



Quest® Recovery Manager for Active Directory Forest Edition 9.0.1

User Guide



Copyright 2018 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at <https://www.quest.com/legal>. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

An information icon indicates supporting information.

Recovery Manager for Active Directory Forest Edition User Guide

Updated - March, 2018

Version - 9.0.1

Contents

Overview	14
About Recovery Manager for Active Directory® Forest Edition	14
Features and benefits	14
Comprehensive Active Directory recovery options	15
AD LDS (ADAM) recovery	15
Granular, selective restore	15
Group Policy recovery	15
Centralized remote administration	16
Audit of objects and operations	16
Management Shell	16
Scheduling and automation	17
Scalability and performance	17
Rapid economic justification	17
Simplified restoration of an Active Directory forest	17
Granular, domain-level recovery	17
Integration with On Demand Recovery for Azure Active Directory	18
Automation of manual operations	18
Creation of virtual test environments	18
Remote quarantine	19
Support for Windows Server Backup	19
Fault tolerance	19
Simultaneous system recovery	19
Support for native Windows tools for restoring domain controllers	19
Recovery pauses	19
Recovery plan	20
Running custom scripts	20
Technical overview	20
Creating backups	21
Backup encryption	22
Creating unpacked backups	22
Using third-party backups	22
Cross-domain backup of group membership	22
Considerations for backing up Active Directory	22
Backup Agent	23
Separate credentials for Backup Agent	23
Using preinstalled Backup Agent	24
Recovering Active Directory	24
Active Directory recovery options	25
Granular online restore	26
Complete offline restore	28
Recovering Group Policy	28

Group Policy restore	29
Comparison reports	29
Getting started	31
Permissions required to use Recovery Manager for Active Directory	31
Recovery Manager Console	34
Icons in the user interface	36
Other Icons	37
Getting and using help	37
Configuring Windows Firewall	37
Manual method	37
Automatic method	41
Using Computer Collections	42
Creating Computer Collections	43
Renaming Computer Collections	43
Modifying Computer Collection properties	43
Deleting Computer Collections	44
Specifying an access account for Backup Agent and backup file storages	44
Adding domain controllers to a Computer Collection	45
Adding containers to a Computer Collection	46
Adding AD LDS (ADAM) hosts and instances to a Computer Collection	46
Removing items from a Computer Collection	47
Managing Recovery Manager for Active Directory configuration	48
Preparing for working with Active Directory or AD LDS (ADAM) backups	48
Settings	49
General tab	49
E-mail tab	50
Unpacked Backups tab (global settings)	50
Logging tab	51
Ports tab	52
Default properties for Computer Collections	52
Properties for an existing Computer Collection	53
Backup tab	53
System State tab	54
Schedule tab	54
Alerts tab	54
Logging tab	55
Performance tab	55
Advanced tab	56
Agent Settings tab	56
Console Storage tab	57
DC Storage tab	58
Unpacked Backups tab	59
Container and site properties	59
Properties for a domain or organizational unit	59
Properties for an Active Directory site	60

Properties for an AD LDS (ADAM) site	61
Sessions node properties	61
Forest properties	62
Domain properties	63
Domain controller properties	63
AD LDS (ADAM) partition properties	64
AD LDS (ADAM) instance properties	64
Showing or hiding AD LDS (ADAM) partitions	64
Showing or hiding domains	65
Showing or hiding sites	65
Licensing	65
Installing license key file	66
Updating license key file	66
Revoking licenses	67
Backing up data	68
Permissions required for the Backup operation	69
Managing Backup Agent	69
Installing Backup Agent automatically	70
Preinstalling Backup Agent manually	71
Discovering preinstalled Backup Agent	72
Updating Backup Agent information	72
Upgrading Backup Agent	72
Uninstalling Backup Agent	73
Removing a Backup Agent entry from the Backup Agent Management node	73
Using a least-privileged user account to back up data	73
Creating backups	74
Selecting components to back up	75
Using the Backup Wizard	76
Retrying backup creation	76
Enabling backup encryption	77
Backing up AD LDS (ADAM)	77
Method 1: Back up AD LDS (ADAM) from the Recovery Manager Console	78
Step 1: Connect to AD LDS (ADAM)	78
Step 2: Back up AD LDS (ADAM)	78
Method 2: Schedule backup creation for AD LDS (ADAM)	78
Step 1: Connect to AD LDS (ADAM)	79
Step 2: Add AD LDS (ADAM) instances to Computer Collection	79
Step 3: Create or modify backup creation schedule	79
Backing up cross-domain group membership	79
Backing up distributed file system (DFS) data	80
Backup scheduling	80
Task scheduler overview	80
Scheduling backup creation	81
Managing backup schedule	82

Setting user account for scheduled tasks	82
Setting performance options	83
Setting advanced backup options	84
Using Forest Recovery Agent	85
Unpacking backups	85
Configuring default settings to unpack backups	86
Configuring Computer Collection-specific settings to unpack backups	86
Unpacking a backup manually	86
Deleting data unpacked from a backup	87
Using e-mail notification	87
Viewing backup creation results	88
Sessions node properties	88
Progress tab	89
General tab	89
Computer properties	89
Computer session properties	89
General tab	89
Events tab	90
Backup tab	90
Backups node properties	90
Filtering backups	91
General tab for Active Directory backups	91
General tab for AD LDS (ADAM) backups	92
Properties of registered AD and AD LDS (ADAM) backups	92
General tab	93
Components tab	93
Restoring data	94
Getting started with Active Directory recovery	94
Choosing an Active Directory recovery method	94
Implications of the online restore	95
Forcing replication	96
Skipping replication	96
Stopping online restore	97
Using agentless or agent-based method	97
Agentless method	98
Agent-based method	98
Managing deleted or recycled objects	99
Recovering deleted objects	100
Recycling deleted objects	101
Recovering recycled objects	102
Restoring backed up System State components	102
Restoring cluster information	103
Using granular online restore	104
Online Restore Wizard overview	105

Compare, restore, and report changes in Active Directory	105
Compare two backups and report the differences	105
Reporting	105
Selecting objects in the Online Restore Wizard	106
Restoring AD LDS (ADAM)	107
Method 1: Restore an AD LDS (ADAM) instance from a backup created with Recovery Manager for Active Directory	108
Step 1: Select a backup	108
Step 2: Restore AD LDS (ADAM) instance	108
Method 2: Restore an AD LDS (ADAM) database from a backup created with third-party software	108
Step 1: Extract and register AD LDS (ADAM) database	108
Step 2: Restore the extracted AD LDS (ADAM) database	109
Selectively restoring Active Directory object attributes	109
Restoring objects in an application directory partition	110
Restoring object quotas	111
Restoring cross-domain group membership	111
Performing a restore without having administrator privileges	112
Reports about objects and operations	113
Reports about Active Directory objects	113
Reports about AD LDS (ADAM) objects	114
Reports about Group Policy objects	114
Reports about who modified Active Directory objects	115
Using complete offline restore	116
Repair Wizard overview	116
Offline restore implications	117
Non-authoritative restore	118
DIT database	118
SYSVOL	118
Authoritative restore	118
DIT database	118
SYSVOL	119
Restoring SYSVOL authoritatively	119
Performing a granular restore of SYSVOL	120
Recovering Group Policy	121
Group Policy Restore Wizard overview	121
Restoring data from third-party backups	122
Using the Extract Wizard	122
Creating a Windows Server 2003-based domain controller from a backup	123
Creating a Windows Server 2008-based domain controller from a backup	124
Step 1: Create and extract a backup	124
Step 2: Use IFM to create a domain controller	124
Creating a Windows Server 2012-based domain controller from a backup	125
Step 1: Create and extract a backup	125
Step 2: Install AD DS on the Windows Server 2012-based computer	125

Step 3: Use the Install-ADDSDomainController cmdlet to install from media	125
Restoring passwords and SID history	126
Preserving passwords and SID history in object tombstones	126
Step 1: Make sure prerequisites are met	126
Step 2: Modify the searchFlags attribute value	126
Fault tolerance	128
Full replication	128
Replication of backup information only	129
Replicating data using Recovery Manager Console	130
Replicating data using PowerShell	131
Monitoring Recovery Manager for Active Directory	135
Supported versions of Microsoft Operations Manager	135
Importing Management Pack	135
Rules provided in Microsoft System Center Operations Manager	136
Health dashboards	137
Using Management Shell	140
About Management Shell	140
Installing and opening Management Shell	140
Installation requirements	140
Installing Management Shell	141
Opening Management Shell	141
Getting Help	142
Recovering an Active Directory forest	143
Permissions required to use Forest Recovery Console	143
Forest Recovery Console	144
Toolbar	146
Project summary	147
List of domain controllers	147
Filtering the list of domain controllers	147
Connecting to a domain controller via RDP	148
Domain controller recovery settings and progress	148
Settings tab	148
Progress tab	151
Recovery Events tab	151
Configuring advanced settings	152
Managing a recovery project	154
Creating a recovery project	155
Opening a recovery project	155
Opening a legacy recovery project	155
Saving a recovery project	156
Updating a recovery project	156
Specifying recovery project settings	156

Verifying recovery project settings	160
Scheduling project verification	160
Specifying recovery settings for a DC	161
Selecting backups for recovery	162
Method 1: Automatically select backups based on your criteria	162
Method 2: Manually select backups	163
Using recovery alerts	163
Creating an alert	165
Viewing active alerts	166
Modifying an alert	166
Deleting an alert	166
Using recovery pauses	167
Managing manual pauses	167
Monitoring active pauses	168
Managing automatic pauses	168
Copying a backup file to a new location	171
Managing Forest Recovery Agent	172
Installing or upgrading Forest Recovery Agent	172
Viewing installed Forest Recovery Agent version	173
Uninstalling Forest Recovery Agent	173
Rebooting domain controllers manually	174
Resetting DSRM Administrator Password	175
Managing the Global Catalog servers	175
Managing FSMO roles	176
Manage DNS Client Settings	177
Configuring Windows Firewall	177
Forest recovery overview	179
Developing a custom forest recovery plan	180
Backing up domain controllers	181
Assigning a preferred DNS server during recovery	181
Forest recovery methods	182
Recovery method 1: Restore as many domain controllers from backups as possible	182
Recovery method 2: Restore one domain controller from backup in each domain	183
Deciding which backups to use	184
Running custom scripts while recovering a forest	184
Overview of steps to recover a forest	185
Viewing forest recovery progress	186
Viewing recovery plan	186
Viewing a report about forest recovery or verify settings operation	186
Handling failed domain controllers	187
Adding a domain controller to a running recovery operation	187
Selectively recovering domains in a forest	187
Step 1: Select domains to recover	188
Step 2: Specify recovery settings for domain controllers	188
Step 3: Start recovery	189

Recovering SYSVOL	189
Deleting domains during recovery	189
Resuming an interrupted forest recovery	190
Recovering read-only domain controllers (RODCs)	192
Checking forest health	192
Collecting diagnostic data for technical support	194
Step 1: Use Diagnostic Data Collector to automatically gather data	195
Step 2: Gather remaining data manually	195
Creating virtual test environments	197
About Active Directory Virtual Lab	197
Permissions	198
Communication ports	199
Microsoft SCVMM 2012 or 2012 SP1 Environment	200
Microsoft SCVMM 2012 R2 or 2016 Environment	201
VMware Environment	201
Deployment	202
User interface	203
Toolbar	204
List of source computers	205
Virtual machine creation settings and events	205
General tab	205
Hardware tab	206
Active Directory tab	206
Events tab	206
Virtual lab project default settings	206
How to create a virtual test environment	207
Considerations	207
Isolated virtual network and DNS	207
Virtualization agent behavior	208
Working with SCVMM 2012 R2 or higher	208
Forest Recovery Agent is required	209
Opening a legacy virtual lab project	209
Precautions	210
Step-by-step instructions	210
Step 1: Create a virtual lab project	210
Step 2: Add source computers to virtual lab project	211
Step 3: Modify virtual machine creation settings	212
Step 4: Verify virtual machine creation settings	212
Step 5: Start virtual test environment creation	213
Step 6: Enable network adapters	214
Using Recovery Manager for Active Directory Web Interface	215
About Recovery Manager Portal	215
Installing Recovery Manager Portal	216

Connecting to Recovery Manager Portal	217
Administering Recovery Manager Portal	218
Configuring portal for working with Recovery Manager for Active Directory	218
Step 1: Install Recovery Manager Remote API Access Service	218
Step 2: Configure Recovery Manager for Active Directory	219
Step 3: Add Recovery Manager for Active Directory instances	219
Step 4: Configure recovery settings for Active Directory domains	220
Modifying recovery settings for domains	220
Assigning roles to portal users	221
Delegating restore or undelete permissions	221
Configuring e-mail notification	222
How Recovery Manager Portal recovers data	222
Integrating with On Demand Recovery for Azure Active Directory	223
Viewing health summary for Recovery Manager for Active Directory instances	224
Viewing backup creation history	224
Recovering data using Recovery Manager Portal	225
Restoring objects from a backup	225
Undeleting objects	225
Appendices	226
Frequently asked questions	226
Why do I need to restore deleted users or groups, rather than re-create them?	226
How can I restore a user or group in Active Directory?	227
How does online restore work?	227
When an object is undeleted, what is restored from the tombstone and what is restored from the backup?	227
What's the difference between an online restore and an authoritative restore?	228
What's the difference between the agentless restore method and the agent-based restore method?	228
Can I undelete a mailbox-enabled user?	229
In the Group Policy Restore Wizard, a GPO link is shown as deleted, but the link actually exists in Active Directory. What's wrong?	229
What is a primary restore of the SYSVOL?	229
How do I change the Backup Agent port number?	229
How does Recovery Manager for Active Directory Forest Edition select a DC for an authoritative (primary) restore of SYSVOL during forest recovery?	230
How does Recovery Manager for Active Directory Forest Edition isolate domain controllers during forest recovery?	231
How does Recovery Manager for Active Directory Forest Edition select a DC to add the global catalog during forest recovery?	232
Best practices for creating backups for forest recovery	232
How many instances of the Recovery Manager Console to deploy?	232
How many domain controllers to back up?	232
How many domain controllers to back up at once?	233
What data to back up?	233
Using data compression	234
Using unpacked backups	234

Best practices for recovering a forest	234
How many Instances of the Forest Recovery Console to deploy?	234
Where to Install the Forest Recovery Console?	235
Backing up the Recovery Manager for Active Directory Forest Edition configuration	235
Descriptions of recovery or verification steps	235
Backup wizard	240
What to Back Up	240
Where to Store Backups	241
When to Back Up	241
Computer Collection Name (optional)	242
Completing the Backup Wizard	242
Online Restore Wizard	242
Wizard Operation Mode	243
Domain Selection	243
Backup Selection	244
Backup for Comparison (optional)	244
Unpacked Backups Folder Selection	245
Backup Data Preparation	245
Domain Access Options	245
Objects to Be Processed	246
Operation Selection	247
Processing Options	248
Select Object Types	248
Select Attributes to Be Processed	248
Reporting Options	249
Operation Start	249
Operation Progress	249
Password Settings	249
Operation Option	250
Objects to Be Restored	250
Where to Restore Deleted Objects	251
Operation Results	251
Completing the Online Restore Wizard	251
Online Restore Wizard for AD LDS (ADAM)	252
Wizard Operation Mode	252
AD LDS (ADAM) Instance Selection	252
Backup Selection	253
Backup for Comparison	253
Unpacked Backups Folder Selection	254
Backup Data Preparation	254
AD LDS (ADAM) Access Options	254
Objects to Be Processed	255
Processing Options	256
Reporting Options	256
Operation Start	257

Operation Progress	257
Operation Option	257
Objects to Be Restored	257
Operation Results	258
Completing the Online Restore Wizard for AD LDS (ADAM)	258
Group Policy Restore Wizard	259
Backup Source Domain	259
Backup Selection	259
Unpacked Backups Folder Selection	260
Backup Data Preparation	260
Target Domain Controller	260
Group Policy Object Selection	261
GPO Restore Options	262
Link Restore Options	262
Restore Process Start	263
Completing the Group Policy Restore Wizard	263
Repair Wizard	263
Computer and Backup Selection	263
Target Computer	264
Computer Restart	264
Primary Restore of SYSVOL	265
Restore Process Start	265
Restore Progress	266
Authoritative Restore Selections	266
Computer Restart in Normal Mode	266
Completing the Repair Wizard	266
Extract Wizard	267
Backup Selection	267
Folder Selection	268
Operation Start	268
Operation Progress	268
Completing the Extract Wizard	268
Events generated by Recovery Manager for Active Directory	268
Common Events	269
Recovery Manager Console events	270
Backup Agent events	273
Management Agent events	274
Restore Agent events	274
Recovery Manager Portal events	275
Forest Recovery Agent events	277
Forest Recovery Console events	279
AD Virtual Lab events	281
About us	283
Contacting Quest	283
Technical support resources	283

Overview

- [About Quest® Recovery Manager for Active Directory Forest Edition](#)
- [Features and benefits](#)
- [Technical overview](#)

About Recovery Manager for Active Directory® Forest Edition

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

Recovery Manager for Active Directory Forest Edition simplifies and automates the process of Active Directory forest or domain recovery: it 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 patented 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 for Active Directory Forest Edition allows for quick, online recovery of data. In enterprisescale 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 for Active Directory 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 for Active Directory 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 for Active Directory 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.

AD LDS (ADAM) recovery

Recovery Manager for Active Directory 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 for Active Directory 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 for Active Directory Forest Edition ensures that the restored object is a member of the proper groups.

Group Policy recovery

One of the key features of Recovery Manager for Active Directory Forest Edition is the ability to quickly recover individual Group Policy objects using a 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 for Active Directory 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 for Active Directory 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 for Active Directory 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.

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 for Active Directory 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 for Active Directory 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 for Active Directory 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 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 ChangeAuditor for Active Directory at

<http://quest.com/products/changeauditor-for-active-directory>.

Management Shell

The Recovery Manager for Active Directory 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 for Active Directory 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, textbased 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

Creation of Backups

Recovery Manager for Active Directory 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 for Active Directory 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 for Active Directory Forest Edition.

Recovery Manager for Active Directory 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.

Project Settings Verification

Recovery Manager for Active Directory Forest Edition allows the administrators to schedule the forest recovery project verification. This functionality lets you automate the settings verification to ensure that the recovery project is in valid state and can be used for forest recovery.

Scalability and performance

Recovery Manager for Active Directory 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 for Active Directory 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 for Active Directory 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.

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 for Active Directory 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.

Integration with On Demand Recovery for Azure Active Directory

From version 9.0, Recovery Manager for Active Directory can be integrated with Recovery for Azure Active Directory to restore and undelete on-premises objects that are synchronized with cloud by Azure AD Connect. For more details, please see <http://support.quest.com/technical-documents/on-demand-recovery-for-azure-active-directory/user-guide/integration-with-recovery-manager-for-active-directory>.

Automation of 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 for Active Directory Forest Edition automates those numerous manual steps not only saving vast amounts of time but also eliminating the risk of human error.

