

# Disaster Recovery Option Guide

Arcserve® Backup

18.0

arcserve®

## Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

© 2021 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

## Arcserve Product References

This document references the following Arcserve products:

- Arcserve® Backup
- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent for Windows
- Arcserve® Unified Data Protection Agent for Linux
- Arcserve® Replication and High Availability

## Arcserve Backup Documentation

Arcserve Backup documentation contains specific guides and release notes for all major releases and service packs. Click links below to access documentation.

- [Arcserve Backup r18 Release Notes](#)
- [Arcserve Backup r18 Bookshelf](#)

## Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

### [Contact Support](#)

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles that contains the field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss the best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve product.

# Contents

---

<b>Chapter 1: Introducing Disaster Recovery Option</b> .....	<b>9</b>
Introduction .....	10
Disaster Recovery Option .....	11
Disaster Recovery Methods .....	12
Windows Server 2008 or later /Windows 7 or later .....	13
Disaster Recovery Option Support .....	14
Global Options for Disaster Recovery .....	15
Disaster Recovery on Database Applications .....	16
How Arcserve Backup Protects System Volumes Without a Drive Letter .....	17
<b>Chapter 2: Installing the Disaster Recovery Option</b> .....	<b>19</b>
Preinstallation Tasks .....	20
Prerequisite Software .....	21
Documentation .....	22
Alternate Location for Disaster Recovery Information Configuration .....	23
Set Up Alternate Machine Locations to Replicate Disaster Recovery Information .....	24
General Considerations .....	29
Install and Configure the Option .....	30
How to Perform Disaster Recovery Using the Incremental and Differential Sessions .....	31
Perform Disaster Recovery Using a Synthetic Full Backup Session .....	32
Disaster Recovery Utilities .....	33
Post-installation Tasks .....	35
<b>Chapter 3: Recovering from a Disaster using WinPE</b> .....	<b>37</b>
Overview of Windows PE Disaster Recovery .....	38
WinPE Disaster Recovery Limitations .....	40
WinPE Requirements on Windows 8, Windows Server 2012 and 2016 or later .....	41
Recover Windows Server 2008 or later and Windows 7 or later versions from a Disaster using WinPE .....	44
How to use Arcserve Backup Disaster Recovery Utilities .....	56
Create Customized WinPE Disaster Recovery Images .....	58
<b>Chapter 4: Disaster Recovery Scenarios</b> .....	<b>61</b>
Disaster Recovery Scenarios on Windows Server 2008 .....	62
Scenario 1: Primary Server Disaster Recovery .....	63
<b>Chapter 5: Troubleshooting</b> .....	<b>67</b>
General Usability .....	68

---

Full System Backup .....	69
Perform Incremental and Differential Backups .....	70
Local DR using Remote FSD .....	71
Additional Drivers .....	72
Disaster Recovery from a Different Server .....	73
Remote Computer Backup Over a Network .....	74
Ghost Application Duplicating System Configuration .....	75
Remote Disaster Recovery Cannot Use Local Backups .....	76
Specific Session Restoration .....	77
Boot-Kit Update .....	78
Alternate Location Reconfiguration .....	79
File Sharing Violations .....	80
Major Hardware or Software Upgrades .....	81
Indicating Backup can be used for DR .....	82
Unable to Detect Second Sequence Tape, when Restoring from a Tape Drive .....	83
Manual Changes to Disk Configuration During Disaster Recovery .....	84
Raw Partition Restoration .....	85
Use Locally Attached Disk .....	86
Back Up English Client Machine from Non-English Server .....	87
DNS Record .....	88
Windows ASR cannot restore the disk partition layout for multi-path SAN disk .....	89
ASDB Sessions Cannot be Restored .....	90
Operating Systems .....	91
Command Prompt Access During Disaster Recovery Mode .....	92
Hardware Changes .....	93
Cannot Connect to Server Message .....	94
Recover Virtual Hard Disk (VHD) Using Disaster Recovery Option .....	96
Media Verification .....	97
Verification of Storage Device Attachment .....	98
Windows Setup Message .....	99
Cannot See Partitions .....	100
Certificate Server Fails to Start .....	101
System Running Out of Free Space .....	102
Applications .....	103
Citrix .....	104
<b>Chapter 6: Recovering SAN Configurations .....</b>	<b>105</b>

---

---

Recover the SAN .....	106
How SAN Disaster Recovery Works .....	107
<b>Chapter 7: Recovering Clusters .....</b>	<b>109</b>
Cluster Failure Scenarios .....	110
Requirements .....	111
Special Considerations .....	115
Terminology .....	116
Cluster Disaster Recovery Requirements .....	117
Scenario 1: No Shared Disk Failure .....	118
Recover Secondary Node .....	119
Recover the Primary Node .....	120
Scenario 2: Shared Disk Failure .....	121
Recover Cluster Non-quorum Shared Disks with No Node Failures .....	122
Recover Cluster Quorum Disks with No Node Failures .....	123
Recover All Shared Disks with No Node Failures in the Cluster .....	125
Recover Primary Nodes with Shared Disk Failure in the Cluster .....	126
Recover Entire Clusters .....	127
Recover Clusters with Partial Shared Disk Configurations .....	128
<b>Chapter 8: Recovering NEC Clusters .....</b>	<b>129</b>
Disaster Recovery on NEC CLUSTERPRO/ExpressCluster SE .....	130
Arcserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster SE Cluster .....	131
Arcserve Backup Installed on the NEC CLUSTERPRO/ExpressCluster SE Cluster .....	136
Disaster Recovery on NEC CLUSTERPRO/ExpressCluster LE .....	144
Arcserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster LE Cluster .....	145
NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk is Damaged .....	146
Recover Data if NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk Data is Corrupted .....	147
Recover if One NEC CLUSTERPRO/ExpressCluster LE Cluster Node Fails .....	148
Recovery if All NEC CLUSTERPRO/ExpressCluster LE Nodes Fail .....	150
Active/Passive Configuration .....	151
Damaged Mirrored Disk in Active/Passive Configuration .....	152
Corrupted Mirrored Disk Data in Active/Passive Configuration .....	153
Recover One Failed Cluster Node in Active/Passive Configuration .....	156
All Cluster Nodes Fail in Active/Passive Configuration .....	157
<b>Chapter 9: Staging Using File System Devices .....</b>	<b>159</b>
Special Consideration for Staging .....	160
<b>Chapter 10: Recovering Windows 2008 Small Business Server .....</b>	<b>161</b>

---

---

Windows Small Business Server 2008 Default Settings .....	162
Arcserve Backup Requirements .....	163
Disaster Preparation for Windows Small Business Server 2008 .....	164
Windows Small Business Server 2008 Disaster Recovery .....	165
Other Applications .....	166
Microsoft SharePoint Service Restoration .....	167
How to Recover Microsoft SharePoint Service Data .....	168
Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint .....	169
Reinstall Microsoft SharePoint and MSDE .....	170
Restore Microsoft SharePoint Service .....	172
Microsoft Exchange Restoration .....	173
<b>Chapter 11: Recovering Data from a Physical to Virtual Machine</b>	<b>175</b>
Prerequisites .....	176
Operating Systems .....	177
Virtual Infrastructures .....	178
<b>Chapter 12: Glossary</b> .....	<b>179</b>
Advanced Mode .....	180
Alternate Machine Name .....	181
ASDB Recovery Configuration .....	182
Boot Volume .....	183
Client Agent Service .....	184
Cluster Configuration .....	185
Disaster Recovery .....	186
Hard Disk Status .....	187
iSCSI Configuration .....	188
Network Status .....	189
Password .....	190
Password Management .....	191
Path .....	192
Pre-flight Check .....	193
System Volume .....	194
Tape Engine Service .....	195
USB Backup Device Configuration .....	196
User Name .....	197
<b>Chapter 13: Index</b> .....	<b>199</b>

---



---

# Chapter 1: Introducing Disaster Recovery Option

This section contains the following topics:

---

<a href="#">Introduction</a> .....	10
<a href="#">Disaster Recovery Option</a> .....	11
<a href="#">Disaster Recovery Methods</a> .....	12

## Introduction

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic events or natural disasters. Disasters can be caused by fire, an earthquake, employee sabotage, a computer virus, or a power failure.

There are many time consuming tasks—including installation of the base operating systems and setup of the servers—that would usually have to be manually performed after a disaster. The Arcserve Backup Disaster Recovery option lets you restore your server reliably, making more efficient use of time by taking you from boot media, to backup media, to an operational state and allows users with minimal server configuration experience to recover sophisticated systems.

## Disaster Recovery Option

The Disaster Recovery Option is based on the concept of collecting and saving machine-specific information before a disaster strikes. When you submit a full backup job, the option automatically generates and saves emergency data for each protected machine locally on the backup server, on backup media, and, optionally, on a remote computer. In the event of a disaster, the option can recover its protected computers to their most recent backup state.

The option generates or updates information for disaster recovery when it performs a full, synthetic full, incremental or differential backup of a computer or a local backup server whenever the Arcserve Backup database is backed up (when the volume on which it resides is backed up).

## Disaster Recovery Methods

This section provides the disaster recovery methods for the following specific versions of Windows:

[Windows Server 2008/Windows 7](#)

[Disaster Recovery Option Support](#)

[Global Options for Disaster Recovery](#)

[Disaster Recovery on Database Applications](#)

[How Arcserve Backup Protects System Volumes Without a Drive Letter](#)

## Windows Server 2008 or later /Windows 7 or later

The Disaster Recovery Option supports local and remote disaster recovery for Windows Server 2008 and remote disaster recovery for Windows 7. For more details, refer to [Compatibility Matrix](#).

**Important!** The Windows Server 2008 or Windows 7 installation media that you use to perform disaster recovery must be the same version you used to install before the disaster happened.

## Disaster Recovery Option Support

For details, refer to [Compatibility Matrix](#).

## Global Options for Disaster Recovery

The Disaster Recovery option supports two global job options. You can access these options from the Advanced tab of the option's dialog when creating a backup job.

### **Generate DR information for partially selected nodes**

Lets you explicitly force disaster recovery information to be generated when backing up a subset of a machine. By default, disaster recovery information is generated for a machine after every full backup of that machine. A full backup requires that you select the entire machine node by selecting the green marker completely.

**Note:** This option only takes effect if the version of the Arcserve Backup Client Agent for Windows on your Windows machine is the same as the version of Arcserve Backup running on your server.

### **Include filtered sessions when generating restore session information**

Lets you explicitly force the option to include the filtered sessions. When generating disaster recovery information for a machine, the latest backup sessions of all drive volumes and system states are recorded for the machine. By default, the option skips all sessions set with a filtered flag, so these sessions are never used by the option to recover a machine.

**Note:** Arcserve Backup sets the filtered flag if any file in a session is not backed up because of a filtering policy on the backup job.

## Disaster Recovery on Database Applications

Arcserve Backup has special agents to back up database applications. Some of the commonly used database applications include:

- Oracle
- Microsoft SQL Server
- Microsoft Exchange Server
- Lotus Notes

If you have backed up one or more of these databases using Arcserve Backup database agents, the databases are *not* automatically restored as part of the disaster recovery process.

When Arcserve Backup backs up database sessions, additional media sessions are created, separate from the rest of the machine backup. Disaster recovery does not automatically restore these database sessions. However, after you restore the rest of the server using the Disaster Recovery Option, you can start Arcserve Backup and begin a normal database restore procedure using the corresponding application agent. See the corresponding agent guide for more information.



## How Arcserve Backup Protects System Volumes Without a Drive Letter

A system volume is the disk volume that contains the hardware-specific files required to start Windows, such as BOOTMGR. A boot volume is the disk volume that contains the Windows operating system files and its supporting files. A computer contains one system volume; however, there is one boot volume for each operating system in a multiboot system.

The files contained in the system volume can reside in the system drive (c:\), in a volume that does not contain a drive letter, or in a named volume. On Windows Server 2008 R2 systems, the system volume may not necessarily reside in the boot system drive (c:\). By default, the system volume is usually a volume without a drive letter.

The Arcserve Backup protect the system volumes as part of the computer's system state. You can back up the system state explicitly or dynamically.

**Note:** For information about explicit job packaging and dynamic job packaging, see the [Arcserve Backup Administration Guide](#).

Arcserve Backup lets you back up the entire boot volume as part of the system state. To recover one file, several files, or all files from the system state, and data files contained in the boot volume, you must perform a full recovery of the system state. You can then recover the system state, or system volume, as part of the disaster recovery process. To use this approach, you must create an Arcserve Backup Disaster recovery CD.



---

## Chapter 2: Installing the Disaster Recovery Option

This chapter describes how you can install the Disaster Recovery option. It also provides information on the pre-installation and post-installation tasks.

This section contains the following topics:

---

<a href="#">Preinstallation Tasks</a> .....	20
<a href="#">Post-installation Tasks</a> .....	35

## Preinstallation Tasks

This section describes the information that you must review before you install, and the software you must have while you configure the option.

This section contains the following topics:

[Prerequisite Software](#)

[Documentation](#)

[Alternate Location for Disaster Recovery Information Configuration](#)

[Set Up Alternate Machine Locations to Replicate Disaster Recovery Information](#)

[General Considerations](#)

[Install and Configure the Option](#)

[How to Perform Disaster Recovery Using the Incremental and Differential Sessions](#)

[Perform Disaster Recovery Using a Synthetic Full Backup Session](#)

[Disaster Recovery Utilities](#)

## Prerequisite Software

Verify that you have Arcserve Backup installed before installing the option. You can install Arcserve Backup and the option in the same session or at different times.

## Documentation

Before you install the option, we recommend that you review the following documents:

### **Readme**

Contains the operating system requirements, hardware and software prerequisites, last minute changes, and all known issues with the software. The readme file is provided in HTML format and is located at the root level on the product CD.

### **Implementation Guide**

Provides an overview of product features and functions, basic concepts, installation information, and an introduction to the product. It is provided as a printed document, and in Adobe Portable Document Format (PDF) on the product CD.

### **Release Summary**

Lists new features and changes to the existing features that are included in the release. The Release Summary is provided in PDF format.

## Alternate Location for Disaster Recovery Information Configuration

When you back up a local or remote Arcserve Backup client computer, the Arcserve Backup server saves the computer-specific information required to perform disaster recovery tasks.

If the Arcserve Backup server fails, the computer-specific disaster recovery information can be lost as well. To avoid this type of data loss, the option can store machine specific disaster recovery information to a remote location on an alternate computer. This feature allows you access disaster recovery information and create machine specific disks even if the Arcserve Backup server fails.

**Note:** If you are upgrading or migrating from an earlier version of Arcserve Backup and you previously configured an alternate location to store disaster recovery information, you can use the same location with the Disaster Recovery Option.

The alternate location used to maintain disaster recovery information has a dedicated folder for each machine protected by the option.

You can enable the alternate location while configuring the option after installation or at a later time. To enable this feature, you must first create a shared folder on the remote computer, and then configure the option to send information to that shared folder.

## Set Up Alternate Machine Locations to Replicate Disaster Recovery Information

You can set up alternate locations to replicate disaster recovery information.

Arcserve Backup uses the following process to replicate information:

- Creates a temporary operating system working environment.
- Sets the environment's configuration to be the same as the disk and the network.
- Restores data to the system so that the computer can return to its latest backup state.

These operations cannot be executed automatically if there is no record of the original system settings. Therefore, the relevant system information must be gathered during backup operations for disaster recovery purposes.

When you perform a full backup of a client computer, specific disaster recovery information is generated for that computer. This information is stored on the backup server and is used to create the disaster recovery media to recover the protected computer in the event of a disaster.

**Important!** We recommend that you set up an alternate location for disaster recovery to allow you to replicate the information to a remote computer as backup copies. If the backup server itself fails, you can recover it automatically using disaster recovery.

### To set up an alternate location for disaster recovery information

1. Create a shared folder on the remote computer to receive the replicated information.
2. Click Config on the Create Boot Kit wizard dialog.  
The Alternate Location for DR dialog opens.
3. Enter information to set the alternate location.
4. Run the Create Boot Kit wizard to continue the disaster recovery process.

#### More information:

[Create Shared Folders for Disaster Recovery Alternate Locations](#)



## Create Shared Folders for Disaster Recovery Alternate Locations

You can create shared folders to replicate disaster recovery information in alternate locations.

### To create the shared folder

1. Create a folder and give it an appropriate name.

You can create this folder anywhere on the system where shared folders are allowed.

**Note:** The volume must be located on a fixed disk.

2. Right-click the folder and select Properties from the pop-up menu.

The Properties dialog opens.

3. Click the Sharing tab.

4. Select the Share this folder option and enter the share name.

5. Set the User limit you require and click Permissions.

The Permission dialog opens.

**Note:** We recommend that you specify the Maximum Allowed option.

6. Click Add to add the user account you used when you set up your alternate location for disaster recovery information to the Share Permissions list.

You can add this account explicitly or you can specify a user group to which the account belongs (this information also applies if you add a domain account):

#### Add Account Explicitly

If the user account exists on the machine and is part of a local user group, you can add that specific user account to add it explicitly.

#### Add User Account Implicitly

If the user account exists on the machine and is part of a local user group, you can add the entire local user group to add the user account implicitly.

7. Click the boxes in the Allow column to specify Full Control on the share folder.

8. Click Apply, and then click OK.

9. In the Properties dialog, click the Security tab.

Edit the security list on this tab to ensure the user account used during the setup of the alternate location has Full Control on permissions. The user account can be

added explicitly or implicitly (as part of a user group) as described in the previous steps.

10. Click Apply and click OK.
11. Verify that the shared folder works properly. To do so, from a remote computer, try to connect or map to the shared folder with the user account you used when setting up the alternate location and, when connected, verify that you can create, modify, and remove files and directories on the shared folder.

## Set Up Alternate Locations with the Disaster Recovery Wizard

The Config option in the Disaster Recovery wizard lets you specify information about the alternate location where you store information about the disaster recovery. You can also set up an alternate location for disaster recovery information when you install the Disaster Recovery Option.

### To set up an alternate location using the Disaster Recovery Wizard

1. Click Config.

The Alternate Location for DR Information dialog opens.

**Alternate Location for DR Information**

At the end of a full backup, the local machine's disaster recovery information is saved on the Arcserve Backup server.

