

StandbyServer™ for OS/2 Warp


User's Guide




The hardware and software described in this document are furnished under a license agreement or nondisclosure agreement. The hardware and software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Vinca® Corporation.

Information in this document is subject to change without notice and does not represent a commitment on the part of Vinca Corporation.

The mirroring techniques involved in *StandbyServer*™ and discussed in this document are part of IBM LAN Server and/or Cyranex Corp. EZRAID Lite. Vinca Corporation takes no responsibility for limitations or any problems that occur due to the nature of these products.

 **Note:** Vinca discontinued shipping IBM's NetFinity Manager when IBM included it with its OS/2 Warp Server. NetFinity is used in conjunction with *StandbyServer* for OS/2, but is not required. If you want to use the features that NetFinity Manager adds, including alerting and automatic failover, you must obtain NetFinity from IBM of an IBM reseller.

 **Note:** EZRAid is not a product of Vinca Corporation and is not included as a part of *StandbyServer* for OS/2. EZRAid can be purchased through Vinca or your local reseller.

Part number DOC-OS2CP20-971100.

StandbyServer is patent pending.

StandbyServer is a trademark of Vinca Corporation. Vinca is a registered trademark of Vinca Corporation. LAN Server and OS/2 Warp are registered trademarks of IBM. EZRAID Lite is a trademark of Cyranex Corp. All other brand and product names are trademarks or registered trademarks of their respective companies.



Copyright © 1993-1997 Vinca Corporation.

Contents



Chapter 1 Introduction and Overview

What Is StandbyServer for OS/2 Warp	9
What StandbyServer Does	11
Disks, Partitions, and Mirroring	12
StandbyServer and Disk Devices	12
StandbyServer and Partitions	13
StandbyServer and Mirroring	15
Benefits of StandbyServer	16
Concepts and Definitions	17
Roles of the Primary and Standby Machines.	17
Terminology	17
Frequently Asked Questions about StandbyServer for OS/2 Warp	17
Where Do I Go Now?	18
Vinca Technical Support	19
Pre-Assistance Checklist	20
Services	20

Chapter 2 Installing on LAN Server Advanced Systems

Requirements/Preinstallation Checklist	21
General Prerequisites	21
LAN Server Advanced-Specific Requirements.	22
Using Hardware RAID Host Adapters	22
Installation Overview	23
Step 1: Install StandbyServer Hardware	24
IBM PRO/100 Cards	24
ISA 16-bit Vinca Cards	24
EISA 32-bit Vinca Card	28
MCA 32-bit Vinca Card	29
Step 2: Install or Modify Disk Configuration.	31
What To Do With Existing Data	31
Disk Device Configuration	31
Step 3: Install or Modify LAN Server Advanced	32
Installation Instructions.	32
Step 4: Understanding the Evaluation/Validation Option	33
Step 5: Install StandbyServer Software	34
Copying FTMONIT.EXE (LAN Server Advanced 3.0 only).	38
Step 6: Set Local Disks for the Standby Machine	38
Step 7: Install and Configure NetFinity.	39
Installation Instructions.	40
Installing NetFinity Services on the Primary Machine	40
Installing NetFinity Manager on the Standby Machine	43
Starting NetFinity on the Standby Machine	46
Step 8: Install Mirroring and Edit CONFIG.SYS.	52
Install Mirroring	52
Edit CONFIG.SYS on Primary Machine	54
Step 9: Modify Switchover and Recovery Command Files.	55

Step 10: Test the Installation	56
Uninstalling Vinca Software.	58
Chapter 3 Installing on OS/2 Systems without LAN Server Advanced	
Requirements/Preinstallation Checklist.	61
General Prerequisites	61
EZRAid (non-LAN Server Advanced) Requirements.	62
Using Hardware RAID Host Adapters	62
Installation Overview	63
Step 1: Install StandbyServer Hardware	64
IBM PRO/100 Cards	64
ISA 16-bit Vinca Cards	65
EISA 32-bit Vinca Card	69
MCA 32-bit Card.	70
Step 2: Install or Modify Disk Configuration.	72
What To Do With Existing Data	72
Disk Device Configuration	72
Step 4: Understanding the Evaluation/Validation Option	73
Step 5: Install StandbyServer Software	74
Step 5: Set Local Disks for the Standby Machine	79
Step 6: Install and Configure NetFinity.	81
Installation Instructions.	81
Installing NetFinity Services on the Primary Machine	81
Installing NetFinity Manager on the Standby Machine	84
Starting NetFinity on the Standby Machine.	88
Step 7: Install Mirroring, Edit CONFIG.SYS.	93
Install EZRAID Lite	93
Configure Mirroring	95
Edit CONFIG.SYS on the Primary Machine	97

Contents

Step 8: Modify Switchover and Recovery Command Files	98
Step 9: Test the Installation	99

Chapter 4 Recovery Procedures

Fault Tolerance Recovery Process—LAN Server Advanced	101
General Guidelines for Recovery	102
What to Do When the Primary Machine Fails	103
What to Do If the Primary Machine is Booted Without the Standby Machine	104
Disk Device Failure on the Primary or Standby Machine	106
What to Do When the Standby Machine Fails	108
Vince Link Cable Failure.	109
What to do when the Mirror is Detached and the Data is Out of Synchronization	110
Fault Tolerance Recovery—OS/2 without LAN Server Advanced.	113
General Guidelines for Recovery	113
What to Do When the Primary Machine Fails	114
What to Do If the Primary Machine is Booted Without the Standby Machine	115
Disk Device Failure on the Primary or Standby Machine	116
What to Do When the Standby Machine Fails	117
Vince Link Cable Failure.	118

Chapter 5 Using StandbyServer

Using the Link Statistics view	120
Using the Drive Information View.	121
Using the Card Information View	122

Chapter 6 Customizing NetFinity

The Basic NetFinity Operation	123
Generating NetFinity Alerts	124
Setting Up Actions in the Alert Manager	125
Other Settings and Procedures	126

Chapter 7 LAN Server Advanced Fault Tolerance and Domain Replication

General IBM Fault Tolerance Information	128
Fault Tolerance Mirror Characteristics	128
Fault Tolerance Mirror Requirements	128
Fault Tolerance Files	129
Primary and Secondary Partitions	130
Partition Tables	130
Drive Letter Assignments	131
Fault Tolerance Mirror Partitions	131
Maintaining the Mirror - Other Fault Tolerance Files	132
Booting With Fault Tolerance Installed	132
Potential Problems with Booting	133
Fault Tolerance Mirror Status	134
No Errors	134
Non-fatal Errors	134
Fatal Errors	134
Replicator Services Setup	134
Primary Server Setup	135
Standby Machine Setup	136

Chapter 8 Reference Information

Routing over TCP/IP	137
Sample Configuration	138
Router	138
Client	138
Primary	138
Standby	138
Sample Illustration	139
StandbyServer Files	140
Creating Emergency OS/2 Boot Diskettes	143
Boot Disk Changes for EZRAID Lite	143
Boot Disk Changes for LAN Server Advanced with Fault Tolerance	144
Using Fault Tolerance Alerts with StandbyServer for Lan Server	145
Using Netfinity Services with StandbyServer for Lan Server	146
Index	147

Chapter 1

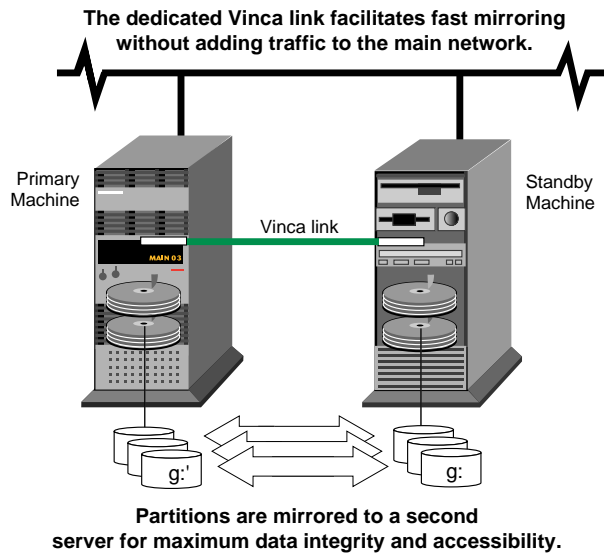
Introduction and Overview

What Is StandbyServer for OS/2 Warp

Nowhere is high server availability more critical than in IBM OS/2 environments. Because of the robust feature set available in OS/2, many corporations run large, mission-critical applications such as IBM LAN Server Advanced, DB/2, and Lotus Notes on OS/2. Continuous access to data is vital.

Vinca's StandbyServer for OS/2 Warp connects a *standby machine* directly to a *primary server* via a dedicated communications channel called the *Vinca link*. StandbyServer software running on the standby machine exports disk devices in the standby to the primary server where they are treated as local disks of that primary server. Using standard mirroring software, data is duplicated to both the disks in the primary machine and the disks exported from the standby machine via the Vinca link.

Figure 1.1 StandbyServer Overview

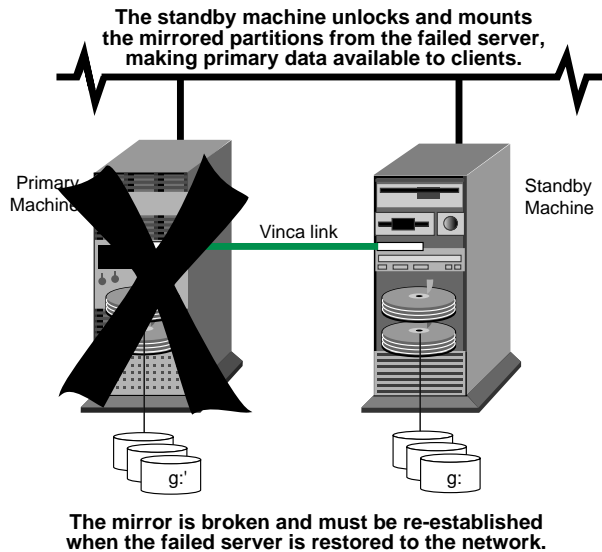


Because the mirrored data is located in a physically separate file server the data is protected against any failure of the primary machine. A RAID can provide data duplication protection, but failure of a disk controller or CPU means that data is unavailable until the RAID is moved to another machine. By putting the second disk devices in another active server, data is both protected and available in case of primary system failure.

What StandbyServer Does

Vinca's StandbyServer provides complete server protection against hardware or software failure. As data is written to the primary server it is instantly mirrored to a second partition for data protection. If the primary fails for any reason, the mirrored data is as recent as the last disk write.

Figure 1.2 *If the Primary Fails...*



If the primary server fails for any reason—becoming inaccessible to the standby machine via either the main network or the Vinca link—the standby machine offers the failed server's data to clients as though it were the failed server. Clients can continue to access data after only a short pause as the failover happens.

StandbyServer uses existing mirroring software and mirrors data from the primary machine to the standby machine across the Vinca link. For IBM LAN Server Advanced file servers, StandbyServer works with LAN Server Advanced's built-in disk mirroring facility; for application servers that use OS/2 but not LAN Server Advanced, Vinca provides Cyranex Corporation's EZRAID Lite for mirroring.

IBM's NetFinity software can be used to automate switchover from the primary machine to the standby machine. NetFinity also allows a system administrator to customize alerts which can be sent to a local client, a remote console, or even a digital pager.

Disks, Partitions, and Mirroring

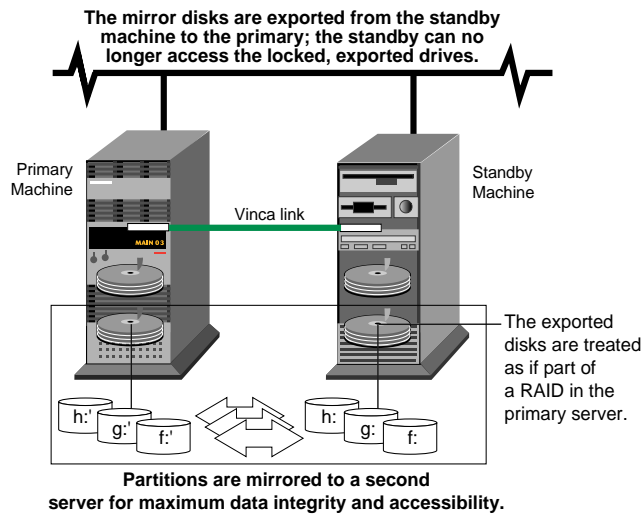
In a StandbyServer installation the standby machine is a fully functioning file server that also acts as a backup for a single primary server. This allows a tremendous amount of flexibility in determining how resources are allocated and maximizes the use of expensive server hardware.

StandbyServer and Disk Devices

StandbyServer lets you choose which disks are exported from the standby machine. The exported disks are locked from the standby machine, and are treated by the primary server as though they were local to that server. Exported disks cannot be accessed by the standby machine until the primary server fails and the standby fails over.


The standby machine must have at least two disk devices—one that serves as the boot disk and stores local data and services, and one that is exported to the primary server to act as the second half of the mirror.

Figure 1.3 *Disk Exported to the Primary Server*



The local disk device(s) in the standby machine services local file server processes while the locked, exported disks serve as the second half of the mirrored pair established from the primary server. The mirrored data is as recent as the last disk write, providing full data protection.

When the standby machine stands in for the failed primary, the standby machine gives full access to the mirrored data. The standby machine now functions as the failed primary.

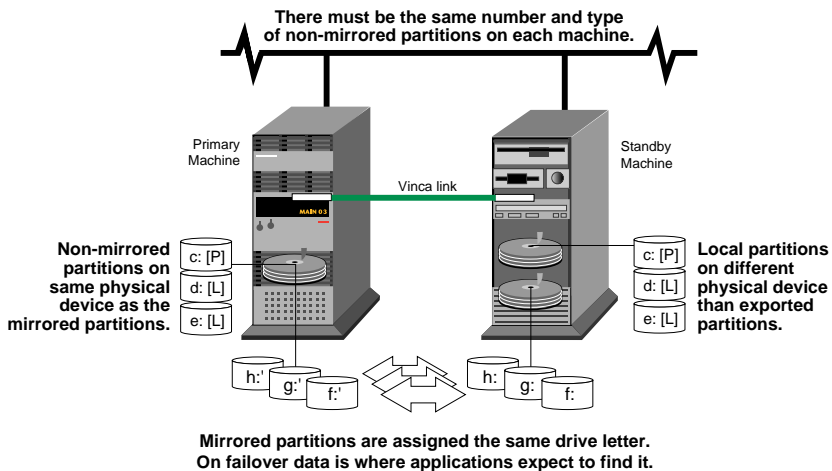
 **Important!** *StandbyServer* does require that the local disk devices on the standby machine be consecutive devices starting with device 0. At least one disk device must remain local to the standby machine to function as the boot device and to hold any local data.

The number and type of disks in the standby machine is limited only by the disk controller and operating system.

StandbyServer and Partitions

The mirroring software mirrors partitions, not physical devices, so there is no need to have similar numbers of disks in the primary and standby machines. It is necessary, though, that each machine have the same number and types of partitions on the local disk device to ensure that drive letter designations remain consistent both during mirroring and after failover.

Figure 1.4 *Number and Type of Partitions Must Match*

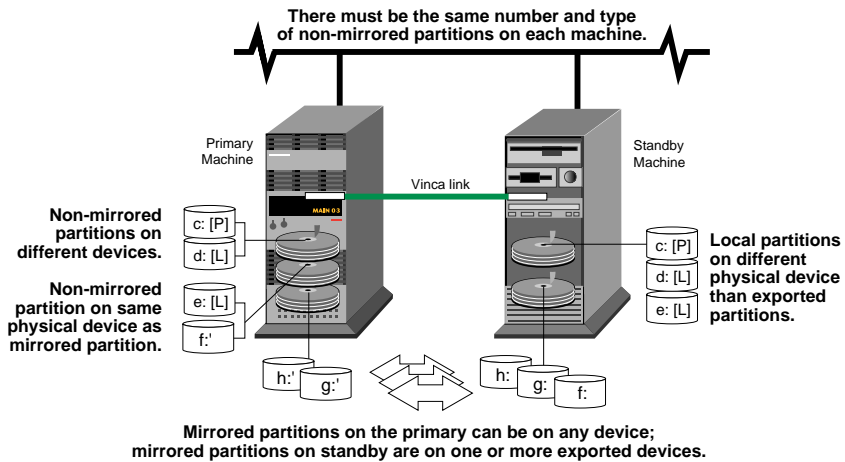


In this example (Figure 1.4) the boot device in each machine has three local partitions, one primary partition and two logical partitions. It doesn't matter that these partitions be on the same disk or that there be an equivalent number of disks in each machine. All that is important is that the number and type of non-mirrored partitions be the same in each machine so that the operating system

assigns the same drive letter designation to both halves of the mirror. This ensures that data is still accessible after failover.

For example, the partitions shown in Figure 1.4 could be arranged as shown in the following example (Figure 1.5). What's important is that the operating system be able to assign the original partition and the mirrored partition the same drive letter, not that there be a similar number of disk devices or that each machine have similar partitions on corresponding disk devices.

Figure 1.5 *Partitions Over Multiple Disks*



This may mean that you need to create partitions as place holders on either the primary or standby machine; these partitions can be very small or may contain no data. Again, what is important is that the number and type of non-mirrored partitions be the same, not that the partitions be a particular size or contain any particular data.

Notice in each example above that the primary partition of the mirrored set is actually located on the standby machine, not the primary machine. While this may seem counter-intuitive, it is necessary to ensure that on failover the standby machine recognizes the exported disks in the standby machine and can access them. The fault tolerance software running on the primary machine assigns the secondary partition in a mirrored set a partition type of 87 which is ignored by that machine's boot sequence. Because the fault tolerance software only runs on the primary machine, the secondary partitions on the primary machine are recognized as normal at startup.

StandbyServer and Mirroring

Depending on the individual system configuration, different software is used to establish mirrored pairs. With LAN Server Advanced systems Vinca uses IBM's own mirroring software; for application servers that do not use LAN Server Advanced Vinca includes Cyranex Corporation's EZRAID Lite to establish mirrored pairs.

While each system uses different software to establish the mirror, there are a set of common considerations that must be observed for successful fault tolerance protection. This list reviews what has been discussed earlier in this section.

- ▼ The device containing the boot partition on the standby machine is not mirrored. Separate backup arrangements must be made to protect that data.
- ▼ There must be sufficient space on the primary machine to accommodate the exported disk(s) from the standby machine to mirror all desired partitions. For example, if the standby contains three 200 MB partitions, the primary machine must have at least 600 MB of space to accommodate the mirror.
- ▼ There must be the same number and type of non-mirrored partitions on each machine to ensure that partition lettering is consistent after failover.
- ▼ The primary partition in a mirrored pair resides on the standby machine, not the primary. This is taken care of by creating the partition on the standby machine.
- ▼ For the standby machine to access the data on the exported mirror disks after failover, the standby must be properly configured for, and have access to, the applications that use that data. Make sure that the standby machine can run the applications that are loaded on the primary, even if the application is not installed on the standby machine (but is installed on the mirrored disks).

Benefits of StandbyServer

Vinca's StandbyServer mirroring system can virtually eliminate server downtime and offers the following benefits for an OS/2 LAN Server Advanced network or OS/2 application server.

- ▼ Complete server fault tolerance.
Because data is mirrored to a completely separate computer, all server components are redundant. In addition, because data is mirrored to a separate computer, the Vinca solution can even recover from a software failure on the primary machine.
- ▼ Primary machine and standby machine do not need to be identical.
A less expensive computer can be used as the standby machine.
- ▼ Automatic switchover to the standby machine.
When the primary machine fails, the standby machine is initialized as the working server without user intervention.
- ▼ Easy to install and maintain.
No complex software needs to be installed or maintained. LAN Server Advanced systems use LAN Server Advanced's built-in Fault Tolerance system, while other OS/2 systems use the easy-to-install EZRAID Lite software.
- ▼ Customizable remote notification features.
Using NetFinity, Vinca's StandbyServer can notify a system administrator of a server failure at a remote workstation or even on a digital pager.
- ▼ Enhanced diagnosis of server failure.
StandbyServer allows system failures to be diagnosed while users continue to have access to their data and network services.
- ▼ Does not impact network traffic.
Data is mirrored through a high-speed dedicated link rather than over the network wiring. StandbyServer does not affect network traffic and in some configurations actually enhances network performance.

Concepts and Definitions

StandbyServer for OS/2 Warp requires that the system be configured in a specific manner. Some prerequisites are general to both the LAN Server Advanced and non-LAN Server Advanced (EZRAID Lite) implementations of StandbyServer; others are specific to each environment.

Roles of the Primary and Standby Machines


The primary machine serves the role of the server only—it is never assigned the role of standby. In normal operation the standby machine is treated like an external disk sub-system of the primary machine. Users log in to the primary machine to use files and applications. The standby machine silently mirrors the data unless the primary machine has a failure, in which case the standby machine takes on the role of the primary machine.

The standby machine must be running the StandbyServer software prior to the primary machine being booted. In addition, the standby machine must not be shut down until after the primary machine has been shut down.

Terminology

The term *mirrored drive* refers to the Fault Tolerance mirror as it is viewed by the operating system, i.e., as a single logical drive with an associated letter. The term *mirrored partition* refers to either of the component partitions of the mirrored disk device.

- ▼ One partition of the mirror is designated as *primary*, while the other partition is designated as *secondary*. The primary and secondary partitions have different partition types and are treated differently by the base operating system.

 **Note:** The use of the terms *primary* and *secondary* as partition titles should not be confused with the use of the terms *primary* and *standby* to refer to the roles of the two server machines in a StandbyServer installation.

Frequently Asked Questions about StandbyServer for OS/2 Warp

How long does switching over take?

It takes about 1.5 to 2 minutes to switch from the primary machine to the standby machine in the LAN Server Advanced environment. For non-LAN Server Advanced systems, it depends on how long critical applications (e.g. Notes, DB2/2) take to load.

What if the standby machine fails?

The primary machine continues to operate normally. If the primary machine must be rebooted in a LAN Server Advanced environment, first use FTSetup to recover the secondary partition of the mirrored pair to be the primary partition (do this before rebooting). Rebooting the primary without the standby presents no special problems in the non-LAN Server Advanced environment.

What if my software (LAN Server Advanced, Notes, etc.) quits, but the primary machine itself is still functioning?

Use NetFinity 3.0 or higher to monitor the application software and force a switchover to the standby machine in the event of software failure.

How long will it take to mirror my drive?

This is machine dependent. In Vinca's test labs, an IBM PS/2 model 77i (486, MCA bus, SCSI disk) took 23 minutes to mirror a 1 GB drive.

Is my current system compatible with the Vinca solution?

If the system meets the criteria for LAN Server Advanced then it is generally okay. In the LAN Server Advanced environment the most common question in this area deals with the requirement that disk drive geometries be the same. The Vinca distribution disk includes a utility program, GEO.EXE, which examines the currently installed drives and reports their geometries. This program (but no others on the disk) may be freely distributed for pre-installation checking. EZRAID's requirements are less stringent. In general, review the prerequisites earlier in this chapter to see if the system is compatible.

Where Do I Go Now?

LAN Server Advanced—If installing *StandbyServer* for OS/2 Warp on an IBM LAN Server Advanced file server, go to **Chapter 2**.

OS/2 *without* LAN Server Advanced—If installing *StandbyServer* on an OS/2 system that does not run LAN Server Advanced (for example a database or Notes server), go to **Chapter 3**.

Vinca Technical Support

Vinca Technical Support is now available through the following support programs:

- ▼ Premium Support—24 hour toll-free telephone support.
- ▼ Priority Support—7:00 am–6:00 pm (MST) telephone support.
- ▼ Incident Support*—Per incident charge telephone support.
- ▼ Basic Support—Free fax and e-mail support.
- ▼ Extended Incident Support—Weekend telephone support by appointment.

These programs are discussed in detail in the Technical Support Programs insert included in the product box. Some manuals contain misprinted information about Vinca's support programs and are superseded by this information.

*One free Incident Support is included with each product purchase. An incident is defined as the resolution of one issue, problem or question, regardless of the number of telephone calls required. To use this free incident support, you will need to give the Incident Number located on the back of the Quick Setup Card to the support technician.

For more information about Vinca's support programs contact your nearest Vinca sales representative, Vinca Sales at 800-934-9530, Vinca Technical support, or visit our Web site.

Before accessing technical support for any issues, please complete the Pre-Assistance Check List (next page).

Pre-Assistance Checklist

Check the following conditions on the system before calling technical support:

- ▼ Verify card settings, including the coprocessor settings.
- ▼ Ensure that there are no interrupt or I/O conflicts.

When calling for technical support, please have the following information available, it will be needed to assess your system's problem:

- ▼ Vinca registration number
- ▼ Brand and model of the primary and standby machines.
- ▼ Processor type and speed (e.g., Pentium 200).
- ▼ Type and size of disk devices used.
- ▼ Type of disk controllers used.
- ▼ Configuration changes made to the StandbyServer cards.
- ▼ Version of the operating system.
- ▼ Version of LAN Server Advanced.
- ▼ Version of any application software.

