
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>LICENSE OR ACKNOWLEDGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boost 1.34.1</td>
<td>Boost Software License 1.0</td>
</tr>
<tr>
<td>ZLib 1.1.4</td>
<td>ZLib 1.2.3</td>
</tr>
</tbody>
</table>

Recovery Manager for Active Directory Forest Edition - Product Overview
Updated - March 11, 2011
Software Version - 8.0
## CONTENTS

### INTENDED AUDIENCE

5

### CONVENTIONS

5

### ABOUT QUEST SOFTWARE, INC.

6

- Contacting Quest Software ........................................... 6
- Contacting Quest Support ............................................. 6

### ABOUT RECOVERY MANAGER FOR ACTIVE DIRECTORY

Forest Edition .................................................................. 7

### FEATURES AND BENEFITS

8

- Comprehensive Active Directory Recovery Options .............. 8
- Comprehensive AD LDS (ADAM) Recovery Options ............... 8
- Granular, Selective Restore ........................................... 8
- Comprehensive Group Policy Recovery Options ................... 9
- Centralized Remote Administration .................................. 9
- Cloning a Production Domain Controller to a Test Lab ....... 9
- Audit of Objects and Operations ..................................... 9
- Management Shell ...................................................... 10
- Scheduling and Automation .......................................... 10
- Scalability and Performance ......................................... 11
- Rapid Economic Justification ......................................... 11
- Virtual Snapshots of Physical Computers ......................... 12
- Simplified Restoration of an Active Directory Forest ........... 12
- Granular, Domain-Level Recovery ................................... 12
- Automation for Manual Operations ................................... 12
- Remote Quarantine ..................................................... 12
- Simultaneous System Recovery ....................................... 13
- Support for Restoring Domain Controllers Using Dcpromo ... 13
- Recovery Pauses ......................................................... 13
- Recovery Plan ............................................................ 13
- Running Custom Scripts ............................................... 14

### TECHNICAL OVERVIEW

15

- Creating Backups ....................................................... 15
  - Backup Encryption .................................................. 16
  - Creating Unpacked Backups ...................................... 16
  - Creating Differential Backups .................................... 16
  - Using Third-Party Backups ....................................... 16
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CROSS-DOMAIN BACKUP OF GROUP MEMBERSHIPS</td>
<td>16</td>
</tr>
<tr>
<td>CONSIDERATIONS FOR ACTIVE DIRECTORY BACKUP</td>
<td>17</td>
</tr>
<tr>
<td>BACKUP AGENT</td>
<td>18</td>
</tr>
<tr>
<td>SEPARATE CREDENTIALS FOR BACKUP AGENT</td>
<td>18</td>
</tr>
<tr>
<td>USING PREINSTALLED BACKUP AGENT</td>
<td>19</td>
</tr>
<tr>
<td>RECOVERING ACTIVE DIRECTORY</td>
<td>19</td>
</tr>
<tr>
<td>ACTIVE DIRECTORY RECOVERY OPTIONS</td>
<td>20</td>
</tr>
<tr>
<td>GRANULAR ONLINE RESTORE</td>
<td>21</td>
</tr>
<tr>
<td>COMPLETE OFFLINE RESTORE</td>
<td>22</td>
</tr>
<tr>
<td>RECOVERING GROUP POLICY</td>
<td>23</td>
</tr>
<tr>
<td>GROUP POLICY RESTORE</td>
<td>24</td>
</tr>
<tr>
<td>COMPARISON REPORTS</td>
<td>24</td>
</tr>
<tr>
<td>DEPLOYING RECOVERY MANAGER FOREST EDITION</td>
<td>26</td>
</tr>
<tr>
<td>DEPLOYING FOREST RECOVERY AGENT</td>
<td>27</td>
</tr>
<tr>
<td>CREATING A RECOVERY PROJECT</td>
<td>27</td>
</tr>
<tr>
<td>NEW RECOVERY PROJECT WIZARD</td>
<td>28</td>
</tr>
<tr>
<td>TESTING YOUR RECOVERY PROJECT</td>
<td>29</td>
</tr>
<tr>
<td>SELECTING BACKUPS TO BE USED FOR RECOVERING DOMAIN CONTROLLERS</td>
<td>29</td>
</tr>
<tr>
<td>FOREST RECOVERY METHODS</td>
<td>29</td>
</tr>
<tr>
<td>METHOD 1: RESTORE AS MANY DCs AS POSSIBLE FROM BACKUPS</td>
<td>29</td>
</tr>
<tr>
<td>METHOD 2: RESTORE ONE DC FROM BACKUP FOR EACH DOMAIN</td>
<td>30</td>
</tr>
<tr>
<td>RECOVERING AN ACTIVE DIRECTORY FOREST</td>
<td>31</td>
</tr>
<tr>
<td>LICENSING</td>
<td>31</td>
</tr>
<tr>
<td>PERMISSIONS REQUIRED TO USE THE APPLICATION</td>
<td>31</td>
</tr>
<tr>
<td>CONSOLE ACCOUNT</td>
<td>31</td>
</tr>
<tr>
<td>DOMAIN CONTROLLER CONNECTION ACCOUNT</td>
<td>31</td>
</tr>
</tbody>
</table>
Intended Audience

This document has been prepared to assist you in becoming familiar with Recovery Manager for Active Directory Forest Edition. The Product Overview contains the information required to install and use Recovery Manager for Active Directory Forest Edition. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>CONVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.</td>
</tr>
<tr>
<td>Bolded text</td>
<td>Interface elements that appear in Quest Software products, such as menus and commands.</td>
</tr>
<tr>
<td>Italic text</td>
<td>Used for comments.</td>
</tr>
<tr>
<td>Bold Italic text</td>
<td>Used for emphasis.</td>
</tr>
<tr>
<td>Blue text</td>
<td>Indicates a cross-reference. When viewed in Adobe® Reader®, this format can be used as a hyperlink.</td>
</tr>
<tr>
<td></td>
<td>Used to highlight additional information pertinent to the process being described.</td>
</tr>
<tr>
<td></td>
<td>Used to provide Best Practice information. A best practice details the recommended course of action for the best result.</td>
</tr>
<tr>
<td></td>
<td>Used to highlight processes that should be performed with care.</td>
</tr>
<tr>
<td>+</td>
<td>A plus sign between two keystrokes means that you must press them at the same time.</td>
</tr>
<tr>
<td></td>
<td>A pipe sign between elements means that you must select the elements in that particular sequence.</td>
</tr>
</tbody>
</table>
About Quest Software, Inc.

