and restarts them when the process is complete.
3. If you obtained a new license from IBRIX, copy the file to `<ibrixhome>` on the Fusion Manager and activate it:
   ```
   <ibrixhome>/bin/ibrix_license -a
   ```
   License activation restarts the Fusion Manager.
4. Verify that the Fusion Manager is operational:
   ```
   /etc/init.d/ibrix_fusionmanager status
   ```
   The status command confirms if the correct services (Quota Monitor, Postmaster, and the Fusion Manager Daemon) are running. Output will look similar to this:
   ```
   ibrix_quotamonitor is running.. pid 18635
   postmaster (pid 31759 31758 31757 31756 31755 31754 31753 31752 31751 31750 18715 18714 18711) is running...
   Fusion Manager Daemon (pid 18748) running...
   ```
5. Run the following command to set the Fusion Manager IP address, reaffirming cluster communication over the cluster interface:
   ```
   <ibrixhome>/bin/ibrix_fm -t -I Fusion_Manager_IP_Address
   ```
7. If Fusion Manager High Availability is implemented in this cluster, repeat these instructions on the second Fusion Manager machine (see below).
Upgrading Fusion Manager High Availability

In order to insure that an automated failover does not occur during the Fusion Manager High Availability upgrade procedure, suspend Fusion Manager High Availability operation before upgrading Fusion Manager on either node by putting the program into administrative mode.

**When to reinstall Fusion Manager High Availability as part of an upgrade.** New versions of IBRIX Fusion often introduce changes and additions to the configuration database. In order to make sure these changes are incorporated into your installation, we recommend you reinstall Fusion Manager High Availability while in administrative mode as shown in this procedure.

To upgrade Fusion Manager High Availability:

1. On the node currently running the Fusion Manager, enter:
   
   `<ibrixhome>/bin/ibrix_fmha -a`

2. On the first Fusion Manager node, run the upgrade procedure as documented above. Then upgrade the second node following the same procedure.

3. On the active Fusion Manager node, start the Fusion Manager:
   
   `/etc/init.d/ibrix_fusionmanager start`

4. Verify the Fusion Manager is operational:
   
   `/etc/init.d/ibrix_fusionmanager status`

5. Install Fusion Manager High Availability. Refer to the installation script (Section 3.3, “Fusion Manager High Availability Installation Scenarios”) as required. Run:
   
   `<ibrixhome>/fm-ha/install_fmha -c`

6. Exit administrative mode on the active Fusion Manager:
   
   `<ibrixhome>/bin/ibrix_fmha -A`

7. Verify the health of the cluster:
   
   `<ibrixhome>/bin/ibrix_health -l -F`

   Output will indicate : Passed / on

Upgrading the Segment Servers

Upgrade the Fusion Manager before upgrading any Segment Servers or Linux Fusion Clients.

Perform this procedure on every Segment Server in the cluster.

1. Manually failover the first Segment Server:
   
   `<ibrixhome>/bin/ibrix_host -f -p -h HOSTNAME`

2. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an ibrix subdirectory containing the installer program. For example, if you expand the tarball in `/root`, the installer is in `/root/ibrix`.

3. Change to the installer directory and execute the following command:
   
   `. /ibrixupgrade -f`
   
   The upgrade automatically stops services and restarts them when the process is complete.

4. Once the Segment Server reboots, verify that it is operational:
   
   `/etc/init.d/ibrix_server status`
   
   Output will look similar to this:
   
   IBRIX Filesystem Drivers loaded
   ibrcud is running.. pid 23325
   IBRIX IAD Server (pid 23368) running...
   
   The IAD service will be running, as shown in the example output above. If it is not, contact IBRIX Customer Support.

5. Execute the following commands to verify that the ibrix and ipfs services are running.
   
   `lsmod|grep ibrix`
   
   `ibrix 2323332 0 (unused`
   
   `lsmod|grep ipfs`
   
   `ipfs1 102592 0 (unused`
If either `grep` returns empty, contact IBRIX Customer Support.