Creation of virtual test environments

Recovery Manager for Active Directory Forest Edition includes a component called the Active Directory Virtual Lab. This component helps you create virtual test environments from an Active Directory forest. You can use the created test environments to design and evaluate Active Directory disaster recovery scenarios, test planned Active Directory changes before deploying them to production, train your staff to perform Active Directory related tasks, and more.

To create a virtual test environment from an Active Directory forest, you first need to select the source computers (domain controllers or standalone servers) you want to include in the test environment, configure settings to create a virtual machine from each source computer, and then have the Active Directory Virtual Lab create the test environment for you.

When creating virtual machines from the source computers, the Active Directory Virtual Lab uses third-party virtualization software, such as Microsoft System Center Virtual Machine Manager (SCVMM), VMware ESX, or VMware vCenter. For a full list of supported virtualization software, see the System Requirements section in the *Recovery Manager for Active Directory Forest Edition Release Notes*.

You can configure virtualization settings to create virtual machines that maintain all the data available on the source computers, including Active Directory, installed programs, and files. To manage the created virtual test environment, you need to use the native tools provided by the virtualization software with which the Active Directory Virtual Lab created the virtual machines in the test environment.

Remote quarantine

Recovery Manager for Active Directory Forest Edition automatically and remotely quarantines corrupt domain controllers so that those individual domain controllers won't replicate with the newly restored environment.

Support for Windows Server Backup

From version 8.7, Recovery Manager for Active Directory (Forest Edition) can perform online restore of Active Directory objects and Group Policy objects from Windows Server Backup. Offline restore and Forest recovery operations are not supported.

Fault tolerance

Recovery Manager for Active Directory supports the data replication between multiple instances of Recovery Manager Console to ensure reliability and fault tolerance in case of any system failure.

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 for Active Directory Forest Edition, eliminating the need to manually interface with each domain controller separately saving a significant amount of time and effort.

Support for native Windows tools for restoring domain controllers

Recovery Manager for Active Directory Forest Edition can restore selected DCs from backups and then recover the remaining DCs by demoting them and reinstalling Active Directory. Depending on the Windows version installed on the target DC, Recovery Manager for Active Directory Forest Edition uses either the Active Directory Installation Wizard (**DCPromo.exe**) or the native Windows PowerShell cmdlets *Install-ADDSDomainController* and *Uninstall-ADDSDomainController*.

Support for the native Windows tools 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 for Active Directory Forest Edition.

IMPORTANT: 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 recovery settings specified for the domain controllers in the recovery project, 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 for Active Directory Forest Edition to automatically run custom scripts on the Recovery Manager for Active Directory Forest Edition computer before, after, or during the recovery operation.

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

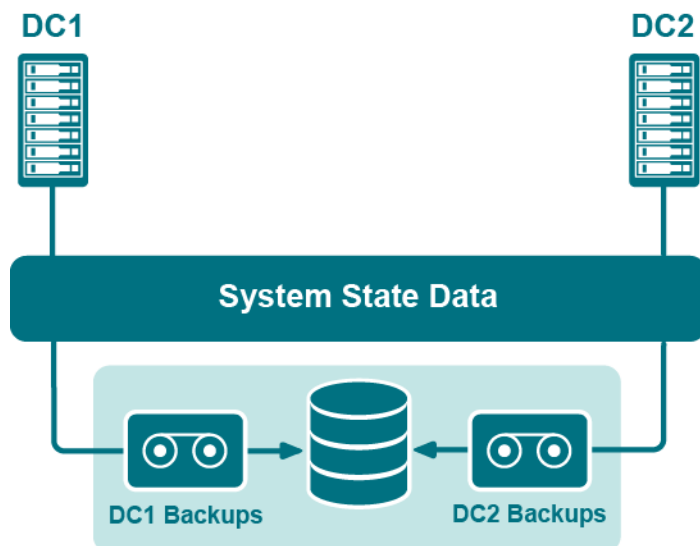


Figure 1: AD Backup Creation

Recovery Manager for Active Directory 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 for Active Directory 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 for Active Directory Forest Edition employs agents that compress the data to be backed up, before sending it across the network.

Recovery Manager for Active Directory 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 for Active Directory 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 for Active Directory 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 AES-256 algorithm from RSA, Inc. (Microsoft Enhanced RSA and AES Cryptographic Provider), with the maximum cipher strength. The use of the Microsoft Enhanced RSA and AES Cryptographic Provider ensures that backups are encrypted with 256-bit cipher strength.

Creating unpacked backups

You can have Recovery Manager for Active Directory 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.

Using third-party backups

Recovery Manager for Active Directory 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 membership

When backing up Global Catalog servers, you have the option to force Recovery Manager for Active Directory 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 backing up Active Directory

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 for Active Directory Forest Edition employs a Backup Agent to back up remote domain controllers and AD LDS (ADAM) hosts. This is because some backup APIs provided by the operating system cannot be used to access a target domain controller or AD LDS (ADAM) host from the Recovery Manager Console. Therefore, Backup Agent must be installed on a remote domain controller or AD LDS (ADAM) host in order to gain access to its specific objects. Recovery Manager for Active Directory Forest Edition can automatically install Backup Agent before starting a backup, and remove it upon the completion of backup operation. Alternatively, you can preinstall Backup Agent manually. For more information on the advantages of using preinstalled Backup Agent, see [Using preinstalled Backup Agent](#) below.

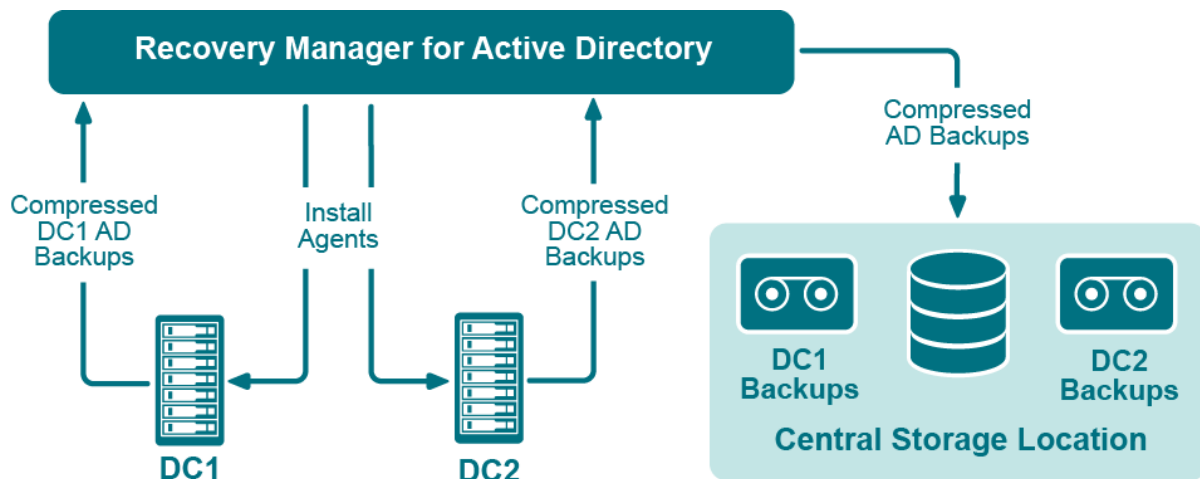


Figure 2: Backup Agents

The figure above illustrates how Recovery Manager for Active Directory Forest Edition 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 for Active Directory Forest Edition, 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 for Active Directory Forest Edition allows to run Backup Agent in the security context of a specific user account. Since Recovery Manager for Active Directory Forest Edition needs administrative access to the domain controller in order to run Backup Agent, the account under which Recovery Manager for Active Directory Forest Edition is running must belong to the Administrators group on that domain controller or AD LDS (ADAM) host, providing administrative access to the entire domain. If Recovery Manager for Active Directory

Forest Edition 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition is running, solving the so-called “no trust” problem.

Recovering Active Directory

Recovery Manager for Active Directory Forest Edition 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 for Active Directory Forest Edition should only be performed by highly trusted directory administrators.

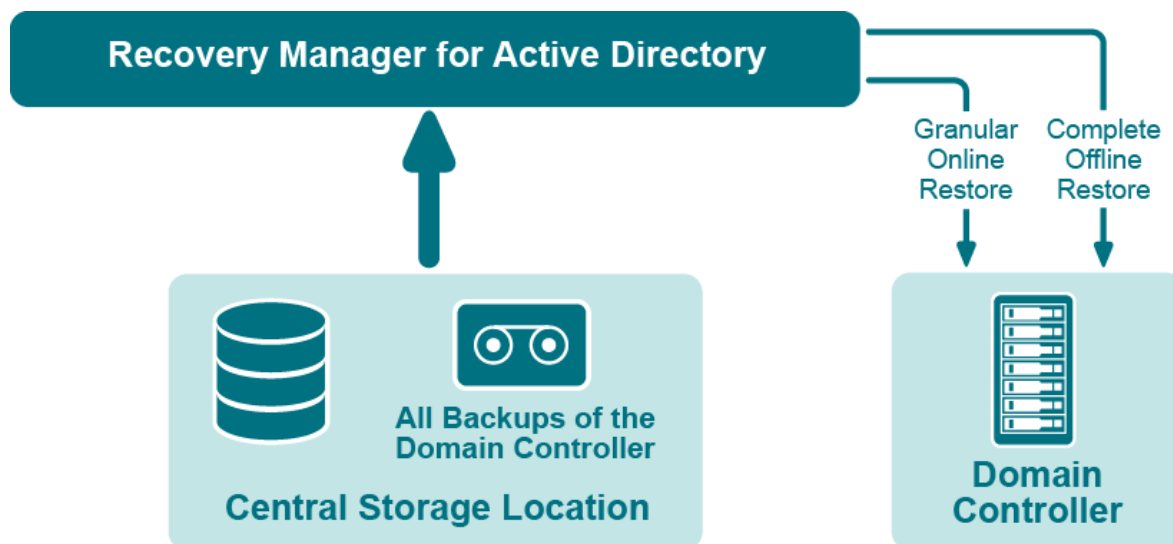


Figure 3: Recovering Active Directory

If certain objects are inadvertently deleted or modified in Active Directory, they can be restored from a 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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.

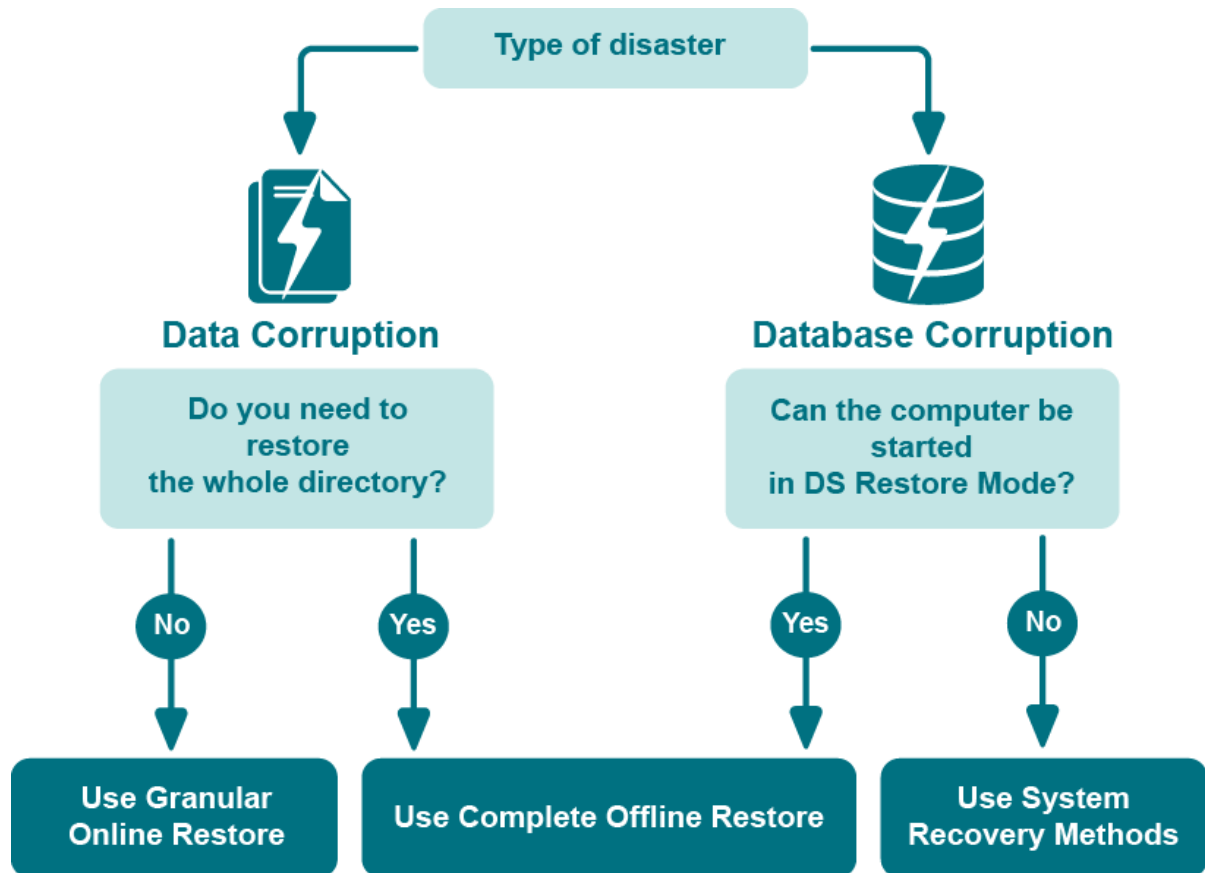


Figure 4: Active Directory Recovery Options

Recovery Manager for Active Directory Forest Edition 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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 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.

The 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition, you can selectively recover deleted Active Directory objects by undeleting (reanimating) them. To undelete (reanimate) an object, Recovery Manager for Active Directory 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) (<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 for Active Directory 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:

- **Deleted state.** 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition.

If necessary, you can use Recovery Manager for Active Directory 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 for Active Directory Forest Edition Management Shell.

- **Recycled state.** 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.

To manage recycled objects, you can use the Deleted Objects container provided by Recovery Manager for Active Directory Forest Edition. In this container, you can view a list of all recycled objects in the domain, selectively recycle deleted objects, and recover recycled objects from backups created with Recovery Manager for Active Directory Forest Edition.

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 for Active Directory Forest Edition enables the recovery of Group Policy data from corruption or inadvertent modification, which can be caused by either hardware failure or human error.

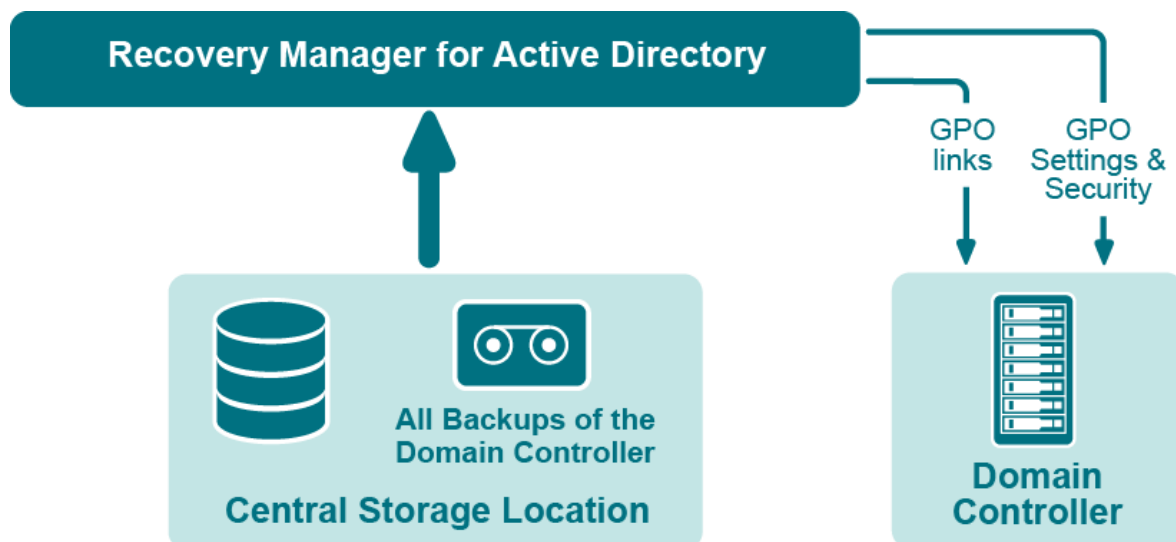


Figure 5: Group Policy Recovery

If specific Group Policy objects or links are inadvertently deleted or modified, they can be restored from a 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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 for Active Directory Forest Edition 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.

Getting started

- [Permissions required to use Recovery Manager for Active Directory](#)
- [Recovery Manager Console](#)
- [Icons in the user interface](#)
- [Other Icons](#)
- [Getting and using help](#)
- [Configuring Windows Firewall](#)
- [Using Computer Collections](#)
- [Managing Recovery Manager for Active Directory configuration](#)
- [Licensing](#)

Permissions required to use Recovery Manager for Active Directory

i **NOTE:** From version 8.8, Recovery Manager for Active Directory supports environments with disabled NTLM authentication and the [Protected Users security group](#).

The table below lists the minimum user account permissions required to perform some common tasks with Recovery Manager for Active Directory.

Table 1: Minimum permissions

Task	Minimum permissions
Install Recovery Manager for Active Directory	The account must be a member of the local Administrators group on the computer where you want to install Recovery Manager for Active Directory. If during the installation you specify an existing SQL Server instance, the account with which Recovery Manager for Active Directory connects to that instance must have the following permissions on the instance: • Create Database • Create Table • Create Procedure • Create Function
Open and use the Recovery Manager Console	The account must be a member of the local Administrators group on the computer where the Recovery Manager Console is installed. The account must also have the following permissions on the SQL Server instance used by Recovery Manager for Active Directory: • Insert • Delete

Task	Minimum permissions
	• Update • Select • Execute
Preinstall Backup Agent manually	The account you use to access the target computer must be a member of the local Administrators group on that computer
Upgrade Backup Agent	
Discover preinstalled Backup Agent instances	The account used to access the target domain controllers must:
Uninstall Backup Agent	• Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer.
Update information displayed about Backup Agent in the Recovery Manager Console	• Be a member of the Backup Operators group on each target domain controller.
Automatically install Backup Agent and back up Active Directory data	To automatically install Backup Agent, the account must have: • Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Local Administrator permissions on the target domain controller. To back up data, the account must be a member of the Backup Operators group on the target domain controller.
Back up Active Directory using preinstalled Backup Agent	The account used to access the target domain controllers must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Be a member of the Backup Operators group on each domain controller to be backed up.
Perform a complete offline restore of Active Directory by using the Repair Wizard	If you restore data to a domain controller where User Account Control (UAC) is not installed or disabled: • The account you use to access the domain controller must be a member of the Domain Admins group. If you restore data to a domain controller where User Account Control (UAC) is enabled: • The account you use to access the domain controller must be the built-in Administrator on that computer. In both these cases, the account you use to access the domain controller must have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer.