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to www.quest.com.

Contacting Quest Software

Email info@quest.com

Mail
Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Web site www.quest.com

Refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

• Quickly find thousands of solutions (Knowledgebase articles/documents).
• Download patches and upgrades.
• Seek help from a Support engineer.
• Log and update your case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf.

Note: This document is only available in English.
About Recovery Manager for Active Directory Forest Edition

Recovery Manager Forest Edition is designed to recover the entire Active Directory forest or specific domains in the forest. The use of Recovery Manager Forest Edition helps you to minimize the downtime caused by the corruption or improper modification of Active Directory forest and data.

Recovery Manager Forest Edition simplifies and automates the process of Active Directory forest or domain recovery. Recovery Manager Forest Edition automates the manual tasks involved in the recovery, remotely quarantines corrupt domain controllers, and restores domain controllers to speed up the overall recovery and restore business operation quickly.

Recovery Manager for Active Directory Forest Edition is based on patent-pending technology.
Features and Benefits

Recovery Manager for Active Directory Forest Edition improves the availability of network environments by providing remote, automated backup management and data restoration for the recovery of Active Directory, AD LDS (ADAM), and Group Policy.

Recovery Manager Forest Edition allows for quick, online recovery of data. In enterprise-scale network environments, it offers a comprehensive, easy-to-implement solution, including:

- Online, selective restoration of Active Directory, AD LDS (ADAM), and Group Policy data
- Fast, remotely managed recovery of Active Directory, AD LDS (ADAM), and Group Policy
- Centralized, remote creation and management of System State backups
- Active Directory, AD LDS (ADAM), or Group Policy comparison reporting and troubleshooting

Recovery Manager Forest Edition simplifies and automates the process of preparing for and recovering from a disaster such as the corruption of directory object data. Such disasters could be caused by hardware or software failures, or by erroneous changes introduced into Active Directory due to human error.

Recovery Manager Forest Edition includes advanced directory management options that enable the recovery of Active Directory and Group Policy with minimal downtime. It offers the following features and benefits.

Comprehensive Active Directory Recovery Options

Recovery Manager Forest Edition provides easy-to-use, wizard-based procedures for recovering Active Directory. Individual Active Directory objects, a single subtree, or the entire Active Directory database can be restored remotely, without the need for an administrator to be physically present at the domain controllers involved in the restoration.

Comprehensive AD LDS (ADAM) Recovery Options

Recovery Manager Forest Edition provides easy-to-use, wizard-based procedures for recovering AD LDS (ADAM). Individual AD LDS (ADAM) objects or a single subtree can be restored remotely, without the need for an administrator to be physically present at the computers hosting AD LDS (ADAM) instances involved in the restoration.

Granular, Selective Restore

To achieve near-zero downtime when restoring Active Directory or AD LDS (ADAM) data, Recovery Manager Forest Edition offers selective, online restore. Individual objects or object attributes can be selected in a backup and then restored to Active Directory or AD LDS (ADAM) without affecting other objects or attributes. Using the granular restore feature, objects that were inadvertently deleted or modified can be recovered in a few minutes. Unlike conventional alternatives, it is not necessary to restore the entire Active Directory or AD LDS (ADAM) database, nor is it necessary to restart domain controllers or AD LDS (ADAM) service.

As granular restore can be done online, the domain controller is never unavailable to users. Online restore function greatly reduces the restore time, thus eliminating the costs associated with downtime.
One more valuable characteristic of granular online restore is the unattended restoration of linked attributes, such as the Member Of attribute. When recovering a user object with granular online restore, you do not need to worry about group memberships: Recovery Manager Forest Edition ensures that the restored object is a member of the proper groups.

**Comprehensive Group Policy Recovery Options**

One of the key features of Recovery Manager Forest Edition is the ability to quickly recover individual Group Policy objects using a normal backup of a domain controller’s System State, eliminating the need for special, Group Policy-related backups. By providing straightforward, wizard-driven procedures for Group Policy restoration, Recovery Manager Forest Edition makes it easy to recover Group Policy information and recoup the time spent configuring Group Policy. Individual Group Policy objects, along with Group Policy links and permission settings can be restored remotely, without the need for an administrator to be present at the domain controllers on which the restore is being performed, and without the need to restart domain controllers.

**Centralized Remote Administration**

Recovery Manager Forest Edition makes it possible to create, update, and apply Active Directory backups remotely across an entire network. It can be installed on an administrator’s workstation, allowing all operations to be performed from a single, central location. These operations include the creation, update, and storage of backups, as well as the restoration of Active Directory and Group Policy data from a backup.

Backups created with Recovery Manager Forest Edition can be stored in a central location, at several locations on a distributed network, or on selected computers with physically restricted access. Access to Active Directory backups can be restricted using backup encryption along with security mechanisms provided by the operating system.

**Cloning a Production Domain Controller to a Test Lab**

Recovery Manager Forest Edition provides the Clone Wizard that helps you to clone a domain controller from a backup created with Recovery Manager to a non-production standalone computer. The wizard ensures that the cloned domain controller will properly work, even on dissimilar hardware.

The Clone Wizard is most helpful if you want to clone an existing source domain controller to use the cloned computer as a test lab.

> Do not use the Clone Wizard to recover a production domain controller or add a new production domain controller to your domain. For these purposes, you can use the Repair Wizard and the Install from Media feature provided in Windows.