6. From the Fusion Manager, verify that the new version of IBRIX FS/IAS has been installed on the Segment Servers.
   ```bash
   <ibrixhome>/bin/ibrix_version -l -S
   ```

7. If the upgrade is successful, failback the Segment Server:
   ```bash
   <ibrixhome>/bin/ibrix_host -f -U -h HOSTNAME
   ```

8. Repeat the failover, upgrade, failback procedure for each Segment Server in the cluster.

When all Segment Servers are upgraded and failed back, continue below.

### Completing the Upgrade

1. From the Fusion Manager, turn automated failover back on:
   ```bash
   <ibrixhome>/bin/ibrix_host -m
   ```

2. Confirm that automated failover is enabled:
   ```bash
   <ibrixhome>/bin/ibrix_host -l -S (Failover will display yes.)
   ```

3. Upgrade the clients.
   Use the Linux Fusion Client upgrade procedure in Section 6.5.
   Use the Windows Fusion Client upgrade procedure in Section 6.6.

4. Verify that all version indicators match for Segment Servers and Fusion Clients by running the following command from the Fusion Manager:
   ```bash
   <ibrixhome>/bin/ibrix_version -l
   ```

5. Propogate a new segment map for the cluster:
   ```bash
   <ibrixhome>/bin/ibrix_dbck -I -f FSNAME
   ```

6. Verify the health of the cluster:
   ```bash
   <ibrixhome>/bin/ibrix_health -l
   ```
   **Output will indicate:** Passed / on

The installation is successful when all version indicators match. If you followed all instructions and the version indicators do not match, contact IBRIX Customer Support.
6.3 Offline Upgrade for a Standard Cluster

This upgrade procedure applies to IBRIX Fusion v3.x or v4.x releases. It requires a temporary shutdown (reboot) of each Segment Server in the cluster.

- **Prerequisite:** xinetd-2.3.14-10.el5 is required in IBRIX v4.3 for the Fusion Manager and the Segment Servers. Verify that the xinetd rpm is installed on each server.
  
  ```
  rpm -qa | grep xinetd
  ```

  Upgrade the Fusion Manager before upgrading any Segment Servers or Linux Fusion Clients. Be sure to read all instructions **before** initiating any upgrade procedure.

### Preparing for the upgrade

1. From the Fusion Manager, disable automated failover on all Segment Servers:
   ```
   <ibrixhome>/bin/ibrix_host -m -U
   ```

2. From the Fusion Manager, verify that automated failover is off:
   ```
   <ibrixhome>/bin/ibrix_host -l -S
   ```
   (Failover will display no.)

3. On all Segment Servers, disable automatic restart:
   ```
   chkconfig ibrix_server off
   ```

4. Stop the NFS and SMB services on all Segment Servers to prevent NFS and SMB clients from timing out.
   ```
   /etc/init.d/{nfs/smb} stop
   ```

5. Shutdown and reboot each Segment Server to ensure existing modules unload from the kernel:
   ```
   <ibrixhome>/bin/ibrix_host -P reset -h HOSTLIST
   ```

While the servers are rebooting, perform the IBRIX upgrade on the Fusion Manager.

### Upgrading the Fusion Manager

1. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an ibrix subdirectory containing the installer program. For example, if you expand the tarball in /root, the installer is in /root/ibrix.

2. Change to the installer directory and execute the following command:
   ```
   ./ibrixupgrade -f
   ```
   The upgrade automatically stops services and restarts them when the process is complete.

3. If you obtained a new license from IBRIX, copy the file to `<ibrixhome>` on the Fusion Manager and activate it:
   ```
   <ibrixhome>/bin/ibrix_license -a
   ```
   License activation restarts the Fusion Manager.