Task	Minimum permissions
Perform a selective online restore of Active Directory objects	The account used to access the target domain controllers must have: • Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Reanimate Tombstones extended right in the domain where objects are to be restored. • Write permission on each object attribute to be updated during the restore. • Create All Child Objects permission on the destination container. • List Contents permission on the Deleted Objects container in the domain where objects are to be restored.
Restore a Group Policy object	The account used to access the target domain controller must: • Be a member of the Group Policy Creator Owners group. • Have Full Control privilege on the Group Policy object. • Be a member of the Backup Operators group. • Have sufficient permissions to read/write Active Directory objects linked to the Group Policy object.
Automatically install Backup Agent and back up an AD LDS (ADAM) instance	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance
Back up an AD LDS (ADAM) instance using preinstalled Backup Agent	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance.
Restore an AD LDS (ADAM) instance	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance.

Recovery Manager Console

Recovery Manager for Active Directory includes an MMC snap-in (also known as the Recovery Manager Console) to ensure intuitive operation and close integration with the Windows operating system.

NOTE: Machine that hosts the Recovery Manager Console must have same or higher version of Windows operating system than the processed domain controllers. Otherwise, the online compare and restore operations cannot be performed via the RMAD console.

To start the Recovery Manager Console

- Complete the steps related to your version of Windows

Table 2: Steps to start Recovery Manager Console

Windows 7

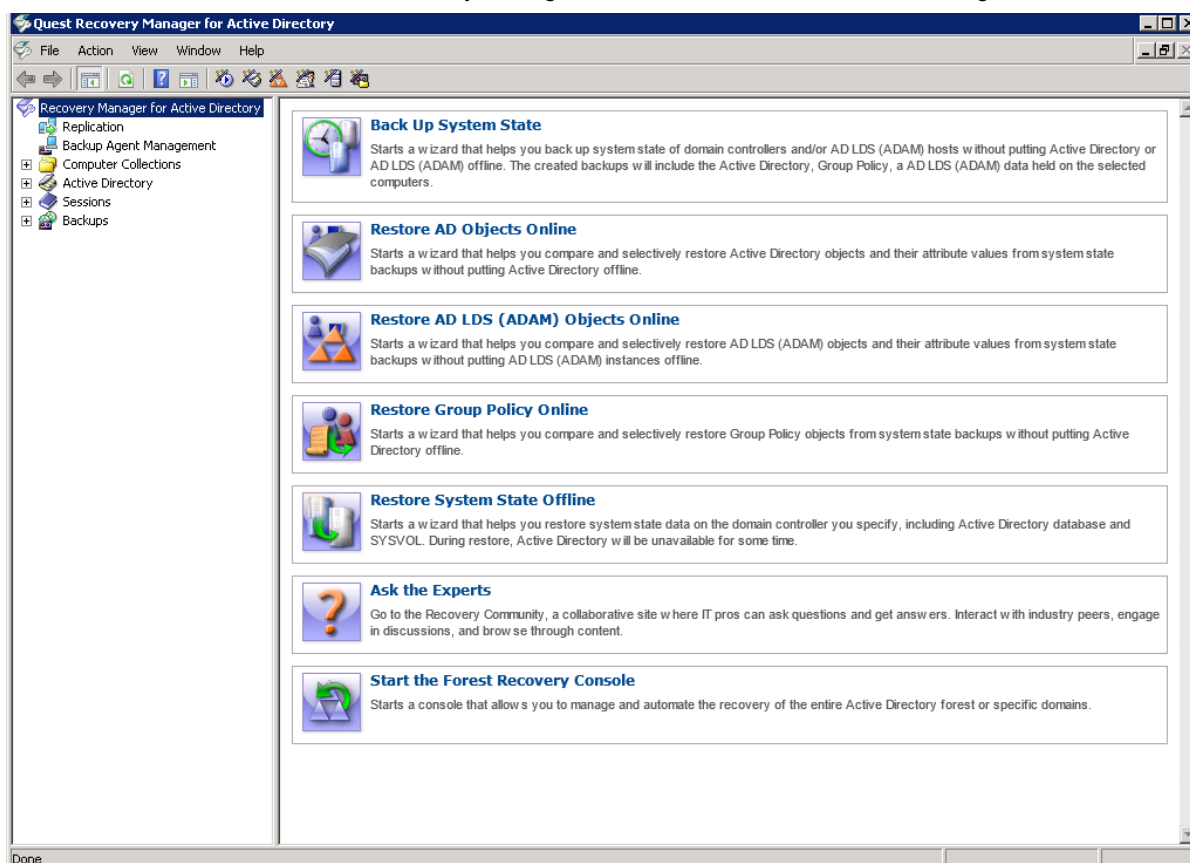
Windows Server 2008 or 2008 R2

A later version of Windows

1. Click **Start**.
2. Point to **All Programs | Quest | Recovery Manager for Active Directory Forest Edition**.
3. Click **Recovery Manager for Active Directory**.

On the **Start** screen, click the **Recovery Manager for Active Directory** tile.

When started for the first time, the Recovery Manager Console looks similar to the following:



The main viewing area of the window is divided into two panes. The left pane contains the console tree, showing the items that are available in the snap-in. The right pane, known as the details pane, is used to display information about those items. The window also contains command menus and toolbars that are provided by both the MMC and the snap-in.

The information in the details pane changes accordingly when you select items in the console tree. To perform management tasks, you can click or right-click entries in the details pane and then use commands on the Action menu or shortcut menu.

You can move objects by selecting them in a source folder and then dragging the selection to a destination folder. If the drop operation is not allowed, the mouse pointer changes accordingly.

For more information about how to navigate an MMC snap-in, refer to Microsoft Management Console Help.

The console tree includes the following items:

- **Replication** Using this node you can add multiple console instances to the replication console list and perform the data replication from source consoles to the local one. For more information, see [Configuring data replication](#).
- **Backup Agent Management**. Provides a central location for managing Backup Agent on computers added to Computer Collections. You can use this node to discover all preinstalled instances of Backup Agent and to manually install, uninstall, or update the agent on computers in Computer Collections (such as domain controllers and AD LDS (ADAM) hosts). For more information, see [Managing Backup Agent](#).
- **Computer Collections**. Contains a list of user-defined collections of computers. When you select a collection in the console tree, the details pane displays a list of all members of that collection. For more information, see [Using Computer Collections](#).
- **Active Directory**. Contains nodes representing the forests and AD LDS (ADAM) configuration sets to which the Recovery Manager Console is currently connected. You can browse forests and AD LDS (ADAM) configuration sets for computers and AD LDS (ADAM) instances, respectively.
 - To add a forest to the list, select **Active Directory**, and then, on the **Action** menu, click **Connect to Forest**.
 - To add an AD LDS (ADAM) configuration set to the list, select **Active Directory**, and then, on the **Action** menu, click **Connect to AD LDS (ADAM)**.
- **Sessions**. Contains a list of all backup-creation sessions performed by Recovery Manager for Active Directory. When you select a session in the console tree, the details pane reports information about that session, such as whether backups were successfully created during the session.
- **Backups**. Contains a list of the Active Directory backups and AD LDS (ADAM) backups registered in the backup registration database of Recovery Manager for Active Directory. When you select **Active Directory or AD LDS (ADAM)** under the **Backups** node, the details pane displays a list of all registered AD backups or AD LDS (ADAM) backups respectively.

You can use the **Properties** dialog box provided for the Active Directory or AD LDS (ADAM) node, to filter the list of backups displayed in the details pane.

The Recovery Manager for Active Directory snap-in adds the following buttons to the MMC toolbar:

Table 3: Button descriptions

Button	Description
	Starts the Backup Wizard. You can back up System State of the selected computers.
	Starts a backup creation for the Computer Collection selected in the console tree. Recovery

Button	Description
	Manager for Active Directory creates backups for computers that belong to the collection, without starting the Backup Wizard. Starts a backup creation for members of the Computer Collection selected in the details pane.
	Starts the Online Restore Wizard. You can recover and compare individual objects and object attributes in Active Directory.
	Starts the Online Restore Wizard for AD LDS (ADAM). You can recover and compare individual objects and object attributes in AD LDS (ADAM).
	Starts the Group Policy Restore Wizard. You can selectively recover Group Policy information using backups of domain controllers' System State.
	Starts the Repair Wizard. You can restore the previously backed up System State of an Active Directory domain controller.
	Starts the Extract Wizard. You can restore previously backed up System State files to an alternate location.
	Shows all explicit objects added to the Computer Collection selected in the console tree.
	Shows only computers to be backed up while backing up the Computer Collection selected in the console tree.

Icons in the user interface

In the Recovery Manager for Active Directory user interface, you may encounter the following icons:

Table 4: Icons in the user interface

Icon	Description
	Indicates that the backup is not unpacked.
	Indicates that the backup is unpacked.
	Indicates that the Active Directory backup is not unpacked.
	Indicates that the Active Directory backup is unpacked.
	Indicates that the AD LDS (ADAM) backup is not unpacked.
	Indicates that the AD LDS (ADAM) backup is unpacked.

Other Icons

Table 5: Other icons

Icon	Description
	Indicates that the scheduled task is created by Recovery Manager for Active Directory.

Getting and using help

Help topics and tips provided with Recovery Manager for Active Directory help you accomplish your tasks. To get assistance while you work:

- On the **Help** menu, click **Help Topics**. This displays the Help Viewer. To find a Help topic, use the **Contents** and **Search** tabs of the Help Viewer.
- To see a brief description of a wizard page or a dialog box, press the F1 key or click the **Help** button.
- To see a brief description of a menu command or a toolbar button, point to the command or button. Descriptions of toolbar buttons appear as tool-tips.

Descriptions of menu commands appear in the status bar at the bottom of the window. If the status bar is not displayed, click **Customize** on the **View** menu, and then select the **Status bar** check box in the **Customize View** dialog box.

Configuring Windows Firewall

A firewall enabled in your environment may block traffic on ports used by Recovery Manager for Active Directory, preventing you from backing up or restoring data. Before you start using Recovery Manager for Active Directory, make sure your firewall does not block traffic on ports used by Recovery Manager for Active Directory. For more information about these ports, see the Deployment Guide supplied with this release.

This section provides instructions on how to configure built-in Windows Firewall on a computer that is running Windows Server 2008 or later (domain controller or AD LDS (ADAM) host), so that Recovery Manager for Active Directory could back up data on that computer.

The section covers the following methods:

- [Manual method](#)
- [Automatic method](#)

Manual method

Create the following firewall rules to allow traffic on ports used by Recovery Manager for Active Directory.

For Backup Agent:

- In case of preinstalled Backup Agent, specify the following installation files instead of <backup agent> in the **Program path** parameter (Rule 3):

- For Windows Server 2008 and above: BackupAgent64.exe for 64-bit systems or BackupAgent.exe for 32-bit systems
- For Windows Server 2003: ErdAgent64.exe for 64-bit systems or ErdAgent.exe for 32-bit systems
- In case of automatic Backup Agent installation, specify ErdAgent.exe instead of <backup agent> in the **Program path** parameter (Rule 3).
- If the specific Backup Agent port is used, you need to configure Rule 1, and Rule 3. Specify <specific TCP port> for Backup Agent in the **Local ports** parameter (Rule 3).
- If RPC dynamic port range is used for Backup Agent, configure Rule 1, Rule 2 and Rule 3. Specify <RPC dynamic port range> for Backup Agent in the **Local ports** parameter (Rule 3).

For Online Restore Agent:

- Specify OnlineRestoreAdapter.exe in the **Program path** parameter (Rule 4).
- If the specific Online Restore Agent port is used, you need to configure Rule 1, and Rule 4. Specify <specific TCP port> for Online Restore Agent in the **Local ports** parameter (Rule 4).
- If RPC dynamic port range is used for Online Restore Agent, configure Rule 1, Rule 2 and Rule 4. Specify <RPC dynamic port range> for Online Restore Agent in the **Local ports** parameter (Rule 4).

For Offline Restore Agent:

- Specify the following installation files instead of <offline restore agent> in the **Program path** parameter (Rule 5).
 - For Windows Server 2008 and above: RestoreAgent64.exe for 64-bit systems or RestoreAgent.exe for 32-bit systems.
 - For Windows Server 2003: RstAgent64.exe for 64-bit systems or RstAgent.exe for 32-bit systems.
- If the specific Offline Restore Agent port is used, you need to configure Rule 1, and Rule 5. Specify <specific TCP port> for Offline Restore Agent in the **Local ports** parameter (Rule 5).
- If RPC dynamic port range is used for Offline Restore Agent, configure Rule 1, Rule 2 and Rule 5. Specify <RPC dynamic port range> for Offline Restore Agent in the **Local ports** parameter (Rule 5).

For Management Agent:

- Specify the ManagementAgent.exe in the **Program path** parameter (Rule 6).
- If the specific Backup Agent port is used, you need to configure Rule 1, and Rule 6. Specify <specific TCP port> for Management Agent in the **Local ports** parameter (Rule 6).
- If RPC dynamic port range is used for Management Agent, configure Rule 1, Rule 2 and Rule 6. Specify <RPC dynamic port range> for Management Agent in the **Local ports** parameter (Rule 6).

For Forest Recovery Agent:

- Specify FRRestoreService64.exe for 64-bit systems or FRRestoreService.exe for 32-bit systems instead of <forest recovery agent> in the **Program path** parameter (Rule 7).
- If the specific Backup Agent port is used, you need to configure Rule 1, and Rule 7. Specify <specific TCP port> for Forest Recovery Agent in the **Local ports** parameter (Rule 7).
- If RPC dynamic port range is used for Forest Recovery Agent, configure Rule 1, Rule 2 and Rule 7. Specify <RPC dynamic port range> for Forest Recovery Agent in the **Local ports** parameter (Rule 7).

Rule 1 (inbound)

- Rule type: Custom
- Program path: System
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 445
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule.

Rule 2 (inbound)

- Rule type: Custom
- Program path: %SystemRoot%\System32\Svchost.exe
- Service settings: Remote Procedure Call (RpcSs)
- Protocol: TCP
- Local ports: RPC Endpoint Mapper
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule.

Rule 3 (inbound)

- Rule type: Custom
- Program path: %SystemRoot%\RecoveryManagerAD\<backup agent>
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: RPC dynamic port range / specific port for Backup Agent
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any

- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule

Rule 4 (inbound)

- Rule type: Custom
- Program path: %systemroot%\RecoveryManagerAD\OnlineRestoreAdapter.exe
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local port: RPC dynamic port range / specific port for Online Restore Agent
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule

Rule 5 (inbound)

- Rule type: Custom
- Program path: %systemroot%\RecoveryManagerAD\<offline restore agent>
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local port: RPC dynamic port range / specific port for Offline Restore Agent
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule

Rule 6 (inbound)

- Rule type: Custom
- Program path: %systemroot%\RecoveryManagerAD\ManagementAgent.exe

- Service settings: Apply to all programs and services
- Protocol: TCP
- Local port: RPC dynamic port range / specific port for Management Agent
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule

Rule 7 (inbound)

- Rule type: Custom
- Program path: %ProgramFiles%\Quest\Recovery Manager for Active Directory Forest Edition\<forest recovery agent>
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local port: RPC dynamic port range / specific port for Forest Recovery Agent
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Leave default values for all other settings of this firewall rule

For more information on RPC dynamic port range, refer to the following Microsoft Support Knowledge Base articles at <http://support.microsoft.com>:

- “How to configure RPC to use certain ports and how to help secure those ports by using IPsec” (article ID: 908472)
- “How to configure RPC dynamic port allocation to work with firewalls” (article ID: 154596)
- “The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008” (article ID: 929851)

Automatic method

Before following the below instructions, make sure that Windows Firewall enabled on the target computer does not block any ports used by the Recovery Manager Console: these ports are required to deploy Backup Agent,

Online Restore Agent, Offline Restore Agent, Forest Recovery Agent and Management Agent. For more information about the Recovery Manager Console ports, see the Deployment Guide.

Use the following options to automatically configure Windows Firewall settings:

- To automatically configure Windows Firewall for Backup Agent, Online Restore Agent, Offline Restore Agent and Management Agent, use the Recovery Manager Console settings. For more details, see the *Ports tab* section [here](#).
- To automatically configure Windows Firewall for Forest Recovery Agent and Management Agent, use the **Agents** tab in the Recovery Project Settings dialog in Forest Recovery Console. For more details, see the [Specifying recovery project settings](#) section.
- You can automatically configure Windows Firewall settings for Backup Agent using the Computer Collection properties in Recovery Manager Console:
 - a. Open the Recovery Manager Console, expand the Computer Collections node in the console tree, and select the Computer Collection that includes the target computers where you want to automatically configure Windows Firewall.
 - b. From the main menu, select **Action | Properties**.
 - c. In the dialog box that opens, go to the **Agent Settings** tab.
 - d. Make sure the **Use preinstalled Backup Agent** check box is cleared. This is required to automatically deploy Backup Agent when the backup creation operation starts. You cannot configure Windows Firewall by using preinstalled Backup Agent.
 - e. Select the **Automatically configure Windows Firewall** check box, and click **OK**
Recovery Manager for Active Directory automatically configures Windows Firewall on each Windows Server 2008-based or later computer in the Computer Collection after the backup creation operation starts on that Collection.
- To automatically configure Windows Firewall settings for Online Restore Agent, you should select the **Automatically configure Windows Firewall** option on the **Domain Access Options** step of Online Restore Wizard.

Using Computer Collections

A Computer Collection is a group of shortcuts to the computers (domain controllers and/or AD LDS (ADAM) hosts) to be backed up with Recovery Manager for Active Directory. You can have multiple Computer Collections, each representing a group of computers you want to back up. You can populate a Computer Collection with shortcuts to specific computers available on your network and containers (for example, Active Directory domains, sites, and organizational units) that include the computers you want to back up.

Each Computer Collection has its individual properties you can use to configure such settings as backup location, backup creation schedule, performance, and backup operation logging. For more information about Computer Collection properties, see [Properties for an existing Computer Collection](#).

Computer Collections help you organize any number of computers into groups with the appropriate settings for backup creation and scheduling. A well-organized set of Computer Collections ensures that up-to-date copy of the backup information is maintained for remote computers. Therefore, it is recommended to group managed computers into Computer Collections and set appropriate properties for every Computer Collection.

This section covers the following tasks:

- [Creating Computer Collections](#)
- [Renaming Computer Collections](#)

- [Modifying Computer Collection properties](#)
- [Deleting Computer Collections](#)
- [Specifying an access account for Backup Agent, backup file storages, and Global Catalog servers](#)
- [Adding domain controllers to a Computer Collection](#)
- [Adding containers to a Computer Collection](#)
- [Adding AD LDS \(ADAM\) hosts and instances to a Computer Collection](#)
- [Removing items from a Computer Collection](#)

Creating Computer Collections

To create a Computer Collection

1. In the Recovery Manager Console tree, select the **Computer Collections** node.
2. From the main menu, select **Action | Create Collection**.

The properties of a newly created Computer Collection are preset with default values. You can change the property values for a Computer Collection, as well as the default property values. For more information, see [Modifying Computer Collection properties](#).