**Audit of Objects and Operations**

To assist with troubleshooting lost or changed Active Directory objects, AD LDS (ADAM) objects, or Group Policy objects, Recovery Manager Forest Edition provides the ability to compare the current state of individual objects in Active Directory or AD LDS (ADAM) with that in an Active Directory or AD LDS (ADAM) backup. This functionality is particularly useful for locating the source of and resolving problems resulting from the deletion or modification of critical objects.
During a restore operation, Recovery Manager Forest Edition allows for the creation of comparison reports, which present the changes that have occurred in Active Directory or AD LDS (ADAM) since the last backup, without actually applying changes to Active Directory or AD LDS (ADAM). Such reports show the objects that were deleted or modified since the backup was made. In addition, they show the properties of directory objects and settings of Group Policy objects that would change during the operation. An administrator can then review these changes and decide whether to apply them.

The Recovery Manager Forest Edition comparison reports on Active Directory objects can provide information on who (which user account) modified the objects being reported. This functionality is based on the auditing capability provided by ChangeAuditor for Active Directory, an award-winning Quest Software product that helps to proactively track, audit, report, and alert on vital Active Directory changes—in real time and without the overhead of native auditing.

You can find out more about Quest ChangeAuditor for Active Directory at http://www.quest.com/changeauditor-for-active-directory.

Management Shell

The Recovery Manager Forest Edition Management Shell, built on Microsoft Windows PowerShell technology, provides a command-line interface that enables automation of backup/recovery-related administrative tasks. With this Management Shell, administrators can manage Computer Collections, backup/recovery sessions, compare, and start backup/recovery jobs.

The Recovery Manager Forest Edition Management Shell command-line tools (cmdlets), like all the Windows PowerShell cmdlets, are designed to deal with objects—structured information that is more than just a string of characters appearing on the screen. The cmdlets do not use text as the basis for interaction with the system, but use an object model that is based on the Microsoft .NET platform. In contrast to traditional, text-based commands, the cmdlets do not require the use of text-processing tools to extract specific information. Rather, you can access portions of the data directly by using standard Windows PowerShell object manipulation commands.

Scheduling and Automation

Recovery Manager Forest Edition enables administrators to schedule the creation of backups. This functionality helps reduce the network workload and can save many hours of the administrators’ valuable time. When scheduling the creation of backups, Recovery Manager Forest Edition relies on Task Scheduler—the native Windows scheduler service. A unified graphical interface and wizard assistance provide easy access to the backup scheduling features of Recovery Manager Forest Edition.

Recovery Manager Forest Edition makes the creation of backups a straightforward task. Once the backup creation options and scheduling are set up, the backup creation process becomes an automatic, unattended operation.
Scalability and Performance

Recovery Manager Forest Edition offers scalability and support for large, multi-domain environments. It provides excellent performance, creates backups for multiple computers in parallel, and is easily scalable to service additional domain controllers. Depending on their roles, locations, or other criteria established by an administrator, serviced domain controllers can be logically grouped into easy-to-manage Computer Collections.

Recovery Manager Forest Edition employs agents when creating or applying backups. In this way, scalability is improved and overhead network traffic is decreased because agents compress the data before sending it over network links, and create backups for multiple domain controllers in parallel.

Rapid Economic Justification

Recovery Manager Forest Edition offers rapid economic justification in Windows network environments, by dramatically decreasing the downtime and administrative overhead involved in Active Directory, AD LDS (ADAM), and Group Policy recovery.
Virtual Snapshots of Physical Computers

This version of Recovery Manager for Active Directory Forest Edition makes it possible to convert all physical computers in a Computer Collection (domain controllers or AD LDS (ADAM) hosts) to virtual machines.

A virtual snapshot created with Recovery Manager Forest Edition is a complete point-in-time image of the source physical computer. The snapshot contains all the data stored on the source physical computer, including folders, files, installed applications, Active Directory data, and AD LDS (ADAM) data.

A virtual snapshot can be used to deploy a virtual machine in a virtualization system supported by Recovery Manager Forest Edition, such as VMware ESX or Microsoft Hyper-V. The deployed virtual machine will include all the data that was stored on the source physical computer at the time when the virtual snapshot was taken.

With virtual snapshots, you can create a complete virtual copy of your Active Directory or AD LDS (ADAM) environment for testing or production purposes.

Simplified Restoration of an Active Directory Forest

With the Forest Recovery Console, you can remotely manage the recovery of domain controllers in your forest from one central location.

Granular, Domain-Level Recovery

Recovery Manager Forest Edition makes it possible to selectively recover domains in an Active Directory forest. Instead of restoring the entire forest, you can run the restore operation on one or more domains the forest includes. This method is useful if you have located the domains that include dangerous or unwanted data and want to selectively recover them. Before you proceed with the selective recovery of domains, it is highly recommended you make absolutely sure the dangerous or unwanted data is not replicated to other domains in the forest.

To selectively recover domains, you can either create a new recovery project that will only include the domains you want to recover, or open an existing project for the entire forest, and then select the domains you want to recover in that project.

Automation for Manual Operations

Using native tools to recover a forest requires numerous and lengthy manual steps repeated on each domain controller in the forest. This process results in a very slow and tedious recovery prone to human error. Recovery Manager Forest Edition automates those numerous manual steps not only saving vast amounts of time but also eliminating the risk of human error.

Remote Quarantine

Recovery Manager Forest Edition automatically and remotely quarantines corrupt domain controllers so that those individual domain controllers won’t replicate with the newly restored environment.
Simultaneous System Recovery

All domain controllers in your forest or domain can be restored simultaneously from one centralized location, using backups created with Recovery Manager Forest Edition, eliminating the need to manually interface with each domain controller separately saving a significant amount of time and effort.

Support for Restoring Domain Controllers Using Dcpromo

Recovery Manager Forest Edition can restore selected DCs from backups and then recover the remaining DCs by demoting them and reinstalling Active Directory using the Active Directory Installation Wizard (DCPromo.exe). This allows for a recovery methodology that mirrors the prescriptive guidance laid out the forest recovery method recommended by Microsoft in the Planning for Active Directory Forest Recovery whitepaper.

Recovery Pauses

A recovery pause allows you to automatically suspend the recovery of one or more domain controllers immediately before a certain recovery stage begins for those domain controllers. You can then manually resume the recovery of these domain controllers from the point where it was suspended (paused).

For example, you can temporarily suspend the recovery of particular domain controllers to take a manual action outside of Recovery Manager Forest Edition.