4. Verify that the Fusion Manager started up successfully:
   ```
   /etc/init.d/ibrix_fusionmanager status
   ```
   The status command confirms if the correct services (Quotamonitor, Postmaster, and the Fusion Manager Daemon) are running. Output will look similar to this:
   ```
   ibrix_quotamonitor is running.. pid 18635
   postmaster (pid 31759 31758 31757 31756 31755 31754 31753 31752 31751 31750 18715 18714 18713 18712) is running...
   Fusion Manager Daemon (pid 18748) running...
   ```

5. Run the following command to set the Fusion Manager IP address, reaffirming cluster communication over the cluster interface:
   ```
   <ibrixhome>/bin/ibrix_fm -t -I FusionManager_IP_Address
   ```


7. If Fusion Manager High Availability is implemented in this cluster, repeat these instructions on the second Fusion Manager machine.
Upgrading the Segment Servers

Upgrade the Fusion Manager before upgrading any Segment Servers or Linux Fusion Clients. Perform this procedure on every Segment Server in the cluster.

1. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an ibrix subdirectory containing the installer program. For example, if you expand the tarball in /root, the installer is in /root/ibrix.

2. Change to the installer directory and execute the following command:
   
   ```
   ./ibrixupgrade -f
   ```
   
   The upgrade automatically stops services and restarts them when the process is complete.

3. Execute the following command to verify that the Segment Server is operational:
   
   ```
   /etc/init.d/ibrix_server status
   ```
   
   Output will look similar to this:
   
   IBRIX Filesystem Drivers loaded
   ibrcud is running.. pid 23325
   IBRIX IAD Server (pid 23368) running...
   
   The IAD service will be running, as shown in the example output above. If it is not, contact IBRIX Customer Support.

4. Execute the following commands to verify that the ibrix and ipfs services are running.
   
   ```
   lsmod|grep ibrix
   ibrix 2323332 0 (unused
   lsmod|grep ipfs
   ipfs1 102592 0 (unused
   ```
   
   If either grep returns empty, contact IBRIX Customer Support.

5. From the Fusion Manager, verify that the new version of IBRIX FS /IAS has been installed on the Segment Servers.
   
   ```
   <ibrixhome>/bin/ibrix_version -l -S
   ```

6. On all Segment Servers, enable auto restart:
   
   ```
   chkconfig ibrix_server on
   ```

When all output indicates success, continue below:

Completing the Upgrade

1. From the Fusion Manager, turn automated failover back on:
   
   ```
   <ibrixhome>/bin/ibrix_host -m
   ```

2. Confirm that automated failover is enabled:
   
   ```
   <ibrixhome>/bin/ibrix_host -l -S (Failover will display yes.)
   ```

3. Upgrade the clients.
   
   Use the Linux Fusion Client upgrade procedure in Section 6.5.
   
   Use the Windows Fusion Client upgrade procedure in Section 6.6.

4. Verify that all version indicators match for Segment Servers and Fusion Clients by running the following command from the Fusion Manager:
   
   ```
   <ibrixhome>/bin/ibrix_version -l
   ```

5. Propogate a new segment map for the cluster:
   
   ```
   <ibrixhome>/bin/ibrix_dbck -I -f FSNAME
   ```

6. Verify the health of the cluster:
   
   ```
   <ibrixhome>/bin/ibrix_health -l
   ```
   
   Output will indicate:
   
   Passed / on

The installation is successful when all version indicators match. If you followed all instructions and the version indicators do not match, contact IBRIX Customer Support.
6.4 Upgrading with the Fast Reboot Option

The fast reboot option for upgrading requires minimal unavailable time for each Segment Server and Fusion Client. It is recommended for installations where the client applications can withstand momentary interruptions in service.

To use this upgrade method, your environment must meet the following requirements:

- The fast reboot option requires RHEL 5.x support with kexecd running on each Segment Server.
- Your currently-installed IBRIX Fusion software must be Version 3.1 Release 45 or later.
- Prerequisite: xinetd-2.3.14-10.el5 is required in IBRIX v4.3 for the Fusion Manager and the Segment Servers. Verify that the xinetd rpm is installed on each server.

```
rpm -qa | grep xinetd
```

**Note!** Be sure to read all instructions before beginning the upgrade procedure.

### Preparing for the Upgrade

1. From the Fusion Manager, disable automated failover on all Segment Servers:
   ```
   <ibrixhome>/bin/ibrix_host -m -U
   ```
2. From the Fusion Manager, verify automated failover is off:
   ```
   <ibrixhome>/bin/ibrix_host -l -S
   ```
   (Failover will display no.)