The Backup Wizard creates a new Computer Collection if you select the option **Later (configure backup scheduling)** on the **When to Back Up** page of the wizard. The new Computer Collection includes all objects you selected on the **What to Back Up** page.

Renaming Computer Collections

Recovery Manager for Active Directory assigns a default name to a newly created Computer Collection. You can rename a Computer Collection to assign it a more descriptive name.

To rename a Computer Collection

1. Right-click the Computer Collection and then click **Rename**.
2. Type a new name for the Computer Collection and then press ENTER.

When renaming a Computer Collection for which a backup creation task is scheduled, you may be prompted to supply the user name and password of the account under which you want to run the scheduled backup creation operation. This is because Task Scheduler may need to re-create the backup creation task when a Computer Collection is renamed. When creating a scheduled task, Task Scheduler requires that you supply the user name and password of the user account under which the task will run. For more information, see [Setting user account for scheduled tasks](#).

Modifying Computer Collection properties

To modify properties for a Computer Collection

- In the console tree, right-click the Computer Collection, and then click **Properties**.

The **Properties** dialog box opens, allowing you to specify what to back up, where to store backups, and what kind of logging to use. In addition, the **Properties** dialog box allows you to manage the backup creation schedule for the Collection and specify the user account under which the scheduled backup creation operation will run.

All settings specified in the **Properties** dialog box for a Computer Collection only relate to that Computer Collection. Different Computer Collections may have different properties.

For more information about Computer Collection properties, see [Properties for an existing Computer Collection](#).

Deleting Computer Collections

To delete a Computer Collection

- In the console tree, right-click the Computer Collection you want to delete, and then click **Delete**.

This only deletes the Computer Collection you selected along with the computer and container shortcuts it includes and the backup creation tasks scheduled for that Computer Collection. The containers, domain controllers, and AD LDS (ADAM) hosts whose shortcuts were added to the Computer Collection are not deleted. Deleting a Computer Collection does not delete the backups that were created for that Collection.

Specifying an access account for Backup Agent and backup file storages

For each Computer Collection, you can specify a user account that will be used to access the following:

- Backup Agent that is manually or automatically installed on domain controllers in the Computer Collection.
- Locations on target domain controllers or UNC shares where backup files created for the Computer Collection are to be saved. For more information on how to specify these locations, see *DC Storage tab* section in [Properties for an existing Computer Collection](#).

To specify an access account

1. In the Recovery Manager Console tree, select the Computer Collection for which you want to specify an access account.
2. From the main menu, select **Action | Properties**.
3. On the **Agent Settings** tab, select the **Use the following account to access Backup Agent and backup files** check box.
4. Click **Select Account**, and specify the user name and password of the account with which you want to access Backup Agent, backup file storages, and global catalog servers.
5. When finished, click **OK**.

If no access account is specified and no scheduled tasks exist for the Computer Collection, Recovery Manager for Active Directory will use the account under which the Recovery Manager Console is currently running.

If no access account is specified and a backup creation task is scheduled for the Computer Collection, Recovery Manager for Active Directory will use the account under which the scheduled task is run. You can view and change this account on the **Schedule** tab in the **Properties** dialog box for a Computer Collection. For more information, see *Schedule tab* subsection in [Properties for an existing Computer Collection](#).

Adding domain controllers to a Computer Collection

You can add specific domain controllers to a Computer Collection. You can select domain controllers in the details pane after browsing the console tree and selecting the container that holds the domain controllers you want to add. Domains available for a forest are located under the **Active Directory/Forest <Name>** node; containers are located under domain nodes. You can add forests to the Active Directory node by using the **Connect to Forest** command on the node's **Action** menu. A Computer Collection can hold domain controllers from multiple containers.

To add domain controllers to a Computer Collection

1. Browse the console tree to select the container that holds the domain controllers you want to add.
2. In the details pane, select the domain controllers you want to add. To select multiple domain controllers, hold down CTRL, and click the domain controllers.
3. On the **Action** menu, click **Add to Collection**.
4. In the dialog box that opens, select an existing Computer Collection or click **New Collection** to create and select a new Computer Collection.
5. In the dialog box, click **OK**.

i **NOTE:** Alternatively, you can drag the domain controllers selected in the details pane to the target Computer Collection in the console tree or use the Copy and Paste commands.

You can also select a Computer Collection, and then add domain controllers to the selected Collection.

To add domain controllers to a selected Computer Collection

1. Right-click the Computer Collection, point to **Add**, and then click **Domain Controller**.
2. In the **Select Computers** dialog box, enter the domain controller name or select the domain controller from the list and click **OK**. The **Select Computers** dialog box allows you to specify multiple domain controller names.

You can add domain controllers to a Computer Collection by using an import file that contains a list of domain controller names or IP addresses. Importing domain controllers from a file overcomes the limitations inherent to the **Select Computers** dialog box and is convenient when you need to add a large group of domain controllers.

An import file is a text file that contains one domain controller name or IP address per line. For example:

```
123.123.123.123
Domain Controller Name 1
Domain Controller Name 2
213.213.213.213
```

To add domain controllers by using an import file

1. Create an import file that contains domain controller names or IP addresses.
2. Right-click the Computer Collection, point to **Add**, and then click **Import Computers**.
3. Use the **Open** dialog box to locate and open the import file.

Adding containers to a Computer Collection

You can add containers such as Active Directory domains, sites, or organizational units to a Computer Collection. When a Computer Collection includes a container, it implicitly includes all domain controllers that are in that container. You can select containers in the details pane after browsing the console tree and selecting a node that holds the containers you want to add.

Domains are located under the **Active Directory/Forest <Name>** node, organizational units are located under domain nodes. You can add Active Directory forests to the **Active Directory** node by using the **Connect to Forest** command on the node's **Action** menu.

To add containers to a Computer Collection

1. Browse the Recovery Manager Console tree to select the node that holds the containers you want to add.
2. In the details pane, select the containers you want to add. To select multiple containers, hold down CTRL, and click the containers.
3. On the **Action** menu, click **Add to Collection**.
4. In the dialog box that opens, select an existing Computer Collection or click **New Collection** to create and select a new Computer Collection.
5. In the dialog box, click **OK**.

i **NOTE:** Alternatively, you can drag the containers selected in the details pane to the target Computer Collection in the console tree or use the Copy and Paste commands.

You can also select a Computer Collection, select a container, and then add it to the Computer Collection. In this case, you select a container by browsing the directory tree.

To add a container to a selected Computer Collection

1. Right-click the Computer Collection, point to **Add**, and then click **Container**.
2. In the **Domain** box, select the domain that includes the container or type the DNS name of the domain. If you typed the domain name, click **Connect** to redraw the tree in the **Containers** box.
3. Browse the directory tree in the **Containers** box to locate and select the container.
4. In the dialog box, click **OK**.

i **NOTE:** For a Computer Collection that includes a container, backups are created for all domain controllers in the container, including the newly created DCs that are not explicitly present in the Computer Collection .

Adding AD LDS (ADAM) hosts and instances to a Computer Collection

You can add AD LDS (ADAM) hosts and instances to a Computer Collection. AD LDS (ADAM) instances available for a selected AD LDS (ADAM) configuration set are located under the **Active Directory/AD LDS (ADAM) Configuration Set/All Instances** node. To add an AD LDS (ADAM) configuration set to a Computer Collection, you need to connect to AD LDS (ADAM).

To connect to AD LDS (ADAM)

1. In the Recovery Manager Console tree, select the **Active Directory** node.
2. From the main menu, select **Action | Connect to AD LDS (ADAM)**.
3. In the dialog box that opens, do the following:
 - a. In the AD LDS (ADAM) host box, type the full DNS name of the host to which you want to connect.
 - b. In the **Port number** box, type the port number used by AD LDS (ADAM).
 - c. In the **User name** and **Password** boxes, type the user name and password with which you want to access the AD LDS (ADAM) host. Note that to display these boxes, you may need to click the **Options** button
4. When finished, click **OK**.

To add AD LDS (ADAM) instances to a Computer Collection

1. In the Recovery Manager Console tree, expand the appropriate Active Directory/AD LDS (ADAM) Configuration Set node, and then click **All Instances**.
2. In the details pane, select the instances you want to add. To select multiple instances, hold down CTRL, and click the instances.
3. On the **Action** menu, click **Add to Collection**.
4. In the dialog box that opens, select an existing Computer Collection or click **New Collection** to create and select a new Computer Collection.
5. In the dialog box, click **OK**.

i | **NOTE:** Alternatively, you can drag the selected AD LDS (ADAM) instances to the target Computer Collection in the console tree or use the Copy and Paste commands..

You can also select a Computer Collection, and then add AD LDS (ADAM) hosts to the selected Collection.

To add AD LDS (ADAM) hosts to a particular Computer Collection

1. Right-click the Computer Collection, point to **Add**, and then click AD LDS (ADAM) Host.
2. In the **Select Computers** dialog box, enter the names of the AD LDS (ADAM) hosts you want to add or select the hosts from the list and click **Add**. The **Select Computers** dialog box allows you to specify multiple AD LDS (ADAM) host names.

Recovery Manager for Active Directory backs up all AD LDS (ADAM) instances hosted on the computer you have added to a Computer Collection.

Removing items from a Computer Collection

To remove items from a Computer Collection

1. In the Recovery Manager Console tree, select the Computer Collection from which you want to remove items.
2. In the details pane, select the items you want to remove. Use CTRL and SHIFT to select multiple items.
3. Right-click the selection, and then click **Delete**.

Managing Recovery Manager for Active Directory configuration

In this section:

- [Preparing for working with Active Directory or AD LDS \(ADAM\) backups](#)
- [Settings](#)
- [Default properties for Computer Collections](#)
- [Properties for an existing Computer Collection](#)
- [Container and site properties](#)
- [Sessions node properties](#)
- [Forest properties](#)
- [Domain properties](#)
- [Domain controller properties](#)
- [AD LDS \(ADAM\) partition properties](#)
- [AD LDS \(ADAM\) instance properties](#)
- [Showing or hiding AD LDS \(ADAM\) partitions](#)
- [Showing or hiding domains](#)
- [Showing or hiding sites](#)

Preparing for working with Active Directory or AD LDS (ADAM) backups

To restore data from Active Directory or AD LDS (ADAM) backups, Recovery Manager for Active Directory requires specific dynamic link libraries (DLLs) supplied with the Windows operating system. In case Recovery Manager for Active Directory cannot find these DLLs, the backup restore operation may fail with an error message similar to the following:

“The Active Directory database (ntds.dit) file in the backup is incompatible with the esent.dll file version found on this computer.”

Before you start using Recovery Manager for Active Directory to extract and restore data from Active Directory or AD LDS (ADAM) backups, it is recommended to ensure the required DLLs are available on the Recovery Manager for Active Directory computer.

The following table provides information on how to ensure that the required DLLs are available:

Table 6: How to ensure that required DLLs are available

Operating system on the Recovery Manager for Active Directory computer	Operating system on the backed up computer	Your action
• Windows Vista	• Windows 8	No action required

Operating system on the Recovery Manager for Active Directory computer	Operating system on the backed up computer	Your action
• Windows 7 • Windows 8 • Windows 8.1 • Windows 10 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2	• Windows 8.1 • Windows Server 2003 • Windows Server 2003 R2 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2	

Settings

To configure the various settings of Recovery Manager for Active Directory, you can use the **Settings** dialog box. In the **Settings** dialog box, you can define a TCP port for communications with the Backup Agent, Online Restore Agent, Offline Restore Agent and Management Agent, specify the default location for storing Active Directory backups, select a default method for compare and restore operations, configure settings for creating unpacked backups, or set up e-mail notifications or diagnostic logging.

To open the Settings dialog box

- In the Recovery Manager Console, select the **Recovery Manager for Active Directory** console tree root.
- On the **Action** menu, click **Settings**.

The **Settings** dialog box has the following tabs:

- [General tab](#)
- [Unpacked Backups tab \(global settings\)](#)
- [E-mail tab](#)
- [Logging tab](#)
- [Ports tab](#)

General tab

On this tab, you can specify the default location for storing Active Directory backups, or select a default method for compare and restore operations.

This tab provides the following options:

- **Default backup location.** Allows you to specify the path to the folder where to store backups. You can either type the path or click Browse to locate and select the folder.
- **Maximum number of items displayed per folder under Active Directory node.** Use this box to type the maximum number of objects that you want displayed for any single folder in the console tree under the Active Directory node.
- **Default method for compare and restore operations.** Allows you to select the default method to perform compare and restore operations in the Online Restore Wizard. For more information about the methods you can select from, see [Using agentless or agent-based method](#).
- **Include ChangeAuditor data in reports.** Includes the information on users who modified certain Active Directory objects into the reports you can generate in the Online Restore Wizard. To use this option, you must have ChangeAuditor for Active Directory installed in the home Active Directory forest of Recovery Manager for Active Directory. For more information, see [Reports about who modified Active Directory objects](#).

E-mail tab

On this tab, you can configure e-mail notification settings. Recovery Manager for Active Directory will use these settings to send notification e-mails about backup creation sessions.

This tab provides the following options:

- **SMTP server.** Provides a space for you to specify the SMTP server for outgoing messages.
- **SMTP port.** Provides a space for you to specify the port number to connect to on your outgoing mail (SMTP) server.
- **“From” address.** Provides a space for you to specify the return address for your e-mail notification messages. It is recommended that you specify the e-mail address of the Recovery Manager for Active Directory administrator.
- **SMTP server requires authentication.** When selected, specifies that you must log on to your outgoing mail server.
- **User.** Provides a space for you to specify the account name used to log on to the SMTP server.
- **Password.** Provides a space for you to specify the user password.
- **Test Settings.** Sends a test notification message to the address set in the **“From” address** text box. Use this button to verify that the specified e-mail notification settings are valid.

For more information, see [Using e-mail notification](#).

Unpacked Backups tab (global settings)

On this tab, you can specify some global (or default) settings to automatically unpack backups. By default, these settings will apply to all new Computer Collections.

This tab provides the following options:

- **Unpack each backup upon its creation.** Specifies to unpack each backup upon its creation. This option will only apply to those Computer Collections whose properties are configured to use the global settings. In this option, you can specify the number of recent backup creation sessions from which you want to keep unpacked backups for each domain in the Computer Collections.

- **Prompt me to keep backups unpacked by wizards.** Specifies that the Online Restore Wizard and the Group Policy Restore Wizard will prompt you to keep unpacked backups. Use the **Keep unpacked backups** list to specify for how long you want Recovery Manager for Active Directory to keep the backups unpacked by the wizards.

i | **NOTE:** This retention policy will run and remove all expired unpacked backups only after you create a new backup.

- **Unpacked backups folder.** Provides a space for you to specify the path to the folder where you want Recovery Manager for Active Directory to keep unpacked backups. Each unpacked backup will be saved in a separate subfolder. Type the folder path or click **Browse** to locate and select the folder.

DC selection algorithm that is used to select a DC for unpacking

1. Only one DC backup per domain is chosen for unpacking for each backup session.
2. Not Read-Only DCs are selected first.
-OR-
If there are no Not Read-Only DCs in the domain, all the DCs are supposed to be selected.
3. If several DCs are selected on the Step 2, DC with the Global Catalog role will be selected among them. If there are several DCs with the GC role, it is unpredictable which backup will be selected then.
4. The chosen backup (one per domain) is unpacked.

If there is limit for unpacked backups and it is exceeded, the specified number of the oldest backups are deleted. If individual settings are specified for a collection, backups for that particular collection are taken into account, otherwise backups of all collections that use the global settings are taken into account when comparing against the specified limit.

For more information on managing unpacked backups, see [Unpacking backups](#).

Logging tab

On this tab, you can configure diagnostic logging to write detailed information about the activity of Recovery Manager for Active Directory to log files.

This tab provides the following options:

- **Use diagnostic logging.** Select this check box to enable diagnostic logging in Recovery Manager for Active Directory. Diagnostic logging produces a set of log files detailing the activity of Recovery Manager for Active Directory.

Diagnostic logging can be resource intensive, affecting overall server performance and consuming disk space. Therefore, it should only be used temporarily when more detailed information is needed to isolate and resolve possible problems or to monitor the activity of Recovery Manager for Active Directory on your server.

- **Log files location.** Specifies the location where to create the log files. The default location is %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory\Logs.
- **Create a new set of log files.** Use this list to define how often to create a new set of log files. Each new set of log files is placed in a separate subfolder in the log files location.

Ports tab

On this tab, you can specify TCP ports that will be used by Recovery Manager Console to communicate with Backup Agent, Restore Agents and Management Agent.

This tab provides the following options:

- **Connect to Backup Agent using a specific TCP port.**
Allows you to specify the TCP port number that will be used to connect to Backup Agent installed on a target domain controller. If the option is not selected, the default port 3843 is used.
- **Connect to Online Restore Agent using a specific TCP port.**
Allows you to specify the TCP port number that will be used to connect to Online Restore Agent installed on a target domain controller. If the option is not selected, RPC dynamic port range is used by default.
- **Connect to Offline Restore Agent using a specific TCP port.**
Allows you to specify the TCP port number that will be used to connect to Offline Restore Agent installed on a target domain controller. If the option is not selected, RPC dynamic port range is used by default.
- **Automatically configure Windows Firewall**
If this option is selected, Windows Firewall settings will be configured automatically for Offline Restore Agent.
- **Connect to Management Agent using a specific TCP port.**
Allows you to specify the TCP port number that will be used to connect to Management Agent installed on a target domain controller. If the option is not selected, RPC dynamic port range is used by default..
- **Automatically configure Windows Firewall**
If this option is selected, Windows Firewall settings will be configured automatically for the operations performed by Management Agent. Management Agent is used to deploy Backup Agent, Offline Restore Agent and Forest Recovery Agent.

Default properties for Computer Collections

The default properties for Computer Collections are applied to newly created Computer Collections. Default properties are overridden by Computer Collection properties when Recovery Manager for Active Directory performs backup operations on a Computer Collection.

The default properties are used to specify where to store backups, what to back up, and how many backups to keep for each computer that belongs to a Computer Collection. The default properties include options used for performance tuning, such as bandwidth throttling, CPU usage throttling, parallel backup tuning, and data compression. The default properties also include advanced backup options, such as accessing target computers with a special account, autocorrecting registry quota, and storing a copy of each backup in an alternate location. In addition, the default properties include the logging settings that are used by default.

To view and modify the default properties for Computer Collections

- In the Recovery Manager Console tree, click the **Computer Collections** node, and then click **Collection Defaults** on the **Action** menu.

The elements you can use in the dialog box that opens are similar to those in the properties dialog box for an existing Computer Collection. For more information, see [Properties for an existing Computer Collection](#).

Properties for an existing Computer Collection

The Computer Collection properties are used to specify what data to back up, where to store backups, and how many backups to keep for each computer that belongs to the Computer Collection.

The Computer Collection properties include options used for performance tuning, such as bandwidth throttling, CPU usage throttling, parallel backup tuning, and data compression.

The Computer Collection properties also include advanced backup options, such as accessing target computers with a special account and storing additional backup copies in an alternate location.

To view and modify properties for an existing Computer Collection

- In the Recovery Manager Console tree, under **Computer Collections**, select the Computer Collection, and then click **Properties** on the **Action** menu.