Services

After completing the Pre-assistance Check List, you can contact us in the service that best fits your needs:

Method	Access
Phone support	801-223-3104 Monday – Friday, 7:00 am - 6:00 PM (MST)
Internet	http://www.vinca.com/support
E-mail	support@vinca.com
Fax	801-229-2110
BBS	801-224-1210
Compuserve [®]	74774,1425 (non-priority response only)

Chapter 2

Installing on LAN Server Advanced Systems

Requirements/Preinstallation Checklist

Before beginning the installation make sure the following requirements are met:

General Prerequisites

- The standby machine must have at least two physical disk devices—one to hold the boot partition and local partitions, and one to be exported to function as part of the mirrored pair.
- There must be enough disk space on the disk devices in the primary machine to hold all data to be mirrored from the standby.
- The number and type of partitions on the boot disk devices of both the primary and standby machines must be identical to ensure that the drive letter assignments are consistent after failover.
- Each machine must be properly installed and configured to function as a file server on the network, including software and LAN adapters.
- The LAN cards and connecting cable that will function as the Vinca link must be available. These cards can be Vinca's proprietary cards or PRO/100 fast Ethernet cards.
- Each machine must meet the following minimum hardware requirements:
 - 16 MB RAM minimum
 - 386 CPU minimum
 - 250 MB or larger drive recommended
 - SVGA monitor preferred
 - OS/2 version 2.1 or higher
- All data should be backed up before beginning this installation.

LAN Server Advanced-Specific Requirements

- ❑ The LAN Server Advanced software must be installed on both machines, and must not be mirrored. This duplication allows for LAN Server Advanced configuration variations based on hardware differences between the two machines.
- ❑ The disk devices to be mirrored must not contain a Boot Manager partition.
- ❑ LAN Server Advanced requires the mirrored drives to have identical geometries.
- ❑ LAN Server Advanced only mirrors HPFS partitions, not FAT partitions.
- ❑ Have a working knowledge of OS/2, FDISK (or FDISKPM), LAN Server Advanced, and NetFinity.
- ❑ Have the IBM documentation for OS/2, LAN Server Advanced, and NetFinity available.
- ❑ Depending on configuration, knowledge about the domain features of LAN Server Advanced may be required.
- ❑ The system must run LAN Server Advanced 3.0 or higher.


Using Hardware RAID Host Adapters

Hardware-based RAID host adapters can be used in conjunction with *StandbyServer*. To use hardware RAID adapters with the Vinca products, the RAID adapters must have a native OS/2 driver.

These adapters can be a considerable help in configuring disk device systems to fit the requirement of having at least two physical disk devices in the standby and primary machines. Where RAID adapters are used, the phrase physical disk device is interpreted to mean that the operating system perceives any number of disk devices as a single physical device. The number of physical disk devices can be displayed by using the FDISK utility in OS/2.

Installation Overview

This section summarizes the process for installing StandbyServer for OS/2 Warp with a LAN Server Advanced network, detailed instructions follow. For detailed information on installing OS/2, LAN Server Advanced, and NetFinity, see the appropriate IBM documentation.

 **Important!** Each of the installation steps listed below must be completed on each machine, unless specifically instructed otherwise:

1. Install StandbyServer Hardware
Create the Vinca link between the primary and the standby machines that will carry all mirroring traffic.
2. Install or Modify OS/2
Ensure that OS/2 is set up on both the primary and standby machines to recognize the disk device configuration required for StandbyServer.
3. Install LAN Server Advanced on the primary and standby machines with the User Accounts, Domains, Replication services, and machine names as required.
4. Understand the evaluation/validation option. By default, the StandbyServer software is installed as an evaluation application. To validate StandbyServer you must run VNCKEEP.EXE before you run INSTALL.EXE.
5. Install StandbyServer software on both the primary and standby machines.
6. Set which drives *will not* be exported from the standby machine.
7. Install NetFinity Manager on the standby machine and NetFinity Services on the primary machine to enable automatic switching of the server function between the primary and the standby machines.
8. Install mirroring and edit CONFIG.SYS on the primary machine.
9. Modify failover command files as needed to ensure proper switch.
10. Test the system, under controlled conditions, to ensure that it functions properly and that data is accessible after a system failure.

Step 1: Install StandbyServer Hardware

In this procedure the high-speed communication cards that will be used for the Vinca link are installed; these cards can be IBM's PRO/100 fast Ethernet cards or Vinca's proprietary cards.

Be aware of the following for Vinca's proprietary cards:

- ▼ The port and interrupt are set manually with ISA cards, or through software with EISA and MCA cards, and the interrupts are not sharable.
- ▼ The link speed jumper is for a single link in a bi-directional pair and there are four pairs of links on StandbyServer cards.
- ▼ Processor speed settings on the StandbyServer cards are based on the co-processor installed on the card, not the speed of the processor in the machine in which the card is being installed.

IBM PRO/100 Cards

The IBM PRO/100 PCI fast Ethernet card provides a 100 Mbps Vinca link using industry-standard 100 BaseT Ethernet cables. This link must be a dedicated network, isolated from all other Ethernet networks.



Note: Do not install the LAN driver that came with the card.

StandbyServer for OS/2 Warp uses a specialized driver that is installed automatically during the software installation.

1. Turn the machine's power off.
2. Install the adapter card into a free PCI *busmaster* slot.

Not all PCI slots will be busmaster slots. Please consult the computer manufacturer's documentation to identify which slot to install this card in.

3. When cards have been installed in both machines, connect the two using a Category 5 twisted-pair cable. *Do not install the software driver supplied with the card; StandbyServer installs a custom driver for this card.*

When each machine is rebooted it will automatically recognize and configure the PCI card.

ISA 16-bit Vinca Cards

Vinca's 16-bit ISA link cards provide 80Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any ISA or EISA bus machine, though they cannot take advantage of EISA's 32-bit wide data path.

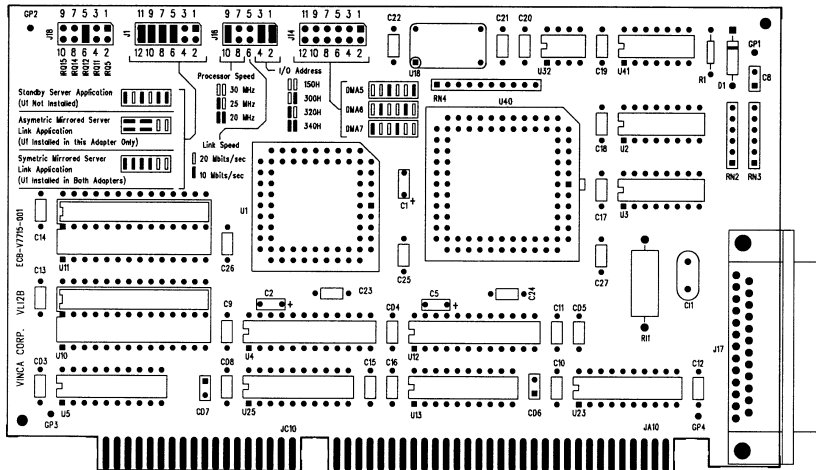
Step 1: Install StandbyServer Hardware

These cards require that the IRQ (interrupt) and port addresses be set manually using jumpers. This section describes how to install the card and set the jumpers.

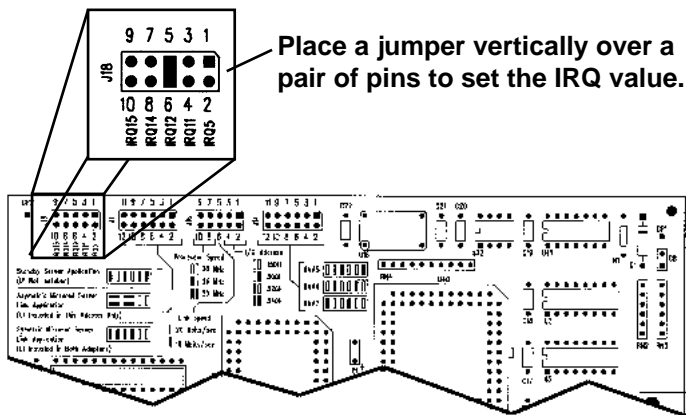
To install the ISA Vinca link cards do the following.

4. Orient the card so the edge connectors are down, the jumpers are at the top left, and the card is facing with the chip side toward you.

The card looks like the following.



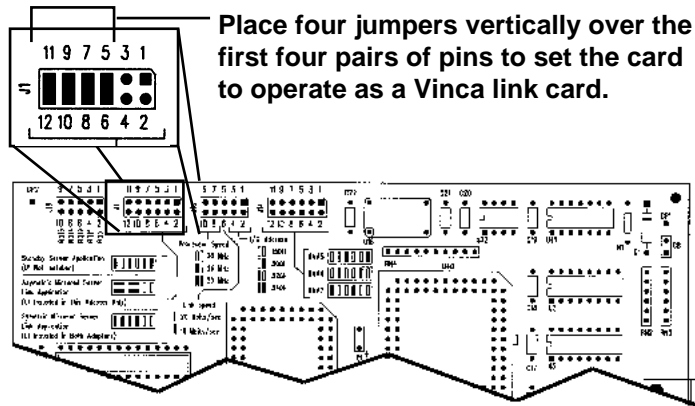
5. Set the IRQ using jumper block J18 at the top left corner of the card. Valid settings are 5, 11, 12, 14, and 15; the default value is IRQ 12. Make sure this interrupt does not conflict with any other installed cards.



To set a jumper, turn the jumper plug vertically and push it down over a column of two pins as shown above. This example shows it set to IRQ 12.

6. Ensure that jumper block J1 is properly jumpered for the "Symmetric Mirrored Server Link Application" setting.

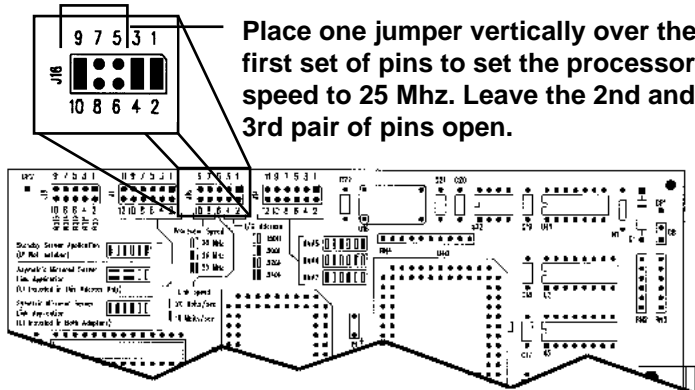
The first four columns of pins should be jumpered.



If the pins are not jumpered as shown above, do so now.

7. Ensure that the processor speed is set to 25 Mhz and that the link speed is set to 20 Mbps using jumper block J16.

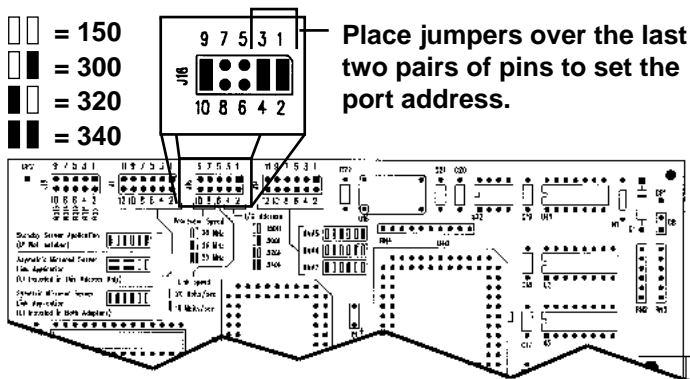
The first pair of pins should be jumpered.



If the pins are not jumpered as shown above, do so now.

- Set the I/O address, also called the port address, using the last two jumpers in J16.

Valid settings are the hexadecimal values 150, 300, 320, and 340; the default value is 340. Make sure this setting does not conflict with any other installed cards.



To set a jumper, turn the jumper plug vertically and push it down over a pair of pins as shown above. This example shows the port address set to 340 hex.

There is one more jumper block labelled J14, but this group is not used for this installation. Those pins should all be unjumped.

Note: Write down the IRQ and port address values set here for each card.

<i>Primary</i>	<i>Standby</i>
IRQ: _____	IRQ: _____
Port: _____	Port: _____

- Insert the properly configured Vinca link card into an appropriate open slot in the file server.

Seat the card firmly in the expansion slot and secure it. Repeat this procedure on each machine.

- When these steps are completed for both machines, connect the two machines using the green high-speed serial communications cable supplied with the cards.

Firmly connect the cable to the Vinca link card and secure it using the connector screws. Be careful not to bend any of the cable's pins when attaching the cable.



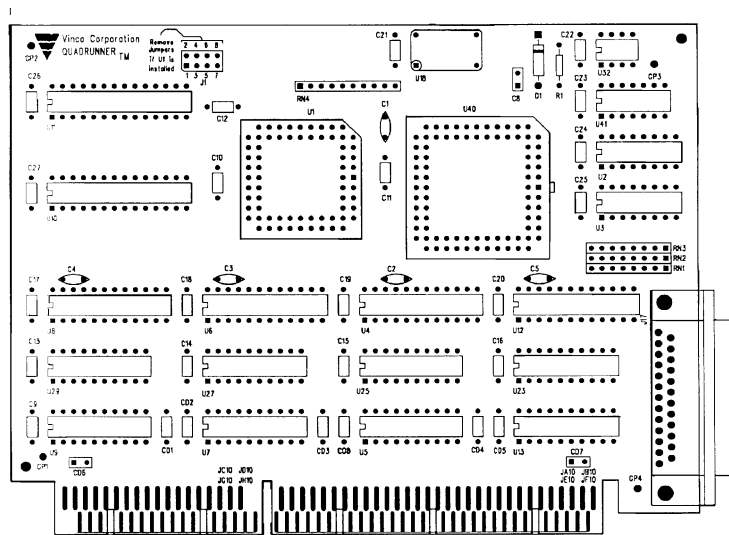
Note: The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if a 50 foot cable is needed, contact Vinca at (801) 223-3100 or contact an authorized Vinca reseller.

The cards and cable are now properly installed.

EISA 32-bit Vinca Card

Vinca's 32-bit EISA link cards provide 160Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any EISA bus machine and use EISA software configuration.


To install the EISA Vinca link cards do the following.



1. Verify that J1 has no jumpers installed.
2. Turn the machine's power off.
3. Install the adapter card into a free slot.

4. Turn on the machine.
5. Run the EISA configuration for that machine.
6. When prompted insert the Vinca diskette containing the !VNC7261.CFG file.
7. Configure the settings to non-conflicting port and IRQ settings.
8. Verify that the link speed is set at 20 Mbit/sec and the processor speed is set at 25MHz.
9. When these steps are completed on both machines, connect the two machines using the green high-speed serial communications cable supplied with the cards.


Firmly connect the cable to the Vinca link card and secure it using the connector screws. Be careful not to bend any of the cable's pins when attaching the cable.

 **Note:** The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if a 50 foot cable is needed, contact Vinca at (801) 223-3100 or contact an authorized Vinca reseller.

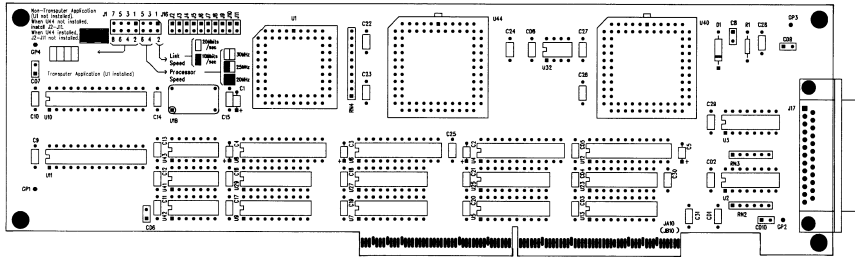
The cards and cable are now properly installed.

MCA 32-bit Vinca Card

Vinca's 32-bit MCA link cards provide 160Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any MCA bus machine and use software configuration.

 **Warning:** The current version of this card does not support shared interrupt request levels. Select a unique interrupt request level for this adapter so no other adapters share it. Allowed interrupt levels are IRQs 5, 11, 12, and 15. IRQ levels can be viewed and/or set with the MCA Reference utility.

To install the MCA Vinca link cards do the following.



1. Verify that J1 has no jumpers installed.
2. Turn the machine's power off.
3. Install the adapter card into a free slot.
4. Insert the reference diskette into the floppy disk drive.
5. Turn the machine's power on.
6. Follow the prompts as they appear on the screen.
7. When prompted, insert the Vinca diskette (which contains the @5131.ADF file).
8. Configure the settings to non-conflicting port and IRQ settings.
9. Follow the screen prompts until system resources are configured.
10. When these steps are completed on both machines, connect the two machines using the green high-speed serial communications cable supplied with the cards.

Firmly connect the cable to the Vinca card and secure it with the connector screws. Do not bend any of the cable's pins when attaching the cable.



Note: The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if a 50 foot cable is needed, contact Vinca at (801) 223-3100 or contact an authorized Vinca reseller.

The cards and cable are now properly installed.

Step 2: Install or Modify Disk Configuration

This section helps ensure that both the primary and standby machines have the disk device configuration required for StandbyServer for OS/2 Warp. The OS/2 installation documentation and software are needed to complete this procedure.

Be familiar with the following:

- ▼ Drive letter assignments for all partitions.
- ▼ Drive formats—FAT and/or HPFS (verify that all devices are formatted correctly—LAN Server Advanced can only mirror HPFS partitions).
- ▼ The drive letter where OS/2 will be installed in each of the two machines.
- ▼ Drive letter of the primary partition on the first disk device in each of the two machines.

Sufficient free space must be available on the target disk devices (the devices in the primary machine). Fault Tolerance Setup in the mirroring installation process automatically partitions the free space as a mirror.

If existing data has not been backed up yet, do so now.

What To Do With Existing Data

If there is existing data, make sure it is on an HPFS partition on a disk device in the standby machine that is not the first disk device. It may be necessary to back up and restore data, or move a disk device from one machine to another to put it in this state, but it must be on a partition that LAN Server Advanced can mirror.

Disk Device Configuration

If installing on an existing system, the configuration must be changed to make it work with StandbyServer. Use OS/2's installation procedure, along with the FDISK or FDISKPM utility on each of the machines, to ensure the following:

- ▼ At least two disk devices in each machine.
- ▼ The first disk device in each machine must have:
 - A primary partition (which may contain Boot Manager).
 - A partition in which OS/2, LAN Server Advanced, StandbyServer software, and NetFinity Manager or NetFinity Services are installed.
 - The same number and type of partitions in both machines.



Note: Partitions on the first disk device aren't mirrored.

- ▼ Mirrored disk devices in both machines must have the same number of heads and sectors/track. If uncertain about this, run GEO.EXE (on the StandbyServer floppy disk).



Note: The term “mirrored disk device” encompasses all of the disk devices installed on either machine that will function as part of a mirrored pair.

- ▼ Each mirrored disk device in the standby machine is treated as if it physically resides in the primary machine. During normal operation, this is the primary disk device despite its location in the standby machine.
- ▼ Mirrored disk devices in the primary machine are the secondary drives of the mirrored pair.
- ▼ Vinca recommends that mirroring be started from the largest disk device to the smallest disk device. This helps to prevent disk fragmentation and maintain the required contiguous free space for the mirrored partitions.

Example: D: 800MB, E: 500MB, F: 450MB.

Step 3: Install or Modify LAN Server Advanced

Installation Instructions

Complete the following instructions to install or modify LAN Server Advanced before installing *StandbyServer*. The instructions below are an example only, the actual system components may automatically detect a different sequence of screen selections.

LAN Server Advanced must be installed on both machines. The order in which they are installed is not important.

1. At one machine, insert the LAN Server Advanced installation diskette or CD and start the installation process as described in the IBM LAN Server Advanced documentation.
2. Install LAN Server Advanced according to the instructions in the IBM documentation, keeping in mind the following:

If the primary machine is installed as a domain controller then the standby machine also must be installed as a domain controller.

The Fault Tolerance component must be installed on the primary machine but not on the standby.

The server name must be the same on both machines.

The domain name must be the same on both machines.

Set **Start the server automatically** to **Yes** for the primary machine, **No** for the standby machine.



Important! Do not select **Start the server automatically** on the standby machine.

3. After the installation program is complete, reboot the machine. Repeat steps 1 and 2 for the other machine.

Step 4: Understanding the Evaluation/Validation Option

Each of the Vinca applications in the Cluster Pack can be run as 30-day evaluation programs. When you decide which program you want to validate, you need to contact Vinca and exchange the Cluster Pack serial number for a Vinca, product-specific serial number. After installing *StandbyServer*, it can be used for 30 days during which pop-up warnings can be invoked (using NetFinity) to remind you how many days are left in the evaluation period. After 30 days, an Expiration notice is invoked and the application will not function.

By default, *StandbyServer* for OS/2 is installed as an evaluation program where you are not prompted to enter a registration number. As an evaluation program, you are prompted to enable and set alerts to notify you when the evaluation time is coming to a close.

Whether or not you evaluate the product first, when you want to validate *StandbyServer* for OS/2, you must contact Vinca to register the product and exchange the Cluster Pack serial number for a *StandbyServer* for OS/2 registration number. Once you have the new registration number, you can perform the standard installation.



Note: If you choose to run *StandbyServer* for OS/2 as an evaluation product and then decide to validate it, you will need to reinstall the product.

Vinca can be contacted by Internet e-mail, phone, fax or U.S. Mail at:

E-mail: validation@vinca.com

Phone: 800-274-6042

Fax: 801-223-0199

U.S. Mail: Vinca Corp., 1815 South State Street, Suite 2000, Orem, Utah 84097.

When contacting Vinca, you will be asked to provide the following information:

- ▼ Cluster Pack serial number
- ▼ Contact person
- ▼ Company name
- ▼ Address
- ▼ Phone
- ▼ Fax (optional)
- ▼ E-mail (optional)

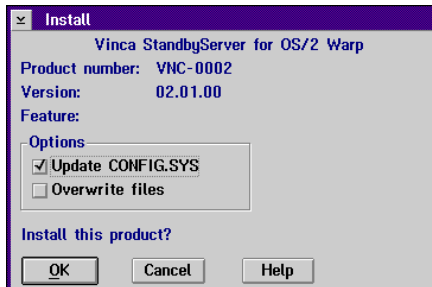
Step 5: Install StandbyServer Software

This procedure is used to install *StandbyServer* on each machine. After installing the software to one server, you must repeat the steps on the other server to complete the install. The installation must be run from the local hard drive, so you will need to copy the contents of the SBSOS2 directory on the CD-ROM to a temporary installation directory on your hard drive.

To install StandbyServer for OS/2

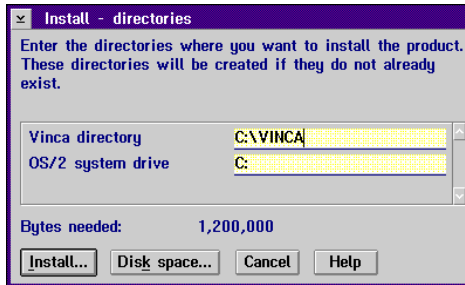
1. Insert the Cluster Pack CD-ROM into the CD-ROM drive of the primary machine.
2. Open an OS/2 command prompt.
3. Create a temporary directory and copy the contents of the SBSOS2 directory on the CD-ROM to the created directory. For example, `md c:\tempinst`. And copy `cd:\sbsos2*. * c:\tempinst`.
4. Change to the newly created directory on the local hard disk.
5. If you want to install the evaluation product skip this step. If you have contacted Vinca and have received your new registration number, from the prompt type `VNCKEEP.EXE` and press Enter.
6. From the prompt, type `INSTALL.EXE` and press Enter.
7. Click Continue.

The Install dialog box appears.



8. Leave "Update CONFIG.SYS" checked. If you previously installed *StandbyServer* for OS/2 Warp on this machine, check "Overwrite files."
9. Click OK.

The Install-directories dialog box appears.



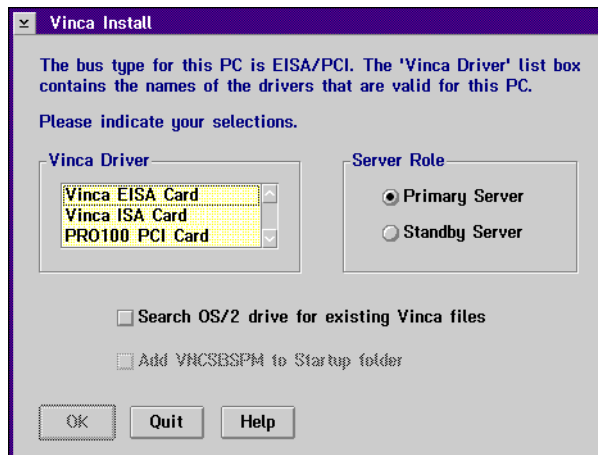
10. Make sure the information is correct and click Install.

The Vinca directory is the directory where Vinca software will be installed. You can use the “Disk space” button to view disk usage on local disks.

After you click Install, a progress bar appears as files are copied to their proper locations. During the file copy stage, you are prompted to enter a registration number, or enable the evaluation warnings depending on which installation you to perform.

11. If this is a standard installation, enter the registration number received from Vinca. If this is an evaluation installation, you can enable NetFinity alerts to notify you when the evaluation period is coming to a close.

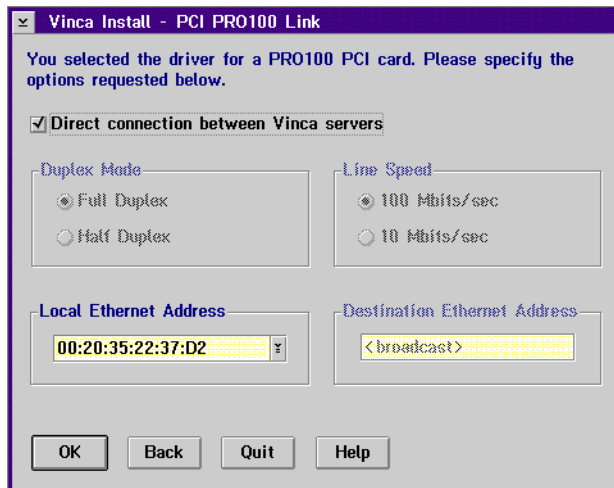
The bus-and-driver information dialog box appears. A sample is shown; yours may vary with the bus type(s) and link card in your machine. If you have only one bus, and Vinca supports only one card for that bus, the Vinca Driver section will not be present.