### Upgrading the Fusion Manager

1. Expand the distribution tarball or mount the distribution DVD in a directory of your choice. This creates an ibrix subdirectory containing the installer program. For example, if you expand the tarball in /root, the installer is in /root/ibrix.
2. Change to the installer directory and execute the following command:
   ```
   ./ibrixupgrade -f
   ```
   The upgrade automatically stops services and restarts them when the process is complete.
3. If you obtained a new license from IBRIX, copy the file to `<ibrixhome>` on the Fusion Manager and activate it:
   ```
   <ibrixhome>/bin/ibrix_license -a
   ```
   License activation restarts the Fusion Manager.
4. Verify that the Fusion Manager started up successfully:
   ```
   /etc/init.d/ibrix_fusionmanager status
   ```
   The status command confirms if the correct services (Quotamonitor, Postmaster, and the Fusion Manager Daemon) are running. Output will look similar to this:
   ```
   ibrix_quotamonitor is running.. pid 18635
   postmaster (pid 31759 31758 31757 31756 31755 31754 31753 31752 31751 31750 18715 18714 18711) is running...
   Fusion Manager Daemon (pid 18748) running...
   ```
5. Run the following command to set the Fusion Manager IP address, reaffirming cluster communication over the cluster interface:
   ```
   <ibrixhome>/bin/ibrix_fm -t -I FusionManager_IP_Address
   ```
7. If Fusion Manager High Availability is implemented in this cluster, repeat these instructions on the second Fusion Manager machine.
## Upgrading the Segment Servers

Upgrading the Segment Servers involves several steps to ensure a smooth transition to the new release. Here is a detailed guide:

**Note!** All of the Segment Servers must reboot “simultaneously” at the end of this upgrade procedure. Specifically, no Segment Server with the new release should come up and mount the file system, while a Segment Server with the old release still has the file system mounted. IBRIX recommends using a utility that issues commands to all configured servers, such as IBRIX’s `node_ctl` or Tentakel. If you do not have a utility, you can open multiple SSH windows and quickly execute the command to all Segment Servers.

Perform this procedure on every Segment Server in the cluster.

1. Verify that the Segment Server is updated with a RHEL 5.x compliant kernel with `kexecd` running.
   
   ```bash
   uname -a
   ```

2. The fast reboot option requires the stopping of all NFS and SMB services prior to performing the upgrade on a Segment Server. In rare cases, NFS or SMB fails to unload from the kernel and the upgrade will fail to complete.
   
   ```bash
   service {nfs|smb} stop
   ```

3. On each Segment Server, run the upgrade script with the fast reboot option `[-r]` from the `ibrix` directory:
   
   ```bash
   ./ibrixupgrade -f -r
   ```

   where `-r` specifies the fast reboot option.

   **Note!** The `ibrixupgrade` command must execute simultaneously on all Segment Servers. See note at the top of this section.

4. Quickly ping all Segment Servers to verify that the `ibrixupgrade` command removed the servers from the network. All pings should return unanswered.

5. When the upgrade completes and the Segment Servers become available again, execute the following command to verify that each Segment Server is operational:

   ```bash
   /etc/init.d/ibrix_server status
   ```

   Output will look similar to this:

   - IBRIX Filesystem Drivers loaded
   - ibrcud is running... pid 23325
   - IBRIX IAD Server (pid 23368) running...

   The IAD service will be running, as shown in the example output above. If it is not, contact IBRIX Customer Support.

6. Execute the following commands to verify that the `ibrix` and `ipfs` services are running.
   
   ```bash
   lsmod|grep ibrix
   ibrix 2323332 0 (unused
   lsmod|grep ipfs
   ipfs 102592 0 (unused
   ```

   If either `grep` returns empty, contact IBRIX Customer Support.