The properties of a newly created Computer Collection are the same as the current default properties. After a Computer Collection is created, its properties can be modified using the **Properties** dialog box. All settings in the **Properties** dialog box are related to the given Computer Collection. Different Computer Collections may have differing settings.

The **Properties** dialog box for a Computer Collection includes the following tabs:

- [Backup tab](#)
- [System State tab](#)
- [Schedule tab](#)
- [Alerts tab](#)
- [Logging tab](#)
- [Performance tab](#)
- [Advanced tab](#)
- [Agent Settings tab](#)
- [Console Storage tab](#)
- [DC Storage tab](#)
- [Unpacked Backups tab](#)

Backup tab

The **Backup** tab allows you to specify a backup storage location and how many backups you want to retain. On this tab, you can also specify to protect backups with a password.

On this tab, you can use the following elements:

- **Backup description.** Provides a space for you to enter an optional description of the backup. The description may include expressions such as %COMPUTERNAME% or %DATETIME%.
- **Encrypt and protect backups with password.** Select this option to encrypt backups and protect them with a password. You will be prompted to specify a password for backup protection immediately after you select this check box.

When restoring data from a password-protected backup, Recovery Manager for Active Directory prompts you to type the corresponding password. The password you specify using this option is case-sensitive

and can contain any combination of letters, numerals, spaces, and symbols. If you forget or lose the password, you cannot use the corresponding password-protected backup.

- **Set Password.** Click this button to modify the password for backup protection.

System State tab

The **System State** tab is used to specify what System State components to back up.

On this tab, you can use the following elements:

- **Back up the following System State components.** Select the check boxes next to the system state components you want to back up on all the domain controllers added to the current Computer Collection.
- **When backing up Global Catalog servers, collect group membership information from all domains within the Active Directory forest.** This option works when backing up Global Catalog servers. Select this check box to ensure that objects' membership in all groups is backed up. Using a Global Catalog backup created with this option assures complete restoration of objects membership in groups in all domains within the forest, including membership in domain local groups. The use of this option may slow down the backup creation in case of a big number of domains or slow network links.
- **Collect Forest Recovery metadata.** Select this check box to create backups to be used by Recovery Manager for Active Directory Forest Edition for recovering a forest.

Schedule tab

The **Schedule** tab is used to specify the backup creation scheduling.

On this tab, you can use the following elements:

- **Backup creation schedule.** Displays a list of backup creation schedules for the currently selected Computer Collection.
- **Schedule enabled.** Enables the backup creation schedules listed in the Backup creation schedule box. To disable the schedules, clear this check box. All the task schedules are retained, and you can enable them when needed by selecting this check box.
- **Modify.** Modifies the Backup creation schedule list. In the dialog box that appears on the screen, specify new triggers or delete existing triggers.
- **User account the product will run under when creating backups.** Identifies the user account under which Task Scheduler performs the backup creation task for the currently selected Computer Collection. To change the user account, click **Select Account**.
- **Select Account.** Click this button to change the user account under which Task Scheduler performs the backup creation task for the currently selected Computer Collection.

Alerts tab

The **Alerts** tab is used to specify the logging settings to be applied when creating backups for the given Computer Collection.

 **NOTE:** SSL data encryption is not supported for email notifications.

On this tab, you can use the following elements:

- **E-mail notification.** Specifies whether to send information about backup creation sessions by e-mail.
- **To.** Provides a space for you to type a recipient's e-mail address
- **Send notification upon errors or warnings only.** Select this check box to not receive notification unless an error and/or warning is written to the log.
- **Text file.** Specifies whether to log information about backup creation sessions to an additional text file.
- **File name.** Provides a space for you to enter the path and name of a text file to be used as an additional log file.
- **View.** Click this button to view the additional log (text file) using Notepad.
- **Browse.** Click this button to locate a text file to be used as the additional log file.
- **Append to file if it already exists.** Select this check box if you never want to overwrite the log records, and always want to append entries.
- **Write to file upon errors or warnings only.** Select this check box if you want a record to be added to the text file upon errors and/or warnings only.
- **What to record.** Use this list to select what sort of information you want to be included in the notification e-mail message or written to the text file.

Logging tab

The Logging tab is used to enable the extended logging during backup.

The following options are available:

- **Global settings** - Use the default logging settings from the Recovery Manager Console root node: **Recovery Manager for Active Directory->Settings...>Logging.**
- **Enable** - If you select this option, extended logging will be enabled for all domain controllers within the collection during the backup operation.
- **Disable** - If you select this option, the log will contain only Warnings and Error messages.

The log files will be created in the **%ProgramData%\Quest\Recovery Manager for Active Directory\Logs** folder:

- Agent side (domain controller): **ErdAgent.log**
- Recovery Console: **ErdServer.log**

Performance tab

The **Performance** tab is used to configure the throttling and performance tuning settings to be applied when creating backups for the given Computer Collection.

On this tab, you can use the following elements:

- **Enable bandwidth throttling.** Limits the total bandwidth used by Backup Agent when transferring data over network links. Use bandwidth throttling to prevent excessive network traffic Backup Agent may cause.
- **Maximum network use.** Provides a space for you to specify the maximum total bandwidth Backup Agent can use when transferring data over network links.

- **Enable backup agent CPU throttling.** Limits the percentage of CPU processing time Backup Agent can use on each computer.
- **Maximum CPU use.** Provides a space for you to specify the maximum percentage of CPU processing time Backup Agent can use on each computer.
- **Create backups on at most <Number> computers in parallel.** Specifies the maximum number of computers serviced in parallel when creating backups. Increasing this number can speed backup creation. However, network saturation problems may occur. Symptoms of network saturation include slow network response when transferring data by Backup Agent, and possibly “RPC server unavailable” error messages when connecting to Backup Agent.
- **Data compression.** Specifies the compression method Backup Agent uses when processing the data before sending it over network links. Using higher compression reduces network traffic, but increases CPU load on the computers being backed up. If you are planning that backups created with Recovery Manager for Active Directory be used by other MTF-compliant backup tools, set data compression to **None**.

Advanced tab

The **Advanced** tab is used to configure a number of advanced backup settings.

On this tab, you can use the following elements:

- **Store a copy of each backup.** Stores a copy of each backup in an alternate location.
- **Specify format for backup file name.** Provides a space for you to specify format for paths and names of .bkf files where to store copies of backups. You can use UNC names to store backups in a shared network folder. The path format may include optional expressions that enable the automatic creation of subfolders. The file name format may also include expressions. For example, you might specify C:\DIRNAME\%COMPUTERNAME%\%DATETIME%.

As a result, copies of backups for different computers will be saved in separate subfolders. In addition, the file name of each backup will be composed of the date and time of the backup creation.

- **Expression.** Click this button to specify optional path and file name notations in Specify format for backup file name. You can choose the following expressions:
 - **Default backup storage (%BACKUPS%).** Path to the default backup storage folder. The default path is as follows: %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory\Backups.
 - **Domain (%DOMAIN%).** Name of the home domain of the computer being backed up.
 - **Computer name (%COMPUTERNAME%).** Name of the computer being backed up.
 - **Date and Time (%DATETIME%).** Date and time of the backup creation.
- **Browse.** Click this button to locate the folder where the copies of backups are to be stored.
- **Sample path and file matching the specified format.** Displays an example of the path and file name that matches the format string supplied in **Specify format for backup file name**.
- **Limit maximum backup time.** This option limits the maximum backup session time.

Agent Settings tab

The **Agent Settings** tab is used to specify settings for Backup Agent and Forest Recovery Agent.

The elements of the Agent Settings tab are defined as follows:

- **Use the following account to access Backup Agent and backup files.** Allows you to explicitly specify a user account under which you want the Recovery Manager Console to access Backup Agent and backup files. When this check box is cleared, the Recovery Manager Console uses the account under which it is running to access Backup Agent and backup files. To explicitly specify a user account, select this check box, and then click **Select Account** to specify the account credentials.
- **Use preinstalled Backup Agent.** Allows you to enable or disable the automatic installation of the Backup Agent. The next table explains how Recovery Manager for Active Directory behaves when this check box is selected or cleared.

Table 7: Product behavior

When this check box is selected	When this check box is cleared
Recovery Manager for Active Directory backs up only those computers where the Backup Agent is preinstalled manually.	Recovery Manager for Active Directory automatically installs the Backup Agent before backing up a computer where the agent is not preinstalled manually.
Recovery Manager for Active Directory does not automatically install the Backup Agent on the computers in the Computer Collection.	When the backup operation completes, Recovery Manager for Active Directory removes the automatically installed Backup Agent. If the Backup Agent was manually preinstalled on the computer to be backed up, Recovery Manager for Active Directory will use that agent to back up data on the computer. Recovery Manager for Active Directory does not remove preinstalled Backup Agent after the backup operation completes.

For more information on how to install, update, and uninstall the Backup Agent or discover the Backup Agent instances that were manually preinstalled in your environment, see [Managing Backup Agent](#).

- **Automatically configure Windows Firewall.** Select this check box to have Recovery Manager for Active Directory automatically configure Windows Firewall on target Windows Server 2008- or Windows Server 2012-based DCs, so that Recovery Manager for Active Directory can back up these DCs.
- **Ensure Forest Recovery Agent is deployed.** Select this check box if you want the application to verify whether Forest Recovery Agent is installed on each domain controller the Collection includes. The application reinstalls Forest Recovery Agent, if necessary. For more information, see [Using Forest Recovery Agent](#).

Console Storage tab

This tab includes the following elements:

- **Save Backups on the Recovery Manager Computer or a UNC Share.** Select this check box to save backup files either on the Recovery Manager for Active Directory computer or on the Universal Naming Convention (UNC) share you specify. Enter the location for backup files in the **Backup file name format** box. If you specify a UNC share, backup files will be streamed to that share via the Recovery Manager for Active Directory computer.

- **Backup file name format.** Use the provided space to specify format for paths and names of .bkf files where to store backups. The path format may include optional expressions that enable the automatic creation of subfolders. The file name format may also include expressions. For example, you might specify C:\DIRNAME%\COMPUTERNAME%\%DATETIME%. As a result, backups for different computers will be saved in separate subfolders. In addition, the file name of each backup will be composed of the date and time of the backup creation.
- **Expression.** Click this button to specify optional path and file name notations in **Backup file name format**. You can choose the following expressions:
 - **Default backup storage (%BACKUPS%).** Path to the default backup storage folder. The default path is as follows: %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory\Backups.
 - **Domain (%DOMAIN%).** Name of the home domain of the computer being backed up.
 - **Computer name (%COMPUTERNAME%).** Name of the computer being backed up.
 - **Date and Time(%DATETIME%).** Date and time of the backup creation.
- **Browse.** Click this button to locate the folder where backups are to be stored.
- **Sample path and file name matching the specified format.** View an example of the path and file name that matches the format string supplied in **Specify format for backup file name**.
- **For each computer, delete all backups except the last <Number>.** Select this check box to retain only a limited number of backups for each computer, and then specify the number in question. This check box can be selected only when Recovery Manager for Active Directory stores backups separately. To ensure that Recovery Manager for Active Directory does so, add the %DATETIME% expression to the path or file name in the **Backup file name format** box.

DC Storage tab

This tab includes the following elements:

- **Save Backups on the DC Being Backed Up or a UNC Share.** Select this check box to save backup files either on the domain controller being backed up or on the Universal Naming Convention (UNC) share you specify. Enter the location for backup files in the **Backup file name format** box. If you specify a UNC share, backup files will be directly streamed to that share from Backup Agent installed on the DC being backed up. Backup Agent accesses the DC being backed up and/or the specified UNC share under the account specified on the **Agent Settings** tab.
- **Backup file name format.** Use the provided space to specify format for paths and names of .bkf files where to store backups. If you want to store backups on remote computers, the path must include UNC names. The path format may include optional expressions that enable the automatic creation of subfolders. The file name format may also include expressions. For example, you might specify \\RemoteHost\ShareName%\COMPUTERNAME%\%DATETIME%. As a result, backups for different computers will be saved in separate subfolders. In addition, the file name of each backup will be composed of the date and time of the backup creation.
- **Expression.** Click this button to specify optional path and file name notations in **Backup file name format**. You can choose the following expressions:
 - **Domain (%DOMAIN%).** Name of the home domain of the computer being backed up.
 - **Computer name (%COMPUTERNAME%).** Name of the computer being backed up.
 - **Date and Time (%DATETIME%).** Date and time of the backup creation.

- **Sample path and file name matching the specified format.** View an example of the path and file name that matches the format string supplied in Specify format for backup file name.
- **For each computer, delete all backups except the last <Number>.** Select this check box to retain only a limited number of backups for each computer, and then specify the number in question. This check box can be selected only when Recovery Manager for Active Directory stores backups separately. To ensure that Recovery Manager for Active Directory does so, add the %DATETIME% expression to the path or file name in the **Backup file name format** box.

Unpacked Backups tab

This tab allows you to override the global (or default) settings used to automatically unpack backups for all Computer Collections.

On this tab, you can use the following elements:

- **Use global settings.** Specifies to use the global settings to automatically unpack each backup upon its creation.
- **Unpack each backup upon its creation.** Allows you to configure settings specific to the Computer Collection to automatically unpack each backup upon its creation. In this option, you can specify the number of recent backup creation sessions from which you want to keep unpacked backups for each domain in the Computer Collection or select the domain controllers you need. Other backups created for the Computer Collection will be automatically deleted.
- **Do not unpack backups.** Specifies not to unpack backups created for the Computer Collection.

For more information on managing unpacked backups, see [Unpacking backups](#).

Container and site properties

For a container such as an Active Directory domain, organizational unit, or site added to a Computer Collection, the properties are used to specify an explicit list of the domain controllers or AD LDS (ADAM) instances for which backups are not to be created.

To view and modify properties for a container or site

1. In the Recovery Manager Console tree, select the Computer Collection that holds the container or site.
2. In the details pane, click the container or site, and then click Properties on the Action menu.

The next subsections provide descriptions for the following:

- [Properties for a domain or organizational unit](#)
- [Properties for an Active Directory site](#)
- [Properties for an AD LDS \(ADAM\) site](#)

Properties for a domain or organizational unit

The **Properties** dialog box for a domain or organizational unit added to a Computer Collection includes the following elements:

- **Exclusion list.** Lists domain controllers that reside in the selected container for which backups are not to be created when backing up the Computer Collection. In the list, each entry includes the following fields:
 - **Name.** Displays the name of domain controller.
 - **Site.** Displays the name of the site in which domain controller is located.
- **Modify.** Opens a dialog box that allows you to modify the **Exclusion** list. The dialog box includes the following elements:
 - **Available domain controllers.** Lists domain controllers to be backed up when backing up Computer Collection. To exclude domain controllers from backup, select them in the list, and then click **Add**.
 - **Domain controllers excluded from backup.** Lists domain controllers excluded from backup when backing up Computer Collection. To have Recovery Manager for Active Directory back up domain controllers, select them in the list, and then click **Remove**.
 - **Add.** Adds domain controllers selected in Available domain controllers to the **Domain controllers excluded from backup** list.
 - **Add All.** Adds all domain controllers from Available domain controllers to the **Domain controllers excluded from backup** list.
 - **Remove.** Moves the domain controllers selected in **Domain controllers excluded from backup** to the **Available domain controllers** list.
 - **Remove All.** Clears the **Domain controllers excluded from backup** list. After you click this button, the list **Available domain controllers** will include all domain controllers that are located in the selected OU or domain.

Properties for an Active Directory site

You can view properties for an Active Directory site added to a Computer Collection or located in the Active Directory node in the console tree.

The **Properties** dialog box for an Active Directory site located in the Active Directory node in the console tree provide general information about the selected site, such as its location and description.

The **Properties** dialog box for an Active Directory site added to a Computer Collection includes the following elements:

- **Exclusion list.** Lists domain controllers that reside in the selected site for which backups are not to be created when backing up the Computer Collection. In the list, each entry includes the following fields:
 - **Name.** Displays the name of domain controller
 - **Site.** Displays the name of the site in which domain controller is located.
- **Modify.** Opens a dialog box that allows you to modify the Exclusion list. The dialog box includes the following elements:
 - **Available domain controllers.** Lists domain controllers to be backed up when backing up Computer Collection. To exclude domain controllers from backup, select them in the list, and then click Add.
 - **Domain controllers excluded from backup.** Lists domain controllers excluded from backup when backing up Computer Collection. To back up domain controllers, select them in the list, and then click Remove.

- **Add.** Adds domain controllers selected in Available domain controllers to the Domain controllers excluded from backup list.
- **Add All.** Adds all domain controllers from Available domain controllers to the Domain controllers excluded from backup list.
- **Remove.** Moves the domain controllers selected in Domain controllers excluded from backup to the Available domain controllers list.
- **Remove All.** Clears the Domain controllers excluded from backup list. After you click this button, the list Available domain controllers will include all domain controllers that are located in the selected site.

Properties for an AD LDS (ADAM) site

The **Properties** dialog box for an AD LDS (ADAM) site added to a Computer Collection includes the following elements:

- **Exclusion list.** Lists AD LDS (ADAM) instances located in the selected site for which backups are not to be created. In the list, each entry includes the following fields:
 - **Name.** Displays the name of an AD LDS (ADAM) instance.
 - **Host.** Displays the name of the computer that hosts the AD LDS (ADAM) instance.
 - **Port.** Displays the port number the AD LDS (ADAM) instance uses.
- **Modify.** Opens a dialog box that allows you to modify the Exclusion list. The dialog box includes the following elements:
 - **AD LDS (ADAM) instances to back up.** Lists the AD LDS (ADAM) instances to be backed up when backing up Computer Collection. To exclude an AD LDS (ADAM) instance, select the instance in the list, and click **Add**.
 - **Excluded AD LDS (ADAM) instances.** Lists the AD LDS (ADAM) instances not to be backed up when backing up Computer Collection. To back up an excluded AD LDS (ADAM) instance, select the instance in the list, and click **Remove**.
 - **Add.** Adds the AD LDS (ADAM) instances selected in AD LDS (ADAM) instances to back up to the **Excluded AD LDS (ADAM) instances** list.
 - **Add All.** Adds all AD LDS (ADAM) instances from AD LDS (ADAM) instances to back up to the **Excluded AD LDS (ADAM) instances** list.
 - **Remove.** Moves the AD LDS (ADAM) instances selected in **Excluded AD LDS (ADAM) instances** to the **AD LDS (ADAM) instances to back up** list.
 - **Remove All.** Clears the **Excluded AD LDS (ADAM) instances** list. After you click this button, the **AD LDS (ADAM) instances to back up** will include all ADAM instances located in the selected AD LDS (ADAM) site.

Sessions node properties

The properties of the **Sessions** node are used to specify the way backup creation sessions are to be displayed in the details pane.

To view and modify properties for sessions

In the Recovery Manager Console tree, click **Sessions**, and then click **Properties** on the **Action** menu.