To save this disaster recovery information to another computer for added disaster protection of the Arcserve Backup server, please provide the following information and click OK. This wizard only changes the information on the local machine.

Use alternate path for added disaster protection.

Alternate Machine Name:

Windows Domain:

User Name:

Password:

Path (with the Share Name)

( Example: C:\DR\alternate or DR\alternate if it is a shared folder )

**Warning: You should create a bootable image as soon as possible so that you can recover your computer from a disaster.**

OK Exit

This dialog contains the following fields:

#### Alternate Machine Name

The hostname of the machine where the shared folder resides. The IP address of this machine can also be used but we do not recommend this, particularly in DHCP environments.

#### Windows Domain

If the user account used is part of a domain, enter the domain name. If a local account is used, enter the name of the local machine.

**Note:** Ignore this field if you specified domain information in the User Name field.

#### User Name

The user account used to connect to the machine on which the alternate location resides. The domain part of the user name is optional. For example, if the full user account name is domainX\userX, you can enter userX.

**Password**

The password for the specified user account.

**Path**

The path for the shared folder in which to store the replicated disaster recovery information.

2. When you have specified all of the required information, click OK.

## General Considerations

Consider the following points when setting up an alternate location for disaster recovery information:

- Although you can set up an alternate location for disaster recovery information on the local backup server and replicate this information locally, we recommend that you use a remote machine.
- Although this is not recommended, when specifying the shared folder name in the Disaster Recovery Wizard, you can use a shared drive and any folder or subfolder on that drive to specify that disaster recovery information is to be replicated to that folder. If you must do so, ensure that the folder itself and all parent folders, including the shared drive, have proper security and permission settings for the user account being used.
- Connection to the remote shared folder is established using Windows network services. This is fully supported by Microsoft but the service itself has a limitation. If a connection already exists to the remote machine hosting the shared folder, the wizard cannot verify and use the user account information you provide. The replicating operation relies on the existing connection and the credential supplied there.

**Note:** For information, refer [Microsoft Knowledge Base](#).

## Install and Configure the Option

You must install Arcserve Backup before you install the Disaster Recovery Option. You cannot install the option if Arcserve Backup has not been installed. You can, however, install the option with Arcserve Backup in the same session.

For more information about installing Arcserve Backup, see the [Implementation Guide](#).

### To install and configure the option

1. In the Select Product dialog, choose Disaster Recovery Option and click Next.

The option is installed in the same directory as the base product.

2. If you are installing Arcserve Backup and the option at the same time, then select your database, set your password, and enter system account information.

The Product List opens.

3. Verify the components to be installed, and then click Install.

The licensing information opens.

4. Click Continue.

A summary of the components that have been installed opens. This summary identifies the components you are installing that require configuration. The summary identifies the option as one of the components requiring configuration.

5. Click Next.

6. Configure an alternate location on a remote computer in which to store a backed up copy of your disaster recovery information.

We strongly recommend that you use the alternate location feature, to let you create machine specific disks even after a disaster on your backup server.

7. Select the Alternate Location for DR information by clicking the Config option.

8. Fill up information for alternate machine name, the Windows domain, user name, password, and the name of the shared folder on the remote server where the disaster recovery information will be stored.

**Note:**To use an alternate location on a remote computer to store disaster recovery information, you must have previously created a shared folder on the remote computer in which to store this information. If you have not previously created this shared folder, you can enable this feature at any time after configuring the option. To configure alternate location, start the Disaster Recovery Configuration Wizard and click Config.

The option is now installed.

## How to Perform Disaster Recovery Using the Incremental and Differential Sessions

You can perform disaster recovery using the incremental and differential sessions. This can be done after all backups are run or after every incremental or differential backup. This process works for all the Windows platforms.

### To perform disaster recovery using incremental and differential sessions

1. Run series of full and incremental and differential backups using the GFS rotation or custom rotation methods.

The full, incremental, and differential sessions can reside on different media or the same media.

2. Create a machine specific disk after all backups are run or after every incremental or differential backup.

The machine specific disk would have information about all backups (full, incremental or differential) that were performed before the MSD was created.

If you configure an alternate location, you can also create machine specific disks before you perform disaster recovery.

3. Run the disaster recovery process.

**Note:** The Disaster Recovery Option will not automatically scan any additional sessions that are backed up after you create machine specific disks.

The Disaster Recovery Option will automatically restore all the sessions, including full, incremental, and differential sessions shown in the list.

## Perform Disaster Recovery Using a Synthetic Full Backup Session

You can perform disaster recovery using a synthetic full backup session. This can be done after the synthetic full backup is run since a synthetic full backup synthesizes a previous full backup session and all incremental sessions to a full session, without the need to utilize previous incremental or differential backups.

**Note:** Synthetic full backup is only supported on r16 or higher Windows Client Agents.

### To perform disaster recovery using a synthetic full backup session

1. Run a synthetic full backup using the GFS rotation or custom rotation methods.
2. Create a machine-specific disk after the synthetic full backup is run.

The machine-specific disk will contain information about the backup that was performed before the MSD was created.

If you configure an alternate location, you can also create machine-specific disks before you perform disaster recovery.

3. Run the disaster recovery process.

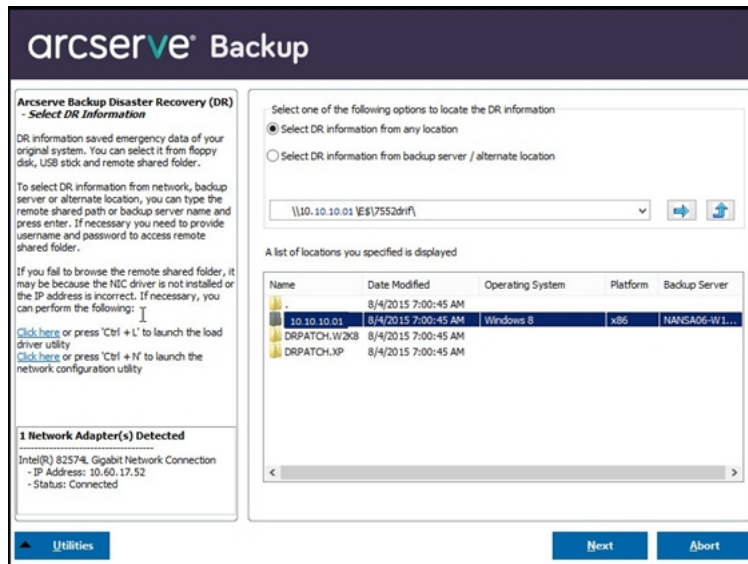
**Note:** The Disaster Recovery Option will not automatically scan any additional sessions that are backed up after you create machine specific disks.

The Disaster Recovery Option automatically restores the session shown in the list.



## Disaster Recovery Utilities

Disaster Recovery Utilities is composed of a set of options that help you perform disaster recovery. You can access these utilities from the disaster recovery Choose Mode dialog.



The Disaster Recovery Utilities displays the following options:

### Load Driver Utility

Lets you load the third-party drivers. The attached devices are categorized as follows:

- Storage devices.
- Network devices
- Other devices and
- Unknown devices

You can select any device listed in the unknown devices category and install drivers. Also, you can specify a folder to help the Disaster Recovery wizard to find a driver for the selected device.

**Note:** During disaster recovery only SCSI, FC, and NIC drivers are required.

### IP Configuration Utility

Lets you configure the Network IP address. You can select a network adapter and configure the IP address. This utility can be launched anytime during the disaster recovery process.

**Note:** While loading DR information, Disaster Recovery wizard will reset the IP address according to the one recorded in the DR information. So if you configure IP address before loading DR information, the IP address might change. System reboot can change the IP address.

### **Troubleshooting Utility**

Displays the default troubleshooting dialog that you can use to resolve errors.

### **Run Utility**

Provides access to the command-line interface to execute commands.

## Post-installation Tasks

The online help provides field descriptions, step-by-step procedures, and conceptual information related to the product dialogs. Online help provides a quick and convenient way to view information while you are using the product. In addition, you can obtain diagnostic help for error messages. To access the diagnostic help, double-click the message number in the Activity log.



---

## Chapter 3: Recovering from a Disaster using WinPE

This section contains the following topics:

---

<a href="#">Overview of Windows PE Disaster Recovery</a> .....	38
<a href="#">WinPE Disaster Recovery Limitations</a> .....	40
<a href="#">WinPE Requirements on Windows 8, Windows Server 2012 and 2016 or later</a> .....	41
<a href="#">Recover Windows Server 2008 or later and Windows 7 or later versions from a Disaster using WinPE</a> .....	44
<a href="#">How to use Arcserve Backup Disaster Recovery Utilities</a> .....	56
<a href="#">Create Customized WinPE Disaster Recovery Images</a> .....	58

## Overview of Windows PE Disaster Recovery

WinPE (Windows Preinstallation Environment) is a minimal operating system that lets you prepare computers for Windows installations, copy disk images from network shared folders, and initiate Windows setup. Arcserve Backup lets you recover computers running the following operating systems from a disaster using Windows PE recovery CDs:

- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016
- Windows Server 2019

To create Windows PE recovery disks, Windows Assessment and Deployment Kit 8/8.1/10 (Windows ADK 8/8.1/10) or Windows Automation Installation Kit (Windows AIK) must be installed on the Arcserve Backup primary server or stand-alone server.

### Be aware of the following considerations:

- It is required to install Windows Automated Installation Kit (AIK) when you use the WinPE image to restore virtual machines on VMware Workstation 7 or ESX Server 4.0/4.1 or later. You can download AIK using the [link](#).

The following operating systems that AIK supports are:

- Microsoft Windows Vista SP1
- Microsoft Windows Server 2008 family
- Microsoft Windows 7 family
- Microsoft Windows Server 2008 R2 family

**Note:** By default, if both ADK and AIK are installed, the Create Bootable Image utility uses AIK to create WinPE images.

- When you use WinPE to perform a disaster recovery, you may not be able to connect to the backup server or the disaster recovery information (DRIF) loc-

ation through the network. To correct this behavior, perform one of the following tasks:

- Copy the following directory from the primary or stand-alone backup server to a USB drive.

ASBU\_Home\DR\PrimaryServerName\AgentName

Then complete the disaster recovery process and select the DRIF from the USB drive.

- Copy the following directory from the primary or stand-alone backup server to a machine-specific disk (MSD).

ASBU\_Home\DR\PrimaryServerName\AgentName

Then complete the disaster recovery process and select the DRIF from the MSD.

**Note:** When the MSD does not contain sufficient free disk space (1.44 MB) to copy the DRIF, do not copy the directory named DRV to the MSD.

## WinPE Disaster Recovery Limitations

Consider the following limitations when performing a WinPE Disaster Recovery:

- The option does not support Disaster Recovery for devices from the Cloud.
- The option does not support recovering Itanium-based operating systems from a disaster.



## WinPE Requirements on Windows 8, Windows Server 2012 and 2016 or later

To perform disaster recovery operations effectively on computers running Windows 8 or Windows Server 2012 and 2016 or later, Windows Assessment and Deployment Kit (Windows ADK) must be installed on the Arcserve Backup primary server or stand-alone server. Windows ADK is a Microsoft tool that lets you deploy Windows operating systems to computers. For more information about Windows ADK, see [Windows Assessment and Deployment Kit \(ADK\) for Windows 8](#) on the Microsoft website.

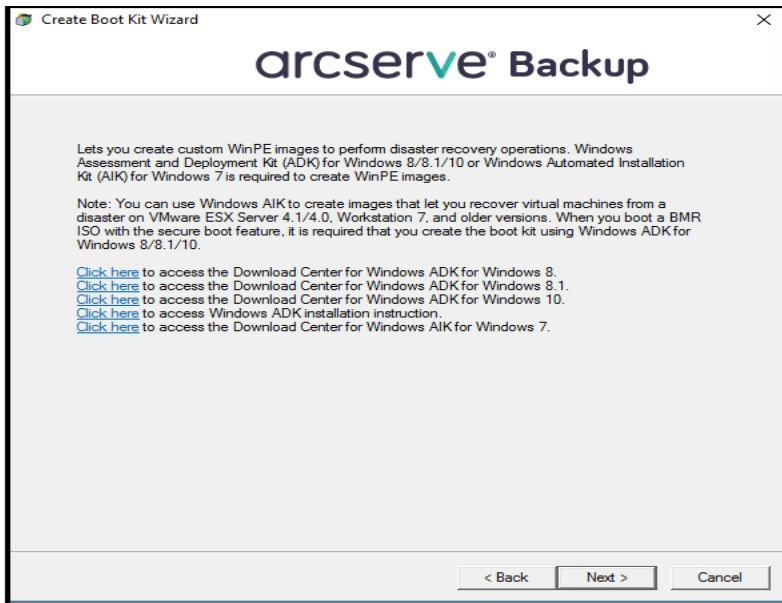
You can install Windows ADK on backup servers running the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows Server 2012 R2
- Windows 2016 or later
- Windows 10

You can install Windows ADK using either of the following methods:

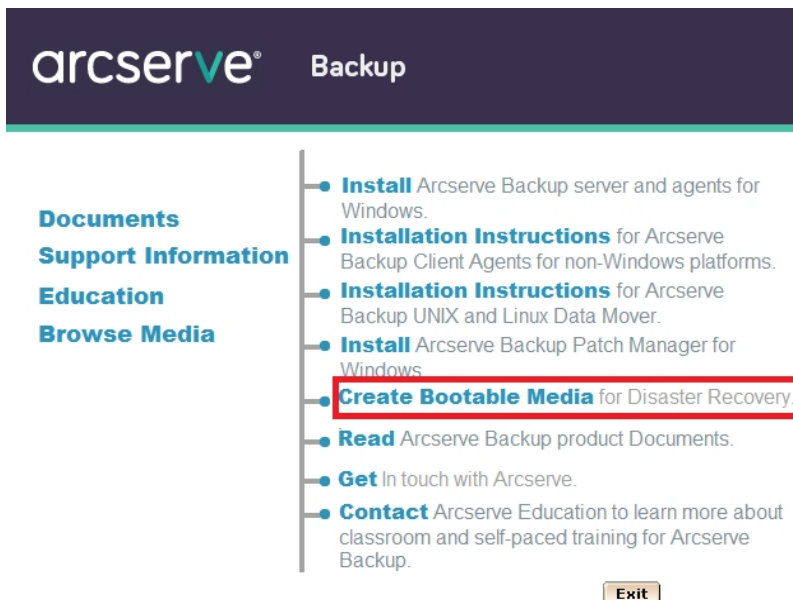
- Download the installation media from the Microsoft website and install it on the backup server.  
**Note:** For more information, see [Installing the Windows ADK](#) on the Microsoft website.
- Use the Arcserve Backup Create Boot Kit Wizard to create bootable media. When you use the wizard to create bootable media, click the option Customize

WinPE DR image on the Select Disaster Recovery Boot Kit Type dialog.



Then click the link on the dialog to open the Microsoft website so that you can download the kit and install it on the backup server. After you install the kit, click Next to continue creating the boot kit

**Note:** Optionally, you can start the wizard from the Arcserve Backup installation media.



**Note:** When you install Windows ADK on computers running Windows 8, verify that the following Windows ADK features are selected:

- Deployment Tools
- Windows Preinstallation Environment (WinPE)

## Recover Windows Server 2008 or later and Windows 7 or later versions from a Disaster using WinPE

This section describes the process of recovering the following operating systems from a disaster using WinPE (Windows Pre-installation Environment) recovery CD:

- Windows Server 2008
- Windows 7
- Windows Server 2012
- Windows 8
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016
- Windows Server 2019

**Note:** Arcserve Backup Disaster Recovery provides various utilities on each screen that help you resolve problems that you encounter during this process. For more details on these utilities, see [How to use Disaster Recovery Utilities](#).

Be aware of the following:


- The WinPE Disaster Recovery image is not integrated with the Arcserve Backup installation media. You create the WinPE Disaster Recovery image (or disk) manually. To create WinPE recovery disks, Windows Assessment and Deployment Kit (Windows ADK) must be installed on the Arcserve Backup primary server or stand-alone server.

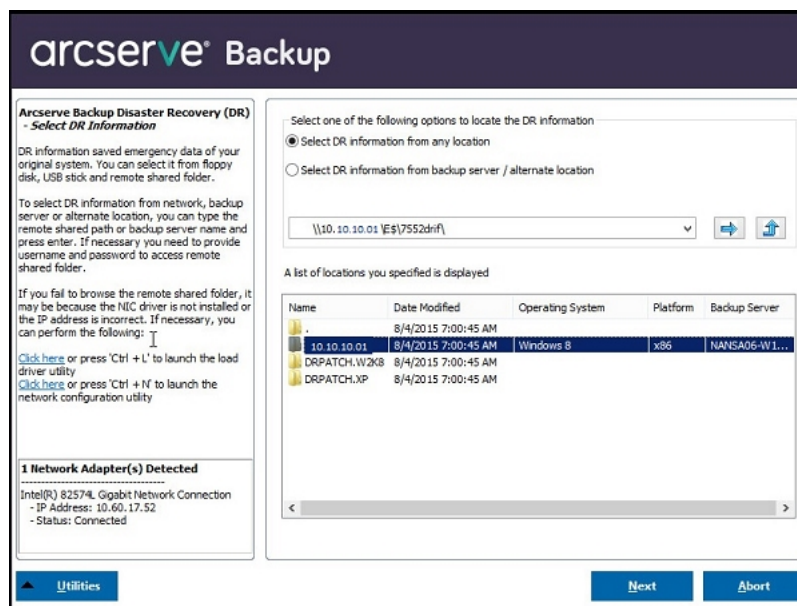
**Note:** For more information, see [Installing the Windows ADK](#) on the Microsoft website.


- Use the WinPE recovery image (or disk) to recover computers from a disaster. You can obtain disaster recovery information from the backup server, network, and local locations, such as local disks, MSD or USB sticks.
- When you perform disaster recovery of a guest operating system that resides on a Hyper-V server, create the WinPE disaster recovery image using Windows Automated Installation Kit (WAIK) for Windows 7.

**Note:** After a full backup, you can save the disaster recovery information to the location where it can be used during the disaster recovery process.