7. From the Fusion Manager, verify that the new version of IBRIX FS /IAS has been installed on the Segment Servers:

   ```bash
   <ibrixhome>/bin/ibrix_version -l -S
   ```

   When all output indicates success, continue below.
Completing the Upgrade

1. From the Fusion Manager, turn automated failover back on:
   `<ibrixhome>/bin/ibrix_host –m`

2. Confirm that automated failover is enabled:
   `<ibrixhome>/bin/ibrix_host -l -S` *(Failover will display yes.)*

3. Upgrade the clients.
   - Use the Linux Fusion Client upgrade procedure in Section 6.5.
   - Use the Windows Fusion Client upgrade procedure in Section 6.6.

4. Verify that all version indicators match for Segment Servers and Fusion Clients by running the following command from the Fusion Manager:
   `<ibrixhome>/bin/ibrix_version -l`

5. From the Fusion Manager, propagate a new segment map for the cluster:
   `<ibrixhome>/bin/ibrix_dbck -I -f FSNAME`

6. Verify the health of the cluster:
   `<ibrixhome>/bin/ibrix_health -l`
   
   Output will indicate: Passed / on

The installation is successful when all version indicators match. If you followed all instructions and the version indicators do not match, contact IBRIX Customer Support.
6.5 Upgrading Linux Fusion Clients

Upgrading Linux Fusion Clients

Upgrade the Fusion Manager before upgrading any Segment Servers or Linux Fusion Clients. Perform this procedure on every Linux Fusion Client.

1. Expand the upgrade tarball or mount the upgrade DVD.
2. On each Fusion Client, run the upgrade script from the ibrix directory:
   
   ```
   ./ibrixupgrade -f
   ```
   
   The upgrade software automatically stops the necessary services and restarts them when the upgrade is complete.
3. Execute the following command to verify the client is running IBRIX Fusion:
   
   ```
   /etc/init.d/ibrix_client status
   ```
   
   IBRIX Filesystem Drivers loaded
   IBRIX IAD Server (pid 3208) running...
   The IAD service will be running, as shown in the example output above. If it is not, contact IBRIX Customer Support.

6.6 Upgrading Windows Fusion Clients

Upgrading Windows Fusion Clients

Perform this procedure on every Windows Fusion Client.

1. Uninstall the old Windows Fusion Client software via the Add or Remove Programs utility in the Control Panel.
2. Copy the Windows Fusion Client MSI file for the upgrade to the machine.
3. Launch the Windows Installer and follow the instructions to complete the upgrade.
4. Check Administrative Tools | Services to verify that the IBRIX Client service is started.
5. Launch the Windows Fusion Client. On the Active Directory Settings tab, click Update to retrieve the current settings.

Note!

If you are using Remote Desktop to perform an upgrade, you must log out and log back in to see the IBRIX drive mounted.

6.7 Troubleshooting Problems with an Upgrade

6.7.1 ibrixupgrade Hangs

The RPM database is corrupted, a problem caused by bugs in the Redhat Package Manager. Rebuild the RPM database using the following commands and then attempt the install/upgrade again. Note that `rm` is followed by a space and then two underscores, and `rpm` is followed by a space and then two dashes:

```
    cd /var/lib/rpm
    rm __*  
    rpm --rebuilddb
```

On the Fusion Manager, `ibrixupgrade` may also hang if the NFS mountpoints are stale. In this case, clean up the mountpoints, reboot the Fusion Manager, and run the upgrade procedure again.
Chapter 7  Finishing the Cluster Setup

7.1 Setting Up the Fusion Manager GUI

The Fusion Manager GUI is a browser-based interface to the Fusion Manager. To use it, the Fusion Manager must be installed with a browser that supports Java and the Java plug-in for Firefox version 1.5 or later. In addition, for large clusters (100 or more Segment Servers), the Java memory pool on the Fusion Manager must be large enough to prevent the GUI from running out of memory.

7.1.1 Checking Firefox Plug-In Installation

To determine whether the Fusion Manager has the required browser plug-in, navigate to http://hostname:8080 in your browser, where hostname is the name or IP address of the Fusion Manager host. If the plug-in is present, the GUI opens to the login page. If it is not, the GUI displays a window with the URL for the plug-in download site. Download either the 32-bit or the 64-bit plug-in (depending on the architecture of the Fusion Manager machine), install the plug-in, and restart the browser.