12. Choose the server role (Primary or Standby) for this machine.
If you click Standby Server for the role, the “Add VNCSBSPM to Startup folder” checkbox becomes active.
13. If this is to be the standby machine, check or clear the “Add VNCSBSPM to Startup folder” checkbox as you wish.
If VNCSBSPM is in the Startup folder, the Vinca software will start up automatically; otherwise, you must start the program yourself after a reboot to ensure fault tolerance. However, in some configurations automatic startup can lead to problems—for example, if the primary machine does not boot quickly enough the standby will attempt to switch over. In addition, VNCSBSPM.EXE must not be running if CHKDSK is going to be run on the standby machine.
14. Choose the correct driver for the bus type and card you are using.
15. Click OK to continue with the installation.

The installation program checks the installed Vinca link card.

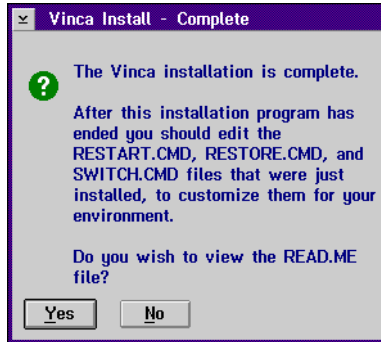
If you are using PRO/100 cards for the Vinca link a settings screen appears where you can set parameters. The **Direct connection between Vinca servers** checkbox should be marked. The Ethernet address of the card is taken from the card itself and should be correct. Press OK to continue.



A confirmation dialog appears reviewing the card settings. Press OK to continue with the installation.

16. If a settings dialog box appears, click OK to continue.

A progress bar appears, and then the installation complete screen.



17. Click Yes or No as appropriate.

A dialog box informing you of changes to CONFIG.SYS appears (this will not take place until after you read the READ.ME file if you click Yes).

18. Click OK.

The installation program returns to the main installation screen.

19. Choose Exit from the File menu.

20. Eject the StandbyServer installation disk from the floppy drive.

If you are using a Vinca ISA card and the port and interrupt settings were changed from the default values, the CONFIG.SYS file must be updated to reflect the altered setting. Edit the CONFIG.SYS file and find the line that begins as follows:

```
BASEDEV=VNCIL01.SYS /I:12 /P:340 /O:2
```

Replace the number in the /I:12 switch to reflect the new IRQ setting, and change value on the /P:340 switch to reflect the correct port address.

21. Properly shut down the machine.

22. Repeat Steps 1 through 17 for the other machine.

When installation is complete, both machines will be shut down.

Copying FTMONIT.EXE (LAN Server Advanced 3.0 only)

Mirroring with Vinca software and hardware requires the LAN Server Advanced 4.0 or higher version of FTMONIT.EXE. If you use LAN Server Advanced 3.0, do the following on the primary machine (only).

1. Insert the *StandbyServer* for OS/2 Warp installation disk into drive A of the primary machine.
2. Copy the file FTMONIT.EXE from the installation disk to the directory where you installed LAN Server Advanced, overwriting the installed version of FTMONIT.EXE.

Step 6: Set Local Disks for the Standby Machine

StandbyServer automatically exports all drives from the standby machine except those specifically excluded from the *StandbyServer* application. When these devices are exported they will appear to the primary machine as local disks. They will be locked and inaccessible to the standby machine until a failover occurs, then the mirrored data on them will be accessible.

Use the Disk Export utility to determine which disks *will not* be exported to the primary machine; all disks are automatically exported except those excluded using this utility.

There are several rules to keep in mind when exporting disks:

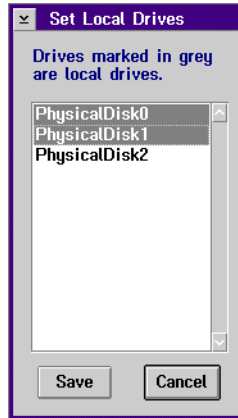
- ▼ Local devices must start with and include PhysicalDisk0.
- ▼ Local devices must be selected in sequence.
- ▼ At least one device must be made available for export.
- ▼ Partitions must be created on the primary server that reflect local usage on the standby machine to ensure drive lettering is consistent when switchover takes place. For example, if there is two physical disk devices in the primary server, and three in the standby machine, the first physical disk device in the primary server must be assigned two drive letters (i.e., C and D), so that drive E in both machines would be available for the mirrored set (i.e., E and E').

Do the following to determine which disks are exported:

1. Start the *StandbyServer* application (VNCSBSPM) on the standby machine.
2. Choose Drives... from the Export menu.

Step 7: Install and Configure NetFinity

The Set Local Drives dialog appears. Physical disk devices are listed in the order reported to the operating system.



3. Mark the drives that *will not* be exported to the primary machine.
Click on a disk or highlight it and press [Space] to keep it from being exported.
4. When all local disks are marked choose the Save button.
StandbyServer checks to make sure you have met the conditions listed earlier. If your selections violate these criteria an error message appears. Press [Enter] to clear the error, alter your selections to meet the criteria listed at the beginning of this section, and choose Save again.
If all conditions are met, a message appears saying that you must restart StandbyServer for your selections to be enabled.
5. Exit and restart StandbyServer.
Choose Exit from the File menu to exit StandbyServer.

Step 7: Install and Configure NetFinity

In this procedure, the switching process between the primary and standby machine will be automated for unattended switchover in the event of a system failure.

The installation of NetFinity is optional. However, if it is not installed, then the roles of the primary and the standby machines must be manually switched in the event of a system failure. The network users must wait until that manual switching takes place to continue working. Automatic switching requires the installation of NetFinity.

Before NetFinity can be installed, the LAN Server requestor must be installed on the standby machine, if required, the requester can be started with a computer override name. For example,

```
NET START REQ /CO:STDBY
```

Installation Instructions

Complete the following instructions to install NetFinity Services on the primary machine and NetFinity Manager on the standby machine:

Some of the following instructions refer to the NetFinity documentation (NetFinity Services and NetFinity Manager manuals). Refer to these manuals as needed for more information about NetFinity.



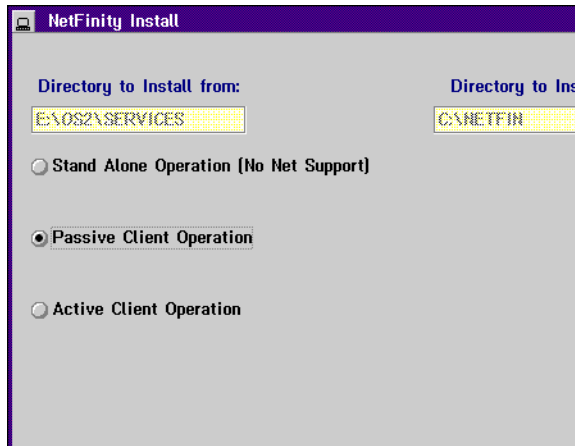
Note: NetFinity includes two programs; NetFinity Services and NetFinity Manager. Each must be installed on the correct machine to function properly, as listed below.

- ▼ NetFinity Services is installed and runs on the primary machine.
- ▼ NetFinity Manager is installed and runs on the standby machine.

Installing NetFinity Services on the Primary Machine

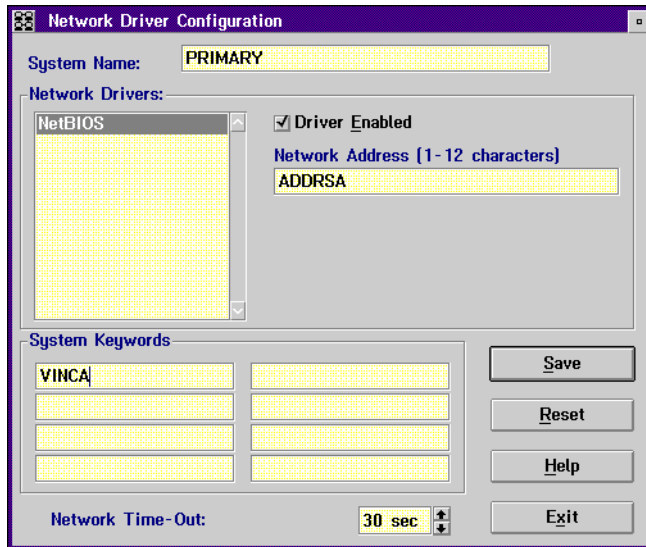
1. Insert the NetFinity Services for OS/2, Services Diskette #1 in the floppy drive in the primary machine (or, if you are installing from CD-ROM, insert the NetFinity CD-ROM into the CD-ROM drive).
2. Open an OS/2 command prompt.
3. Run the NetFinity installation program.

The NetFinity Installation dialog box appears.



4. In the “Directory to Install from” field, type the drive letter of the floppy drive or CD-ROM drive.
5. In the “Directory to Install to” field, type the drive letter and path in the primary machine where NetFinity is to be installed.
See the figure above for an example.
6. Select “Passive Client Operation”.
7. Click Install.

The Network Driver Configuration window appears.



8. In the System Name field, type the System Name selected for the primary machine.



Warning: Both the primary and standby machines must have *unique* names. The name assigned in this window may be the same name assigned the primary machine during LAN Server Advanced installation, but must not be the same name that will be assigned to the standby machine during the installation of NetFinity Manager.

9. Select a Network Driver from those displayed.

When making a selection, the Network Driver assigns a network address to the system. If NetBIOS is selected, a network address will be selected and displayed in the Network Address field. The default name may be displaced by entering any 1-12 character name.

10. Check the Driver Enabled checkbox to activate the driver on start-up.



Note: Refer to the IBM NetFinity manual for additional information about System Keywords, Network Time-Out, and support of multiple network interfaces.

11. Enter one or more keywords into the System Keywords fields.

Later, when NetFinity is configured on the standby machine, at least one keyword must match between the two systems.

12. Select Save to save the configuration on the primary machine.
13. Select Exit.

NetFinity displays a list of commands that must be added to the CONFIG.SYS file.

 **Note:** To change the saved Network Driver Configuration after finishing the installation, select the Network Driver Configuration object from the NetFinity folder.

14. Choose Yes.

If No is chosen, the commands will be saved as CONFIG.NEW in the destination directory and will have to be manually added later.

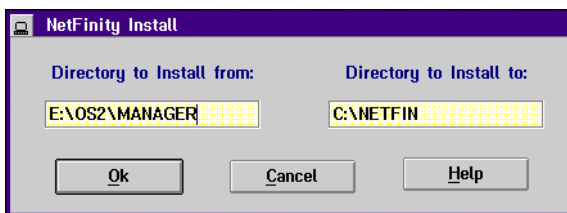
15. Remove the installation diskette.

Installing NetFinity Manager on the Standby Machine

The installation of NetFinity Manager on the standby machine is very similar to the installation of NetFinity Services on the primary machine. Before installing NetFinity Manager on the standby machine, refer to instructions in the IBM NetFinity Manager manual.

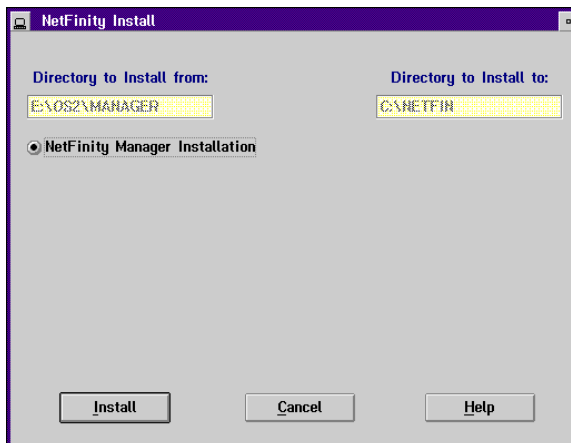
1. Insert the NetFinity Manager for OS/2, Manager Diskette #1 in the floppy drive in the standby machine (or if installing from CD-ROM, insert the NetFinity CD-ROM into the CD-ROM drive).
2. Open an OS/2 command prompt.
3. Run the NetFinity installation program.

The NetFinity Install directory selection window appears.



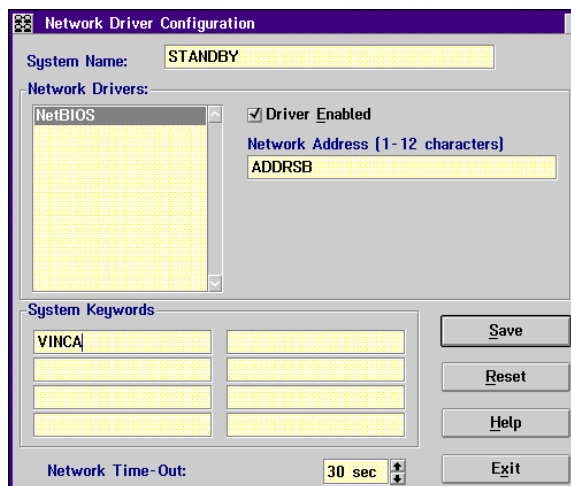
4. Confirm that the dialog box shows the correct directories (modify if necessary) and click OK to go on.

The main NetFinity Install window appears.



5. Select NetFinity Manager.
6. Click Install.

The Network Driver Configuration window appears.



7. In the System Name field, type the System Name selected for the standby machine.



Warning: Both the primary and standby machines must have *unique* names. The name must not be the same name assigned the primary machine during the installation of NetFinity Services.

8. Select a Network Driver from those displayed.

When making a selection, the Network Driver assigns a network address to the system. If NetBIOS is selected, a network address will be selected and displayed in the Network Address field. The default name may be displaced by entering any 1-12 character name.

9. Mark the Driver Enabled box to activate the driver on start-up.



Note: Refer to the IBM NetFinity manual for additional information about System Keywords, Network Time-Out, and support of multiple network interfaces.

10. Enter one or more keywords into the System Keywords fields. Make sure that at least one is the same as a keyword defined for the primary machine. At least one keyword must match between the two systems.

11. Select Save to save the configuration on the standby machine.

12. Select Exit.

NetFinity displays a list of commands that must be added to the CONFIG.SYS file.



Note: To change the saved Network Driver Configuration after finishing the installation, select the Network Driver Configuration object from the NetFinity folder.

13. Choose Yes.

If No is chosen, the commands will be saved as CONFIG.NEW in the destination directory and will have to be added manually later.

14. Remove the installation diskette or CD-ROM.

15. Reboot the machines in the correct order, as follows:
 - a. Shut down the primary machine completely.
 - b. After the primary is shut down, shut down the standby machine.
 - c. Reboot the standby machine.
 - d. Start the StandbyServer application, VNCSBSPM.EXE.
 - e. After the StandbyServer window appears restart the primary machine.
 - f. Verify that the StandbyServer window shows the word **CONNECTED**.

Starting NetFinity on the Standby Machine

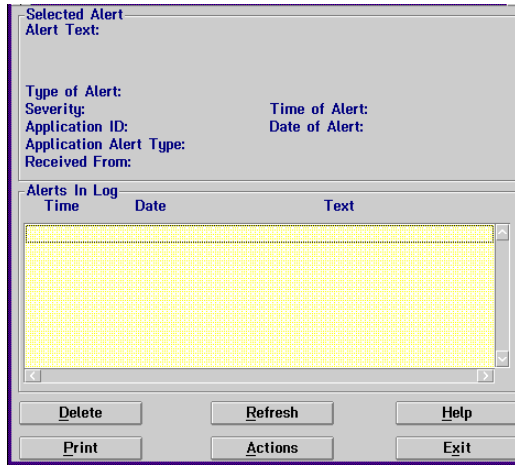
The following instructions start the operation of NetFinity. Refer to the NetFinity Services manual for information about starting NetFinity on the primary machine. Refer to the NetFinity Manager manual for information about starting NetFinity on the standby machine.



Important! This procedure will start NetFinity and configure the automatic switching capability of StandbyServer. These instructions must be performed on the standby machine, not on the primary machine.

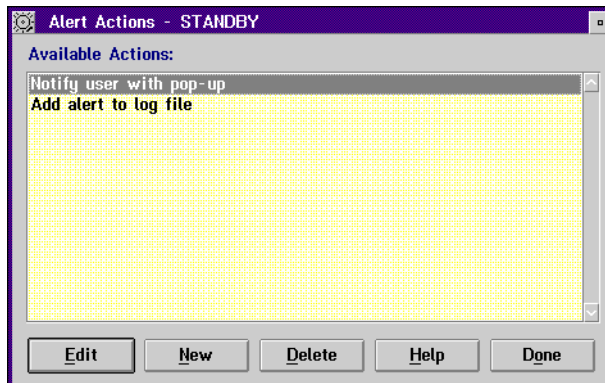
1. Open the NetFinity folder.
2. Open the NetFinity Service Manager icon.
3. From the NetFinity Service Manager folder, open Alert Manager.

The Alert Log dialog box appears.

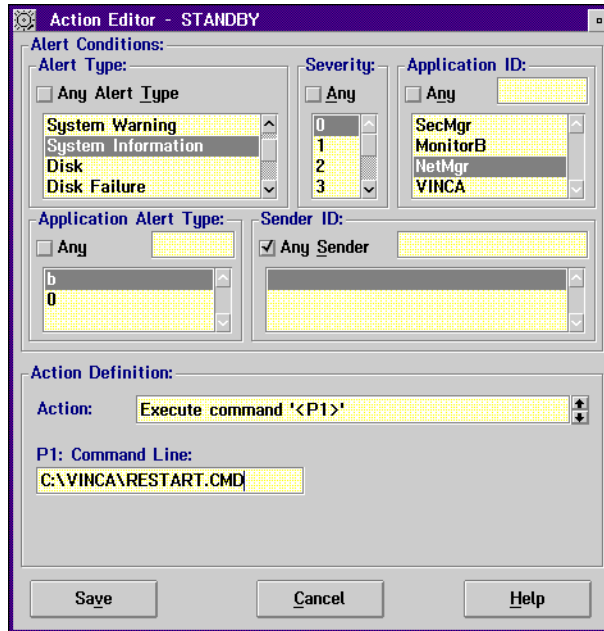



4. From the Alert Log dialog box, select Actions.

The Alert Actions dialog box appears.



- From the Alert Actions dialog box, select New.
The **Action Editor** dialog box appears.



 **Important!** The **Action Editor** dialog box contains vital information and must be completed exactly as in the following step.

- Fill in the fields in the Action Editor dialog box as follows:
If the indicated selection is not available in the list box, type it into the corresponding text entry window and then press [Enter].
 - From the Alert Type list box, select System Information.
 - From the Severity list box, select 0 (zero).
 - From the Application ID list box, select NetMgr.
 - From the Application Alert Type list box, select or type b.
 - Check the Any Sender checkbox in the Sender ID field.
 - From the Action field within Action Definition, select the following:
Execute command '<P1>'
 - In the P1: Command Line field, type the following:
[drive]:\vinca\restart.cmd

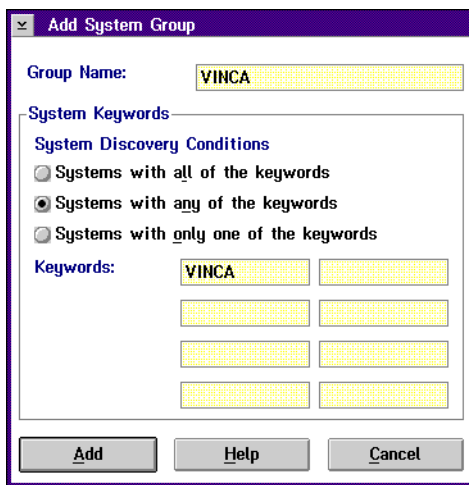
Before exiting the Action Editor dialog box, verify that the P1: Command Line field includes the name of the installed switchover command file.

7. Exit and save out to the NetFinity Service Manager window.
8. Open Remote System Manager.

The **System Group Management** window appears.

9. Choose Add Group from the Group menu.

The Add System Group dialog box appears.



10. In the Group Name field, type an appropriate name.
11. Click “Systems with any of the keywords” under System Discovery Conditions.
12. Enter one or more appropriate keywords into the Keywords fields. At least one keyword must be the same as the matching keyword that was configured in the NetFinity Driver Configuration dialog box when NetFinity was installed on each machine.

In other words, each machine must have at least one keyword that is also configured on the other machine, and that keyword must be entered here.

13. Click Add.

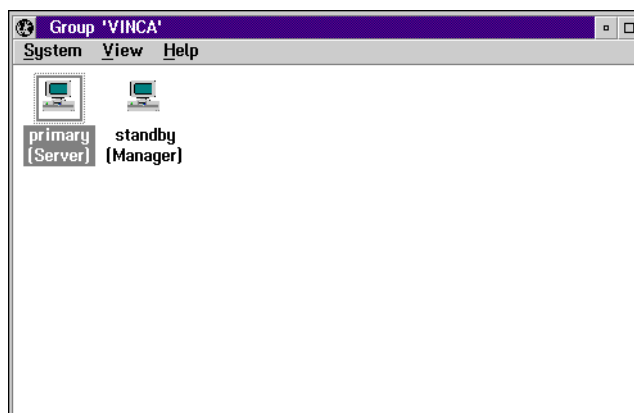
The Add System Group dialog box closes, and the group now appears in the System Group Management window.

14. Double-click on the group just created to open it.

15. From the System menu, choose Discover Systems.

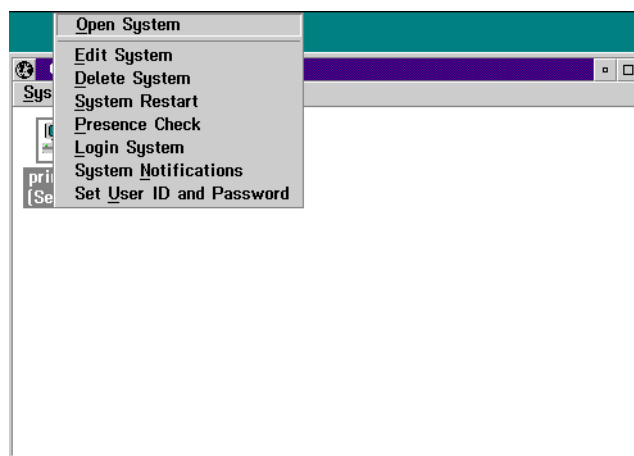
The primary and standby machines will be discovered (assuming the shared keyword was entered in Step 12).

The following illustration is an example of such a group.



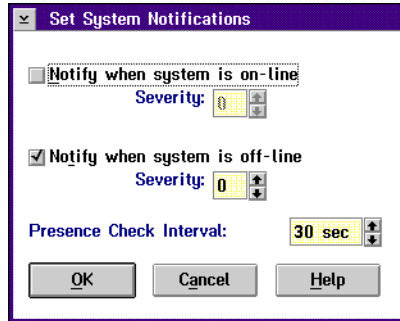
16. In the Group window, click mouse button 2 (usually the RIGHT mouse button) on the icon which represents the primary machine.

A popup menu of options appears, as shown in the next illustration.



17. From the menu, select System Notifications.

The Set System Notifications dialog box appears.



18. In the Set System Notifications dialog box, select Notify when system is off-line.

Note: When this option is enabled, switch over is automatic when the primary server fails. If this option is disabled, the standby machine will not switch over unless the process is done manually.

19. In the Set System Notifications dialog box, set Presence Check Interval to 30 seconds.
20. After System Notifications are set, select OK.

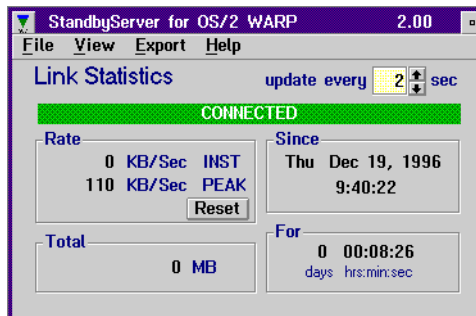
NetFinity is now installed and the standby machine is ready to take over for the primary in the event of a primary machine failure.

Step 8: Install Mirroring and Edit CONFIG.SYS

Install Mirroring

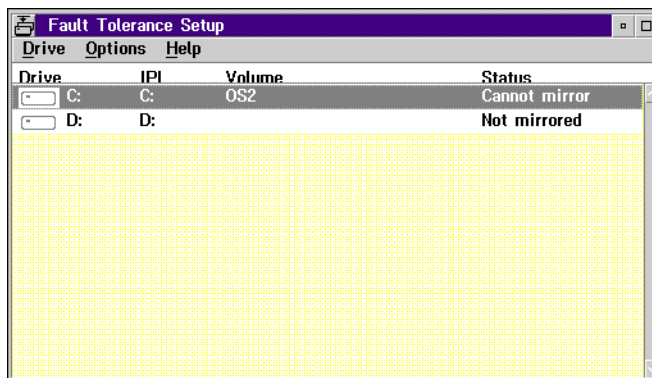
The following steps are a guide to the mirroring installation procedure. If there is existing data, it must be placed on the HPFS formatted drives in the standby machine before beginning this procedure. The procedure assumes that the machines are currently shut down.

1. Reboot the machines in the correct order, as follows:
 - a. Boot the standby machine.
 - b. Start the StandbyServer application, VNCSBSPM.EXE.
 - c. After the Vinca StandbyServer window appears on the standby machine, boot the primary machine.
 - d. Verify that the Link Statistics window of the StandbyServer application shows the word **CONNECTED**. To activate the Link Statistics window, choose Link from the View menu.