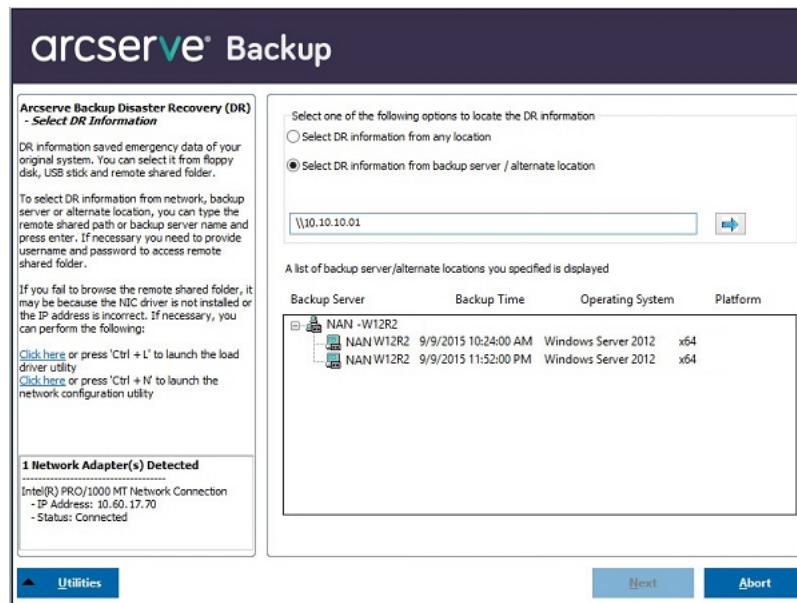
**Follow these steps:**

1. Insert the WinPE recovery disk into the computer that you want to recover to open the Windows Boot Manager screen.
2. Select the preferred language and keyboard layout and click Next to open the Select DR Information screen.
3. Select one of the following options to locate the disaster recovery information:
  - **Select DR Information from any location**--With this option, browse and select Disaster Recovery Information from the alternate location configured in the boot-kit wizard in the appropriate field if it is shared on a network and then click .



- **Select DR Information from backup server / alternate location**--With this option, enter the name of the backup server and then click . A

list of Disaster Recovery Information you specified is displays.



Be aware of the following:

You must provide a Windows user name and password to browse network shared folders.

To browse network shared folders, do the following:

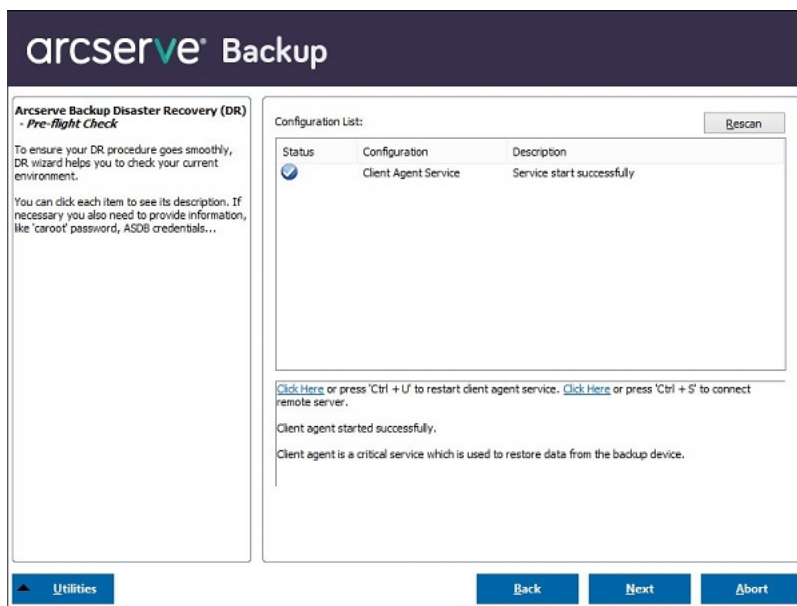
- Verify that the device drivers for the network adapters are installed on the computer that you want to recover from a disaster.
- Verify that the IP addresses for the network adapters are configured properly.

**Note:** To verify that the device driver and IP address are configured properly, click on the appropriate link from the left pane on any Arcserve Backup Disaster Recovery screen.

4. Click **Next** to open the Pre-flight Check screen.

This screen provides a configuration list for you to detect and resolve potential environment issues. Essentially, for each item selected from the Configuration list, a description of that item is displayed at the bottom of the screen describing the issue.

**Note:** For an updated status of the Configuration List, click **Rescan Status**.



Based on the disaster recovery information selected, the following items display on the screen:

- **Network Status**

This item displays the status of the network connection.

- If there is no network connection for Disaster Recovery, this item will be displayed on the Pre-Flight Checking page with one of the following statuses:
  - Error for remote disaster recovery
  - Warning for local disaster recovery
- If the network connection for Disaster Recovery is remote, the status indicates an error.
- If the network connection for Disaster Recovery is local, the status indicates a warning.
- If the network connection for Disaster Recovery is OK, this item will not be displayed.

- **Hard Disk Status**

This item displays the status of a hard disk.

- If a hard disk is not available, the status indicates an error.
- If a hard disk is available, this item will not be displayed.

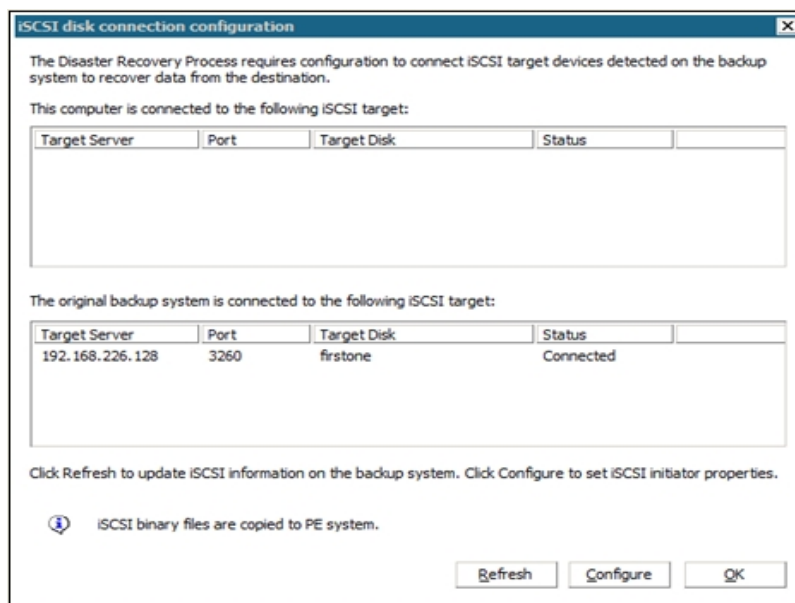
- **Password Management**

If Password Management is used during backup time, a Click Here link appears for you to open the Enter caroot password screen.

▪ **iSCSI Configuration**

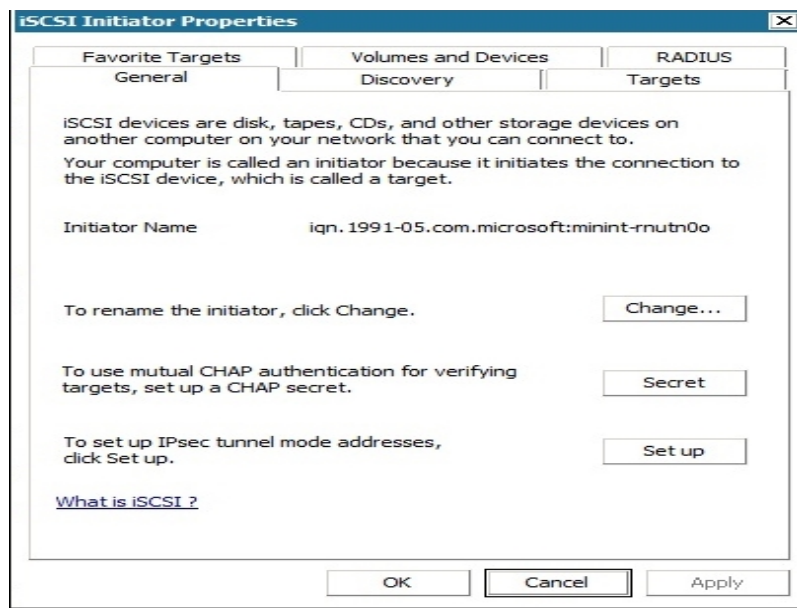
If iSCSI disks are configured during backup time, a Click Here link appears for you to open the iSCSI disk connection configuration screen to help you configure iSCSI connections.

In this screen, the Original backup system iSCSI information section displays the iSCSI connections during backup time and the Current system connected iSCSI target section displays iSCSI connections during disaster recovery time.



Click **Configure** to open the iSCSI Initiator Properties screen.



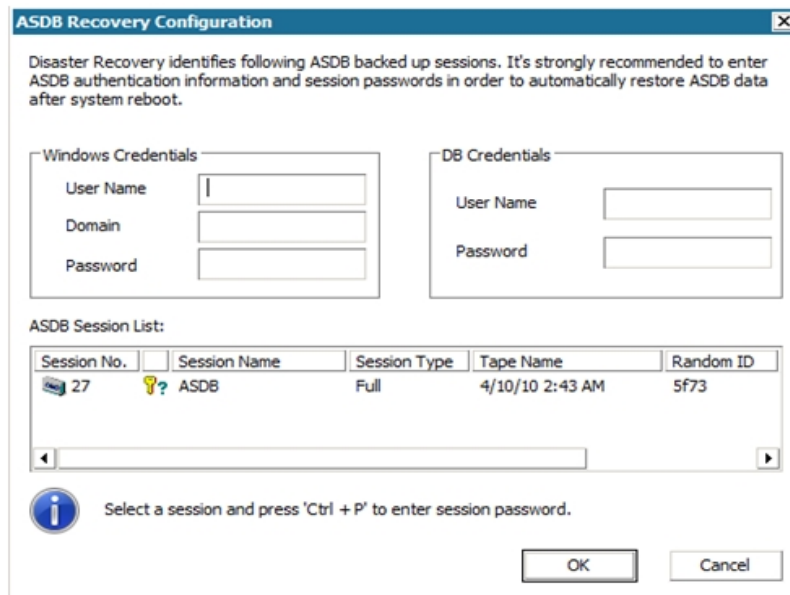


**Note:** The iSCSI configuration and related binaries are saved as part of the disaster recovery information in which disaster recovery restores them by default. If disaster recovery fails to detect iSCSI binaries, then you will have to select a path that contains iSCSI binaries and copy them to the WinPE environment.




- **ASDB Recovery Configuration**

If you are recovering a primary or standalone server with Arcserve Backup Database locally installed, then the below ASDB Recovery Configuration screen opens and lets you recover your sessions automatically. You will need to enter your Arcserve Backup Database

credentials.



The following icons appear next to each Arcserve Backup Database session. They are as follows:

-  Indicates that the session was encrypted. You must provide a password to restore the session.
-  Indicates that Disaster Recovery cannot verify whether the session was encrypted or not. You may or may not need to provide a password to restore the session.
-  Indicates that the session was encrypted and was provided with a password. You do not need to provide a password to restore the session.

▪ **Cluster Configuration**

Cluster Configuration display if the backup server is a cluster node. If it is a cluster node, WinPE searches for an available cluster virtual node. If the cluster virtual node is available, WinPE DR omits the restore process of the cluster shared disk; otherwise Disaster Recovery will restore the cluster shared disk.

▪ **USB Backup Device Configuration**

The USB Backup Device Configuration is used during backup time where you configure backup devices (for example, tape drives, lomega changers, and digital storage drives. For some USB backup devices, you may need to install additional drivers.

- **Client Agent Service**

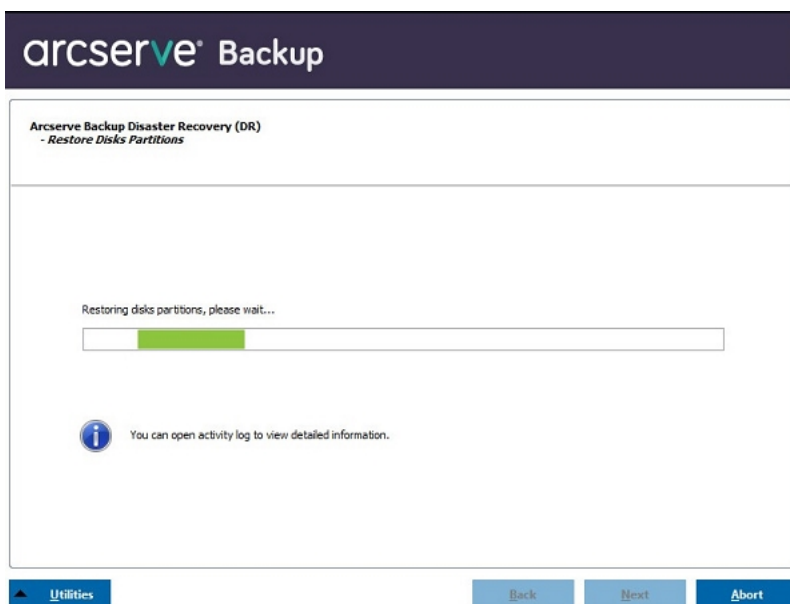
The Client Agent Service is a critical service used to communicate with backup servers for data recovery. Disaster Recovery will always start this service if the disaster recovery is local. If disaster recovery is remote, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Client Agent Service.

- **Tape Engine Service**

The Tape Engine Service is used only for local Disaster Recovery (DR).

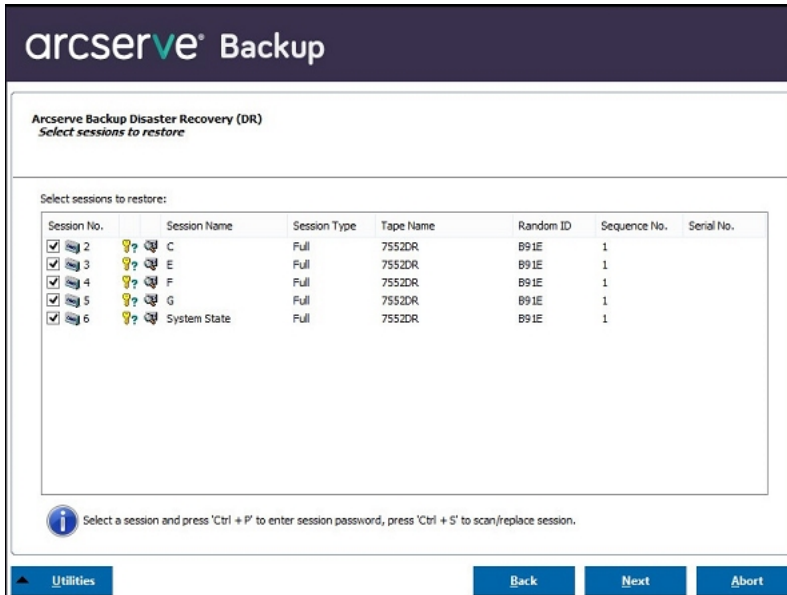
**Note:** If a file system device (FSD) or data deduplication device (DDD) was used during backup time, Disaster Recovery checks for available remote FSDs or DDDs during the start of the Tape Engine Service. If there are remote FSDs or DDDs, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Tape Engine Service. If FSDs or DDDs are not available, you can configure an FSD or DDD in the Device Authentication screen.

5. Click **Next** to restore the disk partitions and open the Restore Disk Partition screen.






Arcserve Backup Disaster Recovery automatically restores your disk partitions according to the saved disk layout information.


6. When the disk partitions are restored, click Next to restore Arcserve Backup Disaster Recovery sessions and open the Select sessions to restore screen.



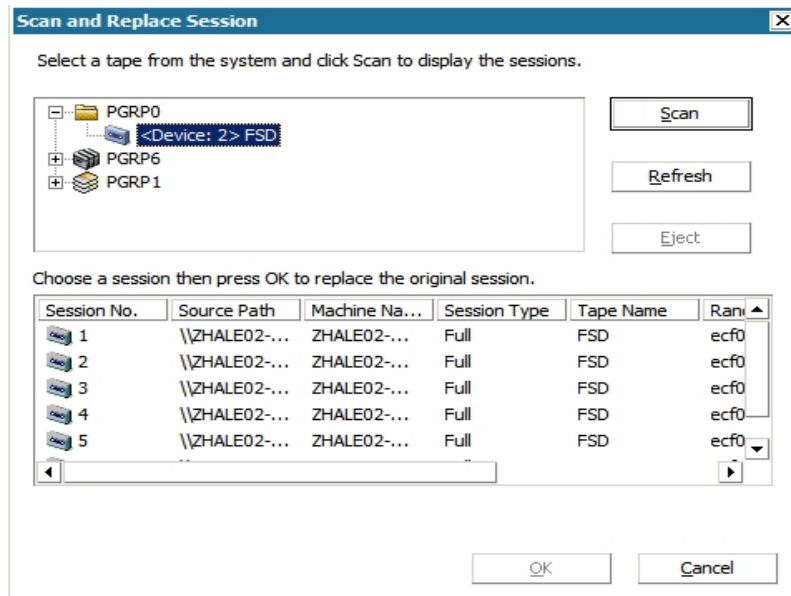
Arcserve Backup Disaster Recovery lets you specify sessions allocated to each drive, in hard disk, and also helps assign a session password. You can also recover incremental/differential backup sessions simultaneously.

Based on the session encryption status, you will find four types of icons in the Select sessions to restore screen:

-  Indicates that the session was encrypted. You must provide a password to restore the session.
-  Indicates that Disaster Recovery cannot verify whether the session was encrypted or not. You may or may not need to provide a password to restore the session.
-  Indicates that the session was encrypted and was provided with a password. You do not need to provide a password to restore the session.

-  Lets you scan or replace an existing session. Click this icon or press Ctrl+S to open the Scan and Replace Session screen.