- To install the plug-in on 32-bit Linux machine

Execute the following commands (version numbers may vary):

```
chmod 777 j2SDK_1_5-linux-i586-rpm.bin
./j2SDK_1_5-linux-i586-rpm.bin
rpm -i j2SDK_1_5-linux-i586.rpm
ln -s /usr/java/j2sdk1.5/jre/plugin/i386/ns610-gcc32/libjavaplugin_oji.so
```

- To install the plug-in on a 64-bit Linux machine

1. Install Firefox 1.5 or later (for Linux i686, available at www.getfirefox.com).
2. Install the latest update for the J2SE Runtime Environment 5.0 for Linux (available at java.sun.com).
3. Change to the Firefox plug-in directory:
cd /usr/firefox/plugin

4. Correct the link to the Java plug-in in the libjavaplugin_oji.so file, for example:
   ln -sf /usr/java/jre1.5.0_06/plugin/i386/ns7/libjavaplugin_oji.so

To install the plug-in on a Windows machine:

Download the plug-in to a temporary directory, double-click the installer, and respond to any installer prompts.

7.1.2 Increasing the Java Memory Allocation Pool

In large clusters it may be necessary to increase the size of the Java memory allocation pool to prevent the GUI from running out of memory. To do this:

1. Open the Control Panel on the Fusion Manager and click the Java tab. In the Java Applet Runtime Settings box, click the View button.
2. In the Java Runtime Parameters column, enter a value of the format XmxNUMm, where NUM is the lesser of 512 or the size of the Fusion Manager's physical memory divided by 2. For example, if the Fusion Manager’s memory size is 512, enter Xmx256m.

7.1.3 Verifying Fusion Manager GUI Operation

The Fusion Manager GUI is a browser-based interface to the Fusion Manager.

To open the GUI, launch a web browser and navigate to http://hostname:8080 in your browser, where hostname is the name or IP address of the Fusion Manager host. The default password is ibrix. The GUI opens in a second browser window, to the Status tab.

You can open multiple GUI windows to simplify your work routine. With multiple windows open, you can monitor the effect of configuration changes on cluster status.

7.1.4 Changing the IBRIX User Password

The default Fusion Manager GUI user password (ibrix) is created during installation. It can be changed on the Fusion Manager with the Linux passwd command. Run the command and enter the new password when prompted:

# passwd ibrix

7.2 Registering Multicluster Clients

A multicluster client is one that is homed to more than one Fusion Manager and is thus a member of more than one cluster. The procedure to configure such a remote client involves running programs as the root user on both the client and the Fusion Manager.

The remote Fusion Client and the new cluster must be in the same subnet and routable to each other. The remote client and the new cluster’s Fusion Manager must be running the same version of IBRIX Fusion.

The Fusion Client must be installed and registered on its first cluster before running this procedure.

1. From the Fusion Client, register the client with the new cluster:
   
   # register_client -p IPADDRESS -c IFNAME

   Where IPADDRESS is the address of the new Fusion Manager and IFNAME is the interface used for cluster communication. The new Fusion Manager entry is added to the client iadconf.xml file, and can be listed with ibrix_host on the new Fusion Manager.
2. Restart Fusion Client services:
   
   /etc/init.d/ibrix_client restart

3. On the new cluster’s Fusion Manager, create a mountpoint for the new client and set the
   mount intent; in this example the file system is ifs1, the mountpoint is /mnt_ifs1, and
   the client’s host name is client1.net.com.
   
   <ibrixhome>/bin/ibrix_mountpoint -c -m /mnt_ifs1 -h client1.net.com
   
   4. On the client, mount the file system and verify.
      
      ibrix_lwmount -f cluster.net.com:ifs1 -m /mnt_ifs1
      # mount

   **Note!** Current IBRIX Fusion versions do not include a command for removing a client
   from a cluster. Contact IBRIX Customer Support for a workaround if necessary.