2. On the primary machine, run Fault Tolerance Setup (in the IBM LAN Services folder).


The Fault Tolerance Setup window appears.



- In the Fault Tolerance Setup window, highlight the disk device to be mirrored.

The disk device to be mirrored is in the standby machine.

 **Note:** The partition in the primary machine must have enough free space to be mirrored from the partition in the standby machine. If there is sufficient free space, the Fault Tolerance Setup program creates the partition on the primary machine's disk device.

 **Important!** When creating multiple partitions of different sizes, always start by mirroring the largest partition first. Then mirror the next largest partition and proceed in descending order, mirroring the smallest partition last.

- From the Drive menu, select Mirror.

The **Status** column changes to **Pending mirror** while the partition is being mirrored.

- Repeat Steps 3 and 4 for each partition to be mirrored.
- After the last partition has been mirrored, exit the Fault Tolerance Setup window.

The **Partition Changes** dialog box appears, confirming the changes.

- Click Save to save the partition changes.
- Wait until the data is copied between the drives in the two machines.

The length of time it takes depends on the size of partitions created, the amount of data, and the speed of the system. The **Copying Data** window displays the drive letter and the percent complete while the system is copying the data within the partitions.

9. Reboot the primary machine.

Make sure the standby machine is running and the Vinca software is running on the standby machine before rebooting the primary.

Edit CONFIG.SYS on Primary Machine

This procedure changes the primary machine's CONFIG.SYS file to keep CHKDSK from running on the mirrored disk devices at boot time, while still allowing CHKDSK to run on disk devices that are not mirrored.



Important! During recovery, it is important that CHKDSK is not run on the mirrored disk devices when the primary machine is booted. These instructions must be completed to give the system administrator control over the direction of the re-mirroring process after a failure of the primary machine. This is absolutely essential to the correct functioning of StandbyServer and the protection of the data on the system.

1. Find the following line in CONFIG.SYS on the primary machine:

```
IFS=(Path)\HPFS386.IFS
```

Example: IFS=D:\IBM386FS\HPFS386.IFS /A:*

2. Change the asterisk (*) in the line shown above to a list of the unmirrored disk devices.

Example: If C: and D: were the unmirrored devices on the primary machine, edit the line to read as follows:

```
IFS=D:\IBM386FS\HPFS386.IFS /A:CD
```

3. Find the following line in the CONFIG.SYS file:

```
RUN=(Fully Qualified Path)FTMONIT.EXE
```

4. Add VERIFY:NO to the statement.

```
RUN=(Fully Qualified Path)FTMONIT.EXE /VERIFY:NO
```

5. Verify that VNCSBS.ADD is the last *.ADD line in CONFIG.SYS.



Warning: The VNCSBS.ADD line MUST be the last *.ADD line in the CONFIG.SYS file. Move all Vinca entries to the end.

6. Reboot the primary machine.

Make sure the standby machine is running and the Vinca software is running on the standby machine before rebooting the primary.

Step 9: Modify Switchover and Recovery Command Files

The RESTART.CMD command file is called in the event NetFinity detects a failure on the primary machine. You can modify RESTART.CMD to call SWITCH.CMD or just exit out under specified failure conditions; SWITCH.CMD controls the actual switchover process. VNCRCVR.CMD is used during recovery to return the standby machine to the standby state before booting the repaired primary machine. These files can contain any valid OS/2 .CMD file commands. For example, if a LAN Server Advanced file server is also a Notes server, have the SWITCH.CMD file start both LAN Server Advanced and Notes after switchover.

The files as installed by Vinca are samples. Modify them to fit system needs, according to the suggestions contained in comments in the files. For VNCRCVR.CMD, ensure that the following things happen when it is run:

1. LAN Server Advanced is stopped on the standby machine.
2. CHKDSK /F is run on each mirrored disk device to update the superblock on the HPFS partition, causing it to differ from its mirror secondary on the primary machine and guaranteeing that the Fault Tolerance system detects that the partitions are not synchronized.

To avoid possible errors, run CHKDSK on each disk device by changing the default drive letter and then running CHKDSK /F instead of running CHKDSK with a drive letter option. For example, enter:

```
E:  
CHKDSK /F
```

```
G:  
CHKDSK /F
```

rather than

```
CHKDSK E: /F  
CHKDSK G: /F
```

3. On the standby machine, any network services required by the configuration (such as Requester and Replicator for a Domain Controller) are started up.
4. Any other services or applications that need to be started before LAN Server Advanced are started up.
5. LAN Server Advanced is started on the standby machine.
6. Any other services or applications that need to be started up after LAN Server Advanced.

Step 10: Test the Installation

In this procedure, the system will be tested under controlled conditions to ensure that it functions properly and that the data is mirrored correctly during a system failure. Create data on the mirrored disk device, force the connection to fail, and then verify that the standby machine took over the role of the server and the data was safely mirrored and is available.

A third machine (a workstation) will be needed from which to verify the mirrored data during the forced server failure condition.



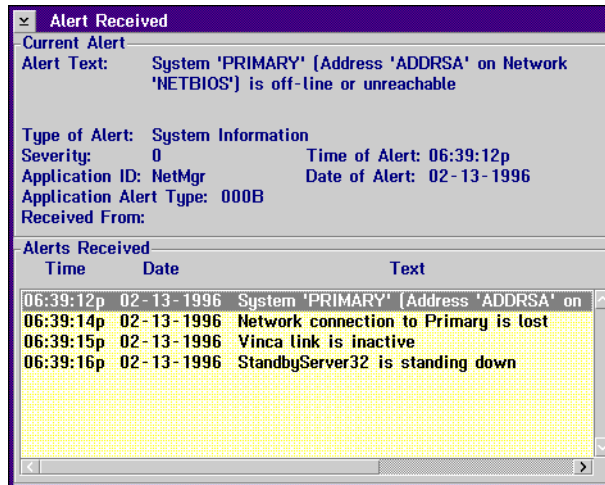
Warning: If there is real data on this system and a backup has not been made, DO IT NOW.

1. From a workstation, create and save a data file on one of the mirrored disk devices.

The data entered in this file can be as simple as a single word.

2. Disconnect first the Vinca cable, then the network cable from the primary machine (leave the standby machine running normally).

This simulates a cable link failure. From the StandbyServer window on the standby machine, the CONNECTED message is replaced by the NOT CONNECTED message. The Alert Received window appears on the standby machine.



3. After the standby machine has completed the switch to the role of the server, from a workstation, verify that the data created in Step 1 is on the correct disk device and the data in the file is identical to what was typed previously.

At this point, the primary machine is unavailable to the network. Next, recover from the situation as if the primary machine had failed and had been repaired.



Warning: Do not reboot the primary machine at this point. If the proper sequence is not followed, the direction of the mirroring process is reversed and the data on the disk devices in the standby machine will be over-written.

4. Run the modified VNCRCVR.CMD file on the standby machine.
5. Shut down the primary server and then reconnect both the Vinca link and the network cables.
6. Reboot the primary machine.
FTMONIT detects a difference in the mirror partitions and logs the errors during the boot process.
7. Start FTADMIN on the primary machine.
The mirrored drives appear cracked in FTADMIN.
8. Select Correct All from the Error menu to restore the mirrors.



Note: If the mirrored disk devices do not appear cracked, it is usually the result of improperly running, or forgetting to run CHKDSK on the primary mirror partitions in the standby machine, before booting the primary machine. Shut down the primary machine, terminate StandbyServer on the standby machine and run CHKDSK on the primary mirror partitions as described above. Restart StandbyServer and re-boot the primary machine. Another possibility is that the FTMONIT line in CONFIG.SYS does not include the /VERIFY:NO parameter—check CONFIG.SYS. If the mirrors still do not appear as cracked mirrors in FTADMIN, call Vinca technical support for help before proceeding.

9. Start LAN Server Advanced on the primary machine.

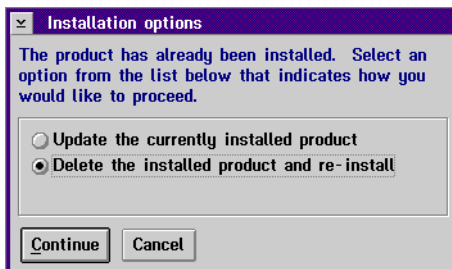
If problems occur during the testing process, refer to *Chapter 4: Recovery Procedures and Technical Support*.

Uninstalling Vinca Software

Use this procedure to remove Vinca software from a machine.

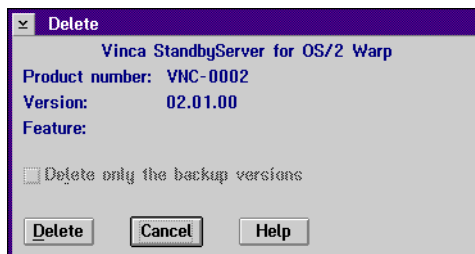
1. Run the Install icon in the Vinca folder.
2. Choose the Continue button.

A dialog box appears indicating that StandbyServer is already installed.



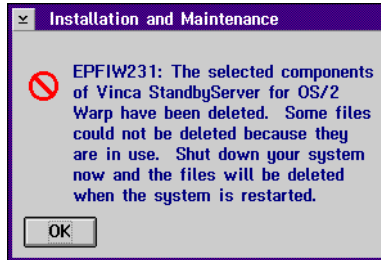
3. Choose the **"Delete the installed products and re-install"** radio button, then choose the Continue button.

The Delete dialog box appears.



4. Click Delete.

A progress bar appears as files are deleted. When *StandbyServer* has been completely removed, the following dialog box appears:



5. Click OK.

StandbyServer components are still loaded in RAM. It is not necessary to shut down the system immediately, but doing so will free up this memory.

6. Choose Exit from the File menu. Restart if desired.

Chapter 3

Installing on OS/2 Systems without LAN Server Advanced

Requirements/Preinstallation Checklist

Before beginning the installation make sure the following requirements are met, and that you are aware of the following issues:

General Prerequisites

- ❑ The standby machine must have at least two physical disk devices—one to hold the boot partition and local partitions, and one to be exported to function as part of the mirrored pair.
- ❑ There must be enough disk space on the disk devices in the primary machine to hold all data to be mirrored from the standby.
- ❑ The number and type of partitions on the boot disk devices of both the primary and standby machines must be identical to ensure that the drive letter assignments are consistent after failover.
- ❑ Each machine must be properly installed and configured to function as a file server on the network, including software and LAN adapters.
- ❑ The LAN cards and connecting cable that will function as the Vinca link must be available. These cards can be Vinca's proprietary cards or PRO/100 fast Ethernet cards.

- ❑ Each machine must meet the following minimum hardware requirements:
 - 16 MB RAM minimum
 - 386 CPU minimum
 - 250 MB or larger drive recommended
 - SVGA monitor preferred
 - OS/2 version 2.1 or higher
- ❑ All data should be backed up before beginning this installation.

EZRaid (non-LAN Server Advanced) Requirements



Note: EZRaid is not a product of Vinca Corporation and is not included as a part of StandbyServer for OS/2. EZRaid can be purchased through Vinca or your local reseller.

- ❑ EZRAID Lite requires the secondary mirrored disk devices to have sufficient free space to mirror the primary disk devices. The mirrored disk devices do not need to have identical geometries.
- ❑ EZRAID Lite disables FDISK and FDISKPM and substitutes its EZUTIL program. FDISK and FDISKPM can only be used to view status information.


Using Hardware RAID Host Adapters

- ❑ Hardware-based RAID host adapters can be used in conjunction with StandbyServer. To use hardware RAID adapters with the Vinca products, the RAID adapters must have a native OS/2 driver.

These adapters can be a considerable help in configuring disk device systems to fit the requirement of having at least two physical disk devices in the standby and primary machines. Where RAID adapters are used, the phrase physical disk device is interpreted to mean that the operating system perceives any number of disk devices as a single physical device. The number of physical disk devices can be displayed by using the FDISK utility in OS/2.

Installation Overview

This section summarizes the process for installing StandbyServer; detailed instructions follow this section. For detailed information on installing OS/2 and NetFinity, see the appropriate IBM documentation.

 **Important!** Each of the installation procedures listed below must be completed on both machines, except when stated otherwise:

1. Install StandbyServer Hardware
Create the Vinca link between the primary and the standby machines that will carry all mirroring traffic.
2. Install or Modify OS/2
Ensure that OS/2 is set up on both the primary and standby machines to recognize the disk device configuration required for StandbyServer.
3. Understand the evaluation/validation option. By default, the StandbyServer software is installed as an evaluation application. To validate StandbyServer you must run VNCKEEP.EXE before you run INSTALL.EXE.
4. Install the StandbyServer software on both machines.
5. Install NetFinity Manager on the standby machine and NetFinity Services on the primary machine to facilitate automatic switching of the server function between the primary and the standby machines.
6. Set which drives *will not* be exported from the standby machine.
7. Install mirroring and edit CONFIG.SYS on the primary machine.
8. Modify failover command files as needed to ensure proper switch.
9. Test the system, under controlled conditions, to ensure that it functions properly and that data is accessible after a system failure.

Step 1: Install StandbyServer Hardware

In this procedure the high-speed communication cards that will be used for mirroring data are installed, these cards can be IBM's PRO/100 fast Ethernet cards or Vinca's proprietary cards.

Be aware of the following for Vinca's proprietary cards:

- ▼ The port and interrupt are set manually with ISA cards, or through software with EISA and MCA cards, and the interrupts are not sharable.
- ▼ The link speed jumper is for a single link in a bi-directional pair and there are four pairs of links on StandbyServer cards.
- ▼ Processor speed settings on the StandbyServer cards are based on the co-processor installed on the card, not the speed of the processor in the machine in which the card is being installed.

IBM PRO/100 Cards

The IBM PRO/100 PCI fast Ethernet card provides a 100 Mbps Vinca link using industry-standard 100 BaseT Ethernet cables. This link must be a dedicated network, isolated from all other Ethernet networks.



Note: Do not install the LAN driver that came with the card. StandbyServer for OS/2 Warp uses a specialized driver that is installed automatically during the software installation.

1. Turn the machine's power off.
2. Install the adapter card into a free PCI *busmaster* slot.

Not all PCI slots will be busmaster slots. Please consult the computer manufacturer's documentation to identify which slot to install this card in.

3. When cards have been installed in both machines, connect the two using a Category 5 twisted-pair cable. *Do not install the software driver supplied with the card; StandbyServer installs a custom driver for this card.*

When each machine is rebooted it will automatically recognize and configure the PCI card.

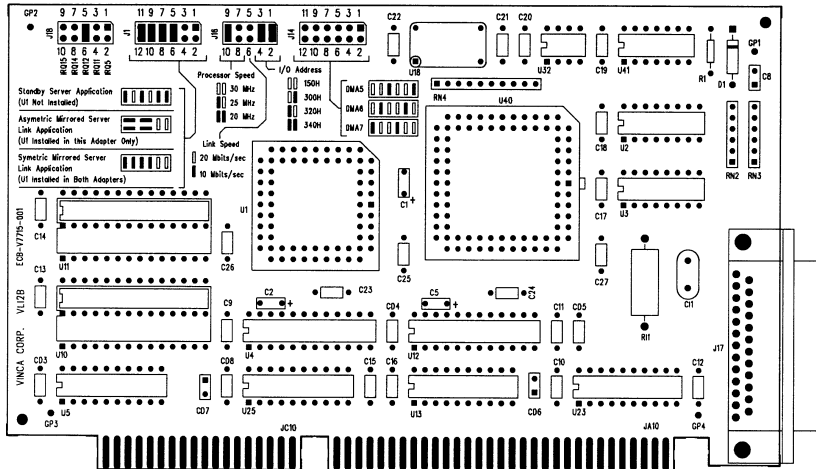
ISA 16-bit Vinca Cards

Vinca's 16-bit ISA link cards provide 80Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any ISA or EISA bus machine, though they cannot take advantage of EISA's 32-bit wide data path.

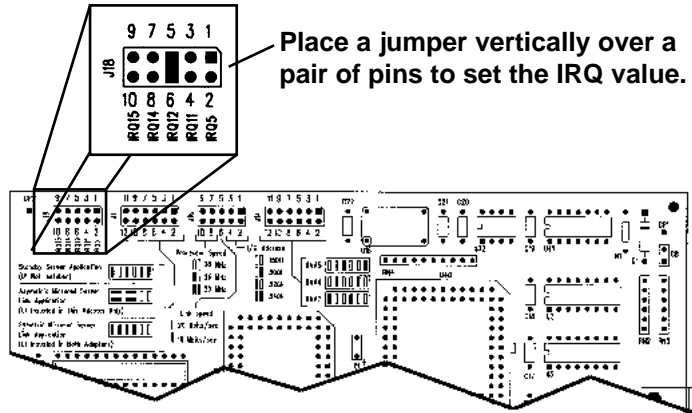
These cards require that the IRQ (interrupt) and port addresses be set manually using jumpers. This section describes how to install the card and set the jumpers.

To install the ISA Vinca link cards do the following.

1. Orient the card so the edge connectors are down, the jumpers are at the top left, and the card is facing with the chip side toward you.



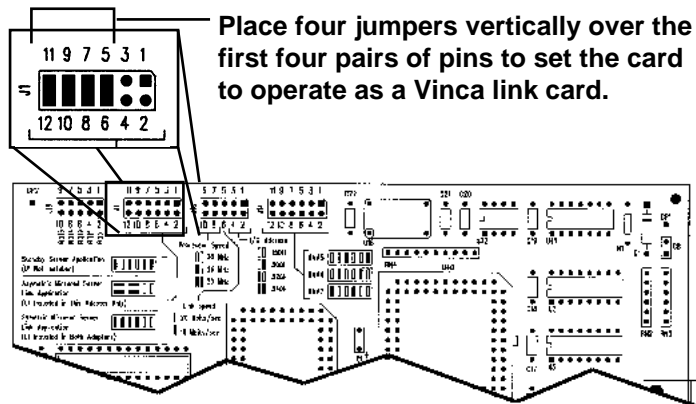
2. Set the IRQ using jumper block J18 at the top left corner of the card.
Valid settings are 5, 11, 12, 14, and 15; the default value is IRQ 12. Make sure this interrupt does not conflict with any other installed cards.



To set a jumper, turn the jumper plug vertically and push it down over a column of two pins as shown above. This example shows the interrupt set to IRQ 12.

3. Ensure that jumper block J1 is properly jumpered for the "Symmetric Mirrored Server Link Application" setting.

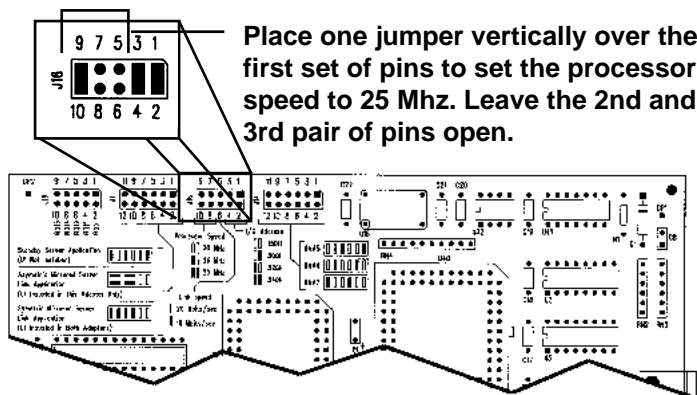
The first four columns of pins should be jumpered.



If the pins are not jumpered as shown above, do so now.

- Ensure that the processor speed is set to 25 Mhz and that the link speed is set to 20 Mbps using jumper block J16.

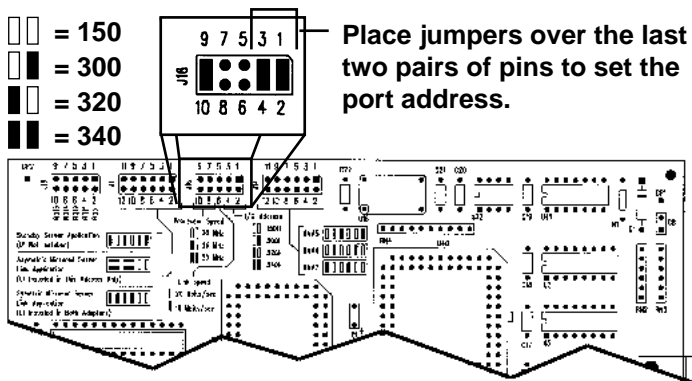
The first pair of pins should be jumpered.



If the pins are not jumpered as shown above, do so now.

- Set the I/O address, also called the port address, using the last two jumpers in J16.

Valid settings are the hexadecimal values 150, 300, 320, and 340; the default value is 340. Make sure this setting does not conflict with any other installed cards.



To set a jumper, turn the jumper plug vertically and push it down over a pair of pins as shown above. This example shows the port address set to 340 hex.

There is one more jumper block labelled J14, but this group is not used for this installation. Those pins should all be unjumped.



Note: Write down the IRQ and port address values set for each card here.

PrimaryStandby

IRQ: _____ IRQ: _____

Port: _____ Port: _____

6. Insert the properly configured Vinca link card into an appropriate open slot in the file server.

Seat the card firmly in the expansion slot and secure it. Repeat this procedure on each machine.

7. After doing the above steps for both machines, connect the two machines using the green high-speed serial communications cable supplied with your cards.

Firmly connect the cable to the Vinca link card and secure it using the connector screws. Be careful not to bend any of the cable's pins when attaching the cable.



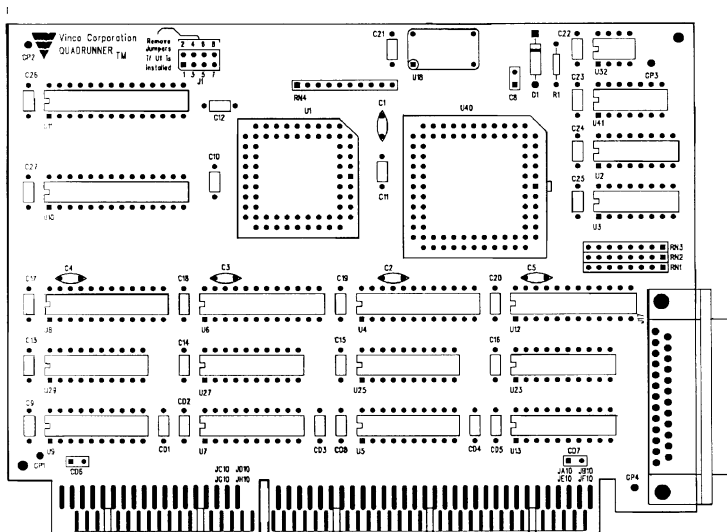
Note: The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if you need to get a 50 foot cable, contact Vinca at (801) 223-3100 or contact your reseller.

The cards and cable are now properly installed.

EISA 32-bit Vinca Card

Vinca's 32-bit EISA link cards provide 160Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any EISA bus machine and use EISA software configuration.

To install the EISA Vinca link cards do the following.




1. Verify that J1 has no jumpers installed.
2. Turn the machine's power off.
3. Install the adapter card into a free slot.
4. Turn on the machine.
5. Run the EISA configuration for that machine.
6. When prompted insert the Vinca diskette containing the \VNC7261.CFG file.
7. Configure the settings to non-conflicting port and IRQ settings.
8. Verify that the link speed is set at 20 Mbit/sec and the processor speed is set at 25MHz.

Installing on OS/2 Systems without LAN Server Advanced

9. After doing the above steps for both machines, connect the two machines using the green high-speed serial communications cable supplied with your cards.


Firmly connect the cable to the Vinca link card and secure it using the connector screws. Be careful not to bend any of the cable's pins when attaching the cable.

 **Note:** The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if a 50 foot cable is needed, contact Vinca at (801) 223-3100 or contact an authorized Vinca reseller.

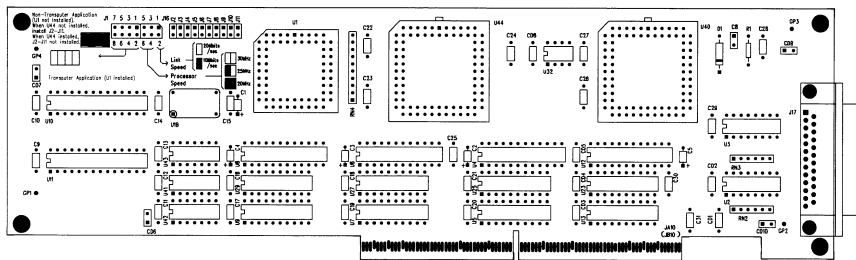
The cards and cable are now properly installed.

MCA 32-bit Card

Vinca's 32-bit MCA link cards provide 160Mbps communication between the primary and the standby machines to maintain the mirror. These cards can be used in any MCA bus machine and use software configuration.

 **Warning:** The current version of this card does not support shared interrupt request levels. Select a unique interrupt request level for this adapter so no other adapters share it. Allowed interrupt levels are IRQs 5, 11, 12, and 15. IRQ levels can be viewed and/or set with the MCA Reference utility.

To install the MCA Vinca link cards do the following.



1. Verify that J1 has no jumpers installed.
2. Turn the machine's power off.
3. Install the adapter card into a free slot.
4. Insert the reference diskette into the floppy disk drive.

5. Turn the machine's power on.
6. Follow the prompts as they appear on the screen.
7. When prompted, insert the Vinca diskette (which contains the @5131.ADF file).
8. Configure the settings to non-conflicting port and IRQ settings.
9. Continue following the screen prompts until the system resources have been configured.
10. After doing the above steps for both machines, connect the two machines using the green high-speed serial communications cable supplied with your cards.

Firmly connect the cable to the Vinca link card and secure it using the connector screws. Be careful not to bend any of the cable's pins when attaching the cable.