**Note:** This dialog opens for full sessions only.

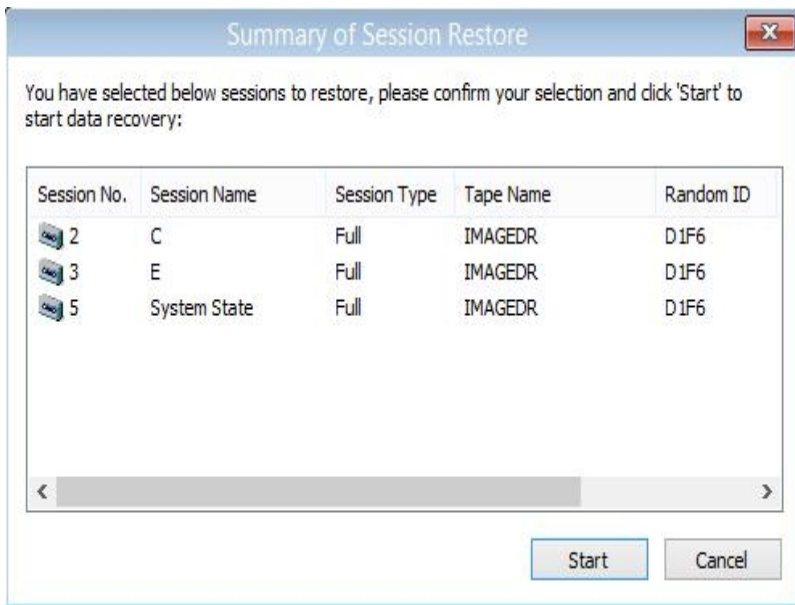


**Note:** The Eject button is used only for removable disk drives, like an RDX drive but some removable disk drives cannot be ejected in Disaster Recovery mode where you will have to switch media.

**Important!** You must restore volume C and System State sessions under the Session Name column, otherwise disaster recovery fails.

7. Click **Next** to open the Summary of Session Restore screens.

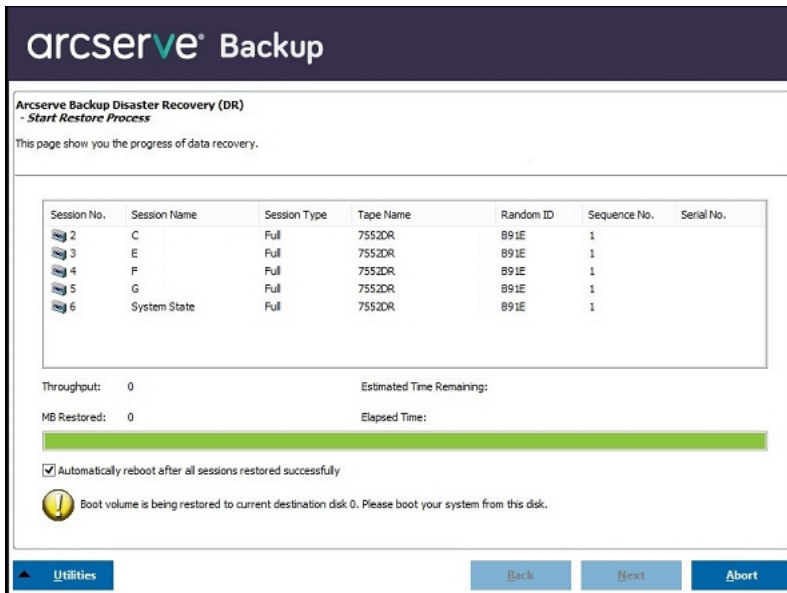
**Note:** This screen confirms the sessions you selected.



- Click **Start** to start the data restore process and open the Start Restore Process screen.

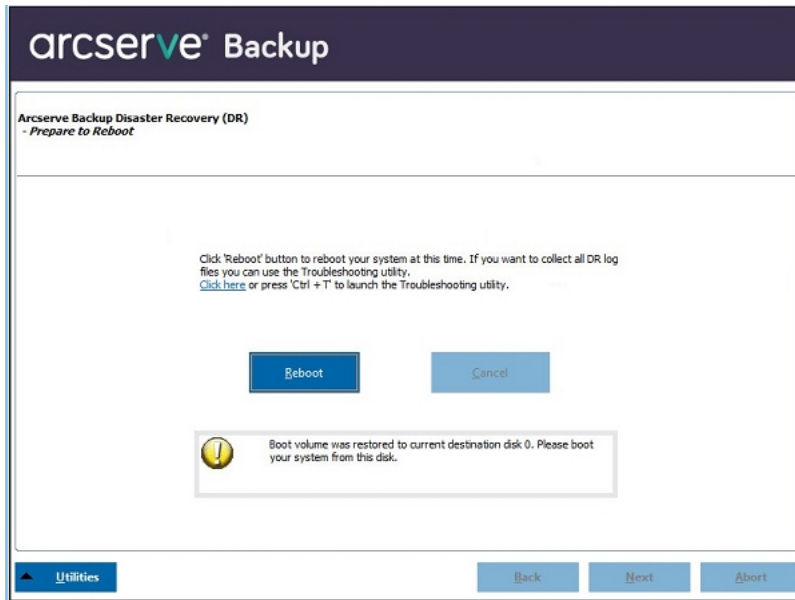
This screen displays a progress bar on the estimated time remaining of the data recovery.

**Note:** During data recovery, if your session password was not set, you will need to provide the password. Arcserve Backup allows three attempts to enter your password. After three attempts, the session will fail to restore.



- Click **Next** to reboot the computer and open the Prepare to Reboot screen.

**Note:** This screen automatically reboots in 30 seconds or gives you 30 seconds to cancel if the option on the Start Restore Process screen: Automatically reboot after all sessions restored successfully, is selected. If the option is not selected, Arcserve Backup Disaster Recovery lets you reboot or cancel manually.



After the computer restarts, Arcserve Backup Database Recovery Wizard opens to help you restore Arcserve Backup Database sessions.

Be aware of the following:

- Arcserve Backup Database recovery wizard only appears when you are restoring a Primary or Standalone backup server with Arcserve Backup Database installed locally. The recovery wizard automatically restores your sessions based on the information you entered on the Pre-flight Check screen.
- If you did not enter any Arcserve Backup Database credentials or what you entered is incorrect in the ASDB Recovery Configuration screen, you need to follow the prompts and complete the required fields on the Arcserve Backup Database Recovery Wizard screens to complete the recovery.

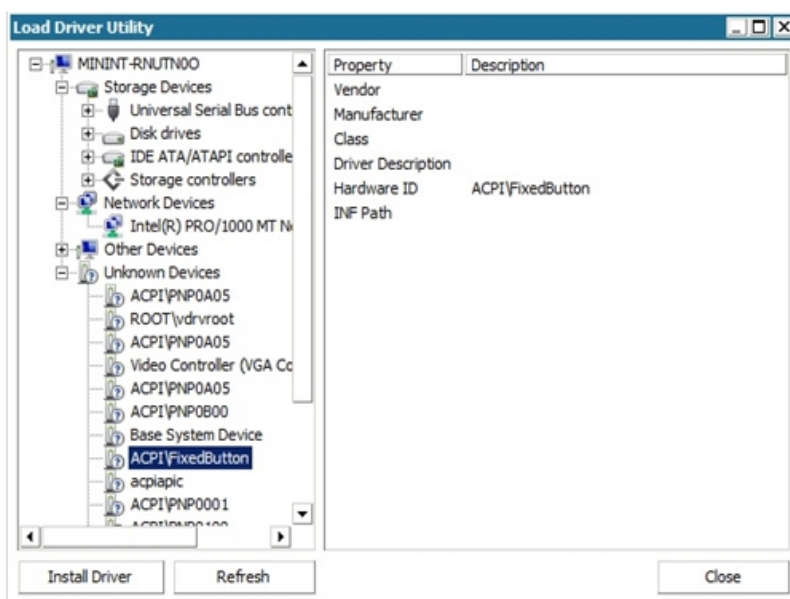
## How to use Arcserve Backup Disaster Recovery Utilities

Arcserve Backup contains various Disaster Recovery utilities that you can use to resolve issues you encounter during the Disaster Recovery process. You can find the Utilities button on the bottom of each Arcserve Backup Disaster Recovery screen.

The Disaster Recovery utilities are as follows:

- Load Driver Utility--Lets you load NIC/SCSI/FC drivers. For example, if the network driver is unavailable or your hard disks and cannot be detected, you can use this utility to load the drivers for you.

In the Load Driver Utility screen, a list of Unknown Devices displays. You can select a device and click Install Driver. This will let you search for the best driver to load or specify a driver for the particular device.

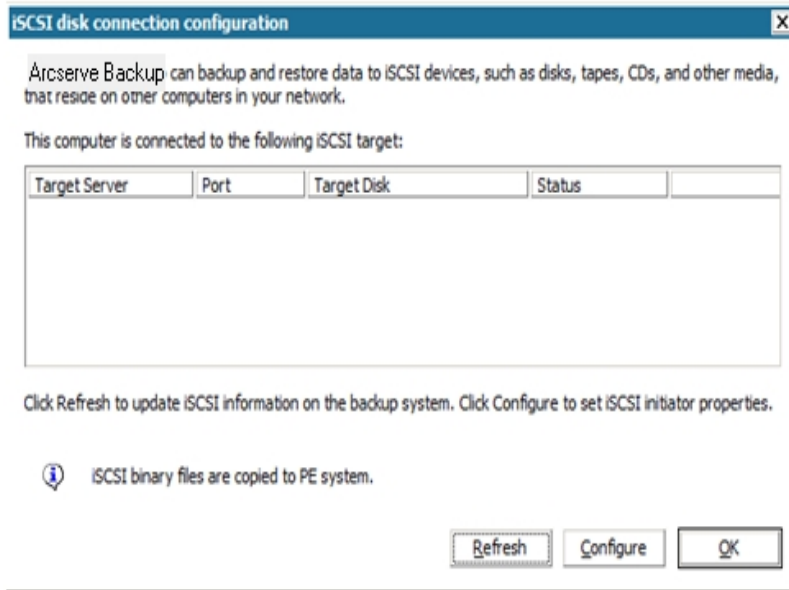


- Network Configuration Utility--Lets you configure IP addresses.
- iSCSI Configuration Utility--Lets you check and configure iSCSI connections for disaster recovery on your current environment.

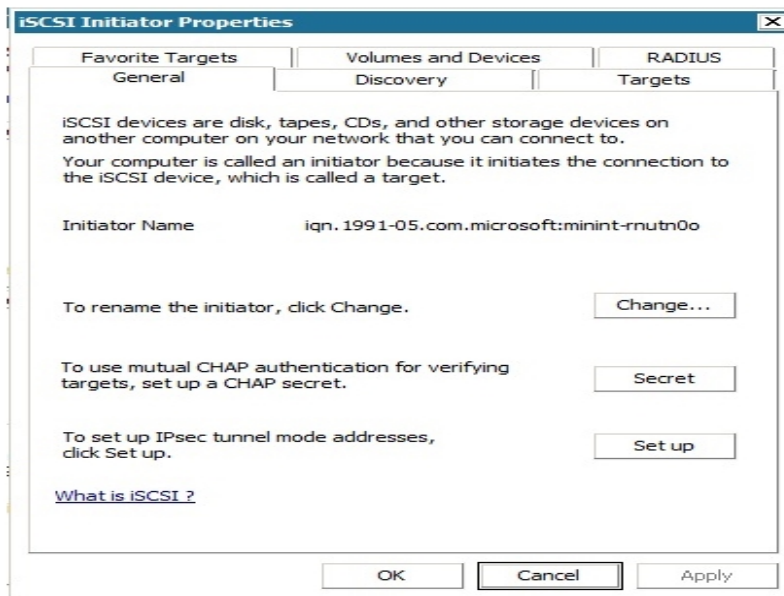
From the iSCSI disk connection configuration screen, you can configure the current system to connect to your iSCSI target remotely. In this screen, the Current system connected iSCSI target section displays iSCSI connections during disaster



recovery time.



Click Configure to open the iSCSI Initiator Properties screen.



- Activity Log--Lets you view all Disaster Recovery activities.
- Troubleshooting Utility--Lets Arcserve Support investigate issues that you encounter during the Disaster Recovery processes (for example, How to set log levels, How to collect log files).
- Run Utility--Lets you run other applications on the Disaster Recovery environment. A dialog box opens for you to enter the name of a program you would like to launch.

## Create Customized WinPE Disaster Recovery Images

Arcserve Backup lets you create customized WinPE Disaster Recovery (DR) images using the Boot Kit Wizard utility. The utility integrates NIC, FC, SCSI, RAID drivers, iSCSI programs, and Disaster Recovery patches into the created ISO image.

### Be aware of the following:

- To complete this task, Windows ADK must be installed on the backup server.
- When you perform disaster recovery of a guest operating system that resides on a Hyper-V server, create the WinPE disaster recovery image using Windows Automated Installation Kit (WAIK) for Windows 7.

### Follow these steps:

1. From the Quick Start menu on the Home Page, select Utilities and click Create Boot Kit to open the Create Boot Kit Wizard.

**Note:** You can also select Create Boot Kit from the Arcserve Backup installation media, the Utilities menu on the home page or the Navigation Bar, and from the Start menu.

2. Confirm the appropriate server and domain details. Enter the domain user name, password, and click Next to open the Select disaster recovery boot kit type screen.
3. Select Customize PEDR image and click Next to open the Select disaster recovery image platform and location screen.
4. Select the platform and location where you want to store the WinPE DR image.

There are two platforms available:

- WinPE DR Image for x86 Platform
- WinPE DR Image for x64 Platform

**Important!** You must select the platform that corresponds to the platform that is running on the source machine that you are recovering. For example, if you are recovering a computer that is running an x64-based operating system, you must select a WinPE DR Image for an x64 platform.

5. Click Next to open the Select Arcserve Backup installation source path screen.
6. Specify the path for the Arcserve Backup installation source.

To create a customized WinPE Disaster Recovery image, you must copy the Disaster Recovery programs from the Arcserve Backup Installation DVD.

- a. Insert the Arcserve Backup Installation DVD into the CD/DVD ROM to copy Disaster Recovery programs.

- b. Select the drive where the installation DVD is mounted from the drop-down list and click Next to open the Select disaster recovery options screen.
- c. Select one of the following drivers and updates to recover your Windows system:

- ◆ **Integrate NIC/SCSI/FC/RAID drivers:** With this option, you do not have to install the drivers again manually during the Disaster Recovery process.

Click Next to open the Specify the drivers to be integrated into the PE image screen.

**Note:** By default, a list of available drivers from the existing Disaster Recovery information displays. To add other drivers from another location, click Add Driver

- ◆ **Integrate Microsoft iSCSI initiator:** With this option, you do not have to install the iSCSI configuration tool manually during the Disaster Recovery process.

**Note:** As a best practice, you should specify this option if you backed up data using iSCSI disks.

Click Next to open the Specify Microsoft iSCSI Initiator binary files screen.

**Note:** The Boot Kit Wizard utility detects iSCSI programs on your current system. When they are detected, the Specify Microsoft iSCSI Initiator binary files screen will not open and you will be directed to confirm your settings. However, when the wizard does not detect the iSCSI programs, you must specify the location where the iSCSI programs are installed.

Click Next.

A message appears to confirm your settings.

7. Click OK to create the customized WinPE DR image.
8. Click Finish to exit the Boot Kit Wizard.



---

## Chapter 4: Disaster Recovery Scenarios

This section contains the following topics:

---

<a href="#">Disaster Recovery Scenarios on Windows Server 2008</a> .....	62
--	----

## Disaster Recovery Scenarios on Windows Server 2008

The scenarios specified in this section provides information and procedures to recover a typical system.

---

## Scenario 1: Primary Server Disaster Recovery

The scenario specified in this section lets you recover a primary server in the SAN environment.

This section contains the following topics:

[Prepare for Disaster During Primary Server Setup](#)

[Disaster Recovery Prerequisites](#)

[Recover Primary Server](#)

## Prepare for Disaster During Primary Server Setup

Planning for a successful disaster recovery begins when you set up your primary server. Perform the following procedure when you install Arcserve Backup and the Disaster Recovery Option on your primary server.

### To prepare for disaster during primary server setup

1. Add the Windows Server 2008 installation media to the disaster recovery kit for this primary server.
2. Save the additional hardware drivers you installed when you set up your primary server. Add these drivers to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery.

**Note:** If you do not know the devices installed on the Windows primary server, look in the Device Manager. If your system is no longer up and running, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

3. Start Arcserve Backup and perform a full backup.



## Disaster Recovery Prerequisites

To begin disaster recovery, you must have all of the following items:

- Arcserve Backup machine specific recovery disk
- A full backup of the primary server
- Windows Server 2008 installation media
- Arcserve Backup Disaster Recovery CD
- Driver disk

## Recover Primary Server

You can recover a primary server from a disaster using the following procedure:

### To recover your system after a disaster

1. Insert the machine specific recovery disk into the machine.
2. Boot the primary server using the Windows Server 2008 installation media.
3. Insert the Arcserve Backup Disaster Recovery media, when prompted and click Next.

**Note:** You must specify the machine specific disk data for restore as multiple machine specific disk data is stored in the disk storage media.

4. On the driver page, load the drivers.
5. Click Next to view the Network configuration screen.

In Advanced mode, give the network configuration details for the remote Disaster Recovery. Network configuration is also required for the local Disaster Recovery for SAN member server and local Disaster Recovery using remote file system devices.

6. Configure the remote file system devices page. Enter the authentication details, if necessary.

The session list opens.

7. You can make changes to this list and click Next.

The Summary page appears listing the sessions that you want to restore. Click Next and follow the instructions.

8. The restore process begins.

Reboot the machine after the restore process is complete.

---

## Chapter 5: Troubleshooting

This appendix provides troubleshooting information that you may need while using the Disaster Recovery Option. To help you find the answers to your questions quickly, the information in this appendix is divided into the following categories and, where appropriate, each category is further divided into questions and answers for specific operating systems.

This section contains the following topics:

---

<a href="#">General Usability</a> .....	68
<a href="#">Operating Systems</a> .....	91
<a href="#">Applications</a> .....	103

## General Usability

This section provides answers to frequently asked questions about using the option to perform disaster recovery.

**Note:** The information in this section applies to all supported Windows platforms.

This section contains the following topics:

---

## Full System Backup

**Valid on Windows Server 2008 and later**

### Symptom

When you recover an Arcserve server that is running Windows Server 2008 or later from a disaster using the bootable CD method, the operating system records many error messages to the Windows Event Log that relate to the Arcserve database. The details of the error messages that are most likely to appear are as follows:

- Error codes: 8355, 17204, and 17207
- Instance: MSSQL\$ARCSERVE\_DB

### Solution

The process of recovering the Arcserve database causes these events occur. You can ignore the error messages.