⚠️ Recovery pauses cannot be used to prioritize the recovery of certain critical domain controllers, domains, or sites in your Active Directory forest.

For a recovery project, you can create multiple pauses, each having different settings. For each recovery pause, you can define the domain controllers to which the pause will apply and specify a recovery stage before which you want to activate the pause.

Recovery Plan

Recovery Plan is designed to improve the overall transparency of the recovery process. The plan is a detailed recovery process roadmap you can generate and view for the current recovery project in the Forest Recovery Console. The plan provides an overview of every single recovery stage and operation the DCs in the project will go through after you start the recovery, thus allowing you to gain a better understanding and control of every aspect of the forest or domain recovery.

Generating and reviewing the recovery plan before you proceed with the recovery helps you identify and if necessary avoid any unwanted recovery actions by adjusting the project settings appropriately. You can also print out the generated project recovery plan or export it to a number of presentation formats provided by Microsoft SQL Server Reporting Services (SRSS) on which the Recovery Plan feature builds, such as PDF, XML, CSV, TIFF, and Excel.
Running Custom Scripts

You can configure Recovery Manager Forest Edition to automatically run custom scripts on the Recovery Manager Forest Edition computer before, after, or during the recovery operation.

This version of Recovery Manager Forest Edition is supplied with the Microsoft Windows Script File (.wsf) file that serves as a template where you can insert your custom scripts written in the VBScript or JScript language.

The .wsf file has a number of XML elements where you can insert your scripts. Depending on the XML element where you insert it, your script will run:

- Before the recovery operation starts in the current project.
- Each time before the restore from backup operation starts for a domain controller in the current project.
- After the restore from backup operation completes for all domain controllers in the current project.
- Before the reinstall Active Directory operation starts in the current project.
- Each time before the reinstall Active Directory operation starts for a domain controller in the current project.
- Each time the reinstall Active Directory operation completes for a domain controller in the current project.
- After the recovery operation completes in the current project.
Technical Overview

Recovery Manager Forest Edition performs the following functions:

- Regular backup of domain controllers’ System State across a network, including the Active Directory database and SYSVOL, and maintenance of one or more secure repositories containing the backed-up System State data.
- Wizard-driven, remotely administered restoration of Active Directory object data and Group Policy information from a point-in-time backup.
- Active Directory, AD LDS (ADAM), and Group Policy comparison reporting, troubleshooting, and investigation.

Creating Backups

Recovery Manager Forest Edition provides the facility to create backups of the System State data on domain controllers, including the Active Directory database.

Recovery Manager Forest Edition allows you to create System State backups for any Active Directory domain controller available on the network. Backup creation is a straightforward task that can be performed on a regular basis without interrupting the operation of the domain controller.

Recovery Manager Forest Edition lets you organize domain controllers into collections, and establish a backup scheduling frequency and “allowed hours” during which the backup process may run. Based on the frequency of updates to the directory data store, you can configure a backup schedule for each collection.

Depending on the requirements of your enterprise, you can configure a retention policy to specify how many backups are retained: for example, all saved backups or a number of the most recent backups. Different policy settings can be specified for different domain controller collections.

It is not necessary to maintain a single, centralized repository of backups: several repositories, perhaps based on the site topology, can make your deployment more WAN-friendly. To minimize bandwidth consumption, Recovery Manager Forest Edition employs agents that compress the data to be backed up, before sending it across the network.
Recovery Manager Forest Edition uses the Microsoft Tape Format (MTF) for backup files. Therefore, MTF-compliant backup applications can catalog the backup files and restore data backed up with Recovery Manager Forest Edition. For example, backed up data can be restored with the Windows backup tools, if no compression and encryption is used during the backup creation.

**Backup Encryption**

Recovery Manager Forest Edition allows backups to be encrypted and protected with a password, to prevent unauthorized access.

For backup encryption, the product uses Microsoft’s implementation of the RC4 algorithm from RSA, Inc. (Microsoft RSA Base Provider), with the maximum cipher strength. The use of the Microsoft RSA Base Provider ensures that backups are encrypted with 128-bit cipher strength.

**Creating Unpacked Backups**

You can have Recovery Manager Forest Edition keep unpacked Active Directory or AD LDS (ADAM) backups in any appropriate location on your network.

Unpacked backups can be reused for subsequent starts of the Online Restore Wizard or Group Policy Restore Wizard. The use of unpacked backups accelerates the backup data preparation step of those wizards, because the unpacking process may be a lengthy operation.

**Creating Differential Backups**

Recovery Manager Forest Edition makes it possible to create differential backups of domain controllers included in Computer Collections. A differential backup saves the Active Directory database changes that have occurred since the last full backup. The data stored in a differential backup includes only the transaction log files up to the time of backup. This feature allows you to decrease the size of the backup files stored in the backup registration database.


**Using Third-Party Backups**

Recovery Manager Forest Edition makes it possible to use Active Directory or AD LDS (ADAM) backups created with third-party backup tools. Before using this feature, unpack the backup to an alternate location with the corresponding third-party backup tool, and then register the database file (ntds.dit or adamntds.dit) using the Online Restore Wizard or Online Restore Wizard for AD LDS (ADAM), respectively.

**Cross-Domain Backup of Group Memberships**

When backing up Global Catalog servers, you have the option to force Recovery Manager Forest Edition to collect group membership information from all domains within the Active Directory forest. This option ensures that group membership spanning multiple domains is fully backed up.
It is recommended that you restore objects from Global Catalog backups that were created with this option. Otherwise, restored objects may not retrieve their membership in some local groups, because even Global Catalog servers do not store full information about group memberships. For example, information about membership in domain local groups is only stored in the home domains of those groups.

**Considerations for Active Directory Backup**

In an Active Directory environment, each domain controller maintains its own Active Directory database. Therefore, a backup of the Active Directory database is domain controller-specific. To completely back up Active Directory, you must back up the directory database on every domain controller.

To restore deleted or corrupted objects, it is recommended to back up at least two domain controllers for each domain for redundancy. If you intend to restore cross-domain group membership information, then it is also necessary to back up a global catalog server.