Note: The Vinca link cable can be a maximum of 50 feet long. The standard cable is 25 feet long; if you need to get a 50 foot cable, contact Vinca at (801) 223-3100 or contact your reseller.

The cards and cable are now properly installed. There is no need to test the connection, that is done during the software installation.

Step 2: Install or Modify Disk Configuration

This section helps ensure that both the primary and standby machines have the disk device configuration required for StandbyServer for OS/2 Warp. The OS/2 installation documentation and software are needed to complete this procedure.

Be familiar with the following:

- ▼ Drive letter assignments for all partitions.
- ▼ The drive letter where OS/2 will be installed in each of the two machines, the primary and the standby.
- ▼ Drive letter of the primary partition on the first disk device in each of the two machines, the primary and the standby.

Free space must be available on the target disk devices (the devices in the primary machine). The mirroring installation process automatically partitions and formats the target drives as mirrors.

If existing data has not been backed up yet, do so now.

What To Do With Existing Data

If there is existing data, make sure it is on a disk device in the standby machine that is not the first disk device. It may be necessary to back up and restore data, or move a disk device from one machine to another, but it must be on a partition that EZRAID Lite can mirror.

Disk Device Configuration


If installing on an existing system, the configuration must be changed to make it work with StandbyServer. Use OS/2's installation procedure, along with the EZUTIL utility on each of the machines, to ensure the following:

- ▼ At least two disk devices in each machine.
- ▼ The first disk device in each machine must have:
 - A primary partition (which may contain Boot Manager).
 - A partition in which OS/2, StandbyServer software, EZRAID Lite, and NetFinity Manager or NetFinity Services are installed.
 - The same number and type of partitions in both machines.



Note: Partitions on the first disk device aren't mirrored.

Step 4: Understanding the Evaluation/Validation Option


- ▼ Mirrored disk devices in standby machine must be formatted (FAT or HPFS).
 -  **Note:** The term “mirrored disk device” encompasses all of the disk devices installed on either machine that will function as part of a mirrored pair.
- ▼ Each mirrored disk device in the standby machine is treated as if it physically resides in the primary machine. During the normal operation of the network, this is the primary drive despite its physical location in the standby machine.
- ▼ Each mirrored disk device in the primary machine is the secondary of the mirrored pair and contains only free space initially.

Step 4: Understanding the Evaluation/Validation Option

Each of the Vinca applications in the Cluster Pack can be run as 30-day evaluation programs. When you decide which program you want to validate, you need to contact Vinca and exchange the Cluster Pack serial number for a Vinca, product-specific serial number. After installing *StandbyServer*, it can be used for 30 days during which pop-up warnings can be invoked (using NetFinity) to remind you how many days are left in the evaluation period. After 30 days, an Expiration notice is invoked and the application will not function.

By default, *StandbyServer* for OS/2 is installed as an evaluation program where you are not prompted to enter a registration number. As an evaluation program, you are prompted to enable and set alerts to notify you when the evaluation time is coming to a close.

Whether or not you evaluate the product first, when you want to validate *StandbyServer* for OS/2, you must contact Vinca to register the product and exchange the Cluster Pack serial number for a *StandbyServer* for OS/2 registration number. Once you have the new registration number, you can perform the standard installation.

 **Note:** If you choose to run *StandbyServer* for OS/2 as an evaluation product and then decide to validate it, you will need to reinstall the product.

Vinca can be contacted by Internet e-mail, phone, fax or U.S. Mail at:

E-mail: validation@vinca.com

Phone: 800-274-6042

Fax: 801-223-0199

U.S. Mail: Vinca Corp., 1815 South State Street, Suite 2000, Orem, Utah 84097.

When contacting Vinca, you will be asked to provide the following information:

- ▼ Cluster Pack serial number
- ▼ Contact person
- ▼ Company name
- ▼ Address
- ▼ Phone
- ▼ Fax (optional)
- ▼ E-mail (optional)

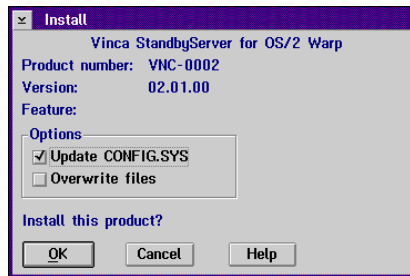
Step 5: Install StandbyServer Software

This procedure is used to install *StandbyServer* on each machine. After installing the software to one server, you must repeat the steps on the other server to complete the install. The installation must be run from the local hard drive, so you will need to copy the contents of the SBSOS2 directory on the CD-ROM to a temporary installation directory on your hard drive.

To install StandbyServer for OS/2

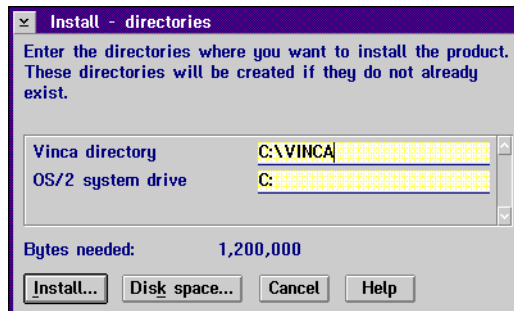
1. Insert the Cluster Pack CD-ROM into the CD-ROM drive of the primary machine.
2. Open an OS/2 command prompt.
3. Create a temporary directory and copy the contents of the SBSOS2 directory on the CD-ROM to the created directory. For example, `md c:\tempinst`. And copy `cd:\sbsos2*. * c:\tempinst`.
4. Change to the newly created directory on the local hard disk.
5. If you want to install the evaluation product skip this step. If you have contacted Vinca and have received your new registration number, from the prompt type `VNCKEEP.EXE` and press Enter.
6. From the prompt, type `INSTALL.EXE` and press Enter.
7. Click Continue.

The Install dialog box appears.



8. Leave "Update CONFIG.SYS" checked. If you previously installed StandbyServer for OS/2 Warp on this machine, check "Overwrite files."
9. Click OK.

The Install-directories dialog box appears.



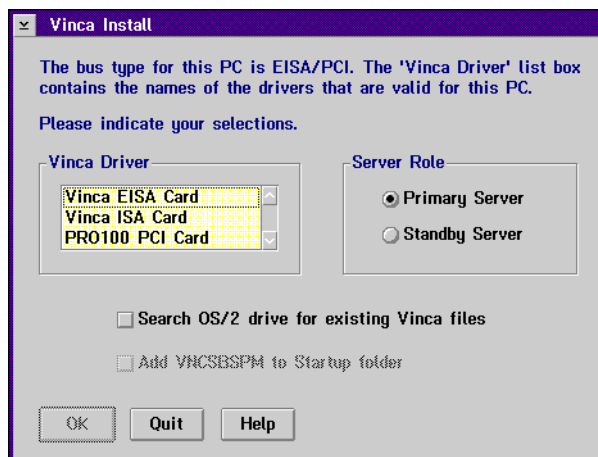
10. Make sure the information is correct and click Install.

The Vinca directory is the directory where Vinca software will be installed. You can use the "Disk space" button to view disk usage on local disks.

After you click Install, a progress bar appears as files are copied to their proper locations. During the file copy stage, you are prompted to enter a registration number, or enable the evaluation warnings depending on which installation you to perform.

11. If this is a standard installation, enter the registration number received from Vinca. If this is an evaluation installation, you can enable NetFinity alerts to notify you when the evaluation period is coming to a close.

The bus-and-driver information dialog box appears. A sample is shown; yours may vary with the bus type(s) and link card in your machine. If you have only one bus, and Vinca supports only one card for that bus, the Vinca Driver section will not be present.

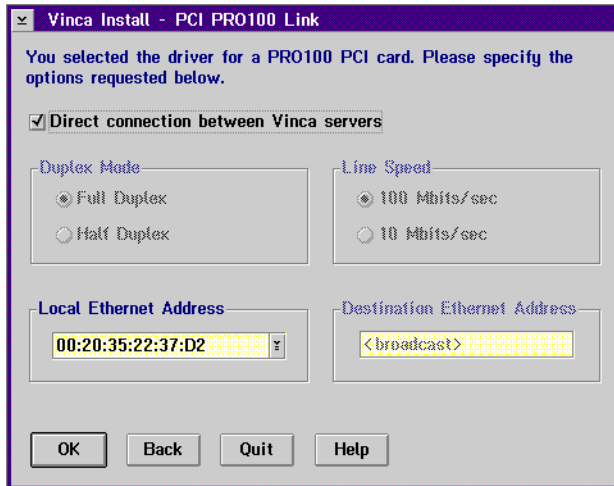


12. Choose the Server Role (Primary or Standby) for this machine.
If you click Standby Server for the role, the “Add VNCSBSPM to Startup folder” checkbox becomes active.
13. If this is to be the standby machine, check or clear the “Add VNCSBSPM to Startup folder” checkbox as you wish.
If VNCSBSPM is in the Startup folder, the Vinca software will start up automatically; otherwise, you must start the program yourself after a reboot to ensure fault tolerance. However, in some configurations automatic startup can lead to problems—for example, if the primary machine does not boot quickly enough the standby will attempt to switch over. In addition, VNCSBSPM.EXE must not be running if CHKDSK is going to be run on the standby machine.
14. Choose the correct driver for the bus type and card you are using.

15. Click OK to continue with the installation.

The installation program checks the installed Vinca link card.

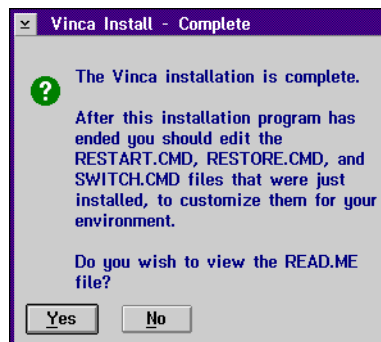
If you are using PRO/100 cards for the Vinca link a settings screen appears where you can set parameters. The **Direct connection between Vinca servers** checkbox should be marked. The Ethernet address of the card is taken from the card itself and should be correct. Press OK to continue.



A confirmation dialog appears reviewing the card settings. Press OK to continue with the installation.

16. If a settings dialog box appears, click OK to continue.

A progress bar appears, and then the installation complete screen.



17. Click Yes or No as appropriate.

A dialog box informing you of changes to CONFIG.SYS appears (this will not take place until after you read the READ.ME file if you click Yes).

18. Click OK.

The installation program returns to the main installation screen.

19. Choose Exit from the File menu.

20. Eject the StandbyServer installation disk from the floppy drive.

If you are using a Vinca ISA card and the port and interrupt settings were changed from the default values, the CONFIG.SYS file must be updated to reflect the altered setting. Edit the CONFIG.SYS file and find the line that begins as follows:

```
BASEDEV=VNCIL01.SYS /I:12 /P:340 /O:2
```

Replace the number in the /I:12 switch to reflect the new IRQ setting, and change value on the /P:340 switch to reflect the correct port address.

21. Properly shut down the machine.

22. Repeat Steps 1 through 17 for the other machine.

When installation is complete, both machines will be shut down.

Step 5: Set Local Disks for the Standby Machine

StandbyServer automatically exports all drives from the standby machine except those specifically excluded from the StandbyServer application. When these devices are exported they will appear to the primary machine as local disks. They will be locked and inaccessible to the standby machine until a failover occurs, then the mirrored data on them will be accessible.

Use the Disk Export utility to determine which disks *will not* be exported to the primary machine; all disks are automatically exported except those excluded using this utility.

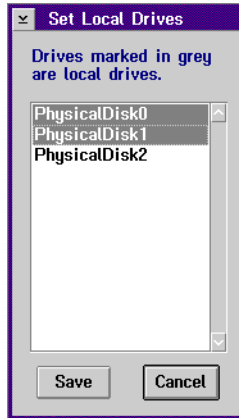
There are several rules to keep in mind when exporting disks:

- ▼ Local devices must start with and include PhysicalDisk0.
- ▼ Local devices must be selected in sequence.
- ▼ At least one device must be made available for export.
- ▼ Partitions must be created on the primary server that reflect local usage on the standby machine to ensure drive lettering is consistent when switchover takes place. For example, if there is two physical disk devices in the primary server, and three in the standby machine, the first physical disk device in the primary server must be assigned two drive letters (i.e., C and D), so that drive E in both machines would be available for the mirrored set (i.e., E and E').

Do the following to determine which disks are exported:

1. Start the StandbyServer application (**VNCSBSPM**) on the standby machine.
2. Choose Drives... from the Export menu.

The Set Local Drives dialog appears. Physical disk devices are listed in the order reported to the operating system.



3. Mark the drives that *will not* be exported to the primary machine.

Click on a disk or highlight it and press [Space] to keep it from being exported.

4. When all local disks are marked choose the Save button.

StandbyServer checks to make sure you have met the conditions listed earlier. If your selections violate these criteria an error message appears. Press [Enter] to clear the error, alter your selections to meet the criteria listed at the beginning of this section, and choose Save again.

If all conditions are met, a message appears saying that you must restart StandbyServer for your selections to be enabled.

5. Exit and restart StandbyServer.

Choose Exit from the File menu to exit StandbyServer.

Step 6: Install and Configure NetFinity


In this procedure, the switching process between the primary and standby machine will be automated for unattended switchover in the event of a system failure.

The installation of NetFinity is optional. However, if it is not installed, then the roles of the primary and the standby machines must be manually switched in the event of a system failure. The network users must wait until that manual switching takes place to continue working. Automatic switching requires the installation of NetFinity.

Installation Instructions

Complete the following instructions to install NetFinity Services on the primary machine and NetFinity Manager on the standby machine:

Some of the following instructions refer to the NetFinity documentation (NetFinity Services and NetFinity Manager manuals). Refer to these manuals as needed for more information about NetFinity.

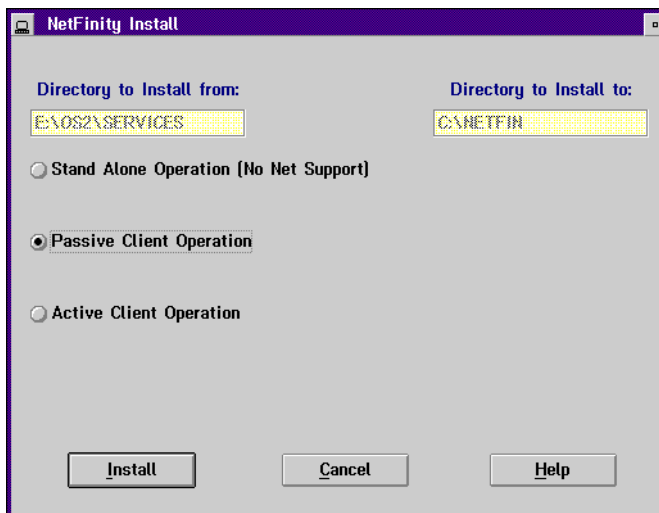
 **Note:** NetFinity includes two programs; NetFinity Services and NetFinity Manager. They must be installed on the correct machine to function properly.

- ▼ NetFinity Services is installed and runs on the primary machine.
- ▼ NetFinity Manager is installed and runs on the standby machine.

Installing NetFinity Services on the Primary Machine

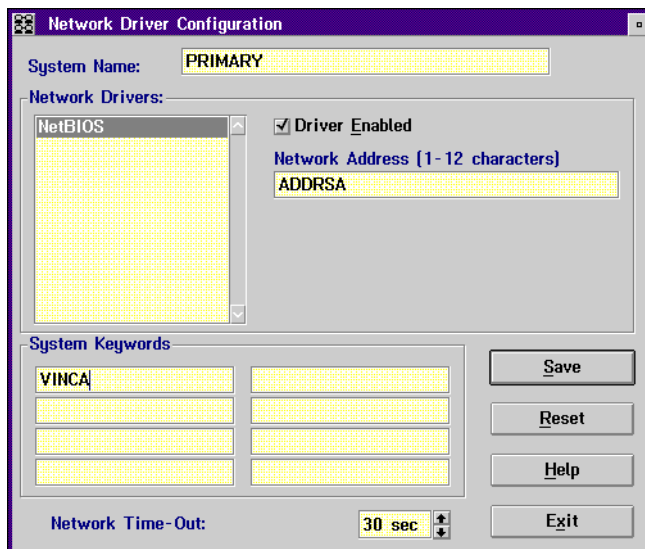
1. Insert the NetFinity Services for OS/2, Services Diskette #1 in the floppy drive in the primary machine (if installing from CD-ROM, insert the NetFinity CD-ROM into the CD-ROM drive).
2. Open an OS/2 command prompt.
3. Run the NetFinity installation program.

The NetFinity Install dialog box appears.



4. In the “Directory to Install from” field, type the drive letter of the floppy drive or CD-ROM drive.
5. In the “Directory to Install to” field, type the drive letter and path in the primary machine where NetFinity is to be installed.
See the figure above for an example.
6. Select “Passive Client Operation”.
7. Click Install.

The Network Driver Configuration window appears.



8. In the System Name field, type the System Name selected for the primary machine.



Warning: Both the primary and standby machines must have *unique* names. The name assigned here may be the same name assigned the primary machine during network requester installation, but must not be the same name to be assigned the standby machine during the NetFinity Manager install.

9. Select a Network Driver from those displayed.

When making a selection, the Network Driver assigns a network address to the system. If NetBIOS is selected, a network address will be selected and displayed in the Network Address field. The default name may be displaced by entering any 1-12 character name.

10. Mark the Driver Enabled box to activate the driver on start-up.



Note: Refer to the IBM NetFinity manual for additional information about System Keywords, Network Time-Out, and support of multiple network interfaces.

11. Enter one or more keywords into the System Keywords fields.

Later, when configuring NetFinity on the standby machine, at least one keyword must match between the two systems.

12. Select Save to save the configuration on the primary machine
13. Select Exit.
NetFinity displays a list of commands that must be added to the CONFIG.SYS file.



Note: To change the saved Network Driver Configuration after finishing the installation, select the Network Driver Configuration object from the NetFinity folder.

14. Choose Yes.
If No is chosen, the commands will be saved as CONFIG.NEW in the destination directory and will have to be manually added later.
15. Edit the CONFIG.SYS file to “REM” out the line containing NFDASD.FLT.

```
rem BASEDEV=NFDASD.FLT
```



Warning: The line with NFDASD.FLT **MUST** be “REM”ed out or the system will **NOT WORK!** Currently, NFDASD.FLT and EZRaid Lite are not compatible!

16. Remove the installation diskette.

Installing NetFinity Manager on the Standby Machine

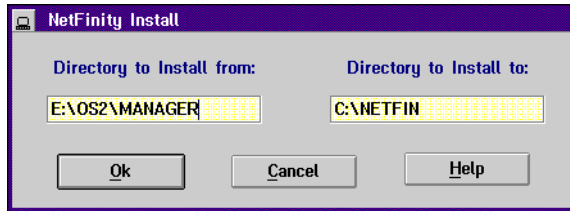
The installation of NetFinity Manager on the standby machine is very similar to the installation of NetFinity Services on the primary machine.

Before proceeding with the installation of NetFinity Manager on the standby machine, refer to instructions in the IBM NetFinity Manager manual.

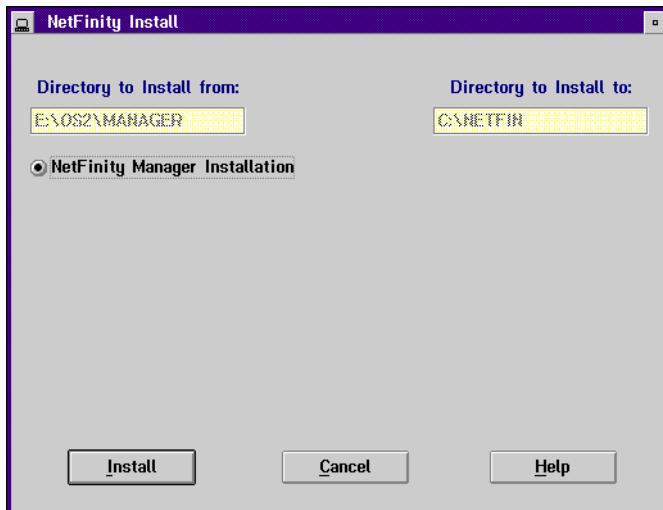
1. Insert the NetFinity Manager for OS/2, Manager Diskette #1 in the floppy drive in the standby machine (if installing from CD-ROM, insert the NetFinity CD-ROM into the CD-ROM drive).
2. Open an OS/2 command prompt.
3. Run the NetFinity installation program.

Step 6: Install and Configure NetFinity

The NetFinity Install directory selection window appears.



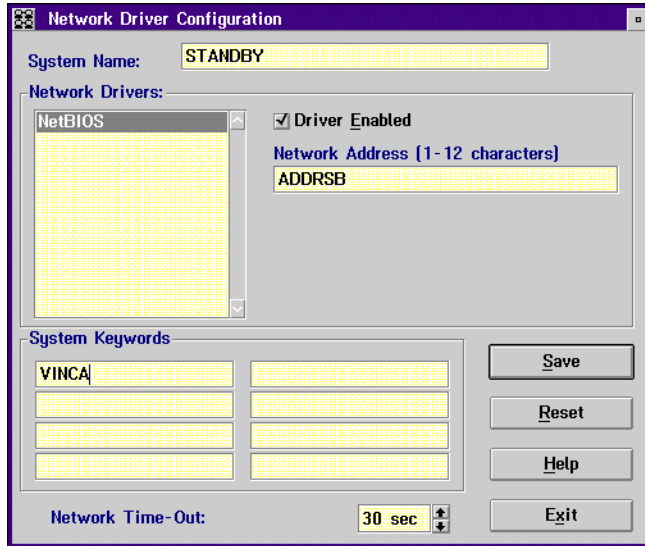
4. Confirm that the directories are correct and click OK to go on.
The NetFinity Install window appears.



5. Select NetFinity Manager.

6. Click Install.

The Network Driver Configuration window appears.



7. In the System Name field, type the System Name selected for the standby machine.



Warning: Both the primary and standby machines must have *unique* names. The name must not be the same name assigned to the primary machine during the installation of NetFinity Services.

8. Select a Network Driver from those displayed.

When making a selection, the Network Driver assigns a network address to the system. If NetBIOS is selected, a network address will be selected and displayed in the Network Address field. The default name may be replaced by entering any 1-12 character name.

9. Mark the Driver Enabled box to activate the driver on start-up.



Note: Refer to the IBM NetFinity manual for additional information about System Keywords, Network Time-Out, and support of multiple network interfaces.

Step 6: Install and Configure NetFinity

10. Enter one or more keywords into the System Keywords fields. Make sure that at least one of them is the same as a keyword defined for the primary machine.

At least one keyword must match between the two systems.

11. Select Save to save the configuration on the standby machine
12. Select Exit.

NetFinity displays a list of commands that must be added to CONFIG.SYS.



Note: To change the saved Network Driver Configuration after finishing the installation, select the Network Driver Configuration object from the NetFinity folder.

13. Choose Yes.

If No is chosen, the commands will be saved as CONFIG.NEW in the destination directory and will have to be manually added later.

14. Remove the installation diskette or CD-ROM.
15. Reboot the machines in the correct order, as follows:
 - a. Shut down the primary machine completely.
 - a. After the primary is shut down, shut down the standby machine.
 - b. Reboot the standby machine.
 - c. Start the StandbyServer application, VNCSBSPM.EXE.
 - d. After the StandbyServer window appears restart the primary machine.
 - e. Verify that the StandbyServer window shows the word **CONNECTED**.

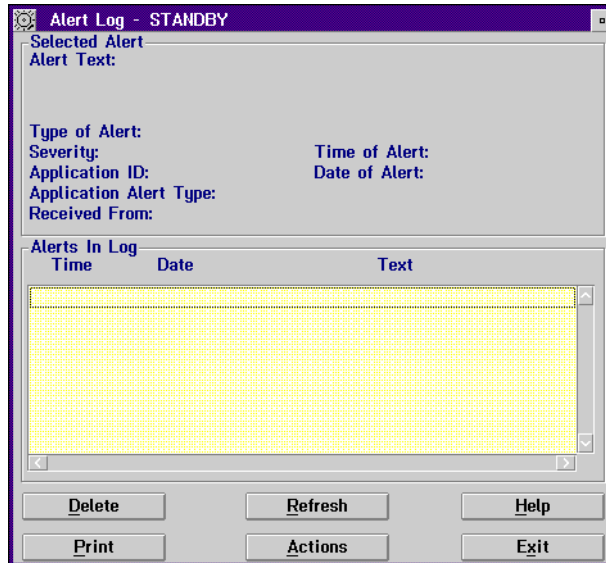
Starting NetFinity on the Standby Machine

The following instructions start the operation of NetFinity. Refer to the NetFinity Services manual for information about starting NetFinity on each machine.

Important! This procedure will start NetFinity and configure the automatic switching capability of StandbyServer. Perform this procedure on the standby machine, not the primary.

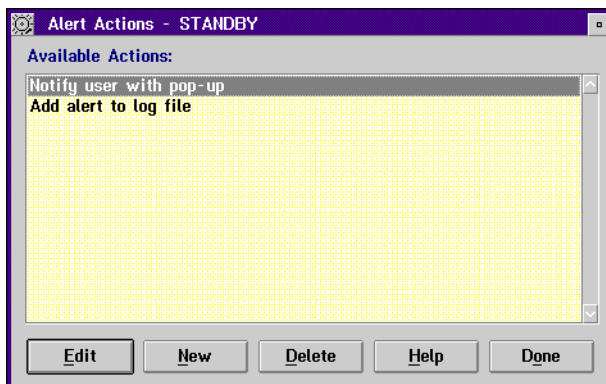
1. Open the NetFinity folder.
2. Open the NetFinity Service Manager icon.
3. From the NetFinity Service Manager folder, open Alert Manager.