## Perform Incremental and Differential Backups

### Symptom

After performing full backup of the server, I schedule incremental and differential backups of the full server. Is this backup information recorded in the boot kit / winPE.iso? Can I recover these incremental and differential backup sessions during disaster recovery?

### Solution

Windows 2008 and later

Yes. The incremental and differential backup sessions of full node backups are recorded in the boot kit / winPE.iso along with the full backups. During disaster recovery, you can select the sessions you want to restore.

## Local DR using Remote FSD

**Valid on Windows 7 and Windows Server 2008 and later**

### **Symptom**

I have backed up the Arcserve Backup server to a remote file system device. During disaster recovery, can I access the remote file system device and restore the backup data from it?

### **Solution**

Yes. The file system device configuration is recorded in machine specific disk and you can restore the backup data while performing disaster recovery. Disaster Recovery Option retrieves this and handles the connection automatically.

If there is any change in the authentication information of the server on which the file system device is located, disaster recovery prompt you to enter the new account and password for authentication.

## Additional Drivers

### Symptom

Should I add extra drivers during the disaster recovery procedure? Why does not the disaster recovery process detect my SCSI, Fiber, and RAID adapters?

### Solution

Mid to high-range servers typically require drivers for RAID and SCSI adapters. The option uses these drivers to access the disks and storage devices in the system. Without these drivers, the option may not function properly.

If you are using a system that requires proprietary drivers for the SCSI, fiber, and RAID cards, it is possible that the drivers are not on the operating system CD. In this case, it is possible that the disaster recovery process cannot detect or load the drivers.

If you have a copy of the proper SCSI, FIBRE, or RAID drivers on a disk, you can reboot using the disaster recovery disks, and add the drivers when prompted. You can add these drivers during the blue screen mode of disaster recovery by pressing F6. You should update the drivers for adapters provided on the Windows installation CD, in the event the Windows CD versions were updated by the manufacturer. This is particularly important for fiber adapters.



## Disaster Recovery from a Different Server

### Symptom

Can I perform disaster recovery from an Arcserve Backup server other than the server from which the backup was performed?

### Solution

Yes, as long as the media can be used by the new server and new server information is present on the on the Boot kit.

### Windows 7 and Windows Server 2008 and later:

You can perform disaster recovery from a different server using the Advanced Disaster Recovery wizard by entering the server details and the IP address, when prompted.

## Remote Computer Backup Over a Network

### Symptom

Can I use the option to back up remote computers over the Network?

### Solution

The Disaster Recovery Option is only supported over the network when the Client Agent for Windows is installed on the remote Windows computer.

## Ghost Application Duplicating System Configuration

### Symptom

Can I use disaster recovery as a “ghost” application to duplicate my system configuration?

### Solution

No. The option is a system restoration application, not a system configuration replication program. Do not use the option to replicate systems.

## Remote Disaster Recovery Cannot Use Local Backups

### Symptom

Can I use a local backup to perform a remote disaster recovery?

### Solution

You cannot use local backups for remote disaster recovery, nor can you use remote backups for local disaster recovery.

## Specific Session Restoration

### Symptom

Can I restore specific sessions during the disaster recovery process?

### Solution

Yes. You can do this by un-assigning sessions from volumes you do not want to restore. Using the disaster recovery process, you can choose specific sessions that you want to restore.

**Note:** The system may not boot after disaster recovery if you do not restore the operating system volumes or other volumes critical for booting the system.

## Boot-Kit Update

### Symptom

How can I update the Boot-Kit if my Arcserve Backup server fails?

### Solution

You can update a Boot-Kit if you configured an alternate location during installation or after installing the option and before performing a full backup.

To update a Boot-Kit on a backup server, access the alternate location and copy the contents of the folder representing the server that you want to recover to a blank disk. This is your Boot-Kit for the failed server.

## Alternate Location Reconfiguration

### Symptom

How do I reconfigure or set up an alternate location after the option has been set up?

### Solution

In the Create Boot Kit wizard, click the Config button at the bottom of the screen.

## File Sharing Violations

### Symptom

If I receive file-sharing violations during a backup operation, can I still use sessions from that tape for disaster recovery?

### Solution

Yes, you can use these sessions for disaster recovery if you did not deselect anything from the drive for the backup.

**Note:** The backup operation does not back up open files. Therefore, these files cannot be restored during the disaster recovery process.



## Major Hardware or Software Upgrades

### Symptom

Which system configurations should I avoid for disaster recovery?

### Solution

Symptom What should I do if I install a different operating system or NIC card, or change between hardware and software RAID? Solution When you perform a major system upgrade (hardware or software), you should delete the Disaster recovery information for that system on both the Arcserve Backup home DR directory and alternate location. After completing these tasks, perform a full system backup.

## Indicating Backup can be used for DR

### Symptom

How can I know if I can recover the full node backup data using the licensed Disaster Recovery Option installed on my machine?

### Solution

You can recover the full node backup data using Disaster Recovery Option if the following information is logged in the Activity log after the full node backup is finished:

```
Information HOSTNAME MM/DD/YYYY HH:MM:SS JobID  
Successfully Generated Disaster Recovery Information for TEST05-W2K3-VM
```

## Unable to Detect Second Sequence Tape, when Restoring from a Tape Drive

### Symptom

I perform disaster recovery using a stand alone tape drive. After tape span, when I insert the next sequence tape into the drive and click OK on the mount tape pop-up dialog, Disaster Recovery Option still asks for the next sequence tape?

### Solution

This error occurs because the driver of that tape drive that is installed in the operating system accepts the media change notice from hardware directly because of which Arcserve Backup fails to detect the media change event.

### To detect the second sequence tape

1. Eject the sequence 2 tape.
2. Click OK on the Mount Tape popup dialog.
3. Insert the sequence 2 tape.
4. Click OK on the Mount Tape popup dialog again.

## Manual Changes to Disk Configuration During Disaster Recovery

### Symptom

Can I change partition information during disaster recovery?

### Solution

No. If the disk configuration is changed manually during the disaster recovery, you may not be able to restore the system.

## Raw Partition Restoration

### Symptom

Can I back up and restore raw partitions using disaster recovery?

### Solution

No. The option does not support restoration of raw partitions.

## Use Locally Attached Disk

### Symptom

Can I use a locally attached disk to perform a file system backup and a disaster recovery of the backup server?

### Solution

Performing a disaster recovery of a backup server using a locally attached file system device is supported only if all of the following criteria are met:

- The backup server is running Windows 2008 server
- The disks containing the file system device do not contain the boot partition
- The disks containing the file system device do not contain the system (Windows) partition
- The disks containing the file system device are not corrupted or damaged
- The disks containing the file system device provide, unchanged, the following properties:
  - ◆ Partition layout
  - ◆ Volume information (for example, drive letter, file system, or label)
  - ◆ Disk signature

**Note:** We strongly recommend that you also maintain a tape backup that can be used if the backup on the file system device is damaged during a disaster. If you use a local disk as a backup device, run a test of the disaster recovery process before deploying it in a production environment.

## Back Up English Client Machine from Non-English Server

### Symptom

My Backup Server is installed on a non-English Windows platform and I use it to backup a client machine running on English Windows platform. When I try to perform disaster recovery on the English client machine, I am getting some error messages saying the backup tape media cannot be found and the DR wizard keeps asking me to mount the tape. I am very sure the tape is mounted. What can be wrong?

### Solution

The problem is caused by difference in the ANSI code page used by the backup server and the client machine. If the tape being used has non-English text name, the recovery process may not be able to locate the tape media correctly. In general, The Disaster Recovery Option does not completely support cross-language Windows environment. If you have to backup an English Windows client machine using a non-English backup server, make sure the backup media used does not contain any non-English character in the name.

## DNS Record

### Symptom

What should I do if the Disaster Recovery machine is unable to connect to the Arcserve Backup server?

### Solution

If you have not updated the Arcserve Backup server's Domain Name Server record, the Disaster Recovery machine cannot connect to the Arcserve Backup server. To avoid this problem, add the correct IP address in the hosts file.



## Windows ASR cannot restore the disk partition layout for multi-path SAN disk

**Valid on Windows Server 2008 or later platforms**

### **Symptom**

While performing restore operation, Windows ASR cannot restore the disk partition layout for multi-path SAN disk.

### **Solution**

During disaster recovery, Windows ASR cannot map the disk and restore the partition correctly. You can only restore the disk partition layout for a single-path SAN disk.

## ASDB Sessions Cannot be Restored

### Symptom

Arcserve Database Recovery wizard fails to find a backup device and gives the error “Please mount the media <media name>”, the media name is the media on which SQL server was backed up.

### Solution

After disaster recovery, the Database Recovery Wizard will be automatically launched to help you recover ASDB. During this procedure, it may fail to find a backup device this happens because the backup device was not included during full machine backup. You can perform the following steps:

#### To restore an ASDB session

1. Recover ASDB from Arcserve Database Recovery Wizard using the Media1 on which full machine backup was taken.
2. You must restore master, msdb, model and user databases manually from Media1 using the Restore Manager.
3. Create a Media2 and point to the location where the SQL server session was backed up.
4. Merge the Media2.
5. Then, restore the user databases manually from Media2 to recover the SQL database to the latest point.

**Note:** For more information about the Arcserve Database Recovery Wizard, see the topic [Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard](#) in the Arcserve Backup Administration Guide.

## Operating Systems

This section provides answers to frequently asked questions related to operating systems.

**Note:** The information in this section applies to all supported Windows platforms.

This section contains the following topics:

---

## Command Prompt Access During Disaster Recovery Mode

### Symptom

How can I open a command prompt window during the disaster recovery mode?

### Solution

**Windows 7 and Windows Server 2008 and later:** To open a command prompt in the Advanced Disaster Recovery GUI, click Utilities, and select Run.

## Hardware Changes

### Symptom

After my server failed, I replaced the hard disk and some outdated hardware. Now, when I run the disaster recovery restoration process, it appears to write everything back to disk, but when I reboot the server I get a blue screen failure. Why?

### Solution

The option is not designed to recover a system on which the hardware has been changed. When you restore a system, it restores all of the previous systems drivers. The option attempts to load the drivers for the old hardware, and, if the driver is incompatible with the new hardware, the operating system fails.

Some hardware changes are permitted, such as audio, video card, and so on. Changes of SCSI/RAID and network cards require special attention.

## Cannot Connect to Server Message

### Symptom

My remote disaster recovery fails with the message *failed to connect to the server*. How can I find out why this happens?

### Solution

To determine why the message *failed to connect to the server* was generated, perform the following steps:

1. Ping the server using IP.

If this fails, verify that the Arcserve Backup server is on the network and that the subnet mask is working.

2. Ping the server using `server_name`.

If this fails, DNS is not working.

3. Verify that DNS is functioning.

If it is not functioning, place the name of the server in the hosts file in disaster recovery system, reboot the system, and continue with the disaster recovery process.

4. Use the following command to connect to the server:

```
net use * \\server_name\Admin$ /user:domain\username
```

If this fails, verify the following:

- a. Verify that you have not changed the Arcserve Backup server user name or password since the last full backup.
- b. Verify the Windows workstation and server services are running on the Arcserve Backup server.
- c. Verify that you can connect to any other system in the network by running the "net use" command.
- d. Verify that you can connect to the Arcserve Backup server from a different system by running the "net use" command.
- e. Verify that you do not have any anti-virus, firewall, or server protection software running on the backup server, thus preventing remote access to the server.
- f. If you are running Windows 2008 on the backup server, you must reduce the security level to allow other systems to connect to the backup server. You must also change the local security policy to allow

blank password connections if you are using a blank password. See the Microsoft documentation, if necessary.

- g. If you are using a non-English version of the option, verify that disaster recovery system and the backup server are in the same code page. If not, change the code page of the disaster recovery system.

## Recover Virtual Hard Disk (VHD) Using Disaster Recovery Option

**Valid on Windows Server 2008 R2 and later**

### Symptom

How can I re-create .vhd files that are mounted as a volume?

### Solution

The Arcserve Backup disaster recovery process cannot re-create .vhd files that are mounted as a volume. You can use the following steps to recover .vhd files from a disaster:

#### To recover .vhd files from a disaster

1. Using the Arcserve Backup Disaster Recovery Option, you must recover the entire computer.
2. Restart the computer.
3. After the computer is restarted, create the virtual hard disk (VHD) and then mount the VHD.

The mounting of the VHD is complete.

4. Create a new volume on the VHD, and then format the new volume.

The formatted volume of the VHD is ready.

5. Open the Arcserve Backup Restore Manager.

The Restore Manager Wizard opens.

6. Recover the VHD by performing a volume level restore of the VHD mounted volume.

The recovery process is complete.

**Note:** When you use this process to recover VHDs using Disaster Recovery Option, Arcserve Backup restores the mounted drives as physical disks. For more information about virtual hard disk, see Microsoft documentation.

Also, Arcserve Backup cannot recover VHD boot systems from a disaster. Arcserve Backup demonstrates this behavior because the Automated System Recovery (ASR) writer cannot back up .vhd files. As a result, there are no mechanisms that you can use to recover VHD boot systems from a disaster.



## Media Verification

### Symptom

During local disaster recovery, I received the message “Please mount media XYZ, Random Id 1234, Sequence 1.” How can I verify that the media is in the tape drive or changer?

### Solution

The system needs some time to inventory all of the tapes in your library. Click Retry to allow more time for the changer to initialize. You can load only the necessary tapes for recovery to shorten the time the system needs to inventory the tape library.

## Verification of Storage Device Attachment

### Symptom

How can I verify that the storage device attached to the system is functioning properly during a local disaster recovery?

### Solution

It usually takes some time for a changer to initialize. Do not stop the disaster recovery process during this time. See the following instructions:

- If you are using a changer, use the chgtest utility from the disaster recovery command prompt. This utility is not copied during the disaster recovery process. You must copy it manually from the Arcserve Backup CD/DVD to the disaster recovery directory to use it.
- If you are performing disaster recovery from a tape drive, run the tapetest utility from the disaster recovery command prompt. This utility can be found in the %WINDIR%\system32\DR directory of the system being recovered.

## Windows Setup Message

### Symptom

During disaster recovery bluescreen mode, I sometimes see the Windows setup message “Setup has performed maintenance on your hard disk. You must restart your computer to continue with setup. If there is a floppy disk in drive A, remove it. To restart your computer, press Enter.” I press Enter to restart my computer and get the message “ntoskrnl.exe is missing” and the disaster recovery fails.

### Solution

If you receive this message, you must press Enter to restart your computer and begin the disaster recovery process from the beginning.

## Cannot See Partitions

### Symptom

I have hardware RAID5 volumes configured in the system and partitions created on the drives. During disaster recovery I cannot see the partitions created by disaster recovery on all the drives. Why?

### Solution

If you are using a hardware RAID adapter, you must always enter the manufacturer provided driver for the RAID adapter during the disaster recovery process. If you did not need the driver during the operating system installation, you must still provide it during disaster recovery. If you do not provide the driver for the RAID adapter, you will experience problems accessing the RAID adapter (although you can see the disks).

## Certificate Server Fails to Start

### Symptom

After I perform a disaster recovery, the Certificate Server on the recovered machine fails to start. How can I start it properly?

### Solution

If the Certificate Server fails to start after disaster recovery, perform the following procedure to bring it back:

1. Reboot the recovered machine.
2. While the machine is starting, press F8 to put the machine into “Directory services recovery mode”.
3. Perform a complete system state restore of the machine.
4. Reboot the machine back to normal mode.

## System Running Out of Free Space

**Valid on Windows 2008, Windows 2008 R2**

### **Symptom**

When recovering a Windows 2008 machine, DR failed during the restore process and the machine rebooted. The machine cannot start because the system state session is not restored. I checked the system and noticed that the 'X:' volume has no free space. Because of this, I am not able to install my NIC driver, so the DR process cannot continue.

### **Solution**

In Windows 2008 and Windows 2008 R2, the DR process runs in WinPE. A temporary 'X:\' volume will be created for the WinPE system. DR related binaries and other files (such as drivers, logs) will be copied to the X:\ volume. The DR option creates 10 MB free space to install drivers during DR. If the size of your drivers is more than 10 MB, you must install the required mini-drivers. Only SCSI, FC, and NIC drivers are required during DR.

To use another solution, you can remove all driver files from MSD (MSD is copied to X:\ and consumes some free space), then install the most necessary drivers with 'Utilities->Load Driver Utility' during the DR process.

## Applications

This section provides answers to frequently asked questions related to specific applications.

[Citrix](#)

## Citrix

### Symptom

After I run a Disaster Recovery on a server running Citrix Presentation Server 4.0, when I start the Citrix Presentation Server Console, I get the error "Pass-through Authentication failed. The service could not be contacted. Make sure the IMA service is installed and running." What should I do?

### Solution

To successfully log into the Citrix Presentation Server Console, start the Independent Management Architecture (IMA) service.

**Note:** If the Citrix Presentation Server was installed using Microsoft SQL Server, you must restore all databases, including the master database before starting the IMA service.

For more information, see the Disaster Recovery section of the [Agent for Microsoft SQL Server Guide](#).



---

## Chapter 6: Recovering SAN Configurations

The Disaster Recovery Option supports backup servers in Storage Area Network (SAN) configurations. You can recover the primary SAN backup servers and any member SAN servers in Windows Server 2008 or later environments.

This section contains the following topics:

---

<a href="#">Recover the SAN</a> .....	106
<a href="#">How SAN Disaster Recovery Works</a> .....	107

## Recover the SAN

There are no special configurations or settings required to recover primary and member servers. The option can recover any SAN server, as long as a full computer backup was performed using Arcserve Backup.

You must, however, collect all necessary drivers for any SCSI cards, Fibre Channel cards, and network cards.

## How SAN Disaster Recovery Works

When recovering primary or member, the option can determine if the current server is a primary server or member server.

- If the current server is a primary server, the option connects to the SAN and uses the devices on the SAN directly.
- If the current server is a member server, the option first contacts the primary server. The option then communicates with the primary SAN server to handle any device operations on the SAN.