Another reason for backing up the directory database on every domain controller is loose consistency. Replication of changes made to Active Directory does not occur immediately. The replication process first accumulates all changes, and then provides them to the participating domain controllers. As a result, the directory database on any domain controller is normally in a state of loose consistency. The directory object data on individual domain controllers differs to some extent, given that replication updates are either in transit between domain controllers, or waiting to be initiated.

The age of the backup must also be considered. Active Directory prevents the restoration of data older than the "tombstone lifetime"—a setting specified in Active Directory. Because of this, an Active Directory backup should be created at least once within the tombstone lifetime. However, it is strongly recommended that backups of the directory database be created more often than this.
Backup Agent

Recovery Manager Forest Edition employs Backup Agent to back up remote domain controllers. This is because some backup APIs provided by the operating system cannot be used to access a target domain controller from the Recovery Manager console. Therefore, Backup Agent must be installed on a remote domain controller in order to gain access to its specific objects. Recovery Manager automatically installs Backup Agent before starting a backup, and removes it upon the completion of backup operation.

The figure above illustrates how Recovery Manager employs Backup Agent when creating backups. Backup Agent is installed on domain controllers DC1 and DC2. Backup Agent compresses the local data and sends it to the computer running Recovery Manager, which in turn transfers the compressed data to the backup repository (Central Storage Location).

Since Backup Agent compresses the data before sending it over the network, the network load is decreased significantly. The average compression ratio is 7:1. The use of Backup Agent also provides increased scalability and performance, by allowing the creation of backups on multiple domain controllers in parallel.

Separate Credentials for Backup Agent

Recovery Manager allows to run Backup Agent in the security context of a specific user account. Since Recovery Manager needs administrative access to the domain controller in order to run Backup Agent, the account under which Recovery Manager is running must belong to the Administrators group on that domain controller, providing administrative access to the entire domain. If Recovery Manager cannot be started under such an account, separate credentials (user logon name and password) should be specified, so that Backup Agent is run under an account that has sufficient privileges.
Using Preinstalled Backup Agent

Recovery Manager allows you to back up Computer Collections using Backup Agent manually preinstalled on each target domain controller. This method enables you to

- Perform a backup operation without having domain administrator privileges. It is sufficient if Recovery Manager runs under a backup operator’s credentials.
- Reduce network traffic when backing up the Computer Collection.
- Back up domain controllers in domains that have no trust relationships established with the domain in which Recovery Manager is running, solving the so-called “no trust” problem.

Recovering Active Directory

Recovery Manager enables the recovery of a portion of the directory or the entire directory, in the event of corruption or inadvertent modification. The granular, object-level, online restore may also be used to undelete directory objects. These powerful, security-sensitive functions of Recovery Manager should only be performed by highly trusted directory administrators.

If certain objects are inadvertently deleted or modified in Active Directory, they can be restored from a normal backup of a domain controller’s System State, without restarting the domain controller or affecting other objects. If the Active Directory database on a particular domain controller has been corrupted, the entire database can be restored from a System State backup created for that domain controller. All the restore operations are administered remotely.

Recovery Manager offers the following restore methods:

- **Granular Online Restore.** Allows you to select Active Directory objects from a backup, and then restore them to Active Directory. This method allows for the recovery of individual Active Directory objects, and selected attribute values in Active Directory objects, with the least amount of administrative effort.

- **Complete Offline Restore.** Restarts the target domain controller in Directory Services Restore mode, restores the Active Directory database from the selected backup, and then restarts the domain controller in normal operational mode. This method enables the recovery of the entire Active Directory database on a domain controller, and is most useful when recovering from database corruption.
Active Directory Recovery Options

Recovery Manager enables the fast recovery of Active Directory from a disaster. The flowchart below indicates the most suitable recovery method depending on the type of disaster, which could be data corruption or database corruption.

Data corruption occurs when directory objects have been inadvertently deleted or modified, and the deletion or modification has replicated to other domain controllers within the environment.

Database corruption refers to a situation in which an Active Directory failure prevents a domain controller from starting in normal mode, or a hardware problem such as hard disk corruption on a domain controller.

Recovery Manager offers two methods for restoring Active Directory object data on a domain controller:

- **Granular Online Restore**
- **Complete Offline Restore**

Granular Online Restore is the most advanced method, allowing you to restore individual directory objects from a backup, without restarting the target domain controller or affecting other directory objects.

Complete Offline Restore only allows you to restore the entire Active Directory database on a domain controller while Active Directory is offline. To take Active Directory offline, Recovery Manager restarts the domain controller in Directory Services Restore Mode (DSRM), resulting in a period of downtime. In addition, Complete Offline Restore affects all directory objects on the target domain controller, which may result in the loss of some of the most recent updates.

All restore operations are remotely administered, so there is no need for an administrator to be physically present at the domain controller. In most cases, it will not be necessary to shut down the domain controller in order to perform the restore: it remains online and functional throughout the recovery.
Granular Online Restore

To achieve near-zero downtime when recovering Active Directory, Recovery Manager provides the Granular Online Restore method. Two options are available with this method:

- **Compare, Restore, and Report Changes in Active Directory.** With this option, you can restore particular objects from a backup, and select the necessary objects based on a per-attribute comparison of the objects in a backup with those in Active Directory. Comparison reports are also available.

- **Compare Two Backups and Report the Differences.** With this option, you can make a per-attribute comparison of the objects in two Active Directory backups. Comparison reports allow you to view the object modifications made in the period between the backups.

The Granular Online Restore method allows you to retrieve individual directory objects from a backup, and then restore them to a domain controller. The operation can be performed on any domain controller that can be accessed remotely. In addition, Granular Online Restore does not require you to restart the target domain controller, nor does it affect any directory objects that are not selected for recovery.

In addition to selectively restoring individual Active Directory objects, the Granular Online Restore method allows you to selectively restore individual attributes of objects in Active Directory, such as the User Password, Group Membership, or User Certificate attributes of a User object. The ability to restore selected attributes ensures that valuable changes, made to Active Directory objects since the time the backup was created, are not overridden. This provides the flexibility to efficiently resolve potential problems that may result from the improper modification of individual attributes of Active Directory objects.