7.3 Configuring the Windows Fusion Client Software

After installing the Windows Fusion Client software, you must perform the following one-time
user management and access control management procedures:

1. Import IBRIX Fusion cluster UIDs and GIDs into the Active Directory Server.
2. Create an Active Directory proxy user with permission to read only UID/GID information.
   Windows Fusion Clients require this proxy user to query the Active Directory server.
3. Configure Active Directory settings on the Fusion Manager.

These procedures are described in the Windows Client chapter of the *IBRIX Fusion User’s Guide*. 
Appendix A  IBRIX Fusion Installation Blueprints

A.1 Blueprint 1: Fusion Client Environment ................................................................. 39
A.2 Blueprint 2: NFS/CIFS Client Environment ............................................................ 40
A.3 Blueprint 3: Mixed Client Environment ................................................................. 42

There are blueprints for three environments in this appendix that will help you set up networks and IBRIX Fusion High Availability high availability for your cluster:

- Fusion Client environment
- NFS/CIFS client environment
- Mixed client environment

Failover configurations are not themselves illustrated in the blueprints but are described. For information on implementing the recommended network and failover configurations, refer to the High Availability chapter in the IBRIX Fusion User’s Guide.

The blue, green and red lines in the blueprint figures signify logical networks, not physical connections.

A.1 Blueprint 1: Fusion Client Environment

This blueprint includes only Fusion Clients and represents the most common environment. There is only one network—the mandatory Cluster network—and it handles all administrative, server-to-server, and data traffic.

Establishing the Network

No additional configuration is required for this blueprint. The Cluster interface is identified during IBRIX Fusion installation.

Network configuration

- Cluster network only.
- No preferred interfaces.

Failover configuration

- Segment Server failover pairs: A1–A2, B1–B2; no standby for servers C or D.
- Network interface failover pairs: None.
- Network interface monitors: None.

Establishing the Failover Configuration

This blueprint allows you to implement both automated and manual failover for Segment Servers.

1. If you plan to enable automated failover, install programmable power sources on the network.
2. Identify failover pairs of Segment Servers. Figure A-1 shows two Segment Server failover pairs: A1-A2 and B1-B2. Failover cannot be set up for servers C and D, which have directly attached storage.

3. If you plan to enable automated failover, turn it on for each Segment Server failover pair.

![Figure A-1 Blueprint 1, FusionClient environment](image-url)

**A.2 Blueprint 2: NFS/CIFS Client Environment**

In this blueprint the environment includes only NFS or CIFS clients. Client access to data is protected by segregating NFS/CIFS traffic to a User network and by implementing automated failover for the interface and for Segment Servers.

**Establish the Networks**

1. Identify one or more User interfaces for NFS/CIFS traffic. The Cluster interface was identified during Segment Server installation. Figure A-2 shows two User networks.

2. Determine whether you want to mount the NFS/CIFS clients to servers manually or via the IBRIX Fusion Autoconnect feature. If you manually mount, make sure that you balance server workload.

Network configuration

- One Cluster network.
• Two User networks.
• No preferred interfaces.

Failover configuration
• Network interface failover pairs: For User1, A1–A2, B1–B2, and C1–C2. For User2, C1–C2.

Establish the Failover Configuration
This blueprint requires you to set up automated failover for Segment Servers and User interfaces.

1. Install programmable power sources on the network
2. Identify a standby for each Segment Server. Figure A-2 shows three Segment Server failover pairs: A1-A2, B1-B2, and C1-C2.
3. Identify standbys for each identified User interface. It is convenient to identify these standbys on Segment Server failover pairs. In Figure A-2 A1-A2, B1-B2, and C1-C2 are also failover pairs for User1, and C1-C2 is also the failover pair for User2. No failover pairs are declared for the Cluster interface because it cannot be failed over.
4. Set up network interface monitoring for each network failover pair. In Figure A-2, the A1-A2, B1-B2, and C1-C2 pairs have been set up to monitor each other over User1, and the C1-C2 pair has been set up to monitor each other over User2.
5. Turn on automated failover for the Segment Server failover pairs.
A.3 Blueprint 3: Mixed Client Environment

In this blueprint the environment includes a mixture of Fusion Clients and NFS/CIFS clients. The Cluster network handles Fusion Client traffic, and one or more failover-protected User networks handle requests from various sets of Fusion Clients and NFS/CIFS clients. NFS/CIFS and IBRIX Fusion clients cannot reside on the same user network.