---

## Chapter 7: Recovering Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although Arcserve Backup makes it easier to recover your mission-critical cluster environment, it still requires some planning and effort. It is important that you understand the concepts described in this guide and test the scenarios suitable for your specific environment.

A server cluster is a group of independent servers running cluster services and working collectively as a single system. Server clusters provide high-availability, scalability, and manageability for resources and applications by grouping multiple servers running Windows 2008 and later operating systems.

**Note:** Windows 2008, Windows 2008 R2, and Windows Server 2012 do not support performing disaster recovery operations using traditional methods. For more information, see the Knowledge Base document on the Arcserve Support Online website named [How to Recover Windows 2008 Cluster from a Disaster](#).

This appendix provides information about recovering cluster-shared disks, failed cluster nodes, or an entire cluster quickly, with minimum interruption to the service.

This section contains the following topics:

---

<a href="#">Cluster Failure Scenarios</a> .....	110
<a href="#">Scenario 1: No Shared Disk Failure</a> .....	118
<a href="#">Scenario 2: Shared Disk Failure</a> .....	121

## Cluster Failure Scenarios

Several types of failures can occur in the cluster environment. The following types of failure can happen separately or at the same time:

- Some cluster nodes fail (primary node failure and secondary node failure)
- Shared disk fails (cluster non-quorum disk failure)
- Partial shared disk fails
- Entire cluster fails including cluster nodes and shared disks

The scenarios specified in this section outline the steps you can take to recover from various types of cluster failure.

**Note:** If no tape device is attached to any of the cluster nodes, you can remotely recover a cluster service using the option. To do so, follow the instructions on performing a remote disaster recovery.

## Requirements

The requirements in this section specifies the Disaster Recovery Option to recover a cluster.

[Software Requirements](#)

[Hardware Requirements](#)

[Shared Disk Requirements](#)

## Software Requirements

To perform disaster recovery on clusters, you must meet the following software requirements:

- Microsoft Windows 2008 or later operating system installed on all computers in the cluster.
- A name resolution method, for example, Domain Naming System (DNS), Windows Internet Naming Service (WINS), or HOSTS.
- A Terminal Server for administering remote clusters.
- Arcserve Backup for Windows and the Disaster Recovery Option, if backup devices such as tape devices or tape library devices are attached to one or all cluster nodes. If no backup devices are attached to the cluster setting, the Client Agent for Windows should be installed on all cluster nodes that require data protection.



## Hardware Requirements

To perform disaster recovery on clusters, you must meet the following hardware requirements:

- The hardware for a cluster service node must meet the hardware requirements for Windows 2008 or later Server.
- Cluster hardware must be on the Cluster Service Hardware Compatibility List (HCL).
- Two HCL-approved computers comprised of the following:
  - A boot disk with Windows 2008 Server installed. The boot disk cannot be located on the shared storage bus.
  - Boot disks and shared disks must be on separate SCSI channels (SCSI PathID); separate adapters (SCSI PortNumber) are not required. You can use a single multi-channel SCSI or Fibre Channel adapter for both boot and shared disks.
  - Two PCI network adapters on each computer in the cluster.
  - An HCL-approved external disk storage unit that connects to all computers. This is used as the clustered disk. A RAID is recommended.
  - All hardware should be identical, slot for slot, card for card, for all nodes. This makes configuration easier and mitigates potential compatibility problems.
  - Backup devices such as tapes or tape library devices can be attached to one or all cluster nodes. It is not always necessary to have backup devices attached to the cluster nodes. If you do not have backup devices attached to the cluster nodes, the Client Agent for Windows should be installed in all cluster nodes that require data protection.

## Shared Disk Requirements

To recover your clusters, you must meet the following requirements:

- All shared disks, including the quorum disk, must be physically attached to a shared bus.
- Verify that disks attached to the shared bus can be seen from all nodes. This can be checked at the host adapter setup level. See the manufacturer's documentation for adapter-specific instructions.
- SCSI devices must be assigned unique SCSI identification numbers and properly terminated, as per manufacturer's instructions.
- All shared disks must be configured as basic, as opposed to dynamic.

We strongly recommend the use of fault-tolerant RAID configurations (for example, RAID level 5) for all disks, rather than stripe sets without parity (for example, RAID level 0) although this is not a shared disk requirement.

## Special Considerations

Special considerations for clusters:

- We do not recommend a partial shared disk configuration in which some disks are owned by one node and some disks are owned by another node.
- To avoid complications when matching disks, shared disks should be the last disks and have the highest number when viewed from Administrative Tools, Computer Management, and Disk Management.
- You can configure disaster recovery information to be saved to an alternate location on a different computer to further protect disaster recovery information.
- On most cluster computers, there is no need to stop the shared disks. The cluster can continue to function during disaster recovery. Check your hardware documentation for more information about how to avoid shutting down the hard disks.

## Terminology

The following defines common cluster terms.

### Primary node

The node that owns all shared disk resources during backup.

### Secondary node

A node that does not own any shared disk resources during backup.

### Quorum Disk

A shared disk used to store cluster configuration database checkpoints and log files that help manage the cluster. This disk is critical to restore the cluster service. The failure of the quorum disk causes the entire cluster to fail.

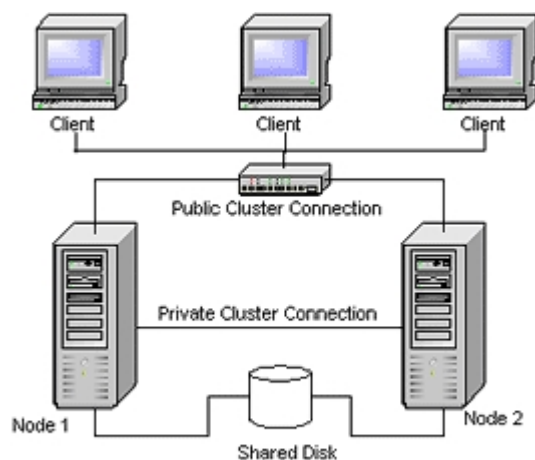
### Non-quorum Disk

A shared disk used to store shared resources including data, database, and application information. These disks are used in the typical fail-over scenario so that the data on the non-quorum shared disks information is always available. The failure of the non-quorum disk does not, in general, cause the entire cluster to fail.

### Partial Shared Disk

A specific type of shared disk. In a partial shared disk configuration, shared disks can have a unique, one-to-one relationship with individual nodes. Some shared disks are owned by one node and some disks are owned by another node during backup.

The following diagram illustrates a typical two-node cluster setting:



## Cluster Disaster Recovery Requirements

You must have the following information to recover failed clusters:

- Cluster name
- Cluster IP address and subnet mask
- Cluster node names
- Cluster node IP addresses
- The assignment of all drive letters including all private and shared hard disks
- All disk signatures (To obtain disk signatures, run one of the following utilities:  
DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012)
- All disk numbering schemes (to find these schemes, select Administrative Tools, Computer Management, Disk Management and note the disk number matching each physical disk for each computer)
- Cluster group name
- Cluster preferred nodes
- Cluster fail over policies
- Cluster resource names
- Cluster resource types
- Cluster group membership
- Cluster resource owners
- Cluster resource dependencies
- Cluster restart properties

## Scenario 1: No Shared Disk Failure

The cases specified in this section are the most common failures in the Windows cluster environment.

[Recover Secondary Node](#)

[Recover the Primary Node](#)

## Recover Secondary Node

### To recover a secondary node in the cluster

1. Disconnect the shared disks from the secondary node.

**Note:** On most cluster computers, there is no need to shut down the shared disks. This allows the cluster to function during disaster recovery. However, shutting down the cluster service on some cluster computers on the primary node might be required. Check your hardware guide for more information about how to avoid shutting down shared disks.

2. Follow the usual disaster recovery process to recover the secondary node.
3. Connect the shared disks to the secondary node when the restoration is complete.
4. Reboot the secondary node.

Your cluster should now be back online.

## Recover the Primary Node

To recover a failed primary node and ensure that the cluster is working properly

1. Disconnect the shared disks from the primary node.

**Note:** On most cluster computers, there is no need to shut down the shared disks. This allows the cluster to function during disaster recovery. However, shutting down the cluster service on some cluster computers on the primary node might be required. Check your hardware guide for more information about how to avoid shutting down shared disks.

2. Follow the usual disaster recovery process to recover the primary node.
3. Connect the shared disks when the restoration is complete.
4. Reboot the primary node.

Your cluster should now be back online.



## Scenario 2: Shared Disk Failure

There are several possible causes for shared disk failure and these are illustrated in the cases specified in this section. The first five cases discuss non-partial shared disk cluster configurations and the sixth discusses partial shared disk cluster configurations.

This section contains the following topics:

[Recover Cluster Non-quorum Shared Disks with No Node Failures](#)

[Recover Cluster Quorum Disks with No Node Failures](#)

[Recover All Shared Disks with No Node Failures in the Cluster](#)

[Recover Primary Nodes with Shared Disk Failure in the Cluster](#)

[Recover Entire Clusters](#)

[Recover Clusters with Partial Shared Disk Configurations](#)

## Recover Cluster Non-quorum Shared Disks with No Node Failures

**To recover cluster non-quorum shared disks with no node failures in the cluster**

1. Stop the cluster service on the secondary node and disconnect the shared disks from the secondary node.
2. If a non-quorum shared disk is physically damaged, perform the following steps:
  - a. Shut down the primary node.
  - b. Replace the cluster non-quorum shared disk with new disks.
  - c. Have the Cluster Disaster Recovery Requirements readily available for reference. For more information, see the [Cluster Disaster Recovery Requirements](#).
  - d. To restore the original disk signature for the shared disk, run one of the following utilities:  
  
DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012
  - e. Restart the primary node and the cluster services.
  - f. Recreate the partitions on the non-quorum shared disk.
  - g. Format the partitions according to the Cluster Disaster Recovery Requirements.
3. Run a restore job from the Arcserve Backup machine to restore the data to a non-quorum shared disk. Select the full volume restore to recover all lost non-quorum volumes in the shared disks.
4. When the restore job finishes, use the Cluster Administrator to bring the shared disk back on line.
5. Reconnect the shared disks and restart the cluster service on the secondary node.  
Your cluster should now be back online.

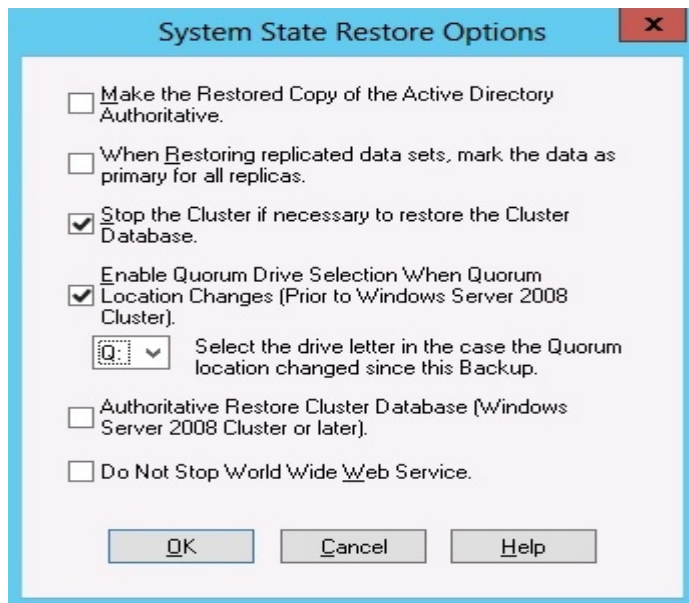
## Recover Cluster Quorum Disks with No Node Failures

### To recover cluster quorum disks with no node failures

1. Stop the cluster services on the secondary node.
2. Shut down the secondary node.
3. On the primary node, from the Windows Service Control Manager, set the cluster service startup type to Manual.
4. From the Device Manager View menu, select Show Hidden Devices and disable the Cluster Disk Driver setting.
5. If the cluster quorum disks are physically damaged, perform the following steps:
  - a. Shut down the primary node.
  - b. Replace the cluster quorum shared disk with new disks.
  - c. Start the primary node.

**Note:** Have the Cluster Disaster Recovery Requirements readily available for reference.
  - d. To restore the original disk signature for the shared disk, run one of the following utilities:  
  
DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012
  - e. Recreate and reformat the partitions on the non-quorum shared disk.
6. From the Device Manager View menu, select Show Hidden Devices and enable the Cluster Disk Driver setting.
7. Restore the system state backup. In Arcserve Backup, select System State session and right-click to select the local option.

The System State Restore Options dialog opens.



**Note:** If the cluster nodes are Active Directory Servers, you must reboot the primary node into directory restore mode when restoring the system state session.

8. Restart the primary node.
9. If the cluster files are not restored to the quorum disk, run the caclurst.exe utility to load the cluster database from the following:  
`%windir%\clubkup`  
caclurst.exe is available in the Home directory.  
`caclurst /s c:\%SystemRoot%\cARCserve\clubkup /q Q:`  
If this is a remote disaster recovery, copy the caclurst.exe file to the Client Agent for Windows directory.
10. Reboot the primary node.
11. Connect the shared disks to the secondary node.
12. Start the secondary node.

## Recover All Shared Disks with No Node Failures in the Cluster

To recover all shared disks with no node failures in the cluster, restore the quorum disk and then restore the other shared disks. For information about restoring the quorum disk, see section [Recover Cluster Quorum Disks with No Node Failures](#).

## Recover Primary Nodes with Shared Disk Failure in the Cluster

**To recover a primary node with shared disk failures in the cluster**

1. Shut down the secondary node.
2. Disconnect the shared disks from the secondary node.
3. Follow the disaster recovery procedure to recover the primary node.
4. When the restoration is complete, reboot the primary node.
5. Start the cluster services on the primary node.
6. Connect the shared disks to the secondary node.
7. Reboot the secondary node.
8. If necessary, start the cluster services on the secondary node.

Your cluster should now be back on line.

## Recover Entire Clusters

### To recover an entire cluster

1. To recover all secondary nodes, perform the following procedure:
  - a. Stop the cluster services on all nodes.
  - b. Disconnect the shared disks from the secondary node.
  - c. Shut down all nodes.
  - d. Follow the disaster recovery procedure to recover the secondary node.
  - e. If there is more than one secondary node, repeat the previous steps to recover all secondary nodes.
  - f. Shut down all secondary nodes while recovering the primary node with shared disks resources.

**Note:**All nodes and shared disks should be shut down at this time.

2. To recover the primary node with shared disks failure, perform the following tasks:
  - a. Follow the disaster recovery procedure to recover the primary node.
  - b. Start all shared disks.
  - c. When the restoration is complete, reboot the primary node.
  - d. Start the cluster services on the primary node.
  - e. Restart all secondary nodes.
  - f. Start the cluster services on the secondary node.

Your cluster should now be back online.

## Recover Clusters with Partial Shared Disk Configurations

In an environment with a partial shared disk configuration, shared disks can have a unique, one-to-one relationship with individual nodes. We recommend that you have the Cluster Disaster Recovery Requirements readily available for reference when performing this disaster recovery process.

You must perform the following tasks:

1. Recover one node with some shared disks first while other shared disks that are not owned by this node are shut down.
2. Recover another node with some shared disks. You must shut down all shared disks not owned by the node.
3. Repeat this process until you have recovered all nodes with shared disk resources.

After performing these actions, you can recover the nodes with no shared disk resources.

### **To recover a cluster with a partial shared disk configuration**

1. Recover one node with some shared disk resources by performing the following steps:
  - a. Stop the cluster services on all nodes.
  - b. Disconnect shared disks not owned by this node during backup. Refer to the Cluster Disaster Recovery Requirements and `dumpcfg.txt` to identify which shared disks are not owned by this node.
  - c. Follow the disaster recovery procedure to recover the node.
2. Repeat the previous step until you have recovered all nodes with some shared disk resources.
3. Recover nodes with no shared disk resources. Follow the disaster recovery procedure to recover the node.
4. Restart all nodes in the following order:
  - a. Restart all nodes with shared disk resources.
  - b. Restart all nodes without shared disk resources.

Your cluster should now be back online.



---

## Chapter 8: Recovering NEC Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although Arcserve Backup makes it easier to recover your mission-critical cluster environment, it still requires some planning and effort. It is important that you understand the concepts described and test the scenarios suitable for your specific environment.

A server cluster is a group of independent servers running cluster services and working collectively as a single system. Server clusters provide high-availability, scalability, and manageability for resources and applications by grouping multiple servers running Windows 2008 Server.

The following sections provide information about recovering the cluster-shared disks, failed cluster nodes, or the entire cluster, quickly and with minimum interruption to the service.

This section contains the following topics:

---

<a href="#">Disaster Recovery on NEC CLUSTERPRO/ExpressCluster SE</a> .....	130
<a href="#">Disaster Recovery on NEC CLUSTERPRO/ExpressCluster LE</a> .....	144

## Disaster Recovery on NEC CLUSTERPRO/ExpressCluster SE

Several types of failures can occur in a cluster environment. The following types of failure can happen separately or at the same time:

- Shared disk fails
- Some cluster nodes fail (primary node failure and secondary node failure)
- Entire cluster fails, including cluster nodes and shared disks

This section provides the procedures to follow to recover from various types of cluster failure.

**Note:** If the cluster node is not a backup server (no tape device is attached to the cluster node), follow the instructions for performing a remote disaster recovery.

## Arcserve Backup Installed Outside NECCLUSTERPRO/ExpressCluster SE Cluster

This section provides the following procedures to resolve cluster failures when Arcserve Backup is installed outside the cluster:

[Recover Data on Failed NEC CLUSTERPRO/ExpressCluster SE Shared Disks](#)

[Recover One Failed Cluster Node on NEC CLUSTERPRO/ExpressCluster SE](#)

[Recover Entire Clusters on NEC CLUSTERPRO/ExpressCluster SE](#)

## Recover Data on Failed NEC CLUSTERPRO/ExpressCluster SE Shared Disks

If the shared disk fails, but the cluster nodes are undamaged, perform the following steps to recover data residing on the shared disks:

### To recover data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:
  - ◆ NEC ExpressCluster Server
  - ◆ NEC ExpressCluster Log Collector
2. Shut down the cluster and turn off all servers.
3. Turn off the shared disk and replace the shared disk if necessary.
4. Turn on the shared disk, and set the parameters for the shared disk.