Granular Online Restore should be used in situations where important object data has been inadvertently deleted or changed in Active Directory, and the changes have been propagated to other domain controllers. To recover from such an event, you can carry out a Granular Online Restore to Active Directory using a backup that was created before the objects in question were deleted or modified.

After Recovery Manager completes a Granular Online Restore on the target domain controller, the restored objects are replicated to the other domain controllers via the normal replication process. Given that the objects recovered by a Granular Online Restore have a higher version number, recently deleted or modified object data is ignored during replication.

Granular Online Restore allows you to roll back changes made to Active Directory, and return individual directory objects and attributes to the state they were in when the backup was created. It is important to note that a Granular Online Restore only affects the objects and attributes selected for recovery. All other objects remain unchanged in Active Directory. Furthermore, if the value of an attribute in Active Directory is identical to the value it has in the backup, the Granular Online Restore does not attempt to change the attribute.

A Granular Online Restore is especially useful when you need to recover some directory objects in a short period. For example, suppose a user account is accidentally deleted from Active Directory, but exists in a backup. To recover that user account, you can perform a Granular Online Restore, selecting the user account from the backup. The selected user account is restored to Active Directory with the same properties and permissions that it had when the backup was created. No other user accounts are affected.
Undeleting (Reanimating) Objects

With Recovery Manager Forest Edition, you can selectively recover deleted Active Directory objects by undeleting (reanimating) them. To undelete (reanimate) an object, Recovery Manager Forest Edition fully relies on the functionality provided by Active Directory, therefore to use this method you need no Active Directory backups. Note that you can only undelete objects in an Active Directory forest whose functional level is higher than Windows 2000.

The result of the undelete operation performed on an object depends on whether Microsoft’s Active Directory Recycle Bin feature is enabled or disabled in your environment. Microsoft’s Active Directory Recycle Bin is a new feature that first appeared in the Windows Server 2008 R2 operating system. For more information on Microsoft’s Active Directory Recycle Bin feature, see What’s New in AD DS: Active Directory Recycle Bin (http://go.microsoft.com/fwlink/?LinkId=141392).

In an Active Directory environment where Microsoft’s Active Directory Recycle Bin feature is not supported or disabled, a deleted object is retained in Active Directory for a specified configurable period of time that is called tombstone lifetime. A deleted object becomes a tombstone that retains only a partial set of the object’s attributes that existed prior to deletion. During that period, you can use Recovery Manager Forest Edition to undelete (reanimate) the object. Performing the undelete operation on the object will only recover the object’s attributes retained in the tombstone.

When an object is deleted in a forest where Microsoft’s Active Directory Recycle Bin feature is enabled, the object goes through the following states:

- **State 1: Deleted.** The object retains all its attributes, links, and group memberships that existed immediately before the moment of deletion. The object remains in this state for a specified configurable period of time that is called deleted object lifetime. When the applicable deleted object lifetime period expires, the object is transferred to the next state—"recycled".

  While an object remains in the "deleted" state, you can use Recovery Manager to undelete (reanimate) the object with all its attributes, links, and group memberships that existed immediately before the moment of deletion.

  Alternatively, you can authoritatively restore the object to its backed-up state from a backup created with Recovery Manager Forest Edition.

  If necessary, you can use Recovery Manager Forest Edition to override the applicable deleted object lifetime setting and manually change a deleted object’s state from “deleted” to “recycled” by using a cmdlet provided by the Recovery Manager Forest Edition Management Shell.

- **State 2: Recycled.** After a deleted object is transferred to the “recycled” state, most of the object’s attributes are purged (stripped away), and the object retains only those few attributes that are essential to replicate the object’s new state to other domain controllers in the forest. The object remains in the recycled state for a specified configurable period of time that is called recycled object lifetime. Recycled objects are not recoverable, but you can use the Deleted Objects container provided by Recovery Manager Forest Edition to view a list of those objects in a domain.

Complete Offline Restore

You can use Complete Offline Restore to restore the entire Active Directory database from backup media without reinstalling the operating system or reconfiguring the domain controller. The restore can be performed on any domain controller that can be accessed remotely. By default, this operation restores all directory objects on the target domain controller non-authoritatively. This means that the restored data is then updated via normal replication. A non-authoritative restore is typically used to restore a domain controller that has completely failed due to hardware or software problems.
A Complete Offline Restore also allows you to mark individual objects for authoritative restore. However, given that the Granular Online Restore process provides the same functionality with much less effort and overhead, it is the recommend method for restoring individual objects to Active Directory.

During the final stage of a Complete Offline Restore, the recovered domain controller is restarted in normal operational mode. Normal replication then updates the domain controller with all changes not overridden by the authoritative restore. It is important to note that until the replication update has completed, some of the directory object data held on the recovered domain controller may be unreliable. Therefore, execution of a Complete Offline Restore may result in additional downtime due to replication delays.

There is one other consideration to make when performing a non-authoritative restore. The restored domain controller may lose information about the directory updates that were made after it was backed up. For example, suppose that some directory objects were added or modified on the domain controller after the backup was created, but the new objects or modifications were not replicated to other domain controllers due to network problems. In this case, when the domain controller is restored, the new objects or modifications will be lost, because they were never replicated to other domain controllers, and therefore cannot be applied to the restored domain controller.

**Recovering Group Policy**

Recovery Manager enables the recovery of Group Policy data from corruption or inadvertent modification, which can be caused by either hardware failure or human error.

**Group Policy Recovery**

If specific Group Policy objects or links are inadvertently deleted or modified, they can be restored from a normal backup of a domain controller’s System State, without restoring the entire System State or Active Directory, restarting the domain controller, or affecting other objects.
Recovery Manager includes the following options for Group Policy recovery:

- **Policy Settings Restore.** If the Group Policy object was modified since the backup was created, this option restores all policy settings to the state they were in at the time of the backup. If the Group Policy object was deleted, this option creates a new object with the same name and policy settings as the backed-up object.

- **Security Settings Restore.** Restores all security information contained in the Group Policy object. As a result, all users and security groups receive the access permissions that were specified in the Group Policy object at the time it was backed up.