Refer to the preceding section for an explanation of the advantages of restricting NFS/CIFS traffic to a User interface.

Establish the Networks

1. Identify a User interface for the NFS/CIFS traffic. In Figure A-3, the User1 interface is dedicated to NFS/CIFS traffic. Optionally, identify one or more User interfaces for specific Fusion Client traffic as well. The Cluster interface was identified during Segment Server installation.

2. Determine whether you want to mount NFS/CIFS clients to servers manually or via the IBRIX Fusion Autoconnect feature. If you manually mount, make sure that you balance server workload.
3. If you want to segregate any Fusion Client traffic to a User interface, prefer that interface locally on the clients. In Figure A-3, the User2 interface is preferred for Fusion Client E. Fusion Clients A and B remain defaulted to the Cluster interface.

Network configuration
- One Cluster network.
- Two User networks.
- Preferred interfaces: User2 for NFS/CIFS client E.

Failover configuration

Establish the Failover Configuration
This blueprint allows you to implement both automated and manual failover.

1. If you plan to implement automated failover, install programmable power sources on the network.
2. Identify a standby for each Segment Server. Figure A-3 shows three Segment Server failover pairs: A1-A2, B1-B2, and C1-C2.
3. Identify standbys for each identified User interface. It is convenient to identify these standbys on Segment Server failover pairs. In Figure A-3 A1-A2, B1-B2, and C1-C2 are also failover pairs for User1, and C1-C2 is also the failover pair for User2. No failover pairs are declared for the Cluster interface because it cannot be failed over.
4. Set up network interface monitoring for each network failover pair. In Figure A-3, the A1-A2, B1-B2, and C1-C2 pairs have been set up to monitor each other over User1, and the C1-C2 pair has been set up to monitor each other over User2.
5. Turn on automated failover for the Segment Server failover pairs.
Figure A-3  Blueprint 3, Mixed client environment
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
</tr>
<tr>
<td>blueprints</td>
</tr>
<tr>
<td>FusionClient environment 39</td>
</tr>
<tr>
<td>mixed client environment 42</td>
</tr>
<tr>
<td>NFS/CIFS environment 40</td>
</tr>
</tbody>
</table>

| F     |
| Fusion Manager |
| checking status 6, 26 |
| Fusion Manager GUI |
| verifying operation 36 |
| Fusion Manager GUI setup |
| browser plug-in requirement 35 |
| changing password 36 |
| increasing memory allocation pool 36 |
| Fusion Manager HA software |
| installing 11–15 |
| prerequisites 11 |
| uninstalling 23 |
| upgrading 27 |
| Fusion Manager software |
| installing 6 |
| uninstalling 23 |
| upgrading 26 |

| I     |
| IBRIX Fusion |
| installation prerequisites 1–3 |
| upgrading 25 |
| install_filha script 12 |
| installation prerequisites |
| Linux-specific 1 |
| networking 3 |
| OS configuration 2 |

| O     |
| OCS installations |
| client (compute node) installations 19 |
| client kit setup 18 |
| frontend installations 17 |

| P     |
| PostgreSQL RPM version requirement 2 |

| S     |
| Segment Server software |
| installing 6 |
| uninstalling 22 |
| upgrading 27, 30, 32 |
| SELinux, disabling (required) 2, 9 |
| SNMP RPM version requirement 2 |

| U     |
| upgrades 25 |
| Fusion Manager 26 |
| Fusion Manager HA 27 |
| Linux Fusion Client 34 |
| Segment Server software 27, 30, 32 |
| Windows Fusion Client 34 |

| W     |
| Windows Fusion Client |
| Active Directory and SFU 3.5 requirements 3 |
| driver signing 9 |
| starting client service 8 |
| version compatibility 25 |
| Windows Fusion Client software |
| installing 8 |
| setup 37 |
| uninstalling 21 |
| upgrading 34 |