The dialog box that opens includes the following elements:

- **Show all sessions.** Select this option to see all backup creation sessions in the details pane.
- **Show last <Number> sessions.** Select this option to see a number of the most recent sessions in the details pane. The box next to this option allows you to specify the number of sessions to be shown.
- **Show sessions in range.** Select this option to see the sessions that occurred within a certain time interval. The boxes below this label allow you to specify the beginning and the end of the time interval.
- **From.** Select this check box to specify the initial date from which to view sessions. The box next to **From** provides a space for you to enter a date. Click the arrow to display a calendar.
- **To.** Select this check box to specify the final date to view sessions. The text box next to this check box provides a space for you to enter a date. Click the arrow to display a calendar.
- **Show sessions for specified collection.** Select this option to see the sessions that occurred for a specific Computer Collection. The box under this label provides a space for you to select or type the name of the Computer Collection whose backup creation sessions you want to see.
- **Specify format for session names in the Sessions list.** This box allows you to specify how sessions are indicated by the **Session** column in the details pane. For example, if you enter %DATETIME% and %COLLECTION% in this box, the **Session** column indicates the date and time when the session occurred and the Computer Collection for which backups were created during the session. To enter expressions in this box, click the **Expression** button.
- **Expression.** Click this button to choose the following expressions:
 - **Collection Name (%COLLECTION%).** Name of the Computer Collection used during the session
 - **Date and Time (%DATETIME%).** Date and time when the session was started
 - **Date (%DATE%).** Date when the session was started
 - **Time (%TIME%).** Time when the session was started
 - **Result (%RESULT%).** Session result, such as success or error
 - **Type (%TYPE%).** How the session was started: manually by user or automatically by Task Scheduler

Forest properties

The **Properties** dialog box for a forest is used to view some of properties of the forest added to the Recovery Manager Console.

To add a forest to the console

1. In the Recovery Manager Console tree, click the **Active Directory** node, and then click **Connect to Forest** on the **Action** menu.
2. In the **Connect to Forest** dialog box, enter the full DNS name or IP address of any domain or domain controller from the forest, specify the user logon name and password you want to use to access the forest, and then click **OK**.

To view properties for a forest

- In the Recovery Manager Console tree, under **Active Directory**, select the forest and then click **Properties** on the **Action** menu.

The dialog box that opens includes the following elements:

- **Forest functional level.** Displays the functional level of the forest.
- **Forest-wide FSMO roles.** Displays the DNS names of domain controllers that hold the Schema Master and Domain Naming Master roles.

Domain properties

The **Properties** dialog box for a domain is used to view some of properties of the domain added to the Recovery Manager Console.

To view properties for a domain

- In the Recovery Manager Console tree, under **Active Directory/Forest/Domains**, select the domain, and then click **Properties** on the **Action** menu.

In the dialog box that opens you can use the following elements:

- **Forest functional level.** Displays the functional level of the forest to which the domain belongs.
- **Domain functional level.** Displays the functional level of the domain.
- **Domain-wide FSMO roles.** Displays the DNS names of the domain controllers that hold the RID Master, Infrastructure Master, and PDC Emulator domain-wide FSMO roles.

Domain controller properties

The **Properties** dialog box for a domain controller is used to view some of properties of the selected domain controller available for the forest added to the Recovery Manager Console.

To view properties for a domain controller

1. In the console tree, expand the **Active Directory** node, and then expand the **Forest** node for the forest where the domain controller is located. If you don't see any **Forest** node, add the forest to the console using the appropriate procedure from [Forest properties](#).
2. In the console tree, click **All Domain Controllers**. This causes the detail pane to display all domain controllers available for the selected forest.
3. In the details pane, select the desired domain controller, and then click **Properties** on the **Action** menu.

The dialog box that opens includes the following elements:

- **Operating system.** Displays the name of the current operating system installed on the domain controller.
- **Site.** Displays the name of the site in which the domain controller is located.
- **Global Catalog.** If this check box selected, the domain controller is enabled as global catalog. A global catalog stores a full replica of the directory data for its own domain and a partial replica of the directory data for every other domain in the forest.
- **FSMO roles.** Lists the forest-wide and domain-wide FSMO roles owned by the domain controller.
- **This DC hosts the following application directory partitions.** Lists the application directory partitions hosted by the selected domain controller.

AD LDS (ADAM) partition properties

You can view the properties of an AD LDS (ADAM) partition located in an AD LDS (ADAM) configuration set to which the Recovery Manager Console is connected.

To view the properties of an AD LDS (ADAM) partition

1. In the console tree, expand the **Active Directory** node, then expand the node representing the AD LDS (ADAM) configuration set that includes the AD LDS (ADAM) partition whose properties you want to view.
2. Expand the **Partitions** node, and then select the partition.
3. From the main menu, select **Action | Properties**.

The **Properties** dialog box for an AD LDS (ADAM) partition provides a list of the AD LDS (ADAM) instances that host that partition. The list includes the following elements:

- **Name.** Displays the AD LDS (ADAM) instance name.
- **Host.** Displays the full DNS name of the computer with the AD LDS (ADAM) installation.
- **Port.** Displays the port number used by AD LDS (ADAM).
- **Site.** Displays the name of the site to which the AD LDS (ADAM) instance belongs.

AD LDS (ADAM) instance properties

You can view the properties of an AD LDS (ADAM) instance located in an AD LDS (ADAM) configuration set to which the Recovery Manager Console is connected.

To view the properties of an AD LDS (ADAM) instance

1. In the Recovery Manager Console tree, expand the **Active Directory** node, then expand the node representing the AD LDS (ADAM) configuration set that includes the AD LDS (ADAM) instance whose properties you want to view.
2. Select the **All Instances** node, and then in the right pane select the instance whose properties you want to view.
3. From the main menu, select **Action | Properties**.

The **Properties** dialog box for an AD LDS (ADAM) instance provides basic information about the instance, including a list of the application directory partitions the instance hosts.

Showing or hiding AD LDS (ADAM) partitions

You can configure the Recovery Manager Console to show or hide specific AD LDS (ADAM) partitions located in an AD LDS (ADAM) configuration set to which the Recovery Manager Console is connected.

To show or hide AD LDS (ADAM) partitions

1. In the Recovery Manager Console tree, expand the **Active Directory** node, then expand the node representing the AD LDS (ADAM) configuration set that includes the AD LDS (ADAM) partitions you want to show or hide.

2. Select the **Partitions** node.
3. From the main menu, select **Action | Show Partitions**.
4. In the **Available AD LDS (ADAM) partitions** list, select the check boxes next to the partitions you want to show or clear the check boxes next to the ones you want to hide.
5. When finished, click **OK**.

Showing or hiding domains

You can configure the Recovery Manager Console to show or hide specific domains located in the Active Directory forest to which the Recovery Manager Console is connected.

To show or hide domains

1. In the Recovery Manager Console tree, expand the **Active Directory** node, then expand the node representing the forest that includes the domains you want to show or hide.
2. Select the **Domains** node.
3. From the main menu, select **Action | Show Domains**.
4. In the **Available domains** list, select the check boxes next to the domains you want to show or clear the check boxes next to the ones you want to hide.
5. When finished, click **OK**.

Showing or hiding sites

You can configure the Recovery Manager Console to show or hide specific sites located in the Active Directory forest to which the Recovery Manager Console is connected.

To show or hide sites

1. In the console tree, expand the Active Directory node, then expand the node representing the forest that includes the sites you want to show or hide.
2. Select the **Sites** node.
3. From the main menu, select **Action | Show Sites**.
4. In the **Available sites** list, select the check boxes next to the domains you want to show or clear the check boxes next to the ones you want to hide.
5. When finished, click **OK**.

Licensing

The Recovery Manager for Active Directory Forest Edition license key file specifies the licensed number of user accounts in the Active Directory domains protected with the product. If the actual number of user accounts exceeds the licensed number, Recovery Manager for Active Directory Forest Edition does not stop functioning but displays a warning message each time you back up data. In this case, you need to purchase and install a new license key file allowing you to back up a greater number of user accounts or revoke licenses from the domains whose backups you no longer need.

To view information about and manage the installed license key file, you can use the **License** tab in the **About** dialog box: in the Recovery Manager Console, right-click the **Recovery Manager for Active Directory** console tree root, and then click **About**.

The **License** tab has the following elements:

- **Licenses purchased.** Displays the maximum allowed number of user accounts you can back up using the installed license file.
- **Licenses allocated.** Displays the number of user accounts backed up with the installed license file. If this number exceeds the number of purchased licenses, Recovery Manager for Active Directory Forest Edition returns a warning message each time you back up data.
- **License usage.** Displays the number of user accounts backed up in each domain.
- **Revoke.** Revokes licenses from the domain selected in the **License usage** list. Be careful, as revoking licenses from a domain deletes all backups Recovery Manager for Active Directory Forest Edition created for that domain.
- **Install License File.** Allows you to install a new license key file purchased from Quest.

In this section:

- [Installing license key file](#)
- [Updating license key file](#)
- [Revoking licenses](#)

Installing license key file

You need to supply a valid license key file when installing Recovery Manager for Active Directory Forest Edition.

To install a license key file

1. In the Setup Wizard, on the **User Information** page, click **Browse license** to display the **Select License File** dialog box.
2. Locate the Quest license file (*.dlv) and click **Open**.

Updating license key file

If you have purchased a new license, use the Recovery Manager Console to update the license key file.

To update the license key file

1. In the Recovery Manager Console, right-click the **Recovery Manager for Active Directory** console tree root, and then click **About**.
2. In the **About** dialog box, click the **License** tab, and then click **Install License File**.
3. In the **Update License** dialog box, enter the path and name of the license key file, and then click **OK**.

Revoking licenses

When the actual number of user accounts exceeds the licensed number, Recovery Manager for Active Directory Forest Edition returns a warning message each time you back up data. In this case, you can revoke licenses from the domains whose backups you no longer need. The revoked licenses are returned to the pool of available licenses and you can allocate them to a different domain.

! CAUTION: When you revoke licenses from a domain, all backups created by Recovery Manager for Active Directory Forest Edition for that domain get deleted. You should only revoke licenses from a domain if you no longer need backups created for that domain.

To revoke licenses from a domain

1. In the console tree, right-click the root node, and then click **About**.
2. In the **About** dialog box, click the **License** tab.
3. On the **License** tab, select the domain from the **License Usage** list, and then click **Revoke**.
4. In the confirmation message box, click **Yes**.

Backing up data

- [Permissions required for the Backup operation](#)
- [Managing Backup Agent](#)
- [Using a least-privileged user account to back up data](#)
- [Creating backups](#)
- [Retrying backup creation](#)
- [Enabling backup encryption](#)
- [Backing up AD LDS \(ADAM\)](#)
- [Backing up cross-domain group membership](#)
- [Backing up distributed file system \(DFS\) data](#)
- [Backup scheduling](#)
- [Setting performance options](#)
- [Setting advanced backup options](#)
- [Using Forest Recovery Agent](#)
- [Unpacking backups](#)
- [Using e-mail notification](#)
- [Viewing backup creation results](#)

Permissions required for the Backup operation

The table below lists the minimum user account permissions required to perform the Backup operation

Table 8: Minimum permissions required for the Backup operation

Task	Minimum permissions	Details
Backing up the AD data using the preinstalled Backup Agent	Membership in the RMAD Backup Operators group -OR- Builtin\Backup Operators domain local group	Create the RMAD Backup Operators group before the Backup Agent installation. For more details, refer Using a least-privileged user account to back up data . If the Ensure Forest Recovery Agent is deployed check box is selected on the Agent Settings tab of the backup collection Properties , the account must be added to the Builtin\Administrators domain local group.
Backing up the AD data using the automatically installed Backup Agent	Membership in the Builtin\Administrators domain local group	This operation is always performed under the Recovery Manager Console account.
Installing the Backup Agent	Membership in the Builtin\Administrators domain local group -OR- Domain Admins group	

Managing Backup Agent

Recovery Manager for Active Directory employs a Backup Agent to back up data on domain controllers and AD LDS (ADAM) hosts added to Computer Collections. For this reason, the Backup Agent must be installed on each computer where you plan to back up data by using Recovery Manager for Active Directory.

For each Computer Collection, you can specify whether you want to use only preinstalled instances of Backup Agent or want to automatically install Backup Agent when necessary. You can configure Recovery Manager for Active Directory in one of the following ways:

- **Use preinstalled Backup Agent only.** When configured this way, Recovery Manager for Active Directory will only use the Backup Agent you manually preinstalled on the computers in the Computer Collection.

- **Use preinstalled Backup Agent and automatically install the agent when necessary.** With this method, Recovery Manager for Active Directory will use preinstalled Backup Agent if it is present on the target computer. If the Backup Agent is missing, Recovery Manager for Active Directory will automatically install it before backing up data on the target computer, and then will automatically remove the automatically installed agent upon the backup operation completion.

You can specify one of these methods in the Computer Collection properties. For more information, see [Agent Settings tab subsection in Properties for an existing Computer Collection](#).

In this section:

- [Installing Backup Agent automatically](#)
- [Preinstalling Backup Agent manually](#)
- [Discovering preinstalled Backup Agent](#)
- [Updating Backup Agent information](#)
- [Upgrading Backup Agent](#)
- [Uninstalling Backup Agent](#)
- [Removing a Backup Agent entry from the Backup Agent Management node](#)

Installing Backup Agent automatically

You can configure Recovery Manager for Active Directory to automatically install the Backup Agent on each computer (domain controller and AD LDS (ADAM) host) added to a particular Computer Collection. After you do so, Recovery Manager for Active Directory will automatically install the Backup Agent before backing up a computer where the agent is not preinstalled. When the backup operation completes, Recovery Manager for Active Directory will remove the automatically installed Backup Agent.

If the Backup Agent is already preinstalled on the target computer to be backed up, Recovery Manager for Active Directory does not automatically deploy the agent and uses the preinstalled agent instead.

In order Recovery Manager for Active Directory could automatically install the Backup Agent, the user account under which Recovery Manager for Active Directory accesses the target Computer Collection must have specific permissions. For more information, see [Permissions required to use Recovery Manager for Active Directory](#).

To install the Backup Agent automatically

1. In the Recovery Manager Console tree, expand the **Computer Collections** node.
2. Locate the Computer Collection that holds the computers on which you want to automatically install the Backup Agent.
3. Right-click the Computer Collection, and then click **Properties**.
4. On the **Agent Settings** tab, make sure that the **Use preinstalled Backup Agent** check box is cleared.

For more information about this check box, see *Agent Settings tab* subsection in [Properties for an existing Computer Collection](#).

5. Click **OK** to close the dialog box.

Preinstalling Backup Agent manually

You can use the Recovery Manager Console to manually preinstall Backup Agent on the computers added to a particular Computer Collection. Alternatively, you can perform a silent installation of the agent.

To preinstall Backup Agent on all computers in a Computer Collection

1. In the Recovery Manager Console tree, expand the **Computer Collections** node.
2. Right-click the Computer Collection that includes the computers on which you want to preinstall the Backup Agent, and then select **Install Backup Agent** from the shortcut menu.
3. Follow the steps in the wizard to complete the Backup Agent installation.

To selectively preinstall Backup Agent on computers in a Computer Collection

1. In the Recovery Manager Console tree, expand the **Computer Collections** node.
2. Right-click the Computer Collection that includes the computers on which you want to preinstall the Backup Agent.
3. In the right pane, select the items representing the computers on which you want to install the Backup Agent.
4. Right-click the selected items, and then select **Install Backup Agent** from the shortcut menu.
5. Follow the steps in the wizard to complete the Backup Agent installation.

To perform a silent installation of Backup Agent

1. Copy the **Backupagent.msi** file supplied in the Recovery Manager for Active Directory Forest Edition installation package to the target computer.
2. On the computer to which you copied the **Backupagent.msi** file, enter the following syntax at a command prompt:
3. `msiexec /i "\\<TargetCompName>\<Path to the backupagent.msi file>" ERDPORT=<PortNumber> /qn`

<TargetCompName> refers to the target computer network name.

<PortNumber> refers to the TCP port number you want Recovery Manager for Active Directory to use to connect to Backup Agent.

By default, the silent installation uses a local system account. To install Backup Agent on a remote DC, this account must have sufficient permissions to access that DC.

Example:

```
msiexec /i "\\MyDC\temp\backupagent.msi" ERDPORT=3355 /qn
```

By default, Recovery Manager for Active Directory uses the TCP port 3843 to connect to Backup Agent. If you have specified some other port number, perform the following steps:

1. Start the Recovery Manager Console (snap-in).
2. In the Recovery Manager Console tree, select **Recovery Manager for Active Directory**, and then click **Settings** on the **Action** menu.
3. On the **General** tab of the **Properties** dialog box, select the **Connect to the backup agent using specific TCP port** check box, and then specify the port number in the **Port** box.

If you have installed Microsoft Windows Firewall, the specified TCP port must be opened. You have to specify the same port number for all target DCs to be backed up.

Discovering preinstalled Backup Agent

You can use the Recovery Manager Console to discover all Backup Agent instances that were manually preinstalled on computers in existing Computer Collections. After the discover operation completes, you can view and manage the discovered Backup Agent instances by using the **Backup Agent Management** node in the Recovery Manager Console.

A Backup Agent instance is automatically discovered and added to the **Backup Agent Management** node only when you use that node to preinstall the agent.

When you preinstall a Backup Agent instance by using any other methods (for example, a silent installation), to display that agent instance in the Backup Agent Management node, you have to run the discover Backup Agent operation.

To discover all preinstalled instances of Backup Agent

1. In the Recovery Manager Console tree, select the **Backup Agent Management** node.
2. From the main menu, select **Action | Discover All Backup Agent Instances**.

When the agent discovery operation completes, all discovered instances of Backup Agent are displayed in the **Backup Agent Management** node.

Updating Backup Agent information

You can update information displayed for a particular preinstalled Backup Agent instance in the **Backup Agent Management** node. When you run the update operation, Recovery Manager for Active Directory checks the version and status of the target Backup Agent instance, and then updates that information in the **Backup Agent Management** node.

You can only update information for already discovered Backup Agent instances. For instructions on how to discover Backup Agent, see [Discovering preinstalled Backup Agent](#).

To update information for a particular Backup Agent instance

1. In the Recovery Manager Console tree, select the **Backup Agent Management** node.
2. In the right pane, right-click the entry representing the Backup Agent instance for which you want to update information displayed in the **Backup Agent Management** node.
3. Select **Update Backup Agent Info** from the shortcut menu.

To update information for all discovered Backup Agent instances

1. In the Recovery Manager Console tree, right-click the **Backup Agent Management** node.
2. Select **Update Backup Agent Info** from the shortcut menu.

Upgrading Backup Agent

You can use the Recovery Manager Console to selectively upgrade Backup Agent preinstalled on the computers added to a Computer Collection. Note that you can only upgrade Backup Agent to the version supplied with the Recovery Manager Console you are using.

You can only perform this operation on already discovered preinstalled instances of the Backup Agent. For more information, see [Discovering preinstalled Backup Agent](#).

To upgrade Backup Agent

1. In the Recovery Manager Console tree, select the **Backup Agent Management** node.
2. In the right pane, right-click the computer on which you want to upgrade the agent.
3. From the shortcut menu, select **Upgrade Backup Agent** and wait for the upgrade operation to complete.