The Alert Log dialog box appears.



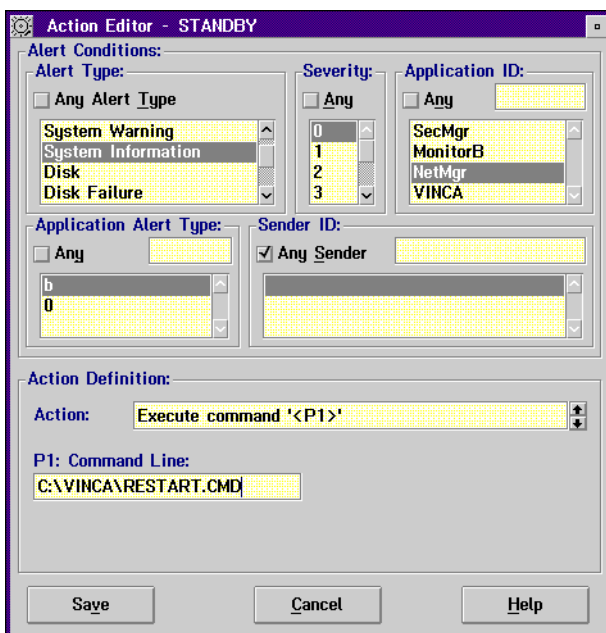
4. From the Alert Log dialog box, select Actions.


The Alert Actions dialog box appears.



5. From the Alert Actions dialog box, select New.

The Action Editor dialog box appears.



 **Important!** The **Action Editor** dialog box contains information that is vital to StandbyServer and must be completed exactly as explained in the following step.

6. Fill in the fields in the Action Editor dialog box as follows:

If the indicated selection is not available in the list box, type it into the corresponding text entry window and then press [Enter].

- a. From the Alert Type list box, select System Information.
- b. From the Severity list box, select 0 (zero).
- c. From the Application ID list box, select NetMgr.
- d. From the Application Alert Type list box, select or type b.
- e. Check the Any Sender checkbox in the Sender ID field.
- f. From the Action field within Action Definition, select the following:

Execute command '<P1>'

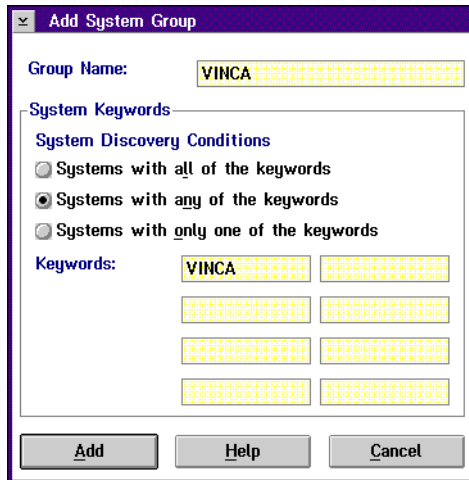
- g. In the P1: Command Line field, type a command like the following example:

[drive]:\vinca\restart.cmd

Before exiting the Action Editor dialog box, verify that the P1: Command Line field includes the name of the installed switchover command file.

7. Exit and save until the NetFinity Service Manager window appears.
8. Open Remote System Manager.
The **System Group Management** window appears.
9. Choose Add Group from the Group menu.

The Add System Group dialog box appears.



10. In the Group Name field, type an appropriate name.
11. Click “Systems with any of the keywords” under System Discovery Conditions.
12. Enter one or more appropriate keywords into the Keywords fields. At least one keyword must be the same as the matching keyword that was configured in the NetFinity Driver Configuration dialog box when NetFinity was installed on each machine.

In other words, each machine must have at least one keyword that is also configured on the other machine, and that keyword must be entered here.

13. Click Add.

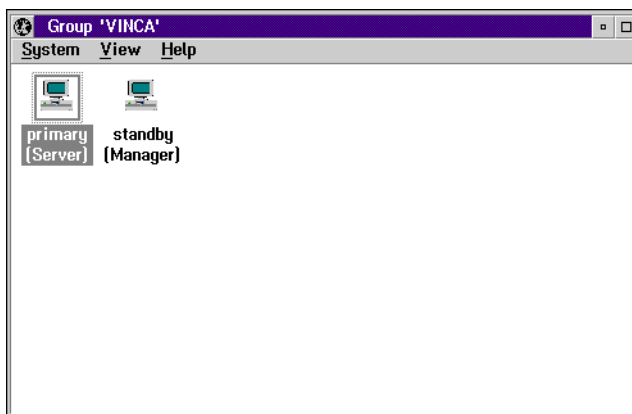
The Add System Group dialog box closes, and the group now appears in the System Group Management window.

14. Double-click on the group just created to open it.

15. From the System menu, choose Discover Systems.

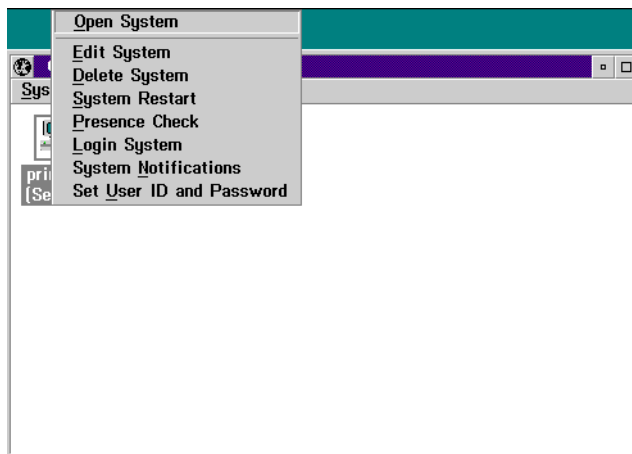
The primary and standby machines will be discovered (assuming a shared keyword was entered in Step 12).

The following illustration is an example of such a group.

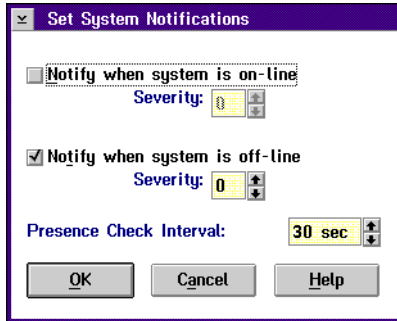


16. In the Group window, click mouse button 2 (usually the RIGHT mouse button) on the icon which represents the primary machine.

A popup menu of options appears, as shown in the next illustration.



17. From the menu, select System Notifications.
The Set System Notifications dialog box appears.



18. In the Set System Notifications dialog box, select Notify when system is off-line.

Note: When this option is enabled, switch over is automatic when the primary server fails. If this option is disabled, the standby machine will not switch over unless the process is done manually.
19. In the Set System Notifications dialog box, set Presence Check Interval to 30 seconds.
20. After System Notifications are set, select OK.

NetFinity is now installed and the standby machine is ready to take over for the primary in the event of a primary machine failure.

Step 7: Install Mirroring, Edit CONFIG.SYS

In this procedure the mirroring software is installed on the primary machine to enable failure recovery.

Install EZRAID Lite

The following steps are a guide to the EZRAID Lite installation procedure. If there is existing data, place all of it on the disk devices in the standby machine before beginning this procedure.



Note: EZRaid is not a product of Vinca Corporation and is not included as a part of StandbyServer for OS/2. EZRaid can be purchased through Vinca or your local reseller.

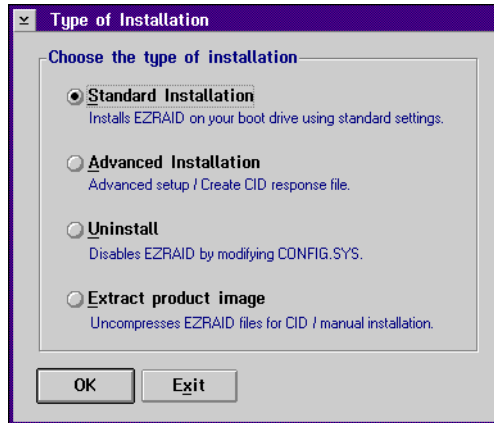


Note: The partition in the primary machine that will be the mirror secondary must have enough free space to be mirrored from the partition in the standby machine. If there is sufficient free space, EZRAID Lite creates the partition on the primary machine's disk device.

The procedure assumes that the machines are currently shut down. Install EZRAID Lite on the primary machine only, not the standby.

1. Restart the machines in the correct order, as follows:
 - a. Boot the standby machine.
 - b. After the *Vinca StandbyServer* window appears on the standby machine, boot the primary machine.
 - c. Verify that the Link Statistics window of the *StandbyServer* application shows the word **CONNECTED**. To display the Link Statistics window choose Link from the View menu.
2. Insert the EZRAID Lite diskette into the floppy drive of the primary machine.
3. At the primary machine, open an OS/2 command prompt window.
4. At the OS/2 command prompt, type A:\SETUP (or B:\SETUP as appropriate) and press [Enter].

The EZRAID Lite installation window appears.



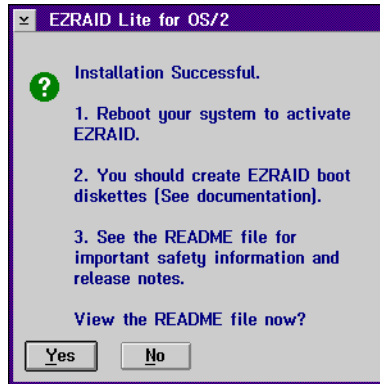
5. Select Standard Installation.

6. Select OK.

A dialog box appears indicating that if EZRAID is already installed, this installation will over-write those files, and that the installation will make changes to the CONFIG.SYS file.

7. Select Yes to proceed with the installation.

When the installation is complete, a dialog box appears.



8. Select No to skip viewing the README file, or Yes to read the README file.

The main installation window appears (if Yes was selected, the main installation window appears when the readme file is closed).

9. Select Exit.
10. Reboot the primary machine.

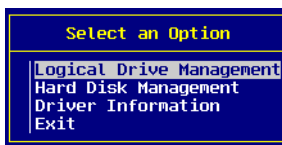
Make sure the standby machine is running and the Vinca software is running on the standby machine before rebooting the primary.

Configure Mirroring

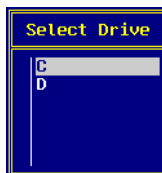
In this procedure EZRAID Lite is configured to mirror data across the Vinca link.

1. At the primary machine, open the EZRAID Lite Disk Management icon.
2. Open the EZUTIL Disk Manager icon.

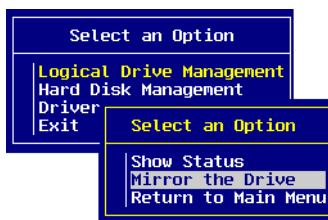
The EZUTIL utility appears.



3. Select Logical Drive Management and press [Enter].
The Select Drive menu appears.



4. From the Select Drive menu, select the drive to mirror and press [Enter].
Another Select an Option menu appears, as shown.



5. Select Mirror the Drive and press [Enter].

A window appears listing disk devices on the primary machine that have free space (unpartitioned space).



6. Select the disk that is to be the mirror image and press [Enter].
EZRAID verifies the disk device and then mirrors the data. The length of time it takes depends on the size of partitions created, the amount of data,

and the speed of the system. A progress window displays the percent complete while the system is performing these tasks.

When EZRAID Lite is finished, the following message appears.

```
The drive is now mirrored
--Press <Esc> to continue--
```

7. Press [Esc] three times, to close the message, the Select an Option menu, and the Select Drive menu.

The original Select an Option menu reappears.

8. Select Exit and press [Enter].

The Exit EZUTIL menu appears.

9. Select Yes and press [Enter] to leave EZUTIL.

Edit CONFIG.SYS on the Primary Machine


This procedure changes the primary machine's CONFIG.SYS file to keep CHKDSK from running on the mirrored disk devices at boot time, while still allowing CHKDSK to run on disk devices that are not mirrored.



Important!

During the recovery process, it is important that CHKDSK is not run on the mirrored disk devices when the primary machine is booted. The following instructions must be completed to give the system administrator control over the direction of the re-mirroring process during recovery from a failure of the primary machine. This is absolutely essential to the correct functioning of StandbyServer and the protection of the data on the system.

1. Find the following line in the CONFIG.SYS file on the primary machine:
IFS=(Path)\HPFS.IFS
Example: IFS=D:\OS2\HPFS.IFS /AUTOCHECK:*
2. Change the asterisk (*) in the line shown above to a list of the unmirrored drives.
Example: If C: and D: were the unmirrored devices on the primary machine, you would edit the line to read as follows:
Example: IFS=D:\OS2\HPFS.IFS /AUTOCHECK:CD
3. Verify that VNC SBS.ADD is the last line in the CONFIG.SYS file.

 **Warning:** The VNCSBS.ADD line MUST be the last *.ADD line in the CONFIG.SYS file. Move all Vinca entries to the end.

4. Delete the line containing NFDASD.FLT from the CONFIG.SYS file.

 **Warning:** The NFDASD.FLT line MUST be deleted from the CONFIG.SYS file, or EZRAID will not function.

5. Reboot the primary machine.

Make sure the standby machine is running and the Vinca software is running on the standby machine before you reboot the primary.

Step 8: Modify Switchover and Recovery Command Files

The RESTART.COM command file is called in the event NetFinity detects a failure on the primary machine. You can modify RESTART.COM to call SWITCH.COM or just exit out under specified failure conditions; SWITCH.COM controls the actual switchover process. VNCRCVR.COM is used during recovery to return the standby machine to the standby state before booting the repaired primary machine. These files can contain any valid OS/2 .COM file commands. For example, if the primary machine is a Notes server, have the SWITCH.COM file start Notes after switchover.

The files as installed by Vinca are samples. Modify them to fit system needs, according to the suggestions contained in comments in the files. For VNCRCVR.COM, ensure that the following things happen when it is run:

1. CHKDSK /F is run on each mirrored disk device. To avoid possible errors, run CHKDSK on each disk device by changing the default drive letter and then running CHKDSK /F instead of running CHKDSK with a drive letter option. For example, enter:
E:
CHKDSK /F
G:
CHKDSK /F
rather than
CHKDSK E: /F
CHKDSK G: /F
2. On the standby machine, any network services required by this specific configuration are started up.
3. Any other services or applications needed are started up.

Step 9: Test the Installation

In this procedure, the system will be tested under controlled conditions to ensure that it functions properly and that the data is mirrored correctly during a system failure. Create data on the mirrored disk device, force the server to fail, and then verify that the standby machine took over the role of the server and the data was safely mirrored and is available.

A third machine (a workstation) will be needed from which to verify the mirrored data during the forced server failure condition.



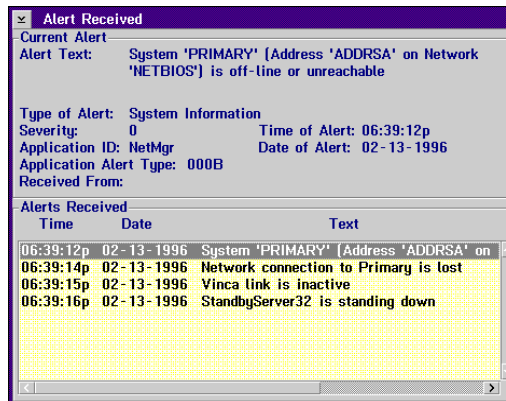
Warning: If there is real data on this system and a backup has not been made, DO IT NOW.

1. From a workstation, create and save a data file on one of the mirrored disk devices.

The data entered in this file can be as simple as a single word.

2. Disconnect first the Vinca cable, then the network cable from the primary machine (leave the standby machine running normally).

This simulates a cable link failure. From the StandbyServer window on the standby machine, the CONNECTED message is replaced by the NOT CONNECTED message. The Alert Received window appears on the standby machine.



3. After the standby machine has completed the switch to the role of the server, from a workstation, verify that the data created in Step 1 is on the correct disk device and the data in the file is identical to what was typed previously.

At this point, the primary machine is unavailable to the network. Next, recover from this situation just as if the primary machine had failed and had just been repaired.



Warning: Do not reboot the primary machine at this point. It is imperative to restore the system in the correct sequence.

4. Run the modified VNCRCVR.COM file on the standby machine.
5. Shut down the primary server and then reconnect both the Vinca link and the network cables.
6. Reboot the primary machine.
7. Start EZUTIL on the primary machine.
8. Select Logical Drive Management.
9. Select the mirrored drive.
10. Select Verify the Raid.
A window appears showing EZUTIL's progress as it verifies and fixes the mirror.
11. Repeat Step 10 until EZUTIL reports no (zero) errors detected.
12. When EZUTIL has finished verifying the mirror, exit EZUTIL.

If problems occur during the testing process, refer to *Chapter 4: Recovery Procedures and Technical Support*.

Chapter 4

Recovery Procedures

Vinca's StandbyServer for OS/2 Warp product is designed to keep network users running even when problems occur. This chapter tells how to restore the network to a fully fault-tolerant state after a problem has occurred with the primary machine, standby machine, or both. In most cases after a failure users will be able to operate, but the following procedures in this chapter must be run as soon as possible because the data is less safe if only one machine is operating than if both primary and standby are functional.

If the procedures in this chapter are not sufficient, please contact Vinca technical support as detailed at the end of the chapter.

Fault Tolerance Recovery Process—LAN Server Advanced

An understanding of how LAN Server Advanced implements disk mirroring helps administrators take the proper corrective actions when failures occur. The following scenarios are representative but not complete. If at any time during a recovery process there is a possibility that data may be lost, contact Vinca's technical support for help before proceeding.

General Guidelines for Recovery

- ▼ When a disk device fails, partition information is lost along with the data on the disk device. The mirror is re-created with a new, unformatted and unpartitioned disk device using the FTSETUP utility.
- ▼ When a machine fails, partition information remains on the disk devices. Because the mirror partitions are split across two machines, a failure of one machine means the mirror partitions become unsynchronized. The mirrors are resynchronized with the FTADMIN utility. Use FTADMIN when the partition information is intact but the data on the two mirror partitions is not synchronized.
- ▼ Correcting errors with FTADMIN does not guarantee that the mirror partitions are synchronized. Use the verify operation to synchronize mirror partitions. Correcting some errors automatically invokes the verification operation, while other corrections will not. If the verification pop-up does not appear while correcting an error on a mirrored disk device, perform manual verification operation.
- ▼ Recovering the system to full Fault Tolerance requires stopping network services. Depending upon the failure and size of the partitions, it may take considerable time to re-establish the mirrors. For these reasons, schedule maintenance at a time least disruptive to network users.
- ▼ If the recovery requires multiple boots of the primary machine, disable NetFinity notifications for the primary machine until recovery is complete. Re-enable the notifications when the system is ready to go back on-line. Disabling NetFinity notifications is performed on the standby machine.
- ▼ Many of the recovery steps shown below can be automated using .CMD files. See the VNCRCVR.CMD file in the VINCA subdirectory on the standby machine for an example of how to automate recovery.
- ▼ If the recovery process creates new partitions on the standby machine (these will be primary mirror partitions), the standby machine must be rebooted before it can function correctly. Rebooting causes the operating system on the standby machine to recognize the new partitions.

What to Do When the Primary Machine Fails

When the primary machine fails, the standby machine automatically switches over to assume the role as network server. Mirrored data remains accessible to the network in the form of the primary mirror partitions on the standby machine. In this case, the Fault Tolerance system has not detected any failures because it was running only on the machine that failed. No partition information has been lost, even though their data has become un-synchronized. The recovery process is designed to cause the Fault Tolerance system running on the primary machine to detect the un-synchronized state of the mirrors and correct it through mirror verification.

To recover, follow these steps:

1. Correct the problem in the primary machine.
2. Schedule network downtime.
3. During scheduled down time, run the modified VNCRCVR.CMD file.

The modifications should ensure that the following things happen when VNCRCVR.CMD is run:

- a. LAN Server Advanced is stopped on the standby machine.
- b. CHKDSK /F is run on each mirrored disk device to update the superblock on the HPFS partition, causing it to differ from its mirror secondary on the primary machine and guaranteeing that the Fault Tolerance system detects that the partitions are not synchronized. To avoid possible errors, run CHKDSK on each disk device by changing the default drive letter and then running CHKDSK /F instead of running CHKDSK with a drive letter option. For example, enter:
E:
CHKDSK /F
G:
CHKDSK /F
rather than
CHKDSK E: /F
CHKDSK G: /F
- c. On the standby machine, any network services required by the configuration (such as Requester and Replicator for a Domain Controller) are started up.
- d. The StandbyServer software is started on the standby machine.

4. Boot the primary machine.
FTMONIT detects a difference in the mirror partitions and logs the errors during the boot process.
5. Start FTADMIN on the primary machine.
The mirrored drives appear cracked in FTADMIN.
6. Select Correct All from the Error menu to restore the mirrors.



Note: If the mirrored disk devices do not appear cracked, it is usually the result of improperly running, or forgetting to run CHKDSK on the primary mirror partitions in the standby machine, before booting the primary machine. If this happens, shut down the primary machine, terminate the StandbyServer application on the standby machine and run CHKDSK on the primary mirror partitions as described in step 3. Restart the StandbyServer application and re-boot the primary machine. Another possibility is that the FTMONIT line in CONFIG.SYS does not include the /VERIFY:NO parameter—check CONFIG.SYS. If the mirrors still do not appear as cracked mirrors when viewed with FTADMIN, call Vinca technical support for help before proceeding to the next step.

7. Start LAN Server Advanced on the primary machine.

What to Do If the Primary Machine is Booted Without the Standby Machine

If the primary machine is booted and any of the following conditions exist, the Fault Tolerance system is not able to find the primary mirror partitions and detaches the secondaries, effectively dissolving the mirrors.

- ▼ The standby machine is off.
- ▼ The StandbyServer application is not running.
- ▼ The Vinca cable is not connected.

To re-establish the mirrors, the primary or detached secondary partitions must be deleted and the mirrors recreated. Complete the following steps:

1. Shut down the primary machine.
When the primary machine is booted, Fault Tolerance does not find the primary partitions of the mirrors. The connection between the mirrored partitions is dissolved.
2. Boot the standby machine and run the StandbyServer application.
3. Boot the primary machine.

4. On the primary machine run `FTSETUP`.

There will be twice as many drives displayed as there were mirrors. Half of them, the ones with the question marks, are the detached secondaries. The others are the primary partitions on the standby machine.

5. Delete the primary partitions by selecting the disk device and then selecting the Delete option from the Drive pull-down menu.
6. Using the volume labels as a guide to verify that the original drive letter sequence is preserved, select each detached secondary in the desired drive letter sequence.
7. From the Drive menu, recreate the mirror by selecting the Recover secondary option.

There are three selections in this sub-menu indicating the ways a detached secondary may be recovered.

8. Choose the Make the drive the secondary of a mirror option.
With each recovery, the drive letter assignment made is displayed adjacent to the disk device following the next boot.
9. Make sure that the drive letter assigned agrees with the volume label.
If the drive letter assignments are incorrect, begin again.



Note: Even though this operation essentially creates primary mirror partitions which are indistinguishable from other HPFS partitions, their drive letters are not added to the autocheck list in the `IFS=` statement in the `CONFIG.SYS` file as they would have been had the partitions been created using `FDISK`.

10. Exit `FTSETUP`
This re-establishes the mirrors.
11. Shut down the primary machine.
12. Shut down and reboot the standby machine.
13. Boot the primary machine.
14. On the primary machine, run `FTADMIN` and correct any remaining errors.

Disk Device Failure on the Primary or Standby Machine

When a disk device fails in either the primary or standby, the Fault Tolerance system provides continuous and uninterrupted access to the mirrored data using the partition on the other machine. Each machine continues to operate in its role as before. The partitions and data on the failed disk device is most likely lost and the disk device has to be replaced. This requires recreating the mirrors and lost partitions on the failed disk device.

Replace the failed disk device during scheduled downtime, leaving StandbyServer running. It is possible to manually take down the machine with the failed disk device, leaving the other machine to act as the network server. The failed disk device can be repaired while the network remains functional. There are two reasons **not** to do this.

1. If there are mirrors other than those affected by the disk device failure, they have to be re-synchronized during the recovery process. If the partitions are large, this could take as much time as was saved.
2. Shutting down one of the machines destroys the server fault tolerance. As long as both machines are running, even with a failed disk device in the primary machine, the system can recover from a server failure.

To recover from the failure complete the following steps:

1. Schedule network downtime.
2. During the downtime, stop LAN Server Advanced on the primary machine.
3. Shut down and power-off the primary machine.

Shutting down the primary machine will cause a NetFinity alert on the standby unless you disable notification before shutting down the primary machine.

4. If the failed disk device is located in the standby machine, complete step a, however, if the failed disk device is in the primary machine, complete step b.
 - a. Shut down and power-off the standby machine.

Replace the failed disk device. The disk device is not partitioned or formatted. Its free space is used to replace the lost primary mirror partitions.

Boot the standby machine and run StandbyServer.

Start any network services required by the configuration, i.e. the Requester and Replicator for a Domain Controller.

- b. Replace the failed disk device in the primary machine. The disk device is not partitioned or formatted. Its free space is used to replace the lost secondary partitions.
5. Boot the primary machine without starting LAN Server Advanced.
If FTMONIT logs any errors during the boot process, it starts the Requester.
6. Start FTSETUP on the primary machine.

Using the volume labels as a guide to verify that the original drive letter sequence is preserved, select each detached secondary in the desired drive letter sequence. The secondary partitions left on the primary machine at this point show up as detached secondaries, meaning that the Fault Tolerance system could not find a corresponding primary partition on the standby machine.