- **GPO Links Restore.** Restores all links associated with the Group Policy object to the state they were in at the time the backup was created. As a result, the object is once again used by the same sites, domains, and organizational units that were linked to it at the time the backup was created.

- **Comparison Reports.** Shows whether Group Policy object was deleted or modified since the backup time.

You can use any combination of these options. For example, suppose some links to a Group Policy object are accidentally deleted. If your backup contains an outdated version of the Group Policy object, you can restore only the links, without restoring the policy settings or security settings.

**Group Policy Restore**

To eliminate downtime when recovering Group Policy, Recovery Manager provides the Group Policy Restore method. This method allows individual Group Policy objects to be restored to a selected domain controller. The operation can be performed on any domain controller that can be accessed remotely. Using this method, domain controllers do not need to be restarted, and only those objects selected for recovery are affected.

For this type of restore, it is not necessary to create any special backups; you may use any regular backup of a domain controller's System State.

A Group Policy Restore is particularly helpful when critical Group Policy objects or links have been inadvertently deleted or changed. To recover from such situations, you may carry out a Group Policy Restore to a domain controller using a System State backup that was created before the objects in question were deleted or modified.

Group Policy Restore allows you to roll back changes made to Group Policy information, and return individual Group Policy objects to the state they were in when the backup was created. It is important to note that a Group Policy Restore only affects the object selected for recovery, and optionally, the links to that object. Any objects that are not involved in the operation remain unchanged in the domain.

**Comparison Reports**

Recovery Manager provides comparison reports to assist with isolating deletion or changes to Active Directory or AD LDS (ADAM), and troubleshooting the resulting problems. These reports are based on per-attribute comparisons of Active Directory, AD LDS (ADAM), or Group Policy objects selected from a backup, with their counterparts in Active Directory, AD LDS (ADAM), or another backup.

By comparing the state of the directory objects or Group Policy objects in Active Directory with those in a backup, comparison reports improve the efficiency of recovering objects, by allowing you to specify precisely which objects should be restored.
By showing the changes that would be made to Active Directory or AD LDS (ADAM) during a restore operation, comparison reports help to highlight possible side effects that could result from restoring data. If such side effects are indicated in the report, you may then reconsider whether to apply the changes to the “live” directory data.

Comparison reports may also be used to monitor changes that occurred in Active Directory or AD LDS (ADAM) since the backup was created, or within the period between two backups. Comparison reports assist with troubleshooting Active Directory, and resolving problems that may result from the deletion of critical objects in Active Directory. The reports also help you monitor changes made to Active Directory or AD LDS (ADAM) by third-party applications.

The ability to compare the current state of objects in Active Directory or AD LDS (ADAM) with their state in a backup helps when troubleshooting problems that may result from the deletion or modification of a user account or an Organizational Unit, or modification of more critical objects. Comparison reports show whether critical objects were deleted or modified since a backup was made.

The deletion of critical objects such as a domain controller’s computer account or the “NTDS Settings” object is one of the most common causes of Active Directory problems. For more information about the impact of and recovery from these problems, please refer to the Microsoft article 298450 “Deletion of Critical Objects in Active Directory in Windows 2000 and Windows Server 2003.”

Other critical, equally sensitive objects include all objects in the System container, such as FRS subscription objects, trusted domain objects (TDO), and DNS objects. By comparing the current state of objects in the System container with the state of the objects in a backup, it is possible to isolate problems that result from the absence or incorrect modification of critical objects.

Recovery Manager serves as a valuable tool when implementing a change management process. The importance of testing changes to Active Directory is paramount, whether you are changing configurations, installing new software, or implementing service packs and patches. The product has the ability to report changes, and if necessary, roll back changes made to Active Directory. This improves the effectiveness of testing application deployment scenarios in a laboratory environment, and monitoring changes made to Active Directory by third-party applications.
Deploying Recovery Manager Forest Edition

The following diagram shows the Recovery Manager Forest Edition deployment:

In this diagram, Recovery Manager Forest Edition is installed on Application Server.

Recovery Manager Forest Edition employs Forest Recovery Agent to remotely restore Active Directory on target domain controllers. Therefore, Forest Recovery Agent must be installed on each domain controller in the forest to be recovered.

The restoration of Active Directory forest or domain is managed from one centralized location (the Forest Recovery Console), eliminating the need to interface with each domain controller individually.

Recovery Manager Forest Edition can use backups created with Recovery Manager for Active Directory.
Deploying Forest Recovery Agent

Recovery Manager Forest Edition employs Forest Recovery Agent to remotely restore Active Directory on target domain controllers. Therefore, Forest Recovery Agent must be installed on each domain controller in the forest to be recovered.

If Forest Recovery Agent was not installed on a target domain controller before a disaster occurred, Recovery Manager Forest Edition will attempt to automatically install the agent and recover that domain controller.

You have the following options to install Forest Recovery Agent on a target domain controller:

- Have the Forest Recovery Console install Forest Recovery Agent.
- Have the Recovery Manager console install Forest Recovery Agent, if necessary, when you back up a Computer Collection that includes the target domain controller. This method is preferable. For more information see “Backing Up Domain Controllers” in the Recovery Manager Forest Edition User Guide.

Creating a Recovery Project

When planning for Active Directory forest recovery, you should first have a detailed topology map of your forests. The map should list all the information about the domain controllers, such as their names, FSMO roles and backup status, and the trust relationships between them.
Recovery Manager Forest Edition provides the user interface shown below (the Forest Recovery Console) that helps you create recovery projects:

A recovery project is where you manage the recovery of a forest or domain. Each recovery project contains a list of domain controllers to be recovered and their recovery settings (such as recovery method and access credentials). Each recovery project is saved in the project (.frproj) file that contains information about the content and properties of the project. For security reasons, all recovery projects are protected with a password.