Uninstalling Backup Agent

You can use the Recovery Manager Console to uninstall Backup Agent preinstalled on a computer added to a Computer Collection. You can only perform this operation on discovered instances of the Backup Agent. For more information, see [Discovering preinstalled Backup Agent](#).

To uninstall Backup Agent

1. In the Recovery Manager Console tree, select the **Backup Agent Management** node.
2. In the right pane, right-click the computer from which you want to uninstall Backup Agent.
3. From the shortcut menu, select **Uninstall Backup Agent** and wait for the uninstall operation to complete.

After the uninstallation operation completes, Recovery Manager for Active Directory removes the uninstalled Backup Agent entry from the list in the **Backup Agent Management** node.

Removing a Backup Agent entry from the Backup Agent Management node

You can selectively remove Backup Agent entries from the list provided in the **Backup Agent Management** node. Removing a Backup Agent entry from that list does not affect the corresponding preinstalled agent instance in any way. Rather, it removes the agent's registration information from the Recovery Manager Console.

You may want remove a Backup Agent entry from the list when, for example, you have uninstalled the corresponding Backup Agent instance from the computer without using the Recovery Manager Console, and the agent entry remained in the **Backup Agent Management** node.

To remove a Backup Agent entry

1. In the Recovery Manager Console tree, select the **Backup Agent Management** node.
2. In the right pane, right-click the Backup Agent entry you want to remove from the list.
3. From the shortcut menu, select **Remove from List**.

Using a least-privileged user account to back up data

You can configure Recovery Manager for Active Directory to back up data in an Active Directory domain under a least-privileged user account. A least-privileged user account is an account that has no other permissions except for those required to back up data with Recovery Manager for Active Directory.

Using a least-privileged account to back up Active Directory offers greater protection from unwanted changes to your Active Directory environment, security attacks, or unsolicited access to sensitive documents or settings.

To run backup operations under a least-privileged user account, in the domain you want to back up, create an Active Directory group named **RMAD Backup Operators**. Add the least-privileged user account you want to that group, and then preinstall the Backup Agent in the domain. As a result, members of the **RMAD Backup Operators** group are automatically granted the necessary permissions to back up data in the domain with Recovery Manager for Active Directory.

To use a least-privileged user account for backup operations

1. In the Active Directory domain you want to back up, create a new Active Directory group with the following name:

RMAD Backup Operators

2. To the **RMAD Backup Operators** group, add the least-privileged user account under which you want to back up the domain.
3. On the domain controllers you want to back up, preinstall the Backup Agent version supplied with this release of Recovery Manager for Active Directory.

Make sure you first create the RMAD Backup Operators group, and then install the Backup Agent in the domain. During its installation, the agent locates that group and grants its members the necessary permissions to back up data with Recovery Manager for Active Directory.

If the Backup Agent supplied with this release is already preinstalled, you can repair the agent's installation so that the agent could locate the **RMAD Backup Operators** group.

4. Add the domain controllers on which you preinstalled the Backup Agent to a new Computer Collection.
5. In the Computer Collection properties, on the **Agent Settings** tab, do the following:
 - Specify to access the Backup Agent with the least-privileged account you have added to the RMAD Backup Operators group.
 - Select the check box to use preinstalled Backup Agent.

For more information, see *Agent Settings tab* subsection in [Properties for an existing Computer Collection](#).

6. Back up the Computer Collection.

Creating backups

Recovery Manager for Active Directory allows you to create backups of system-specific data known as the System State. Note that Recovery Manager for Active Directory creates System State backups for Active Directory domain controllers only.

You can use Computer Collections to create backups for multiple computers. For more information, see [Using Computer Collections](#). You can specify what components of the System State are to be backed up. It is recommended to back up all System State components. For more information, see [Selecting components to back up](#).

To create backups of all computers in a Computer Collection

1. In the console tree, select a Computer Collection, and then click **Create Backup** on the **Action** menu.
2. If prompted, confirm the operation.

You can also use the Backup Wizard to start a backup job:

1. In the console tree, click the root node, and then click **Create Backup** on the **Action** menu.
2. Follow the instructions in the Backup Wizard.
3. On the **When to Back Up** page click **Now**, and then click **Next**.
4. Click **Advanced** to view backup options. You can modify the options as needed. When finished, click **OK** to close the **Properties** dialog box.
5. Click **Finish** to start the backup job.

i **NOTE:** By default, the wizard uses the default settings. You can view and modify the default settings using the **Collection Defaults** command that appears on the **Action** menu when you select the **Computer Collections** node in the console tree.

With the Backup Wizard, backup jobs can be scheduled to run at a specific time. For more information, see *Scheduling backup creation* subsection of [Task scheduler overview](#) and *Using the Backup Wizard* subsection in [Selecting components to back up](#).

While a backup job is running, you can examine the progress of the operation and, if needed, stop the backup job. After a backup job is completed, you can view backup creation results:

1. In the console tree, click **Sessions**.
2. In the details pane, click the backup-creation session, and then click **Properties** on the **Action** menu.
3. In the **Properties** dialog box, click the **Progress** tab, and examine the displayed information.
4. By clicking **Abort** on the **Progress** tab, you can stop the selected session.

Selecting components to back up

When creating a backup, Recovery Manager for Active Directory queries its configuration settings about what components of the System State to be backed up. You specify configuration settings in the **Defaults** dialog box for the **Computer Collections** node or a Computer Collection (Computer Collection properties). You can also view and modify the settings being used by the Backup Wizard.

To select components to back up

1. Do one of the following:
 - Right-click the **Computer Collections** node, and then click **Collection Defaults**.
 - Right-click the **Computer Collection** node, and then click **Properties**.
 - Click **Advanced** on the **Completing the Backup Wizard** page.
2. In the **Properties** dialog box, click the **System State** tab.
3. Under **Back up the following components**, select the check boxes next to the components you want to back up.

Default settings are also used for newly created Computer Collections. By changing the properties of a Computer Collection, you define the settings specific to that collection. Different Computer Collections may have

differing settings. The Backup Wizard uses default settings when creating a new Computer Collection unless other settings are specified using the **Advanced** button on the **Completing the Backup Wizard** page.

Using the Backup Wizard

You can start the Backup Wizard by selecting the console tree root, and then clicking **Create Backup** on the **Action** menu.

On the **What to Back Up** page, the wizard prompts you to specify what domain controllers or AD LDS (ADAM) hosts you want to back up. You can back up specific domain controllers or all computers that are in a specific container, such as an Active Directory domain or organizational unit.

On the **Where to Store Backups** page, the wizard prompts you to specify the path and name format for backup files. You can type the path and name manually, click **Browse** to locate a folder, and use the **Expression** button to have the path and name include macros enabling the automatic creation of separate subfolders and files for different backups.

On the **When to Back Up** page, the wizard asks you whether you want to schedule the backup creation operation. You can click **Now** if you want to start the operation immediately. Otherwise, you click **Later** and configure backup scheduling. If you choose to create backups without scheduling, you can optionally have the wizard create and retain a Computer Collection for the computers and containers you have selected. Later, you may use that collection to schedule backups. If you choose to schedule backups, the wizard creates a Computer Collection for the computers and containers you have selected, and schedules a backup creation task for that collection.

On the **Computer Collection Name** page, you can specify a name and description for the Computer Collection to be created.

By clicking the **Advanced** button on the **Completed the Backup Wizard** window, you can display the **Properties** dialog box to make changes to backup options. If you do not modify those options, the defaults are used. Default options are specified using the **Collection Defaults** command, which appears on the **Action** menu when you select the **Computer Collections** node in the console tree.

Retrying backup creation

Recovery Manager for Active Directory allows you to retry selected backup sessions. You can retry the creation of backups for individual computers or for all computers with a particular backup creation result. Any backup session can be retried regardless of its result.

To retry a backup session

1. In the Recovery Manager Console tree, click **Sessions**.
2. In the details pane, click the backup session to retry, and then click **Retry Backup** on the **Action** menu.
3. In the **Retry Backup** dialog box, select one of the following options:
 - **Computers where errors or warnings occurred.** Retries backup for the computers reported with errors or warnings.
 - **Computers where errors occurred.** Retries backup for the computers reported with errors.
 - **All computers.** Retries backup for all computers in the selected session, regardless of the previous backup results.
4. Click **OK** and then click **Yes**.

To retry backups for individual computers

1. In the Recovery Manager Console tree, expand the **Sessions** node and select a session.
2. In the details pane, select computers.
3. On the **Action** menu, click **Retry Backup**.
4. Click **Yes** to start the backup creation.

Enabling backup encryption

Recovery Manager for Active Directory allows you to protect your backups by encrypting them. You can enable the backup encryption in the **Defaults** dialog box for the **Computer Collections** node or a Computer Collection (Computer Collection properties), as well as in the Backup Wizard.

To enable backup encryption

1. Do one of the following:
 - Right-click the **Computer Collections** node, and then click **Collection Defaults**.
 - Right-click the Computer Collection, and then click **Properties**.
 - Click **Advanced** on the **Completing the Backup Wizard** page.
2. In the **Properties** dialog box, click the **Backup** tab.
3. On the **Backup** tab, select the **Encrypt and protect backups with password** check box.
4. In the **Set Password** dialog box, type and confirm by retyping a password, and then click **OK**.

A password can contain any combination of letters, numerals, spaces, and symbols. Passwords are case sensitive, so if you vary the capitalization when you assign the password, you must type the same capitalization when entering the password. You can change the backup protection password later by clicking **Set Password** on the **Backup** tab. Write the password down and keep it in a secure place. If you lose the password, you cannot restore data from that backup since Recovery Manager for Active Directory asks you to type the password.

i **IMPORTANT:** If you are planning to use the backups created with Recovery Manager for Active Directory in the Windows Backup utility (NTBackup), do not enable backup encryption. The Windows Backup utility cannot restore data from encrypted backups.

To encrypt backups, Recovery Manager for Active Directory uses Microsoft's implementation of the AES256 algorithm from RSA, Inc. (Microsoft RSA Base Provider), with the maximal (normally, 128-bit) cipher strength.

Backing up AD LDS (ADAM)

With Recovery Manager for Active Directory, you can back up Active Directory Lightweight Directory Services (AD LDS), previously known as Active Directory Application Mode (ADAM), by using one of the following methods:

- **Method 1: Back up AD LDS (ADAM) from the Recovery Manager Console.** Use this method to immediately back up one or multiple AD LDS (ADAM) instances.

- [Method 2: Schedule backup creation for AD LDS \(ADAM\)](#). Use this method to schedule backup creation for one or multiple AD LDS (ADAM) instances.

Method 1: Back up AD LDS (ADAM) from the Recovery Manager Console

Complete these steps:

- [Step 1: Connect to AD LDS \(ADAM\)](#)
- [Step 2: Back up AD LDS \(ADAM\)](#)

Step 1: Connect to AD LDS (ADAM)

1. Right-click the **Active Directory** node in the Recovery Manager Console tree and select **Connect to AD LDS (ADAM)**.
2. Use the dialog box that opens to specify parameters for connecting to the AD LDS (ADAM) you want to back up.
3. When finished, click **OK**.

Step 2: Back up AD LDS (ADAM)

1. In the Recovery Manager Console tree, expand the **Active Directory** node, then expand the **AD LDS (ADAM) Configuration Set** node, and select one of the following nodes:
 - **All Instances**. If you want to select one or more AD LDS (ADAM) instances to back up.
 - **Sites**. If you want to back up all AD LDS (ADAM) instances in one or more sites.
2. In the right pane, select AD LDS (ADAM) instances or sites.

These are the AD LDS (ADAM) instances you want to back up or the sites where you want to back up all AD LDS (ADAM) instances. You can select multiple instances or sites by holding down CTRL and clicking the instances or sites you want to select.

3. On the main menu, select **Action | Create Backup** and follow the instructions in the wizard that starts to complete the backup creation operation.

Method 2: Schedule backup creation for AD LDS (ADAM)

Complete these steps:

- [Step 1: Connect to AD LDS \(ADAM\)](#)
- [Step 2: Add AD LDS \(ADAM\) instances to Computer Collection](#)
- [Step 3: Create or modify backup creation schedule](#)

Step 1: Connect to AD LDS (ADAM)

1. Right-click the **Active Directory** node in the Recovery Manager Console tree and select **Connect to AD LDS (ADAM)**.
2. Use the dialog box that opens to specify parameters for connecting to AD LDS (ADAM) you want to back up.
3. When finished, click **OK**.

Step 2: Add AD LDS (ADAM) instances to Computer Collection

1. In the Recovery Manager Console tree, expand the **Active Directory** node, then expand the **AD LDS (ADAM) Configuration Set** node, and select one of the following nodes:
 - **All Instances**. If you want to schedule backup creation for one or more AD LDS (ADAM) instances.
 - **Sites**. If you want to schedule backup creation for all AD LDS (ADAM) instances in one or more sites.

2. In the right pane, select AD LDS (ADAM) instances or sites.

These are the AD LDS (ADAM) instances you want to back up or the sites where you want to back up all AD LDS (ADAM) instances. You can select multiple instances or sites by holding down CTRL and clicking the instances or sites you want to select.

3. On the main menu, select **Action | Add to Collection** and specify the Computer Collection to which you want to add the AD LDS (ADAM) instances. When finished, click **OK**.

You can also add specific AD LDS (ADAM) hosts you want to back up to a Computer Collection. For instructions, see [Adding AD LDS \(ADAM\) hosts and instances to a Computer Collection](#).

Step 3: Create or modify backup creation schedule

If necessary, create or modify backup creation schedule for the Computer Collection to which you have just added the AD LDS (ADAM) instances. For more information, see *Scheduling backup creation* subsection in [Task scheduler overview](#).

Backing up cross-domain group membership

When backing up Active Directory on a Global Catalog server, Recovery Manager for Active Directory enables the backup to include the object's membership in all groups, including those groups that reside in domains outside the object's home domain.

This option is part of the backup creation settings. You can find it on the **System State** tab in the **Properties** dialog box for a Computer Collection. The option only takes effect when backing up Global Catalog servers.

If this option is not selected, group membership spanning multiple domains is not fully backed up, 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.

To ensure that cross-domain group membership information is backed up

1. Do one of the following:
 - When creating backups for a Computer Collection, right-click the Computer Collection, and then click **Properties**.
 - When creating backups using the Backup Wizard, click the **Advanced** button on the **Completion** page of the wizard.
2. In the **Properties** dialog box, click the **System State** tab.
3. On the **System State** tab, make sure the **When backing up Global Catalog servers, collect group membership information from all domains within the Active Directory forest** check box is selected.

Using a Global Catalog backup created with this option ensures the complete restoration of object group memberships in all domains within the forest.

However, this option causes Recovery Manager for Active Directory to retrieve data from all domains within the forest, and therefore may slow down the backup creation in case of a big number of domains or slow network connections.

Backing up distributed file system (DFS) data

When backing up a domain controller, Recovery Manager for Active Directory can also back up the domain-based Distributed File System (DFS) namespace data located on the domain controller. DFS namespace data is backed up as part of SYSVOL. You can use the created backup to recover the domain-based DFS namespace.

To back up domain-based DFS namespace data, make sure you select the SYSVOL component on the System State tab in the **Computer Collection Properties** dialog box. For more information, see [Modifying Computer Collection properties](#).

Note that Recovery Manager for Active Directory cannot back up the DFS namespace links to the actual folders and files, as well as these folders and files. Also Recovery Manager for Active Directory does not support standalone DFS namespace data.

Backup scheduling

In Recovery Manager for Active Directory, a backup for a computer or a collection of computers can be created manually, or the creation of backups can be scheduled to occur at a specific time in the future. Backups can be stored in any appropriate location on your network.

Task scheduler overview

When scheduling backup creation, Recovery Manager for Active Directory employs Task Scheduler, which is an integral part of the operating system. You can access the Task Scheduler GUI by clicking Scheduled Tasks in

Control Panel. The **Scheduled Tasks** dialog box displays all tasks scheduled to run on your computer.

Each scheduled task runs under a certain user account. Therefore, you must supply the user logon name and password of a user account when creating a scheduled task. When performing the scheduled backup job, Recovery Manager for Active Directory runs as if that user started it.

The user account under which Recovery Manager for Active Directory is running when creating backups must

- Belong to the Administrators local group on the Recovery Manager for Active Directory computer.
- Belong to the Administrators local group on each computer to be backed up (serviced computer).

When scheduling a backup job, you should ensure that the account whose credentials you are supplying meets the above requirements. If there are no trust relationships established between the domains where the Recovery Manager for Active Directory computer and the serviced computer reside, then no account can satisfy both of the above requirements. To resolve this problem, you can specify a different account to access the serviced computer.

In the “no trust” situation, when scheduling a backup job, you should use an account that meets the first of the above requirements, and configure advanced backup options so that a different account is used for access to the serviced computers, satisfying the second requirement.

Scheduling backup creation

With Recovery Manager for Active Directory, you can schedule a backup creation job to run at specific times, either once or at recurring intervals. Only backup jobs for Computer Collections can be scheduled. You can schedule a backup job by modifying properties of an existing Computer Collection or you can use the Backup Wizard to schedule a backup job. When you use the Backup Wizard for backup scheduling, the wizard creates a new Computer Collection, and schedules a backup job for that Computer Collection.

To schedule backup creation for a Computer Collection

1. Right-click a Computer Collection and then click **Properties**.
2. On the **Schedule** tab, click **Modify**.
3. In the **Triggers** dialog, click **New** and then specify the task schedule settings and click **OK**.
4. On the **Schedule** tab, click **Select Account** and enter the user logon name and password of the account under which you want to run the scheduled task.

When you schedule backup creation, a new scheduled task is created and assigned to the Computer Collection.

To schedule backup creation with the Backup Wizard

1. Start the Backup Wizard and follow the provided instructions.
2. On the **When to Back Up** page, click **Later (configure backup scheduling)**, and then click the upper button labeled **Change**.
3. In the **Triggers** dialog box, click **New** and then specify the task schedule settings and click **OK**.
4. In the **When to Back Up** window, click the lower button labeled **Change** and enter the user logon name and password of the account under which you want to run the scheduled task.
5. Click **Next** and follow instructions of the wizard to complete the operation.

When you schedule backup creation with the Backup Wizard, a new Computer Collection is automatically created for the computers you have selected in the wizard, and a new scheduled task is assigned to that Computer Collection. Later, you can change, add, or remove backup schedules for that Computer Collection. You can temporarily disable the backup creation task scheduled for a particular Computer Collection, without affecting the other collections. To do so, on the **Schedule** tab in the **Properties** dialog box for that Computer Collection, clear the **Schedule enabled** check box.

Managing backup schedule

You can manage backup schedule by modifying Computer Collection properties:

1. Right-click a Computer Collection and then click **Properties**.
2. On the **Schedule** tab, click **Modify**.
3. Use the **Triggers** dialog box to add, remove, or change existing schedules.

Setting user account for scheduled tasks

Scheduled tasks are always executed under a particular user account. When scheduling backup creation, you need to specify a user account that has administrator privileges on the Recovery Manager for Active Directory computer as well as on the computers for which you plan to create backups (serviced computers).