From the Drive pull-down menu, recreate the mirror by selecting the Recover secondary option. There are three selections in this sub-menu indicating the ways a detached secondary may be recovered.

Choose the **Make the drive the secondary of a mirror** option. With each recovery, the drive letter assignment made following the next boot is displayed adjacent to the drive.

Make sure that the drive letter assigned agrees with the volume label. If the drive letter assignments are incorrect, cancel the operation and begin again.

Shut down and reboot the standby machine (new partitions were created on the standby machine's disk devices).

Start *StandbyServer* and any network services required by the configuration.

Note: Even though this operation essentially creates primary mirror partitions which are indistinguishable from other HPFS partitions, their drive letters are not added to the autocheck list in the `IFS=` statement in the `CONFIG.SYS` file as they would have been had the partitions been created using `FDISK`.

- a. The primary mirror partitions now appear as unmirrored logical drives. Recreate the mirrored disk devices by selecting the **Mirror** option from the **Drive** pull-down menu for each unmirrored logical drive.

Use the volume labels as a guide to preserve the original drive letter

sequence. Exit FTSETUP. This causes the lost mirrors to be correctly recreated.

7. Shut down and reboot the primary machine.
8. On the primary machine, run FTADMIN to correct any remaining errors.
9. Start LAN Server Advanced on the primary machine.

What to Do When the Standby Machine Fails

If the standby machine fails, data remains available to the network through the Fault Tolerance system and the mirror partitions on the primary machine. To the Fault Tolerance system running on the primary machine, it appears that the disk devices containing the mirror primary partitions have failed. The system marks the primary partitions unreachable and further read/write operations are directed to the secondary partitions only.

Any mirrored disk device appears cracked to the Fault Tolerance system after the standby machine fails. The mirrors are restored when the standby machine has been repaired with the FTADMIN utility.

To recover after a failure on the standby machine, follow these steps:

1. Correct the problem in the standby machine.
2. Schedule network downtime.
3. During the downtime, boot the standby machine with the primary machine still running.



Note: Because the standby machine stopped without going through a shut down operation, the logical drives on the machine are dirty and should be repaired with the CHKDSK utility.

The IFS= statement in the CONFIG.SYS file contains an AUTOCHECK parameter with a list of drive letters for which CHKDSK is automatically run at boot time, if required. The boot drive is always included, by default, regardless of the AUTOCHECK parameter. A typical IFS= statement looks like this:

```
IFS=C:\IBM386FS\HPFS386.IFS /A:CDE
```

This statement in the CONFIG.SYS file checks drives C:, D:, and E: automatically at boot time. Although the drive letters were removed from

the AUTOCHECK list on the primary machine, it is important that they are included in the list on the standby machine.

The CHKDSK utility fails when run from the command line after this kind of a failure. If executed from the CONFIG.SYS file during the boot process, CHKDSK runs fine.

If the standby machine boots without running CHKDSK for all logical drives on the machine, but instead prints out warnings, continue the boot process until it completes. Edit the CONFIG.SYS file to include the drive letters in the AUTOCHECK list, shut down and reboot the machine.

4. Run VNCSBSPM.EXE on the standby machine.
5. Run FTADMIN on the primary machine.
6. Select the Correct all option from the Error menu to fix cracked mirrors.
7. Select the Verify all option from the Drive menu to synchronize the mirrors.

Vinca Link Cable Failure

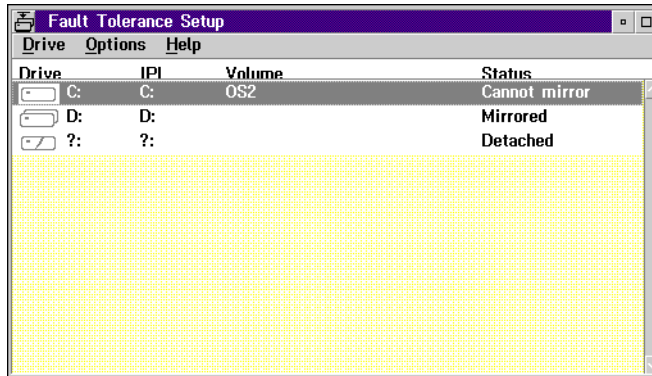
If the Vinca link cable fails or is disconnected, the disk devices in the standby machine are disconnected from the primary machine. A disk I/O request to a mirrored disk device results in a disk device failure error. To recover from this failure, follow these steps:

1. Schedule network downtime.
2. During the downtime, replace or reconnect the Vinca link cable.
3. Verify that a connection has been made by observing the green CONNECT bar on the StandbyServer application window.
4. On the primary machine, run FTADMIN to correct any errors.
5. If not done during the error correction operation, manually verify all of the mirrored disk devices.

What to do when the Mirror is Detached and the Data is Out of Synchronization

When multiple problems occur in servers, it is possible to recover data from the disk device which is not the most current data. When this happens data accumulated when only one server was functional may get overwritten. For example, if the primary machine fails and the standby switches over to take its place, and then if during the repair of the servers the primary machine is booted without the standby running, there will be both a detached disk device and out-of-sync data.

If such a situation has occurred, run Fault Tolerance Setup. The window will look something like the following (note the detached mirror).



Here are some guidelines for determining which machine has the most current data (if unsure):

1. The volume labels listed in the FTSetup drive list can help identify the disk devices.
2. A detached drive is always the secondary partition of a mirrored pair.
3. Newly created files and date/time stamps can be a big help.
4. FDISK will tell you partition types. An 87 is the secondary partition of a mirrored pair while a drive letter indicates the primary partition.

If the Primary Machine has the Most Current Data:

If the disk device attached to the primary machine has the most current data, do the following (this will recover the detached disk device as the secondary of the mirrored pair):

1. Shut down the primary machine.
2. Shut down and reboot the standby machine.
Make sure the StandbyServer software starts up.
3. Reboot the primary machine.
4. Start FTSetup on the primary machine.
5. Click to select disk devices that were mirrored but are not detached.
6. Choose Delete from the Drive menu.
7. Click on the detached disk device.
8. From the Drive menu, choose “Recover secondary”, then “Make the drive the secondary of a mirror”.
9. Click OK.
10. Double-click the close icon (in the upper left corner of the FTSetup window) to exit FTSetup.
An exit dialog box appears asking if you want to save.
11. Click Save.

If the Standby Machine has the Most Current Data:

If the disk device attached to the standby machine has the most current data, you need to do the following.

1. Shut down the primary machine.
2. Shut down and reboot the standby machine.
Make sure the *StandbyServer* software starts up.
3. Reboot the primary machine.
4. Start FTSetup on the primary machine.
5. Click to select any disk devices that are detached.
6. From the Drive menu, choose "Recover secondary", then "Leave the drive unmirrored".
7. Click OK.
8. From the Drive menu, select Delete.
9. Click to select the disk device to be mirrored.
10. From the Drive menu, choose Mirror.
11. Double-click the close icon (in the upper left corner of the FTSetup window) to exit FTSetup.
An exit dialog box appears.
12. Click Save.

Fault Tolerance Recovery—OS/2 without LAN Server Advanced

An understanding of how EZ RAID Lite implements disk mirroring will help in taking the proper corrective actions when failures occur. The following scenarios are representative but not complete. If at any time during a recovery process there is a possibility that data may be lost, contact Vinca's technical support for help before proceeding.

General Guidelines for Recovery

- ▼ When a disk device fails, partition information is lost along with the data on the disk device. The mirror is re-created with a new, unformatted and un-partitioned disk device.
- ▼ When a machine fails, partition information remains on the disk devices. Because the mirror partitions are split across two machines, the failure of one machine means that the mirror partitions become un-synchronized.
- ▼ Recovering the system to full fault tolerance requires stopping network services. Depending upon the failure and size of the partitions, it may take considerable time to re-establish the mirrors. For these reasons, schedule maintenance at a time least disruptive to network users.
- ▼ If the recovery process requires multiple boots of the primary machine, disable NetFinity notifications for the primary machine until the recovery process is complete. Re-enable the notifications when the system is ready to go back on-line. Disabling NetFinity notifications is performed on the standby machine.
- ▼ Many of the recovery steps shown below can be automated using .CMD files. See the VNCRCVR.CMD file in the VINCA subdirectory on the standby machine for an example of how to automate recovery from a primary machine failure.
- ▼ If the recovery process creates new partitions on the standby machine (these will be primary mirror partitions), the standby machine must be rebooted before it can function correctly. Rebooting causes the operating system on the standby machine to recognize the new partitions.

What to Do When the Primary Machine Fails

When the primary machine fails, the standby machine automatically switches over to assume the role as network server. Mirrored data remains accessible to the network in the form of the primary mirror partitions on the standby machine. In this case, EZRAID Lite has not detected any failures because it was running only on the machine that failed. No partition information has been lost, even though their data has become un-synchronized. The recovery process corrects the un-synchronized state of the mirrors.

To recover, follow these steps:

1. Correct the problem in the primary machine.
2. Schedule network downtime.
3. Run `CHKDSK /F` on each mirrored drive in the standby machine.

Run `CHKDSK` on the drive by changing the default drive letter and then running `CHKDSK /F` instead of running `CHKDSK` with a drive letter option. For example, enter:

```
> E:
```

```
> CHKDSK /F
```

rather than

```
> CHKDSK E: /F
```

4. Start `StandbyServer` on the standby machine.
5. Boot the primary machine.
6. Start `EZUTIL` on the primary machine.
7. Select Logical Drive Management.
8. Select the mirrored disk device.
9. Select Verify the Raid.
A window appears showing `EZUTIL`'s progress as it fixes the mirror.
10. Continue selecting Verify the Raid every time `EZUTIL` finishes verifying until zero (0) errors are found.
11. When `EZUTIL` has finished verifying the mirror with zero errors, exit `EZUTIL`.

What to Do If the Primary Machine is Booted Without the Standby Machine

If the primary machine is booted and any of the following conditions exist, EZRAID is not able to find the primary mirror partitions and they will become unsynchronized.

- ▼ The standby machine is off.
- ▼ The *StandbyServer* application is not running.
- ▼ The Vinca cable is not connected.

If any of these occur, the primary machine displays a warning that says:

Partition missing in drive D

The drive is still functional

Press ESC to continue

To synchronize the mirrors, do the following:

1. Shut down the primary machine.
 2. Boot the standby machine.
 3. Run CHKDSK on all disks on the standby machine.
 4. Run the *StandbyServer* application.
 5. Reboot the primary machine.
- EZRAID will automatically re-synchronize the mirrors.

Disk Device Failure on the Primary or Standby Machine

When a mirrored disk device fails on either machine, it should be replaced as soon as possible to restore fault tolerance. To perform this procedure, use a replacement disk device that has the same geometry as the failed disk device.

1. Shut down the primary machine.
2. Shut down the standby machine.
3. Replace the failed disk device.
4. Reboot the standby machine.
5. After the *Vinca StandbyServer* window appears on the standby machine, reboot the primary machine.
6. Verify that the *StandbyServer* window shows *CONNECTED*.
7. Start *EZUTIL* on the primary machine.
8. From the main menu, choose *Hard Disk Management* and press [Enter].
A list of disk devices appears.
9. Highlight the disk device that had failed and press [Enter].
A window appears displaying the status of that disk.
10. From the *Select an Option* menu, choose *Replace Disk* and press [Enter].
A message appears indicating that *I/O* has been suspended.
11. Press [Enter].

If using *SCSI* disk devices, an option will be given to low-level format the replacement disk device. Select *Yes* to proceed with the format. The procedure may take a several minutes.

A message then appears that the disk has successfully been replaced.

What to Do When the Standby Machine Fails

If the standby machine fails, data remains available to the network through EZRAID Lite and the mirror partitions on the primary machine. To EZRAID Lite, it appears that the disk devices containing the mirror primary partitions have failed, and a warning message will appear on the primary machine. The system marks the primary partitions unreachable and further read/write operations are directed to the secondary partitions only.

To recover after a failure on the standby machine, follow these steps:

1. Correct the problem in the standby machine.
2. Schedule network downtime.
3. At the scheduled downtime, shut down the primary machine.
4. Boot the standby machine.
5. Run the StandbyServer application, VNCSBSPM.EXE, on the standby machine.
6. Reboot the primary machine.

During the boot process, a message appears on the primary machine indicating that the partitions are out of synchronization and that the partitions will be automatically synchronized.

7. Press [Esc] to continue.
8. Start EZUTIL on the primary machine.
9. Select Logical Drive Management.
10. Select the mirrored disk device.
11. Select Verify the Raid.
12. Continue selecting Verify the Raid every time EZUTIL finishes verifying until zero (0) errors are found.
13. When EZUTIL has finished verifying the mirror with zero errors, exit EZUTIL.

Vinca Link Cable Failure

If the Vinca link cable fails or is disconnected, the disk devices in the standby machine are disconnected from the primary machine. A disk I/O request to a mirrored disk device results in a disk device failure error. To recover from this failure, follow these steps:

1. Schedule network downtime.
2. During the scheduled downtime, replace or reconnect the Vinca link cable.
3. Verify that a connection has been made by observing the green CONNECT bar on the StandbyServer application window.
4. Reboot the primary machine.
5. On the primary machine, run EZUTIL to verify the mirror.

Chapter 5

Using StandbyServer

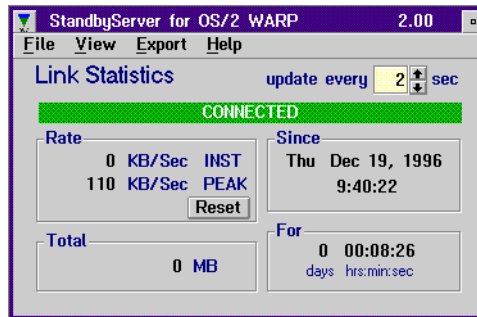
StandbyServer's main window contains three views:

- ▼ Link Statistics
- ▼ Drive Information
- ▼ Card Information

Each of these views is accessed from the View menu.

Using the Link Statistics view

The Link Statistics view displays the current status of the Vinca link. When connected, the status bar displays Connected with a green background. When disconnected it displays Disconnected with a red background.



The Rate section displays the rate of mirrored data across the Vinca link.

INSTThe amount of data in KB during a one second interval.

PEAKThe greatest amount of data in KB during a one second interval.

Reset buttonResets the INST and PEAK statistics.

The Total section displays the total MB of data mirrored since the current session was started.

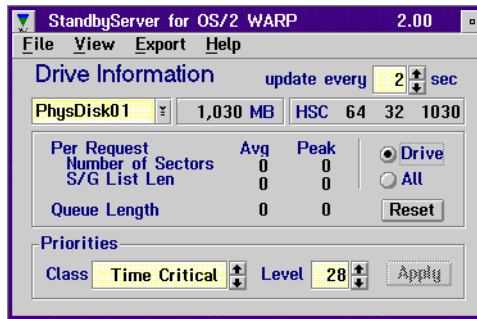
The Since section displays the date and time since the status changed. For example, when the status changes from Connected to Not Connected, this date and time counter changes to reflect the new date and time.

The For section displays the duration of the current status in days, hours, minutes, and seconds. The date and clock time are taken from the system clock. If the clock needs to be reset, consult your systems time adjustments.

The update interval for refreshing the window's statistics can be set from 2 to 10 seconds in two second intervals.

Using the Drive Information View

The Drive Information view displays information for the selected drive, or in the case of read/write requests, information for all drives can be displayed.



The drop-down list box displays the disk devices for which you can display information. The selected device's size (in MB), and the number of heads, sectors, and cylinders.

The Per Request section displays information about the disk requests.

Number of Sectors	Number of sectors transferred per request.
S/G List Len	Length of the scatter gather list.
Queue Length	Number of requests that have been queued.
Drive/All options	Toggles the display information between the selected drive and all drives.
Reset button	Resets the statistics to zero.

The Priorities section displays the selected Class and Level.

Class	Priority class for the program threads that handle disk requests.
Level	Priority level for the Priority Class. Levels are from -32 to +32.
Apply button	Commits the selected changes to the display.

The update interval for refreshing the window's statistics can be set from 2 to 60 seconds in two second intervals below ten and ten second intervals above ten.

Using the Card Information View

The Card Information view displays information about the communication cards in both the primary server and the standby machine. This information varies depending on the card type. This information is displayed for your information, and might be needed in the event of a service call.

Chapter 6

Customizing NetFinity

IBM's NetFinity initiates the switchover process when the primary machine fails and its role switches to the standby machine. NetFinity is flexible and easy to configure but it is impossible to anticipate the requirements for every installation. It is possible to customize the interface between IBM's products and *StandbyServer* for OS/2 Warp to fit special needs.

The Basic NetFinity Operation

NetFinity's Service Manager on the standby machine detects when the primary machine is no longer accessible on the network. When the primary machine is no longer connected to the network, the Service Manager generates a NetFinity alert to the standby's Alert Manager. The Alert Manager then runs a command file containing the actions necessary to start your services (e.g. LAN Server Advanced or Notes) on the standby machine. The example command file, *RESTART.CMD*, generates several NetFinity alerts which are logged and used to chart the progress of the switchover process. If a failure occurs during the switchover process, consult the log file to determine the point of failure.

Generating NetFinity Alerts

RESTART.CMD uses the NetFinity command line program GENALERT to generate NetFinity alerts. Alerts are distinguished from each other by five parameters. These parameters can create event filters for setting up alert actions in the Alert Manager. The five parameters are:

1. Alert Type
2. Severity
3. Application ID
4. Application Alert Type
5. Sender ID

In addition to the parameters, each alert has an associated text string that appears in the alert log. The time and date of the alert is also recorded.

The GENALERT command line follows the form:

```
GENALERT /T:"text" /APP:id_name /SEV:0..7 /TYPE:sssttt /ATYPE:hexnum
```

where:

<code>/T:"text"</code>	is the text string that appears in the alert log
<code>/APP:id_name</code>	is the application ID for the alert (1-8 characters)
<code>/SEV:0..7</code>	is the alert severity (0 = highest, 7 = lowest)
<code>/TYPE:sssttt</code>	is the alert type, selected from the following options:

the `sss` field defines the alert ID -

- UNK unknown
- SYS system
- DSK disk or DASD
- NET network
- OS_ operating system
- APP application
- DEV device
- SEC security

and `ttt` describes the class of the alert -

- UNK unknown
- FLT fault or failure
- ERR error
- WRN warning
- INF information

`/ATYPE:hexnum` is the application-specific alert type, entered as a hexadecimal value ranging from 0x00000000 to 0xFFFFFFFF.

As an example, a system administrator can choose to generate an alert when the standby machine starts the LAN Server Advanced program. This can be done in the `RESTART.COMD` file with the following command:

```
GENALERT /T:"LAN Server restarted" /APP:STANDBY /SEV:0 /TYPE:APPINF /ATYPE:5
```

An action such as forwarding the alert to another workstation, or playing a `.WAV` file, can now be set up in the Alert Manager.

Setting Up Actions in the Alert Manager

Create a new alert action by opening the Alert Manager window and selecting `NEW` in the main panel. The Action Editor appears. The top half of the Action Editor provides filter selections so that the desired action occurs only when an alert with the appropriate attributes is received by the Alert Manager.

There are five selection areas corresponding to the five alert parameters described above. One or more selections can be made for each of the parameters. By checking the `ANY` check box, a "don't care" condition is indicated; a valid selection for each parameter.

The bottom half of the Action Editor defines what action happens when a matching alert is received by the Alert Manager. The Action spin list contains all of the available and pre-defined actions. The list may vary depending upon the capabilities of the machine.

To forward an alert to a machine with the NetFinity name `ALTA`, set the:

1. Alert type to `AppInformation`.
2. Severity to `0`.
3. Application ID to `STANDBY`.
4. Application alert type to `5`.
5. Sender ID to the name of the machine generating the alert, or check the `ANY` check box.

If the selection list boxes do not contain the desired fields (e.g., Application ID and Application ID Type), then the appropriate values must be entered in the text entry fields and made to appear as selected in the list boxes.

6. Scroll the Action field until the Forward alert action appears. Fill in the parameters with the network type and the name of the destination machine (in this example, ALTA).
7. Save the new action. Any alert matching the specified description is forwarded to the destination machine (in this example, ALTA).

Other Settings and Procedures

The Remote Service Manager on the standby machine must be configured to monitor the network connection to the primary machine. An alert action must be created to execute a command file if a primary machine failure is detected.

It is not recommended to have the standby machine monitor other systems in the network. Instead, have a second NetFinity manager installed on the system administrator's machine. This machine monitors the presence of both the primary and standby machines. The NetFinity manager on the standby machine can forward switchover progress alerts to the system administrator's machine, where they are logged, forwarded via pager, or trigger audio .WAV files.

Plan your NetFinity installation to take full advantage of its features and flexibility, particularly during the switchover process.

Chapter 7

LAN Server Advanced Fault Tolerance and Domain Replication

In the LAN Server Advanced environment, *StandbyServer* for OS/2 Warp relies on the IBM Fault Tolerance system provided with LAN Server Advanced to maintain mirroring. This chapter provides a brief introduction to IBM's Fault Tolerance mirroring as a basis of understanding. For a complete treatment of IBM Fault Tolerance, refer to the IBM documentation for network administrators.

This chapter also provides a sample setup for enabling replication services if the primary machine is a Domain Controller or Backup Domain Controller. Again, for complete information refer to the IBM documentation.



Note: This chapter does not apply to machines not running LAN Server Advanced.

General IBM Fault Tolerance Information

A Fault Tolerance mirror consists of two partitions, connected together by software, which appear to the operating system as a single logical drive and, therefore, share a single drive letter. The term *mirrored drive* refers to the Fault Tolerance mirror as it is viewed by the operating system, i.e., as a single logical drive with an associated letter. The term *mirrored partition* refers to one of the component partitions of the mirrored disk device.

Fault Tolerance Mirror Characteristics

- ▼ The mirrored partitions will be on different physical disk devices. If the disk devices are connected to the system through separate host adapters, the mirror is also duplexed and further guards against the failure of either of the host adapters. This minimizes exposure to single points of failure.
- ▼ The mirrored drive is formatted for HPFS. The Fault Tolerance utilities perform this function automatically.
- ▼ A write operation directed to a mirrored disk device results in a write to both partitions of the mirror, which are located on different physical disk devices. This double-write operation adds extra time to write operations (considered to be the cost of the added security that mirroring provides).
- ▼ A read operation directed to a mirrored disk device is handled by the least busy physical disk device of the mirror. This is called split reads and can result in improved file system access times under some conditions.
- ▼ One partition of the mirror is designated as *primary*, while the other partition is designated as *secondary*. The primary and secondary partitions have different ID values and are treated differently by the base operating system.



Note: The use of the terms *primary* and *secondary* as partition titles should not be confused with the use of the terms *primary* and *standby* to refer to the roles of the two server machines in a StandbyServer installation.

- ▼ If one of the physical disk devices containing a mirrored partition fails, the operating system will continue to access the mirrored data by directing I/O operations to the other partition in the mirror. Fault Tolerance utilities will detect and log the errors, and provide a mechanism for error recovery.

Fault Tolerance Mirror Requirements

The physical disk devices containing the partitions of a Fault Tolerance mirror must report the same geometry (i.e., number of heads and number of sectors per track) to the operating system. When the operating system accesses the

physical disk device it first builds a sector map table. Fault Tolerance mirroring requires that sector maps for the physical disk devices containing the mirrored partitions must be the same. In practical terms, this means that the physical disk devices must report the same number of heads and number of sectors per-track to the operating system. The number of cylinders may be different (which only affects the overall capacity of the drive.)

The host adapter may provide some hardware re-mapping. In hardware RAID systems, for instance, several disk devices are combined to form, as it appears to the operating system, a single, large disk device. This level of re-mapping is transparent to the Fault Tolerance system.

Fault Tolerance Files

The IBM Fault Tolerance system consists of five software components:

DISKFT.SYS

- ▼ Appears in the first line of CONFIG.SYS as a loadable device driver.
- ▼ Loads before all the other loadable device drivers, but after all base devices, such as OS2SCSI.ADD and OS2DASD.DMD.
- ▼ Intercepts disk device I/O requests from the operating system.
- ▼ Redirects I/O requests to the appropriate physical disk devices.
- ▼ Manipulates the I/O request as needed to implement the mirror.
- ▼ Creates a new buffer for write operations, copies the request information, and dispatches both requests to appropriate physical disk devices.
- ▼ determines which physical disk device of the mirror is least busy and routes read requests to that disk device.

FTMONIT.EXE

- ▼ Runs as a detached process.
- ▼ Monitors disk device I/O operations for errors.
- ▼ Detects and logs all disk device errors, whether or not they are mirrored.

FTSETUP.EXE

- ▼ Creates Fault Tolerance mirrors.
- ▼ Adds the appropriate lines to the CONFIG.SYS file when run the first time so that DISKFT and FTMONIT load automatically the next time the computer is booted.
- ▼ Unmirrors disk devices.
- ▼ Recovers detached secondary partitions that have lost their connections to their primary disk device.

FTADMIN.EXE

- ▼ Displays the Disk Device Error Log.
- ▼ Provides a mechanism for error recovery.
- ▼ Verifies mirrored disk devices.
- ▼ Restores synchronization between the mirrored partitions.

FTREMOTE.EXE

- ▼ Uses a response file to automate operation of FTSETUP and FTADMIN.

Primary and Secondary Partitions

A Fault Tolerance mirror consists of a primary and secondary partition. Each partition is on a distinct physical disk device and is connected to the other by a software driver, DISKFT.SYS, to form a single logical disk device.

Partition Tables

Partition tables store information about disk partitions, including location, size, and type. A partition table can contain four sets of information and is located at the end of the Master Boot Record (MBR) of every disk device. Partitions can be added using a chain of partition tables with the chain's root in the first partition table of the disk device. Only one chain is allowed per disk device.