If RAID reconstruction or LUN configuration change is necessary, use the setting tool attached with the shared disk. See the shared disk documentation for information about the setting tool.

To perform any setting or configuration from a cluster node, turn on only one server at a time.

5. On the primary cluster node only, perform the following procedure:
  - a. Write a signature (identical to the original) to the disk with the operating system's disk administrator, if one does not already exist.
  - b. Recreate the original partitions on the disk. If X-Call settings have been performed to HBA, you must connect the partition using the NEC ExpressCluster disk administrator before formatting.

**Note:** X-Call is a setting that enables viewing of the shared partition from both the active and passive sides. See the CLUSTERPRO/ExpressCluster products document for more information about the setting for X-Call.
  - c. Using the operating system's disk administrator, specify the original drive letter to the shared disk.
  - d. Use Arcserve Backup to restore the backed up data to the shared disk.
  - e. If you have performed X-Call settings for a disk, start the NEC ExpressCluster disk administrator and specify the recovered shared disk as X-CALLDISK in X-CALL DISK configuration.

If you have performed X-Call settings for HBA, these settings are not changed. Go on to the next step.

- f. If the disk access path has been dualized, confirm that the access path is dualized.
  - g. Reboot the server.
  - h. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.
  - i. Check the cluster letters on the CLUSTER disk partition with the NEC ExpressCluster disk administrator. If the cluster letter does not appear, set it to the original letter.
  - j. Shut down the cluster node.
6. Perform the following steps on all cluster nodes:
- a. Boot up the cluster node.
  - b. Using the operating system's disk administrator, specify the original drive letter to the shared disk, if necessary.
  - c. Set the Startup type of the following services from Manual to Automatic:
    - ◆ NEC ExpressCluster Server
    - ◆ NEC ExpressCluster Log Collector
  - d. Shut down the server and shut down the cluster node.
7. Start all cluster nodes and perform the Return to cluster(R) operation from the NEC ExpressCluster Manager. Recover all servers to Normal.

## Recover One Failed Cluster Node on NEC CLUSTERPRO/ExpressCluster SE

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

### To recover the failed cluster node

1. Shut down the failed node.
2. Disconnect shared disks from the node.
3. Follow the normal remote disaster recovery process to recover the node.  
**Note:** Restore only the local disk partitions during the disaster recovery.
4. Connect the shared disks to the node.
5. Reboot the node after restoration.
6. Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:
  - ◆ Select a server name and select Control, Return to Cluster.
  - ◆ Right-click a server and select Return to Cluster from the pop-up menu.
  - ◆ Select a server and click the Return to Cluster icon on the toolbar.

The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

## Recover Entire Clusters on NEC CLUSTERPRO/ExpressCluster SE

You can recover an entire cluster.

### To recover an entire cluster

1. Stop the cluster services on all nodes.
2. Disconnect shared disks from the all nodes.
3. Ensure that all cluster nodes are shut down.
4. To recover all cluster nodes one by one, follow the procedure provided in the section Recover One Failed Cluster Node on NEC CLUSTERPRO/ExpressCluster SE in this document.

**Note:** Perform the recovery of one node at a time, and ensure that all other nodes are shut down and the shared disk is disconnected during this process.

5. Shut down all cluster nodes.
6. To recover the cluster shared disks, perform the procedure provided in the section Recover Data on Failed NEC CLUSTERPRO/ExpressCluster SE Shared Disks in this document.

## Arcserve Backup Installed on the NEC CLUSTERPRO/ExpressCluster SE Cluster

Performing disaster recovery with Arcserve Backup installed on an NEC CLUSTERPRO/ExpressCluster cluster requires special consideration when creating your backup jobs:

- Do not use filters to exclude files or folders residing on volumes containing the Arcserve Backup installation when submitting backup jobs using the physical node name.
- You can use filters to exclude files or folders residing on other shared disk or mirrored volumes from backups when creating backup jobs using the physical node name. These volumes should be backed up using the virtual hostname.

This section contains the following topics:

[Shared Disk Failure on NEC CLUSTERPRO/ExpressCluster SE](#)

[Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node](#)

[Recover Entire NEC CLUSTERPRO/ExpressCluster SE Clusters](#)



## Shared Disk Failure on NEC CLUSTERPRO/ExpressCluster SE

This section provides the procedures to follow to recover your data if your shared disk fails.

[Recover Data with Arcserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks](#)

[Recover Data with Arcserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks](#)

## Recover Data with Arcserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks

To recover the data residing on the shared disks, if the Arcserve Backup was installed on the shared disk, perform the following procedure:

### To recover the data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:
  - NEC ExpressCluster Server
  - NEC ExpressCluster Log Collector
2. Shut down the cluster and turn off all servers.
3. Turn off the shared disk. Replace the shared disk, if necessary.
4. Turn on the shared disk and set the shared disk parameters.

If you must reconstruct a RAID configuration or change a LUN configuration, use the setting tool belonging to the shared disk. See the shared disk product documentation for more information about the setting tool.

If you perform any settings or configuration from a cluster node, turn on only one server at a time.

5. Perform the following steps on the primary cluster node:
  - a. Perform local disaster recovery on the primary cluster node. Ensure that the data on the shared disk containing the Arcserve Backup installation is restored.
  - b. If you have performed X-Call settings for a disk, start the NEC ExpressCluster Disk Administrator and specify the recovered shared disk as X-CALLDISK in the X-CALL DISK configuration.

If you have performed X-Call settings for HBA, these settings are unchanged. No action is necessary.
  - c. Confirm that the disk access path is dualized, if applicable.
  - d. Reboot the server.
  - e. From the NEC ExpressCluster Disk Administrator, verify that the cluster letters on the CLUSTER disk partition are the same as the original letters.
  - f. Shut down the cluster node.

6. Perform the following steps on all cluster nodes:
  - a. Boot up the cluster node.
  - b. Using the operating system disk administrator, specify a drive letter for the shared disk, if necessary. This letter should be the same as the original drive letter.
  - c. Reset the Startup type of the following services to Automatic:
    - ◆ NEC ExpressCluster Server
    - ◆ NEC ExpressCluster Log Collector
  - d. Shut down the server and shut down the cluster node.
7. Start all cluster nodes and, from the NEC ExpressCluster Manager, perform the Return to Cluster(R) operation to recover all servers to Normal.

## Recover Data with Arcserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks

If the shared disk fails, but the cluster nodes are undamaged, perform the following steps to recover data residing on the shared disks:

### To recover data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:
  - ◆ NEC ExpressCluster Server
  - ◆ NEC ExpressCluster Log Collector
2. Shut down the cluster and turn off all servers.
3. Turn off the shared disk and replace the shared disk, if necessary.
4. Turn on the shared disk and set the shared disk parameters.

If you must reconstruct a RAID configuration or change a LUN configuration, use the setting tool belonging to the shared disk. See the shared disk product documentation for more information.

To perform any setting or configuration from a cluster node, turn on only one server at a time.

5. On the primary cluster node, perform the following procedure:
  - a. Write a signature (identical to the original) to the disk with the operating system's disk administrator, if one does not already exist.
  - b. Recreate the original partitions on the disk. If X-Call settings have been performed to HBA, you must connect the partition using the NEC ExpressCluster Disk Administrator before formatting.
  - c. Using the operating system's disk administrator, specify the original drive letter to the shared disk.
  - d. Use Arcserve Backup to restore the backed up data to the shared disk.
  - e. If you have performed X-Call settings for a disk, start the NEC ExpressCluster Disk Administrator and specify the recovered shared disk as X-CALLDISK in the X-CALL DISK configuration.

If you have performed X-Call settings for HBA, these settings are not changed. No action is necessary.
  - f. Confirm that the disk access path has been dualized, if applicable.
  - g. Reboot the server.

- h. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.
    - i. From the NEC ExpressCluster Disk Administrator, ensure that the cluster letter appears on the CLUSTER disk partition. If the cluster letter does not appear, set it to the original letter.
    - j. Shut down the cluster node.
6. Perform the following steps on all cluster nodes:
  - a. Boot up the cluster node.
  - b. Using the operating system disk administrator, specify the original drive letter to the shared disk, if necessary.
  - c. Reset the Startup type from Manual to Automatic for the following services:
    - ◆ NEC ExpressCluster Server
    - ◆ NEC ExpressCluster Log Collector
  - d. Shut down the server and shut down the cluster node.

Start all cluster nodes and perform the Return to Cluster(R) operation from the NEC ExpressCluster Manager to recover all servers to Normal.

## Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

### To recover the failed cluster node

1. Shut down the failed node.
2. Disconnect shared disks from the node.
3. Follow the normal remote disaster recovery process to recover the node.  
**Note:** Restore only the local disk partitions during the disaster recovery.
4. Connect the shared disks to the node.
5. Reboot the node after restoration.
6. Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:
  - Select a server name and select Control, Return to Cluster.
  - Right-click a server and select Return to Cluster from the pop-up menu.
  - Select a server and click the Return to Cluster icon on the toolbar.

The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

## Recover Entire NEC CLUSTERPRO/ExpressCluster SE Clusters

You can recover an entire cluster using the following procedure.

### To recover an entire cluster

1. Stop the cluster services on all nodes.
2. Disconnect shared disks from the all secondary nodes.
3. Ensure that all cluster nodes are shut down.
4. To recover the primary cluster node, perform the procedure provided in section [Recover Data with Arcserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk](#).
5. To recover all other cluster nodes one by one, perform the procedure provided in section [Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node](#).  
**Note:** You must recover one node at a time, and ensure that all other nodes are shut down and that the shared disk is disconnected during this process.
6. Shut down all cluster nodes.
7. To recover the cluster shared disks, perform the procedure provided in section [Recover Data with Arcserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk](#).

## Disaster Recovery on NEC CLUSTERPRO/ExpressCluster LE

Several types of failures can occur in a cluster environment. The following types of failure can happen separately or at the same time:

- Mirror disk fails
- Cluster nodes fail (primary node failure and secondary node failure)
- Entire cluster fails including cluster nodes and mirror disks

The scenarios in this section outline the steps you can take to recover from various types of cluster failure.

**Note:** If no tape device is attached to any of the cluster nodes, you can remotely recover a cluster service using the Disaster Recovery Option. To do so, follow the instructions on performing a remote disaster recovery.



## Arcserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster LE Cluster

This section provides procedures to help you recover your data if Arcserve Backup is installed outside the cluster.

### **More information:**

[NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk is Damaged](#)

[Recover Data if NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk Data is Corrupted](#)

[Recover if One NEC CLUSTERPRO/ExpressCluster LE Cluster Node Fails](#)

[Recovery if All NEC CLUSTERPRO/ExpressCluster LE Nodes Fail](#)

[Active/Passive Configuration](#)

[Damaged Mirrored Disk in Active/Passive Configuration](#)

[Corrupted Mirrored Disk Data in Active/Passive Configuration](#)

[Recover One Failed Cluster Node in Active/Passive Configuration](#)

[All Cluster Nodes Fail in Active/Passive Configuration](#)

## NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk is Damaged

If any disk in a mirror set becomes damaged, but the cluster nodes are undamaged, you must replace the disk without halting the current application. See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance]* 4.2.9 *Replacement of Damaged Disk* for information.

## Recover Data if NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk Data is Corrupted

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, perform the following procedure to recover your data:

### To recover your data from the cluster node

1. From the Start menu, select Programs, and select Computer Management. Select Services and change the Startup type of the NEC ExpressCluster Server services to Manual:

Perform this task on all servers.

2. Shut down the cluster and replace the failed mirrored disk, if necessary.
3. Reboot the servers.
4. Start the Mirror Disk Administrator on the server to be restored.
5. From the Mirror Disk Administrator menu bar, select Disk Operation, Enable Access, and set the mirrored disk to make it accessible.
6. Use Arcserve Backup to restore data to the mirrored disk.

**Note:** Use your normal restore settings when restoring this data.

7. From the Mirror Disk Administrator menu bar, select Disk Operation, Disable Access, and return the mirrored disk setting to restrict access.
8. Open Services and set the startup type of the NEC ExpressCluster Server service to Automatic.

Perform this task on all servers.

9. From the Start menu, select Shut Down to reboot all of the servers.

## Recover if One NEC CLUSTERPRO/ExpressCluster LE Cluster Node Fails

When a problem occurs on the server system disk and the system does not operate properly, you must replace the disk and restore the data. To do so, perform the following procedure:

### To recover the cluster

1. If the server to be recovered is running, from the Start menu select Shut Down to shut down the server. If NEC ExpressCluster is running, wait until the failover finishes.
2. If NEC ExpressCluster is running, select the cluster from the NEC ExpressCluster Manager, choose CLUSTER(M), Property(P) from the menu bar, and check Manual return(F) on the Return mode tag.
3. Follow the normal disaster recovery process to recover the node.
4. From the Start menu select Settings, Control Panel, and select Date and Time to confirm that the Date and Time of the server operating system to be restored is identical to the other servers in the cluster.
5. On the server to be restored, change the Startup type of the following NEC ExpressCluster-related services to Manual:
  - ◆ NEC ExpressCluster Server service
  - ◆ NEC ExpressCluster Log Collector service
  - ◆ NEC ExpressCluster Mirror Disk Agent service
6. From the Start menu, select Shut Down to shut down the server to be restored.
7. On the server to be restored, start the operating system disk administrator and, if necessary, modify the drive letter of the switched partitions so that it is the same as when the backup was performed. Close the disk administrator.
8. On the server to be recovered, set the Startup type of the following services to Manual and reboot:
  - ◆ NEC ExpressCluster Server services
  - ◆ NEC ExpressCluster Log Collector services

**Note:** The NEC ExpressCluster Mirror Disk Agent service Startup type should remain set to Automatic.
9. On the server to be recovered, from the Start menu, select Programs, and select NEC ExpressCluster Server.

10. Start the Mirror Disk Administrator, select Change, and click Reconstitution.
11. Check the name of target mirror sets and click OK.
12. On the server to be restored, reset the startup type of the following services to Automatic and reboot:
  - ◆ NEC ExpressCluster Server services
  - ◆ NEC ExpressCluster Log Collector
13. On the other server, shut down the cluster and reboot.
14. When the servers have been restarted, from the NEC ExpressCluster Manager, return the server to be recovered to the cluster.
15. Select the cluster from the NEC ExpressCluster Manager, select CLUSTER(M), and Property(P) from the menu bar, and reset the Return Mode setting to Auto Return.
16. Shut down the cluster.

## Recovery if All NEC CLUSTERPRO/ExpressCluster LE Nodes Fail

To recover an entire cluster, follow the normal disaster recovery process to recover the primary node and the secondary node. To return all nodes to the cluster, see the NEC documentation for more information.

## Active/Passive Configuration

Performing disaster recovery in this configuration requires special considerations while creating your backup jobs:

- Do not use filters to exclude files or folders residing on volumes containing the Arcserve Backup installation (either shared disk volume or mirrored volume) when submitting backup jobs using the physical node name.
- You can use filters to exclude files or folders residing on other shared disks or mirrored volumes while creating backup jobs using the physical node name. Back these volumes up using the virtual hostname.

## Damaged Mirrored Disk in Active/Passive Configuration

If a disk in a mirror set becomes damaged, you must replace the disk without halting the current application.

**Note:** See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance] 4.2.9 Replacement of Damaged Disk* for information.



## Corrupted Mirrored Disk Data in Active/Passive Configuration

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, perform one of the procedures specified in this section, depending upon whether Arcserve Backup is installed on the mirrored disk.

## Recover Data with Arcserve Backup Installed on Mirrored Disks

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, and Arcserve Backup is installed on the mirrored disk, perform the following procedure to recover your data:

1. Shut down the cluster.
2. Replace the damaged mirrored disk, if necessary.
3. Perform local disaster recovery on the primary cluster node. Ensure that the data on the mirrored disk containing the Arcserve Backup installation is restored.

**Note:** See the special considerations in section [Active/Passive Configuration](#).

4. From the Start menu, select Shut Down to reboot all servers.

## Arcserve Backup Not Installed on Mirrored Disks

If any disk in a mirrored set becomes damaged, but the cluster nodes are undamaged, and Arcserve Backup is not installed on the mirrored disk, you must replace the disk without halting the current application.

**Note:** See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance] 4.2.9 Replacement of Damaged Disk* for information.

## Recover One Failed Cluster Node in Active/Passive Configuration

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

### To recover the failed cluster node

1. Shut down the failed node.
2. Disconnect shared disks from the node.
3. Follow the normal remote disaster recovery process to recover the node.  
**Note:** Restore only the local disk partitions during the disaster recovery.
4. Connect the shared disks to the node.
5. Reboot the node after restoration.
6. Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:
  - Select a server name and select Control, Return to Cluster.
  - Right-click a server and select Return to Cluster from the pop-up menu.
  - Select a server and click the Return to Cluster icon on the toolbar.

The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

## All Cluster Nodes Fail in Active/Passive Configuration

You can recover an entire cluster node using the following procedure.

### To recover an entire cluster

1. To recover the primary node, perform the procedure provided in section [Recover Data with Arcserve Backup Installed on Mirrored Disk](#).
2. To recover the secondary nodes, perform the procedure provided in section [Recover One Failed Cluster Node in Active/Passive Configuration](#).
3. Return all nodes to the cluster. To do so, see the NEC documentation for more information.



---

## Chapter 9: Staging Using File System Devices

Arcserve Backup lets you create backup sessions that can be used for disaster recovery operations and store the sessions on file system devices using Arcserve Backup disk staging functionality. When you migrate the backup sessions one location (staging devices) to another location, or purge backup data on the staging devices, an update of your disaster recovery information is automatically triggered. This ensures that your disaster recovery information is always up-to-date.

This section contains the following topics:

---

<a href="#">Special Consideration for Staging</a> .....	160
---	-----

## Special Consideration for Staging

When using the disk staging feature, there are some special considerations that can potentially affect the disaster recovery process. The consideration specifically for disaster recovery:

Do not stage the backup of the local backup server itself on disks.



---

## Chapter 10: Recovering Windows 2008 Small Business Server

Windows Small Business Server 2008 is an important member of the Microsoft Windows product family, providing a comprehensive IT solution for small to medium enterprises. The Windows Small Business Server 2008 installation package provides some commonly used Windows services and applications including Internet Information Service (IIS), ASP.Net, Microsoft Exchange Server and Microsoft SharePoint service. This appendix describes how to back up and restore these services and applications appropriately for disaster recovery purposes.