**New Recovery Project Wizard**

To facilitate the creation of recovery projects, the application provides the New Recovery Project Wizard. The wizard retrieves the full list of domain controllers in your forest. The New Recovery Project Wizard provides the following options to retrieve the forest infrastructure:

- Connect to any available domain controller in the forest.
- Retrieve the forest infrastructure from an Active Directory backup taken from any domain controller in the forest. This method can be employed in a situation where you cannot retrieve reliable information about the forest infrastructure from a live domain controller due to the extent of the Active Directory failure.
Testing Your Recovery Project

To ensure that you can recover your forest or domain with a minimum downtime, it is recommended you regularly test your recovery project using the test mode feature provided by the Forest Recovery Console.

When testing a recovery project, the application polls domain controllers to be recovered and Forest Recovery Agent installed on those domain controllers. The application verifies whether Forest Recovery Agent is installed and running. The application also ensures that the specified credentials allow

- The Forest Recovery Console to access the domain controllers.
- Forest Recovery Agent to access backup files.

The test results are reported to the Forest Recovery Console user.

The use of the test mode makes the forest recovery and troubleshooting easier, because it allows you to detect the possible problems you might face.

Selecting Backups to Be Used for Recovering Domain Controllers

It is strongly recommended that you restore domain controllers using backups that were taken a few days before the occurrence of the failure. In general, you need to trade off between recentness and safeness of restored data. Choosing a more recent backup recovers more useful data, but it might increase the risk of reintroducing dangerous data into the restored forest. The backups you select must be created at a similar point in time to mitigate the risk of discrepancy after the forest is recovered.

Forest Recovery Methods

Recovery Manager Forest Edition ensures the forest recovery flexibility by supporting the following recovery methods.

Method 1: Restore As Many DCs As Possible from Backups

To use this method, you must have recent and trusted backups for as many DCs as possible in each domain in the forest. These backups must be created at a similar point in time to mitigate the risk of discrepancy after the forest is recovered.

At a high level, Method 1 includes the following stages:

1. Recovery Manager Forest Edition restores as many DCs as possible in each domain from the recent and trusted backups you specify. The more DCs you restore from backups, the faster the forest recovery operation completes.
2. Recovery Manager Forest Edition uses the Active Directory Installation Wizard (Dcpromo.exe) to automatically reinstall Active Directory on the DCs for which no backups are available.
3. The DCs where Active Directory was reinstalled replicate AD data from the DCs restored from reliable backups.
Pros of Method 1

- **Fast recovery of the entire forest.** Since most DCs are simultaneously restored from backups, the forest recovery operation completes faster than in Method 2 (to be discussed later.)
- **Stability of the forest recovery process.** Owing to the large number of backups used, the entire forest is recovered even if the restore of some DCs fails.
- **The original forest infrastructure is retained.** Since many DCs are restored from backups, you can recover the forest to its original pre-failure condition.

Cons of Method 1

- **The risk of reintroducing corrupted or unwanted data is higher than in Method 2.** Because of the large number of backups used in Method 1, you cannot guarantee that corrupted or unwanted data from the backups will not be reintroduced into the recovered forest.

Method 2: Restore One DC from Backup for Each Domain

This recovery method is recommended by Microsoft in the Planning for Active Directory Forest Recovery whitepaper.

To use this method, you must have a recent and trusted backup for one DC in each domain in the forest. These backups must be created at a similar point in time to mitigate the risk of discrepancy after the forest is recovered.

At a high level, this method includes the following stages:

1. Recovery Manager Forest Edition restores one DC in each domain from the recent and trusted backup you specify.
2. Recovery Manager Forest Edition uses the Active Directory Installation Wizard (Dcpromo.exe) to automatically reinstall Active Directory on all other DCs.
3. The domain controllers on which Active Directory was reinstalled replicate AD data from the DCs restored from reliable backups.

Pros of Method 2

- **Recommended by Microsoft.** This recovery method is recommended in the Microsoft’s whitepaper, Planning for Active Directory Forest Recovery.
- **Health of recovery is easier to verify as compared to Method 1.** The limited number of backups used in Method 2 (one backup per each domain) allows you to check them all to make sure the backups do not include any corrupted or unwanted data before the recovery begins.

Cons of Method 2

- **Forest recovery requires significant time to complete.** Method 2 requires more time to complete than Method 1.
- **Recovery of entire domain depends on a successful restore of a single DC.** A successful restore of one DC from a backup is required before Active Directory can be reinstalled on all other DCs within a domain.
- **The original forest infrastructure is not retained.** Because Active Directory is reinstalled on most DCs in the forest, the forest infrastructure cannot be restored to its exact pre-failure state.
Recovering an Active Directory Forest

The Forest Recovery Console allows you to remotely recover domain controllers specified in your recovery project. No operator intervention is required during the recovery, but you should ensure that the recovery settings specified for each domain controller are valid and that domain controllers are running and connected to the network.

When performing the forest recovery operation, the Forest Recovery Console displays the operation progress for each domain controller.

After termination of the forest recovery operation, the application allows you to generate the recovery report that provides detailed information about the forest recovery results including a list of domain controllers that were not recovered. This allows you to adjust the recovery settings and retry the recovery of the failed domain controllers.

If the restore of some domain controllers failed, Recovery Manager Forest Edition performs the following steps to complete the forest recovery:

1. Removes any information about the failed domain controllers from Active Directory.
2. Tries to assign the FSMO roles taken by the failed domain controllers to the recovered (succeeded) domain controllers.
3. Configures some of the recovered domain controllers as global catalog servers, if necessary.

Licensing

Recovery Manager Forest Edition licensing is based on the total number of user accounts in the Active Directory forest to be recovered. A license key file for Recovery Manager Forest Edition specifies the licensed number of user accounts.

If the actual number of user accounts exceeds the licensed number, Recovery Manager Forest Edition does not cease functioning, but the product will return a warning message each time you recover the forest. In this case, you must install a new license key file purchased from Quest Software.

Recovery Manager Forest Edition can only use backups created by Recovery Manager for Active Directory after the Recovery Manager Forest Edition license was applied.

Permissions Required to Use the Application

The requirements for the user accounts that Recovery Manager Forest Edition uses are as follows.

Console Account

The account under which the Forest Recovery Console is running must have Read access to the Recovery Manager Forest Edition backup registration database.

Domain Controller Connection Account

Recovery Manager Forest Edition must use the built-in Administrator account to access domain controllers to be recovered.