The partitions defined in the first partition table are *Primary Partitions* (not to be confused with the primary partitions of a Fault Tolerance mirror). The partitions defined in the chain are collectively called the *DOS Extended Partition*, with each partition in the chain called a *Logical Partition*. There can be as many partitions in the chain of logical partitions as there are disk device letters in the operating system to support them.

A physical disk device can then be partitioned into four primary partitions, or three or fewer primary partitions and a DOS Extended Partition, containing as many logical partitions as the system can support.

A number stored in the partition table indicates the partition type. For instance, type number 7 indicates an OS/2 (HPFS) partition. Type number 4 indicates a DOS 16-bit FAT partition. There are type numbers for other operating systems and formatting options.

Type number 5 indicates an extended volume in the DOS Extended Partition. The table holds the location of the extended volume. Each extended volume begins with an MBR with its own partition table (although this MBR is not used for booting). One entry in the table indicates the type of the extended volume, (i.e., HPFS or DOS 16 bit FAT). If there is another entry in the partition table, it must be a link to the next extended volume in the DOS Extended Partition, as

indicated with the type number 5. There can never be more than two valid partition table entries in an extended volume's partition table. An arbitrary number of extended volumes can be created using the type 5 chaining algorithm.

Drive Letter Assignments

When the operating system boots, it scans all of the physical disk devices in its system and assigns drive letters to each volume. The operating system follows these rules in making the drive letter assignments:

- ▼ Disk devices are scanned beginning with the first disk device on the first host adapter and proceeding through all of the disk devices on that host adapter. It then proceeds to the first disk device on the second host adapter and continues through the rest of the disk devices on that host adapter. This scanning sequence is maintained until it has scanned all of the disk devices on all of the host adapters.
- ▼ All primary partitions are assigned a drive letter in the order they appear, before any drive letters are assigned to logical drives.
- ▼ After all of the primary partitions are assigned, the extended volumes are assigned drive letters in the order they are encountered, following the pointer chain rooted in the first Partition Table of each disk device.

Fault Tolerance Mirror Partitions

The secondary partition in a Fault Tolerance mirror does not have the same partition type identifier as the primary partition of the mirror. These Fault Tolerance mirror partition rules apply:

- ▼ The primary partition of the mirror will have a type number of 7, indicating that it has been HPFS formatted.
- ▼ The primary partition of the mirror is not necessarily a primary volume.
- ▼ The secondary partition of the mirror will be a type number 87.
- ▼ While the primary partition of the mirror is recognized by the base operating system, the secondary partition is not recognized. It is, in essence, an invisible partition.
- ▼ Loading `DISKFT` at boot time makes the secondary partition visible and ties it to its primary partition of the mirror. `DISKFT.SYS` must be included as the first line of the `CONFIG.SYS` file to establish this link.

Maintaining the Mirror - Other Fault Tolerance Files

The Fault Tolerance system maintains the connections between the primary and secondary partitions of its mirrors by storing the information in two redundant sets of hidden files.

A Fault Tolerance master file, `FTCFG.SYS`, resides in the C: root directory and contains the following system-wide information in its header:

- ▼ A special signature.
- ▼ The number of logical disk devices in the system (mirrored and non-mirrored).
- ▼ The file version number.
- ▼ The number of times the file has been updated.

Following the header is an array of records containing the following information:

- ▼ A record, arranged in drive letter order, for each logical disk device in the system. Each record has the location and status information for one partition (or two partitions, in the case of a Fault Tolerance mirror).
- ▼ The record status; if the disk device is not mirrored, it is marked as non-mirrored and the information for the secondary partition is ignored.
- ▼ The location of a mirrored disk device including the physical disk device number and extents of both partitions.
- ▼ Additional information about the mirror status to indicate the relative health of the mirror.

The second hidden file, `FTCFG.DRV` resides in the root directory of every logical drive. These `.DRV` files contain the system-wide and device information for the disk device on which they reside.

Booting With Fault Tolerance Installed

Load `DISKFT` (an installable device driver) after all base device drivers including adapter device drivers, filters, and device manager drivers. Its position in the `CONFIG.SYS` file ensures that it loads before installable file systems, especially `HPFS386`.

`DISKFT` analyzes the partition information as it scans the partition tables of the disk devices in the system. It compares this information with the contents of the `FTCFG.SYS` file.

If the `FTCFG.SYS` file is not accessible or has been corrupted, `DISKFT` reads the `FTCFG.DRV` files to reconstruct the information. It then combines this information

into an internal data structure representing the current state of the Fault Tolerant system. In the process, it adjusts the contents of the hidden files if necessary.

DISKFT now receives all disk I/O requests from the file system and passes them to the disk subsystem, OS2DASD. When an I/O request is directed to a mirrored disk device, DISKFT makes the necessary adjustments to implement the mirror.

After DISKFT loads, run the FTMONIT program. FTMONIT connects to DISKFT and copies its internal data structure. It detects the presence of DISKFT and logs any disk device I/O errors DISKFT generates.

After DISKFT loads and FTMONIT is running, the Fault Tolerance system is complete.

Potential Problems with Booting

If the machine is booted without having completed a proper OS/2 shutdown (such as a power disruption or other comparable condition), it is likely that the logical drives in the system are dirty. A dirty drive is one with file system information that was left in an incomplete state. This may prevent DISKFT from reading the FTCFG files from the logical drives. In this situation, DISKFT cannot match the primary and secondary partitions of the Fault Tolerance mirrors to complete its normal function. If this occurs, DISKFT detaches the secondary partitions of the mirrored drives and alerts the system administrator.

The system administrator has the following alternatives:

1. Re-establish the mirrors.
2. Recover the secondary partitions as normal logical drives.
3. Eliminate the secondary partitions altogether.

Running CHKDSK normally corrects the file system errors associated with a system crash, allowing the FTCFG files to be read. The repair utility cannot be run, however, until after loading DISKFT and the file system by which time the damage has been done.

Fault Tolerance Mirror Status

The hidden `FTCFG` files contain information about how `DISKFT` views the current status of the mirrored disk devices. There are five valid Fault Tolerance mirror states which are divided into three error condition categories: No Errors, Non-fatal Errors, and Fatal Errors.

No Errors

- ▼ `DISKFT` reads from either mirrored partition and writes to both partitions of the mirror.

Non-fatal Errors

- ▼ `DISKFT` attempts to read from the primary partition first.
- ▼ `DISKFT` attempts to read from the secondary partition first. In either case write operations are directed to both partitions of the mirror.

Fatal Errors

- ▼ `DISKFT` reads from and writes to the mirror's primary partition.
- ▼ `DISKFT` reads from and writes to the mirror's secondary partition. The current state of the Fault Tolerance mirrors can be determined by running the `FTVIEW` program in the `VINCA` subdirectory on the primary machine.

Replicator Services Setup

This is a sample setup for enabling replicator services, so that the Vinca solution can be used to mirror data from a Domain Controller. Replicator services allow the standby machine to take over the Domain Controller functions at switchover.

This sample assumes the following:

1. There is a user account on the file server (primary) called **standby**.
2. The user account **standby** has all administrator privileges.
3. The password for standby is **password**.

When setting up the system up we recommend using a more secure password!

Primary Server Setup

On the primary machine in our example, IBMLAN.INI contains the following:

```
[replicator]
    replicate = EXPORT
    exportpath = C:\IBMLAN
    interval = 5
    guardtime = 2
    pulse = 3
    random = 60

[server]
```

;Add REPLICATOR to this line for autostart.

```
SRVSERVICES = NETLOGON,LSSERVER,REPLICATOR
```

Also on the primary machine, a REPL.INI file must be created in each subdirectory for which replication is needed. In the example, the \IBMLAN\ACCOUNTS, \IBMLAN\USERS, and \IBMLAN\DCDB subdirectories all have identical REPL.INI files. The example REPL.INI file contains only the following two lines:

```
EXTENT=TREE
INTEGRITY=FILE
```

Standby Machine Setup

On the standby machine in our example, IBMLAN.INI contains the following:

```
[replicator]
    replicate = IMPORT
    importpath = C:\IBMLAN
    tryuser = yes
    logon = standby
    password = password
```

```
[requester]
    ;Add this line for autostart.
    WRKSERVICES = REPLICATOR
```

Use NET START REQ /CO:STANDBY to start the requester. Do not log on.

Chapter 8

Reference Information

Routing over TCP/IP

In some installations OS/2 NETBIOS traffic is routed over a TCP/IP router or gateway. It is possible to use *StandbyServer* for OS/2 Warp in such an installation. This chapter presents a sample configuration, not detailed instructions. It is necessary to have a good knowledge of NETBIOS, NetBIOS over TCP/IP routing, and the characteristics of the router before using this information as a guide to configuring the system.

Vinca recommends that the router be capable of self configuring its internal routing tables. Most routers do this by generating a broadcast ARP (address resolution protocol) and adding the response to the internal route table. This allows the router to “find” the standby machine when a switchover occurs. Most routers do this automatically.

An appropriate names list must be generated on the OS/2 server using the IBM OS/2 NETBIOS OVER TCP/IP configuration menu. This will equate NETBIOS names to IP addresses. On client workstations, the IBM OS/2 NETBIOS OVER TCP/IP protocol must be configured with a broadcast list that includes the primary and standby machines.

Sample Configuration

The IP address setup of the test configuration was as follows:

Router

LAN A—204.99.142.204 Subnet mask 255.255.255.0

LAN B—205.150.50.10 Subnet mask 255.255.255.0

Client

IP address 205.150.50.30

NETBIOS name = "WKSTATION"

Broadcast list:

204.99.142.201

204.99.142.202

Primary

IP address 204.99.142.201

NETBIOS server name = "RIVERBEND"

Names list:

"ETHER1" 204.99.142.204

"ETHER2" 205.150.50.10

"RIVERBEND" 204.99.142.201

"WKSTATION" 205.150.50.30

"STANDBY" 204.99.142.202

Standby

IP address 204.99.142.202

NETBIOS server name = "STANDBY"

Names list:

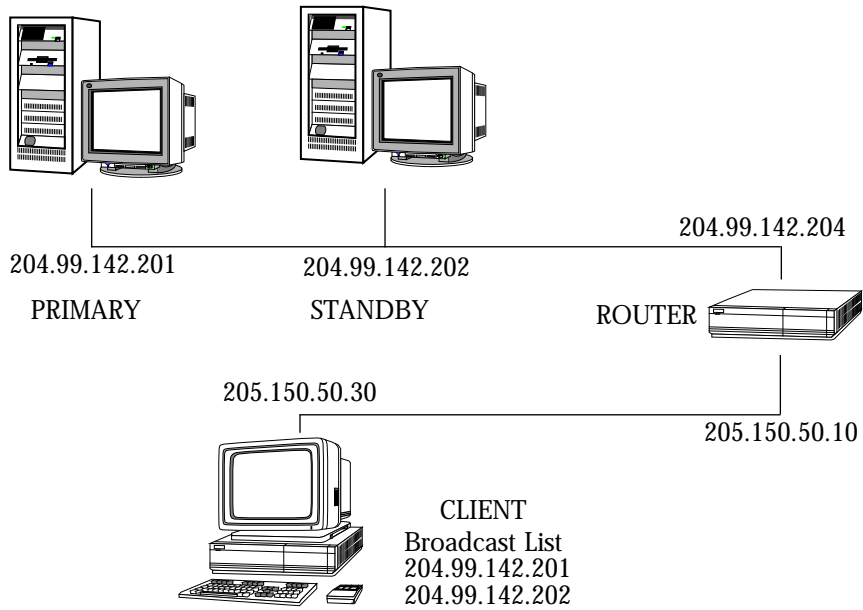
"ETHER1" 204.99.142.204

"ETHER2" 205.150.50.10

"RIVERBEND" 204.99.142.202

"WKSTATION" 205.150.50.30

Sample Illustration



Reference Information

StandbyServer Files

After installation using the default directory structure, Vinca files are added to both the C:\OS2 directory and the C:\VINCA directories on both the primary and standby machine. This section describes the StandbyServer's program files. Files located in the VINCA directory that are not listed below are used in the install / uninstall process. Files with an "*" next to them are on the standby machine only.

FTVIEW.EXE	viewing utility for the FTCFG.SYS hidden file. It displays the state of the Fault Tolerance system as seen by DISKFT.SYS and FTMONIT.EXE.
GEO.EXE	describes every disk in the system and gives drive geometry information for those disks.
RESTART.CMD*	sample command file that determines whether a switchover will take place. If a switchover is needed, this command file calls SWITCH.CMD which actually causes the switch.
SWITCH.CMD*	sample command file that effects the switchover from standby to server. This file may be called from another command file as part of an automated switch over or executed from the command line as part of a manual switchover.
SYSLEVEL.VNC	is an OS/2 SYSLEVEL information file.
TSTLNK.EXE*	tests the Vinca line connectivity. It returns a 0 if the link is connected, a 1 otherwise. Normally, this program is used in a command file to determine whether a switchover will take place.
VNCEL01.SYS	link device driver for Vinca EISA cards. Loads in CONFIG.SYS with the BASEDEV=VNCEL01.SYS entry. The VNCEL01\$ parameter at the command line links this driver to the adapter device driver or the inter-device communication driver.
VNCIDC.SYS	device driver to connect the StandbyServer application with the Vinca link driver. It changes the synchronous I/O calls made by the application into asynchronous calls expected by the link driver. It loads in CONFIG.SYS with the command line DEVICE=VNCIDC.SYS VNCXLXX\$ (where VNCXLXX\$ is the name of the Vinca link driver, e.g., VNCEL01\$ would be used for an EISA system).

- VNCIL01.SYS** link device driver for Vinca ISA cards. It loads in `CONFIG.SYS` with the `BASEDEV=VNCEL01.SYS` entry. The `VNCIL01$` parameter at the command line links this driver to the adapter device driver or the inter-device communication driver.
- VNCKILL.EXE*** unlocks the `NET.ACC` file at the standby machine. This facilitates updating the file during the switchover process. This is required if *StandbyServer* is used on a domain controller and replicator services is being used.
- VNCML01.SYS** device driver for Vinca MCA cards. It loads with the command `BASEDEV=VNCML01.SYS` in the `CONFIG.SYS` file. The `VNCML01$` parameter at the command line links this driver to the adapter device driver or the inter-device communication driver.
- VNCPE01.SYS** device driver for IBM PRO/100 Fast Ethernet PCI cards. It loads with the command `BASEDEV=VNCPE01.SYS` in the `CONFIG.SYS` file. The `VNCPE01$` parameter at the command line links this driver to the adapter device driver or the inter-device communication driver.
- VNCRCVR.CMD*** sample command file used in the fault tolerance recovery process when the primary machine has failed.
- VNCSBS.ADD** allows the primary machine to manage disk drives on the standby machine as though they were local. This file is the Adapter Device Driver which communicates with the *StandbyServer* application running on the standby machine. This driver loads in the `CONFIG.SYS` file with the command `BASEDEV=VNCSBS.ADD VNCXLXX$` where `VNCXLXX$` is the name of the Vinca link driver, e.g. `VNCEL01$` would be used for an EISA system. This `.ADD` must be the last adapter device driver loaded in the `CONFIG.SYS` file.
- VNCSBSDN.EXE*** guarantees that the *StandbyServer* application has terminated before returning. A utility normally used in a command file in connection with `VNCSBSSD.EXE` to ensure that critical processes are not started during a switchover operation, before the *StandbyServer* application has fully stopped.
- VNCSBSPM.EXE*** runs on the standby machine when the primary machine is booted. This file is the *StandbyServer* Presentation Manager application. It gives static and dynamic views of the operation of *StandbyServer*.

Reference Information

VNCSBSSD.EXE*	notifies the StandbyServer application to shut down. Normally part of a command file used in the automatic switchover from primary to standby. It operates asynchronously, that is, it does not wait for VCNSBSPM to terminate, which may take several seconds, before returning. This means that other processes can be initiated while the application is shutting down.
VINS.ABT	contains installation information for the “About...” dialog in the StandbyServer application, and contains disk export data.
VINSABT.EXE	displays the “About...” dialog box in the StandbyServer application.
VINSDELL.COMD	deletes the Vinca software from the system. This is the command file that is run when the Vinca UnInstall utility is run.

Creating Emergency OS/2 Boot Diskettes

IBM recommends that OS/2 users create boot diskettes so they can access information on HPFS drives even if the machine cannot boot from its internal hard drive. Machines that have disk mirroring on them require specific changes to the CONFIG.SYS file on the boot diskette to make the mirrored disks available.

Boot Disk Changes for EZRAID Lite

Cyranex Corporation, makers of EZRAID Lite for OS/2, recommends the following procedure for creating EZRAID-capable boot floppies.

1. Diskcopy the OS/2 installation diskette number 1.
2. Return your original OS/2 installation diskettes to their usual storage location.
3. Copy the following files from the EZRAID directory on your hard drive to the diskette you created in Step 1:

BOOT.DAT
SYSSERR.DAT
SYSSMSG.DAT
EZRAID.DMD
EZFLPY.DMD
EZRIOP.EXE
EZUTIL.EXE

If the files do not all fit on your disk, look for IBM-installed files that you may not need. For example, if your system is not an IBM PS/2 you can delete all files that begin with IBM2.

4. Edit the CONFIG.SYS file on the floppy diskette as follows:

a. Insert the word REM at the beginning of the BASEDEV=OS2DASD.DMD line, as follows:

```
REM BASEDEV=OS2DASD.DMD
```

b. Add the following three lines to the CONFIG.SYS file:

```
BASEDEV=EZFLPY.DMD
```

```
BASEDEV=EZRAID.DMD
```

```
RUN=EZRIOP.EXE
```

5. Remove the floppy diskette and store it in a secure location.

Boot Disk Changes for LAN Server Advanced with Fault Tolerance

Vinca recommends the following procedure for creating LAN Server Advanced Fault Tolerance-compliant boot floppy diskettes.

1. Diskcopy the OS/2 installation diskette number 1.
2. Return the original OS/2 installation diskettes to their usual storage location.
3. Use the MAKEDISK utility as described in the IBM documentation to configure the boot disk.

Using Fault Tolerance Alerts with StandbyServer for Lan Server

When an error is detected in the Lan Server mirroring (Fault Tolerance), the error is logged to the file C:\IBMLAN\LOGS\FT.LOG, and alerts (network message) can also be sent to selected machines. For machines to receive notification, their Machine IDs need to be added to the IBMLAN.INI file on the primary server, and Alert Notification needs to be enabled on each machine.

1. Enable the Send Alerts option on the primary server.
 - a. Open the Fault Tolerant Administration window.
 - b. From the Options menu, click Alerts.
 - c. Enable the Send Alerts options.
 - d. Click OK to close the dialog.
2. Edit the primary server's IBMLAN.INI file (C:\IBMLAN\IBMLAN.INI)
 - a. Add the machine IDs to the ALERTNAMES= parameter of the [server] category adding the machine IDs of the machines to receive notification. For Example:
`ALERTNAMES=ADMINX,CLIENTX,CLIENTY`
 - b. Add the ALERTER to the SRVSERVICES= parameter. For example:
`SRVSERVICES=NETLOGON,LSSERVER,REPLICATOR,ALERTER`
3. Enable Network Messaging on each machine to receive alerts.
 - a. From the IBM LAN Services - Icon View, double-click on the Network Messaging icon.
 - b. From the Options menu, click Configure to open the Network Messaging - Configuration dialog box.
 - c. Ensure the Popup on message arrival option is enabled.
 - d. Ensure the Dismiss automatically option is disabled.

Other alert settings can be set as needed.

Using Netfinity Services with StandbyServer for Lan Server

The Netfinity Services can also be used on the primary server in conjunction with the fault tolerance alerts configured in the previous section. After the Netfinity Service is configured, it must remain running to send alerts. It can be minimized, or hidden from the users, but must be running.

Keep in mind that when a "verify" command is executed under Fault Tolerance Administration, the FT.LOG is updated, which results in alerts being sent. Therefore alerts should be either disabled or ignored during this period.

1. Make sure the Netfinity Manager is loaded on the primary server.
2. Ensure the service "Critical File Monitor" is set up to monitor the status of the C:\IBMLAN\LOGS\FT.LOG
3. Create an Alert Action (under Alert Manager) as described in the Netfinity Manager manual.

Index

Symbols

!VNC7261.CFG 29, 69
@5131.ADF 30, 71

Numerics

16-bit ISA link cards 24, 65
30-day evaluation 33, 73
32-bit EISA link cards 28, 69
32-bit MCA link cards 29, 70

A

Action Editor dialog 48, 89
Add System Group dialog 49, 91
Alert Actions dialog 47, 89
Alert Log dialog 88
Alert Log dialog box 47
Alert Manager actions 125
Alert Received window 56, 99
ALERTNAMES= 145
automatic switchover 51, 93

B

BASEDEV= 78
Boot Disk Changes for EZRAID Lite 143
Boot Diskette 143
booting the primary server before the
standby machine 104

booting the primary server without the
standby machine running 115

C

CHKDSK 36, 54, 76
Cluster Pack serial number 33, 74
CONFIG.NEW 43, 45, 87
CONFIG.SYS 34, 37, 45, 54, 78, 84, 95,
104, 107, 108

D

Delete dialog 58
disk devices 38, 72, 79, 131
Disk Export utility 38, 79
DISKFT 132
DISKFT.SYS 129
drive letter assignments 131

E

editing the primary server's CONFIG.SYS
file 54, 97
EISA Vinca link cards 24, 28, 69
Emergency OS/2 Boot Diskette 143
errors 134
evaluation 33, 73
exporting disk devices 38, 79
exporting rules 79

Index

- EXTENT= 135
- EZRAID Lite 11, 62, 94, 143
- EZRAID Lite installation window 94
- EZUTIL utility 95
- F**
- fault tolerance 134
- Fault Tolerance Setup 52, 110
- Fault Tolerance Setup window 53
- FDISK 31, 62
- FDISK utility 22
- FDISKPM 31, 62
- FT.LOG 145
- FTADMIN 102
- FTADMIN.EXE 130
- FTCFG.SYS 132
- FTMONIT 57
- FTMONIT.EXE 38, 129
- FTREMOTE.EXE 130
- FTSETUP 105
- FTSETUP.EXE 129
- FTVIEW.EXE 140
- G**
- GENALERT 124
- GEO.EXE 31, 140
- Group window 50, 92
- H**
- HPFS formatted drives 73
- HPFS formatted drives 52
- HPFS partition 31
- I**
- IBM PRO/100 PCI fast Ethernet card 24, 64
- IBMLAN.INI 145
- Install dialog 34, 75
- installation testing 56
- Install-directories dialog 75
- installing EZRAID Lite 94
- installing NetFinity Manager 43
- installing NetFinity Manager on the standby machine 84
- installing NetFinity services 40
- installing NetFinity services on the primary machine 81
- installing StandbyServer 34
- INTEGRITY= 135
- IP address 138
- J**
- J1 28, 66
- J14 27, 68
- J16 26, 67
- J18 25, 66
- L**
- LAN Server Advanced 32
- LAN Server, using fault tolerance alerts 145
- Link Statistics window 52, 94
- M**
- mirror status 134
- mirror synchronization 110
- mirrored disk device 32, 73
- mirroring 52, 110, 128, 134
- mirroring errors 134
- N**
- NETBIOS 138
- NetFinity 11, 123
- NetFinity alerts 124
- NetFinity Install dialog 82
- NetFinity Install directory selection window 43
- NetFinity Install window 44, 85
- NetFinity Installation dialog 41
- NetFinity Manager 43, 84
- NetFinity services 40, 81
- Netfinity Services 146
- Network Driver Configuration window 42, 44, 83, 86
- NFDASD.FLT 84

O

OS/2 Boot Diskette 143

P

partition 61
 partition tables 130
 partitions 130
 primary role 36, 76, 103, 106
 primary server 134
 primary server failure 103, 114
 primary server's CONFIG.SYS 54

R

RAID 10
 RAID host adapters 22
 READ.ME 37
 recovery with LAN Server Advanced 102
 registration number 35, 76
 135
 replicator services 134
 RESTART.CMD 55, 124, 140
 roles 36, 106
 Routing over TCP/IP 137
 rules for exporting 79

S

Select an Option menu 96
 Select Drive menu 96
 135
 server roles 36, 76
 Set Local Drives dialog 39, 80
 Set System Notifications dialog 51, 93
 simulating a cable link failure 56
 SRVSERVICES 135
 SRVSERVICES= 145
 standby machine 134
 standby machine failure 117
 standby role 36, 76
 status 134
 support 19
 SWITCH.CMD 55, 140
 switchover 51, 93
 synchronization 110
 SYSLEVEL.VNC 140

T

TCP/IP routing 137
 technical support 19
 testing the installation 56
 TSTLNK.EXE 140

U

uninstalling StandbyServer 58
 Using Fault Tolerance Alerts 145

V

validation 33, 73
 Vinca 70
 Vinca link 9, 61, 63, 64, 68, 95
 Vinca link cable 29, 68, 70
 Vinca link card 36
 Vinca link failure 118
 Vinca technical support 19
 VINS.ABT 142
 VINSABT.EXE 142
 VINSDELL.CMD 142
 VNCEL01.SYS 140
 VNCIDC.SYS 140
 VNCIL01.SYS 141
 VNCKILL.EXE 141
 VNCML01.SYS 141
 VNCPE01.SYS 141
 VNCRCVR.CMD 55, 57, 102, 141
 VNC SBS.ADD 141
 VNC SBS.DN.EXE 141
 VNC SBS.PM 36, 79
 VNC SBS.PM.EXE 36, 46, 52, 76, 87, 141
 VNC SBS.SD.EXE 142