**Note:** This appendix contains information on backing up and restoring the default configurations of Windows Small Business Server 2008. It does not serve as a comprehensive reference for all Windows Small Business Server 2008 recovery procedures.

This section contains the following topics:

---

<a href="#">Windows Small Business Server 2008 Default Settings</a> .....	162
<a href="#">Arcserve Backup Requirements</a> .....	163
<a href="#">Disaster Preparation for Windows Small Business Server 2008</a> .....	164
<a href="#">Windows Small Business Server 2008 Disaster Recovery</a> .....	165
<a href="#">Other Applications</a> .....	166
<a href="#">Microsoft SharePoint Service Restoration</a> .....	167
<a href="#">Microsoft Exchange Restoration</a> .....	173

## Windows Small Business Server 2008 Default Settings

By default, Microsoft Windows Small Business Server 2008 installs the following components when setting up a computer:

- Microsoft Active Directory: Also creates a new domain and updates the machine to a Domain Controller.
- IIS 6 integrated with ASP.net: Creates a default website and configures it with Microsoft Frontpage extension.
- DNS
- Microsoft Exchange Server 6.5 integrated with Active Directory
- Microsoft SQL Desktop Engine 2000
- Windows Microsoft SharePoint Services 2.0: Creates a virtual website, called companyweb, and configures it using the Microsoft SharePoint extension.
- Other common network services (for example, optional DHCP, Firewall, and Windows Cluster)

## Arcserve Backup Requirements

In addition to the Arcserve Backup base, the following options are required to back up Windows Small Business Server 2008 data correctly:

- Arcserve Backup Agent for Open Files for Windows
- Disaster Recovery Option
- Arcserve Backup Agent for Microsoft Exchange Server
- Other options relevant to your storage devices

The Windows Small Business Server 2008 Premium Edition also installs the Microsoft SQL 2000 Server (Service Pack 3) and uses it instead of Microsoft Desktop Engine (MSDE). If you install the Premium Edition, you must also install the Arcserve Backup Agent for Microsoft SQL Server.

## Disaster Preparation for Windows Small Business Server 2008

In addition to a regular full machine backup, the following backups are required to protect the applications:

- **Microsoft Exchange Server:** Using the Agent for Microsoft Exchange Server, you can back up your Microsoft Exchange Server data at two levels: Database level and Document level. Database level backups treat all Microsoft Exchange data as a whole and back up all data as one information store (database). Document level backups can provide more subtle granularity. For disaster recovery purposes, we recommend using the Database level backup.
- **Microsoft Desktop Engine (MSDE):** Windows Small Business Server 2008 installs MSDE as the primary storage container for Microsoft SharePoint Services. Certain other applications (such as SBSMonitor) also save data in the MSDE. The Arcserve Backup Client for Microsoft VSS Software Snap-Shot MSDEwriter is used to back up MSDE data.
- **Microsoft SQL Server:** Windows Small Business Server 2008 Premium Edition allows you to use Microsoft SQL Server 2000 instead of MSDE. If you use Microsoft SQL Server, use the Agent for Microsoft SQL Server to back up the Microsoft SQL Server data.

## Windows Small Business Server 2008 Disaster Recovery

To recover a Windows Small Business Server 2008 server machine, first follow the normal disaster recovery procedure for Windows 2008. The regular disaster recovery procedure brings the machine back to its last full backup state but without any database data. This section provides procedures to recover the databases.

For information about recovering Windows 2008 machines, see [Disaster Recovery on Windows 2008](#).

## Other Applications

Windows Small Business Server 2008 default services can be recovered during the operating system disaster recovery process. If you have installed third party applications other than those covered in this section, see the appropriate Arcserve Backup agent or option guide for information about recovering these applications.

## Microsoft SharePoint Service Restoration

If you do not update your Microsoft SharePoint data frequently (for example, if you use the Agent for Open Files), the Microsoft SharePoint Service may run without any special recovery procedures after the disaster recovery process finishes. However, this data can become corrupted and we strongly recommend that you use the following procedures to fully recover your Microsoft SharePoint Service data.

This section contains the following topics:

[How Microsoft SharePoint Service Data is Recovered](#)

[Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint](#)

[Reinstall Microsoft SharePoint and MSDE](#)

[Restore Microsoft SharePoint Service](#)

## How to Recover Microsoft SharePoint Service Data

The following process allows you to fully recover your Microsoft SharePoint Service data:

1. [Delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.](#)
2. [Reinstall Microsoft SharePoint and MSDE to create the MSDE meta databases.](#)
3. [Restore the Microsoft SharePoint Service.](#)



## Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint

You can delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.

### To delete the Microsoft SharePoint website and uninstall Microsoft SharePoint

1. From the Start menu, select Control Panel and click Add or Remove Programs.
2. Select Microsoft SharePoint 2.0 and all MSDE components (SharePoint and SBSMonitoring) to uninstall them.
3. From the Internet Information Service (IIS) Manager Console Administrative Tools, under Websites, delete the companyweb and SharePoint Central Administration Web sites.
4. In the IIS Manager, under Application Pools, right-click StsAdminAppPool and select Delete from the pop-up menu.
5. Delete or rename the Microsoft SharePoint and companyweb folders.
6. Delete the following registry keys:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MicrosoftSQL Server-\SHAREPOINT  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SmallBusinessServer\Intranet

## Reinstall Microsoft SharePoint and MSDE

When you have uninstalled Microsoft SharePoint, you must reinstall Microsoft SharePoint and MSDE to create the MSDE meta databases. To do so, perform the following procedure:

### To reinstall the Microsoft SharePoint and MSDN

1. From the Windows Small Business Server 2008 installation CD, reinstall the Microsoft SharePoint Service from:

X:\SBS\CLIENTAPPS\SHAREPT\setupsts.exe

where X is the drive letter of your CD-ROM drive.

**Note:** If your installation CD has the MSDE core file digital signature issue and it has expired, download the updated Microsoft SharePoint Services setup program (STSV2.exe) to reinstall Microsoft SharePoint Services.

2. During the last stage of the reinstallation, an error message appears, informing you that there has been a Microsoft SharePoint Setup error, and that the installation has failed to update your default website. This error message is specific to the Windows Small Business Server 2008 Microsoft SharePoint installation and can be ignored.
3. Close the page and click **OK**.
4. After installation, STS creates the Microsoft SharePoint Central Administration site and the Microsoft SharePoint configuration database, called STS\_config.

If the Microsoft SharePoint configuration database, STS\_config, is missing, you may have an expired MSDE core file digital signature issue. Perform the following steps to address this problem:

- a. Delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.
  - b. Download the updated Microsoft SharePoint Services setup program (STSV2.exe).
  - c. Return to the beginning of this topic to reinstall Microsoft SharePoint and MSDE
5. In the IIS Manager, under Websites, create a new virtual Website, name it companyweb, and select its home path. The default path is typically c:\inetpub\companyweb. If you use the default location, the path will be restored to the original after all restore operations are complete.
  6. In the STS installation procedure, the setup selects a random TCP port to create the Microsoft SharePoint Central Administration Site. To be consistent with your ori-

ginal settings, use the IIS Manager to change the port to 8081, the original setting before the backup.

7. Launch the Microsoft SharePoint Central Administration Site: <http://localhost:8081> from Microsoft Internet Explorer to create a new Microsoft SharePoint website to restore the original Microsoft SharePoint content.

The Microsoft SharePoint Central Administration home page opens.

8. Click **Extend** or upgrade virtual server and select companyweb from the virtual site list.
9. From the Virtual Server List, select the server you want to update.
10. On the Extend Virtual Server page, select Extend and create a content database.
11. On the Extend and Create Content Database page, enter the appropriate information in the required fields.

A new, randomly named, content database is created in MSDE.

## Restore Microsoft SharePoint Service

Once the Microsoft SharePoint configuration databases have been rebuilt, you must restore the Microsoft SharePoint content databases. To do so, perform the following procedure:

### To restore Microsoft SharePoint service

1. Using the Arcserve Backup Manager, restore all content database backups (STS\_Config and STS\_%machine\_name%\_1) to their original positions. The MSDE writer recreates the original content databases.  
**Important!** Restore only the content databases, STS\_Config and STS\_%machine\_name%\_1 under the MSDE writer.
2. Set the restored databases as the current content databases. To do so, perform the following steps:
  - a. Launch the SharePoint Central Administration Site and select Configure virtual server settings and select the companyweb website.
  - b. Select Virtual Server management and select Manage Content databases.
  - c. On the Manage Content databases page, click the content databases created by the reinstallation process and enable the Remove content database option.
  - d. Click **OK**.
3. On the same page, click **Add a content database** to add the restored databases as the current content databases.

The Add a content database screen opens.

4. Enter the appropriate information in the required fields and click **OK**.
5. Launch <http://companyweb/> to verify the result.

The original Microsoft SharePoint data should be restored.

## Microsoft Exchange Restoration

To restore Microsoft Exchange application data, select the Microsoft Exchange backup session from the Backup Manager and restore the session to its original location. However, you must ensure the following:

- You must be a member of the Exchange Administrator Group to restore Microsoft Exchange Server data.

**Note:** In the Windows Small Business Server 2008 default settings, the administrator is automatically the administrator of the Microsoft Exchange Server.

- Before submitting the restore job, you must enter the Exchange Administrator user name and password

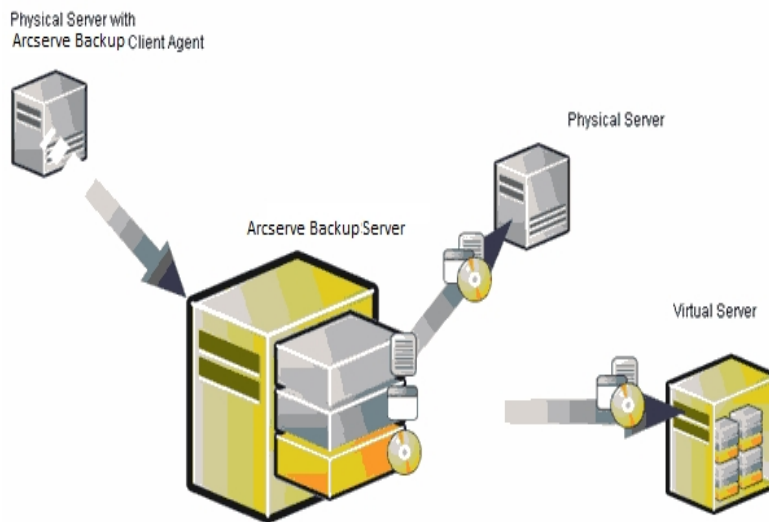
For more information about restoring Microsoft Exchange Server data, see the [\*Agent for Microsoft Exchange Server Guide\*](#).



---

## Chapter 11: Recovering Data from a Physical to Virtual Machine

This section provides you with the information on how to perform Disaster Recovery from physical machines to virtual machines (P2V) using the Arcserve Backup Disaster Recovery Option. The following diagram illustrates a typical P2V setting:



Now, using the Disaster Recovery Option you can recover a physical server to a virtual machine that is depot in some virtual infrastructures like VMware ESX Server and Microsoft Hyper-V Server.

This section contains the following topics:

---

<a href="#">Prerequisites</a> .....	176
-------------------------------------	-----

## Prerequisites

You must have knowledge on Arcserve Backup Disaster Recovery Option, network configuration utility netsh, and the usage of VMware ESX server and Microsoft Hyper-V Server.

**More information:**

[Operating Systems](#)

[Virtual Infrastructures](#)



## Operating Systems

For details about the list of operating systems supporting the disaster recovery from physical machines to VMware virtual machines, refer to [Compatibility Matrix](#).

## Virtual Infrastructures

This feature is supported on VMware ESX Server 5.5 and higher virtual infrastructures from VMware and Microsoft Hyper-V Server.

---

## Chapter 12: Glossary

This section contains the following topics:

---

<a href="#">Advanced Mode</a> .....	180
<a href="#">Alternate Machine Name</a> .....	181
<a href="#">ASDB Recovery Configuration</a> .....	182
<a href="#">Boot Volume</a> .....	183
<a href="#">Client Agent Service</a> .....	184
<a href="#">Cluster Configuration</a> .....	185
<a href="#">Disaster Recovery</a> .....	186
<a href="#">Hard Disk Status</a> .....	187
<a href="#">iSCSI Configuration</a> .....	188
<a href="#">Network Status</a> .....	189
<a href="#">Password</a> .....	190
<a href="#">Password Management</a> .....	191
<a href="#">Path</a> .....	192
<a href="#">Pre-flight Check</a> .....	193
<a href="#">System Volume</a> .....	194
<a href="#">Tape Engine Service</a> .....	195
<a href="#">USB Backup Device Configuration</a> .....	196
<a href="#">User Name</a> .....	197

## Advanced Mode

Advanced Mode assists you in customizing the restore process.

## Alternate Machine Name

The Alternate Machine Name is the hostname of the machine where the shared folder resides. The IP address of this machine can also be used but we do not recommend this, particularly in DHCP environments.

## ASDB Recovery Configuration

ASDB Recovery Configuration lets you recover your sessions automatically when you recover a primary or standalone server with Arcserve Backup Database installed locally.

## Boot Volume

A boot volume is the disk volume that contains the Windows operating system files and its supporting files.

## Client Agent Service

The Client Agent Service is a critical service used to communicate with backup servers for data recovery. Disaster Recovery will always start this service if the disaster recovery is local. If disaster recovery is remote, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Client Agent Service.



## Cluster Configuration

Cluster Configuration displays in the Pre-flight Check screen if the backup server is a cluster node. If it is a cluster node, WinPE searches for an available cluster virtual node. If the cluster virtual node is available, WinPE DR omits the restore process of the cluster shared disk, otherwise Disaster Recovery will restore the cluster shared disk.

## Disaster Recovery

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic events or natural disasters.

## Hard Disk Status

The Hard Disk Status is a potential item that may show up on the Pre-flight Check screen describing the status of a hard disk. The status can be one of the following:

- If a hard disk is not available, the status indicates an error.
- If a hard disk is available, this item will not be displayed.

## ISCSI Configuration

ISCSI Configuration enables you to configure ISCSI connections. This screen displays ISCSI connections during backup time and ISCSI connections during disaster recovery time.

## Network Status

The Network Status is a potential item that may show up on the Pre-flight Check screen describing the status of the network connection. The status can be one of the following:

- If there is no network connection for Disaster Recovery, the status indicates no connection.
- If the network connection for Disaster Recovery is remote, the status indicates an error.
- If the network connection for Disaster Recovery is local, the status indicates a warning.
- If the network connection for Disaster Recovery is OK, this item will not be displayed.

## Password

The password for the specified user account.

## Password Management

Password Management is an item that shows up on the Pre-flight Check screen only if it is used during backup time. A Click Here link appears for you to open the Enter caroot password screen.

## Path

The path for the shared folder in which to store the replicated disaster recovery information.



## Pre-flight Check

The Pre-flight Check option provides a configuration list for you to detect and resolve potential environment issues. Essentially, for each item selected from the Configuration list, a description of that item is displayed at the bottom of the screen describing the issue.

## System Volume

A system volume is the disk volume that contains the hardware-specific files required to start Windows, such as BOOTMGR.

## Tape Engine Service

The Tape Engine Service is used only for local Disaster Recovery (DR).

From the Pre-flight Check screen, a Click Here link is displayed at the bottom of the screen to let you restart the Tape Engine Service in order to maintain the connections when there are remote file system devices or data deduplication devices.

## USB Backup Device Configuration

The USB Backup Device Configuration is used during backup time where you configure backup devices (for example, tape drives, lomega changers, and digital storage drives). For some USB backup devices, you may need to install additional drivers.

## User Name

The User Name is the user account used to connect to the machine on which the alternate location resides. The domain part of the user name is optional. For example, if the full user account name is domainX\userX, you can enter userX.



---

## Chapter 13: Index

---

### A

#### **active/passive configuration**

- all nodes, recovering 157
- considerations 151
- corrupted mirror disk 153
- one cluster, recovering 156

#### **alternate location**

- general considerations 29
- setting up using disaster recovery wizard 27
- shared folder, creating 25

### C

#### **cluster**

- active/passive configuration, all nodes 157
- active/passive configuration, one cluster 156
- all nodes, recovering 127
- all shared disks, recovering 125
- failure scenarios 110
- partial shared disk, recovering 128
- primary node, recovering 120
- primary node, shared disk, recovering 126
- secondary node, recovering 119
- shared disk failure 121

#### **configure, disaster recovery option 30**

#### **creating shared folder, alternate location 25**

### D

#### **disaster recovery**

- configuration 30
- databases 16
- incremental and differential sessions 31

---

## E

### ExpressCluster SE

- all nodes, recovering 143
- one node, recovering 142

### ExpressCluster LE

- all nodes, recovering 150
- corrupted mirror disk 147
- damaged mirror disk 146
- one node, recovering 148
- recovering 144

## F

**failure type, cluster 110**

## G

**general considerations, alternate locations 29**

## I

**incremental and differential sessions 31**

**install, disaster recovery option 19, 30**

## N

### NEC CLUSTERPRO

- all nodes, recovering 143
- corrupted mirror disk 147
- damaged mirror disk 146
- one node, recovering 142



---

## P

- P2V, recovering** 175
- partial shared disk, cluster** 128
- primary node, cluster** 120
- primary node, cluster, shared disk** 126

## R

### recover

- cluster, all nodes 127
- cluster, partial shared disk 128
- cluster, primary node 120
- cluster, primary node, shared disk 126
- cluster, secondary node 119
- cluster, shared disk 121
- Lotus Notes 16
- Microsoft Exchange Server 16
- Microsoft SQL Server 16
- Oracle 16
- physical to virtual 175

## S

### SAN

- Windows Server 2008 63

- secondary node, cluster** 119

## T

### troubleshooting

- applications 103

---

## U

[utilities, troubleshooting](#) 103

## V

[virtual machine, recovering](#) 175

## W

### [Windows Server 2008](#)

[primary SAN](#) 63

### [WinPE Disaster Recovery](#)

[WinPE Disaster Recovery Utilities](#) 56