When specifying a user account to run a scheduled backup creation task, you should consider whether you have explicitly specified an account for accessing Backup Agent and backup files. To check whether such an account is explicitly specified for a Computer Collection, you can use the **Agent Settings** tab in the Computer Collection properties. For more information, see *Agent Settings tab* subsection in [Properties for an existing Computer Collection](#).

The Managed Service Account (MSA) can be specified for scheduled tasks in the Computer Collection properties on the **Schedule** tab or in Task Scheduler.

MSA requirements:

- You can use MSA accounts only if you work with Windows Server 2012 or higher.
- Add the '\$' character at the end of the account name (e.g. domain\computername\$) and leave the **Password** field blank.
- The MSA account must be a member of the local Administrators group on the Recovery Manager for Active Directory machine.

Table 9: Requirements towards the user account

Account specified explicitly	Account specified implicitly
In this scenario, the account under which you run your scheduled backup creation task must: • Belong to the local Administrators group on the Recovery Manager for Active Directory computer.	In this scenario, the account under which you run your scheduled backup creation task must: • Belong to the local Administrators group on the Recovery Manager for Active Directory computer and on each serviced computer that hosts the data you plan to back up by using the scheduled backup creation task.

Account specified explicitly

- Have the “Log on as a batch job” user right on the Recovery Manager for Active Directory computer. This right is granted to the local Administrators group by default.

When you run the scheduled backup creation task, Recovery Manager for Active Directory uses the explicitly specified Backup Agent access account to connect to the serviced computers and back up the data they host.

Account specified implicitly

- Have the “Log on as a batch job” user right on the Recovery Manager for Active Directory computer. This right is granted to the local Administrators group by default.

If you cannot configure the scheduled backup creation task to run under a user account that has administrator privileges on the serviced computers, you may want to configure Recovery Manager for Active Directory to access the serviced computers using a user account different from that under which the scheduled task is being executed.

By doing so, you can access the serviced computers located in domains that have no trust relationships established with the domain where Recovery Manager for Active Directory is running, solving the so-called “no trust” problem. For more information, see [Setting advanced backup options](#).

To specify a user account for a scheduled task

1. Right-click Computer Collection and then click **Properties**
2. On the **Schedule** tab, click **Modify**.
3. On the **Triggers** dialog, click the **New** button and specify the task schedule settings, click **OK**.
4. Click **Select Account** on the **Schedule** tab.
5. In the **Select Account** dialog box, type the user name and password of the account you want to use, and then click **OK**.

Setting performance options

When creating a backup, Recovery Manager for Active Directory queries its configuration settings about what backup options to use. You specify configuration settings in the **Defaults** dialog box for the **Computer Collections** node or a Computer Collection (Computer Collection properties). You can also view and modify the settings being used by the Backup Wizard.

The **Properties** dialog box includes the **Performance** tab where you can set a number of backup options related to backup creation performance tuning.

To set performance options

1. Do one of the following:
 - Right-click the **Computer Collections** node and then click **Collection Defaults**.
 - Right-click the Computer Collection and then click **Properties**.
 - Click **Advanced** on the **Completing the Backup Wizard** page.
2. In the **Properties** dialog box, click the **Performance** tab.

3. To limit the total bandwidth used by backup agents when transferring data over network links, select the **Enable bandwidth throttling** check box. In **Maximum network use**, specify the maximum total bandwidth backup agents can use. Use bandwidth throttling to prevent excessive network traffic backup agents may cause creating backups for particular Computer Collections.
4. To limit the percentage of CPU processing time backup agents can use on each computer when creating backups for particular Computer Collections, select the **Enable backup agent CPU throttling** check box. In **Maximum CPU use**, specify the maximum percentage of CPU processing time backup agents can use. Use CPU throttling to prevent excessive CPU load backup agents may cause on the computers being backed up.
5. Under **Parallel backup tuning**, specify the maximum number of computers Recovery Manager for Active Directory services in parallel when creating backups. The default setting is 10 computers. Increasing this number can speed backup creation. However, when Recovery Manager for Active Directory services a number of computers in parallel and the connection is near its limits, network saturation problems may occur. Symptoms of network saturation include slow network response when transferring data by backup agents, and possibly “RPC server unavailable” error messages when connecting to backup agents. If you are experiencing such problems, decrease the number.
6. From the **Data compression** list, select the compression method backup agents will use when processing data before sending it over network links. Using higher compression reduces network traffic, but increases CPU load on the computers being backed up.

If you are planning that backups created with Recovery Manager for Active Directory be used by the Windows Backup utility (NTBackup), set data compression to **None**. The Windows Backup utility cannot read backups that were created using data compression. Additionally, to enable the Windows Backup utility to restore data from Recovery Manager for Active Directory backups, you should not use the backup encryption (see [Enabling backup encryption](#)). Default settings are used for newly created Computer Collections. By changing properties of a certain Computer Collection, you define the settings specific to that collection. Different Computer Collections may have differing settings.

The Backup Wizard uses default settings unless other settings are specified using the Advanced button on the **Completing the Backup Wizard** page.

Setting advanced backup options

When creating a backup, Recovery Manager for Active Directory queries its configuration settings about what backup options to use. You specify configuration settings in the **Defaults** dialog box for the **Computer Collections** node or a Computer Collection (Computer Collection properties). You can also view and modify the settings being used by the Backup Wizard.

The **Properties** dialog box includes the **Advanced** and **Agent Settings** tabs where you can set a number of advanced backup options.

To set advanced backup options

1. Do one of the following:
 - Right-click the Computer Collections node and then click **Collection Defaults**.
 - Right-click the Computer Collection and then click **Properties**.
 - Click Advanced on the Completing the Backup Wizard page.

2. In the **Properties** dialog box, click the **Advanced** tab. To have Recovery Manager for Active Directory store copies of backups in an alternate location, select the **Store a copy of each backup** check box and specify format for the path and name of the backup file. Having an additional instance of each backup stored in an alternate location may be required to ensure the availability of backups. You can also limit the maximum backup session time using the **Limit maximum backup time** option.
3. In the **Properties** dialog box, click the **Agent Settings** tab, and then do the following:
 - To have Recovery Manager for Active Directory initialize Backup Agent using a different account, select the **Access backup agent and backup files using the specified account** check box and click **Select Account** to supply the user logon name and password of an account that has administrator privileges on the serviced computers. Using a special account for the Backup Agent initialization may be required when Recovery Manager for Active Directory cannot be configured to run under an account with administrator privileges on the serviced computers.
 - To have the application use preinstalled Backup Agent when backing up the Computer Collection, select the **Use preinstalled Backup Agent** check box.

Default settings are used for newly created Computer Collections. By changing properties of a certain Computer Collection, you define the settings specific to that collection. Different Computer Collections may have differing settings.

The Backup Wizard uses default settings unless other settings are specified using the **Advanced** button on the **Completing the Backup Wizard** page.

Using Forest Recovery Agent

Recovery Manager for Active Directory Forest Edition helps you recover the entire Active Directory forest if a forest-wide failure renders all domain controllers in the forest incapable of functioning normally.

To recover an Active Directory forest, Recovery Manager for Active Directory Forest Edition employs a Forest Recovery Agent. The Forest Recovery Agent must be installed on each domain controller in the forest before starting a forest recovery operation.

For more information about the agent, see [Managing Forest Recovery Agent](#) in the Recovery Manager for Active Directory Forest Edition User Guide.

Unpacking backups

Recovery Manager for Active Directory can unpack backups and keep the unpacked data in the location you specify to reuse the data for subsequent starts of the Online Restore Wizard or Group Policy Restore Wizard. The use of unpacked backups accelerates operations the wizards perform during the backup data preparation step, because unpacking a backup can be a lengthy operation.

In this section:

- [Configuring default settings to unpack backups](#)
- [Configuring Computer Collection-specific settings to unpack backups](#)
- [Unpacking a backup manually](#)
- [Deleting data unpacked from a backup](#)

Configuring default settings to unpack backups

You can configure the default settings to automatically unpack backups upon their creation. These settings will apply to all new Computer Collections.

To configure the default settings

1. In the console tree, select the Recovery Manager for Active Directory console tree root.
2. On the **Action** menu, click **Settings**.
3. Specify settings on the **Unpacked Backups** tab. For more information, see **Unpacked Backups** tab (global settings) subsection in [Settings](#).
4. When finished, click **OK**.

Configuring Computer Collection-specific settings to unpack backups

For each Computer Collection, you can override the default (global) settings and configure individual settings to automatically unpack backups.

To configure individual settings for a Computer Collection

1. In the Recovery Manager Console tree, expand **Computer Collections** to select the Computer Collection.
2. On the **Action** menu, click **Properties**.
3. Specify settings on the **Unpacked Backups** tab. For more information, see *Unpacked Backups* tab subsection in [Properties for an existing Computer Collection](#).
4. When finished, click **OK**.

Unpacking a backup manually

You can manually unpack a backup by using the Online Restore Wizard or the Online Restore Wizard for AD LDS (ADAM). When you select the **Backups/Active Directory** or **Backups/AD LDS (ADAM)** node in the console tree, the details pane displays the registered Active Directory or AD LDS (ADAM) backups, respectively. For more information about the icons displayed next to backups in the details pane, see [Icons in the user interface](#).

To unpack a registered backup manually

1. Do one of the following:
 - To unpack an Active Directory backup, start the Online Restore Wizard: select the console tree root, and then on the main menu select **Action | Online Restore Wizard**.
 - To unpack an AD LDS (ADAM) backup, start the Online Restore Wizard for AD LDS (ADAM): select the console tree root, and then on the main menu select **Action | Online Restore Wizard for AD LDS (ADAM)**.
2. Follow the instructions in the wizard until you reach the **Backup Selection** page.

3. On the **Backup Selection** page, select the backup you want to unpack, and then click **Next**.
4. On the **Backup Data Preparation** page, select the **Keep extracted data after completing the wizard** check box, click **Next**, and then click **Cancel**.
5. In the message box, click **Yes** to exit the wizard.

Deleting data unpacked from a backup

Unpacked backup components (data) can occupy a significant amount of disk space, therefore it is recommended to delete the unpacked backup components you no longer need.

To delete unpacked backup components

1. In the console tree, select the **Backups/Active Directory** or **Backups/AD LDS (ADAM)** node.
2. In the details pane, select the backup whose unpacked components you want to delete, and then click **Delete Unpacked Components** on the **Action** menu.

This only deletes the unpacked data, not the backup itself.

Using e-mail notification

You can have Recovery Manager for Active Directory send an e-mail message that contains the log information about the backup creation session when backing up Computer Collections.

To use this feature, set up the appropriate settings on the **Alerts** tab in the **Computer Collection Properties** dialog box and on the **E-mail** tab in the **Recovery Manager for Active Directory Settings** dialog box.

To enable e-mail notification for a Computer Collection

1. In the console tree, click **Recovery Manager for Active Directory**, expand the **Computer Collection** node, and then select the Computer Collection in question.
2. On the **Action** menu, click **Properties**, and then open the **Alerts** tab in the **Computer Collection Properties** dialog box.
3. On the **Alerts** tab, do the following:
 - a. Select the **E-mail notification** check box.
 - b. In the **To text** box, specify the recipient's e-mail address.
 - c. Use the **What to record** list to select what sort of information you want to be included in the notification e-mail message.
 - d. If you do not want to receive notification unless an error and/or warning is written to the log, select **Send notification upon errors or warnings only**.
4. When finished, click **OK**.

To set up the e-mail notification settings

1. In the console tree, click **Recovery Manager for Active Directory**, and then click **Settings** on the **Action** menu.
2. In the **Recovery Manager for Active Directory Settings** dialog box, open the **E-mail** tab.

3. On the **E-mail** tab, specify the following settings:
 - **SMTP server**. Specifies the SMTP server for outgoing messages.
 - **SMTP port**. Specifies the port number to connect to on your outgoing mail (SMTP) server.
 - **“From” address**. Specifies the return address for your e-mail notification messages. It is recommended to use the e-mail address of the Recovery Manager for Active Directory administrator.
 - **SMTP server requires authentication**. When selected, specifies that you must log on to your outgoing mail (SMTP) server.
 - **User**. Specifies the account name used to log on to the SMTP server.
 - **Password**. Specifies the user password.
4. When finished, click **OK**.

Before you start using the e-mail notification, it is recommended that you verify the specified settings. To do so, in the **“From” address** text box, click the **Test Settings** button that sends a test notification message to the address set.

Viewing backup creation results

To view backup creation results, you can examine the properties of backup creation sessions, computers, computers within a backup creation session, and backups registered in the Recovery Manager for Active Directory backup registration database.

In this section:

- [Sessions node properties](#)
- [Computer properties](#)
- [Computer session properties](#)
- [Backups node properties](#)
- [Filtering backups](#)
- [Properties of registered AD and AD LDS \(ADAM\) backups](#)

Sessions node properties

Session properties are used to view the details about a particular backup creation session and to stop the backup creation process, if necessary.

To display the Properties dialog box for a backup creation session

1. In the console tree, click **Sessions**.
2. In the details pane, click the session, and then click **Properties** on the **Action** menu.

The **Properties** dialog box for a backup creation session includes the **Progress** tab and the **General** tab.

Progress tab

You can use the Progress tab to view the progress of the backup creation process. The tab is displayed only while the session is in progress. The tab includes the following elements:

- **Log records.** Lists computers being serviced during the current backup-creation session and displays the session result.
- **Abort.** Stops the backup creation.

General tab

The General tab is used to display general information about the session. You can click **View Settings** to view the settings that were used during the session. The dialog box that opens is similar to the **Properties** dialog box for Computer Collections.

Computer properties

To view the history of backup creation sessions for a computer, you can use the computer's properties.

To view backup history for a computer

1. In the console tree, select the Computer Collection that includes the computer whose backup history you want to view.
2. In the details pane, right-click the computer, and then click **Properties** on the shortcut menu.
3. Use the **Backup History** tab to view a list of backup creation sessions for the selected computer. The list only includes the sessions for which information is available in the internal log.

You can use the **General** tab in the **Properties** dialog box to view general information about the selected computer.

Computer session properties

Once you have identified a session using the **Backup History** tab, you can use the **Properties** dialog box to examine backup creation results for a computer within that session.

To view properties for a computer within a session

1. In the console tree, expand the **Sessions** node, and select the session.
2. In the details pane, select the computer, and then select **Action | Properties** from the main menu.
3. The dialog box that opens includes the **General tab**, the **Events tab**, and the **Backup tab**.

General tab

Displays an overall result of the computer session, indicating the reason of failure if backup creation has failed. You can click the **Copy to Clipboard** button to copy the information displayed on this tab to the Clipboard.

Events tab

Briefly describes all warning and error messages generated by Recovery Manager for Active Directory when creating the computer's backup.

Backup tab

Lists all components that the backup includes, displays the backup description, provides the backup file path and name, and shows whether the backup is encrypted. The Backup tab is displayed only if the backup has been created for the selected computer within the selected session.

The **Backed up components** list displays the System State components included in the backup. The list has the following columns:

- **Component.** Identifies the component; for the Registry component, individual hives are listed.
- **Original Size.** Shows the size, in kilobytes, of a component on the source system, before data compression by Backup Agent.
- **Size in Backup.** Shows the size, in kilobytes, of a component in the backup, after data compression by Backup Agent.
- **Compression Ratio.** Show the ratio, in percents, between the component size in backup and the original component size. For example, the 25% compression ratio means 4:1 compression.
- **View.** Shows backed up system and boot files. This button is only available if the backup includes those files.

Backups node properties

The **Backups** node in the console tree allows you to view a list of backups registered in the Recovery Manager for Active Directory backup registration database.

To view a list of Active Directory backups

- In the console tree, expand the **Backups** node, and then click **Active Directory**. The details pane displays the registered Active Directory backups.

To view a list of AD LDS (ADAM) backups

- In the console tree, expand the **Backups** node, and then click **AD LDS (ADAM)**. The details pane displays the registered AD LDS (ADAM) backups.

You can also register additional backups.

To register additional backups

1. In the console tree, right-click the **Backups** node.
2. On the shortcut menu, point to **Register Backup**, and then click one of the following commands:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf; e.g. Windows Backup file) or Windows Server backup file (.vhd, .vhdx). You must specify the path and name for the file to register.

- **Register Backups in Folder.** Registers all MTF-compliant backup files (.bkf) or Windows Server backup files (.vhd, .vhdx) stored in the specified folder.
- **Register Offline Active Directory Database.** Registers Active Directory database (ntds.file) unpacked from a backup created with third-party backup tools.
- **Register Offline AD LDS (ADAM) Database.** Registers AD LDS (ADAM) database (adamntds.dit file) unpacked from a backup created with third-party backup tools.

Filtering backups

The properties of the **Backups | Active Directory** and **Backups | AD LDS (ADAM)** nodes allow you to have Recovery Manager for Active Directory display all backups or specific backups filtered by the backup source and/or backup dates.

To display the Properties dialog box for the Active Directory node or the AD LDS (ADAM) node

1. In the console tree, click **Backups**, and then select **Active Directory** or **AD LDS (ADAM)** in the details pane.
2. On the **Action** menu, click **Properties**.

The **Properties** dialog box includes the **General** tab.

General tab for Active Directory backups

The **General** tab enables you to filter Active Directory backups displayed in the details pane of the Recovery Manager Console (snap-in).

- **Filter backups view.** Select this check box to activate the backups filtering. You can filter backups based on backups sources or dates. Leave this check box cleared to have Recovery Manager for Active Directory display all registered backups in the details pane.
- **Backup sources.** This option allows you to filter backups based on backup sources. For example, you can have Recovery Manager for Active Directory display only backups taken from the specified domain controller.
 - **Domain controller.** Provides a space for you to type the name of a domain controller. Recovery Manager for Active Directory will display only backups taken from that domain controller.
 - **Domain.** Provides a space for you to type the name of a domain. Recovery Manager for Active Directory will display only backups taken from domain controllers that belong to that domain.
 - **Site.** Provides a space for you to type the name of a site. Recovery Manager for Active Directory will display only backups taken from domain controllers located in that site.
- **Backup dates.** This option allows you to filter backups based on backup dates.
 - **From.** Select this check box to see backups that were taken starting with a specific date. To specify the date, use the list next to the check box.
 - **To.** Select this check box to see backups that were taken till a specific date. To specify the date, use the list next to the check box.

General tab for AD LDS (ADAM) backups

The **General** tab enables you to filter the AD LDS (ADAM) backups displayed in the details pane of the Recovery Manager Console (snap-in).

- **Filter backups view.** Select this check box to activate the backups filtering. You can filter backups based on backups sources or dates. Leave this check box cleared to have Recovery Manager for Active Directory display all registered backups in the details pane.
- **Backup sources.** This option allows you to filter backups based on backup sources. For example, you can have Recovery Manager for Active Directory display only backups taken from the specified AD LDS (ADAM) instance.
 - **Host.** Provides a space for you to type the name of a computer. Recovery Manager for Active Directory will display only backups taken from AD LDS (ADAM) instances hosted by that computer.
 - **Instance.** Provides a space for you to type the name of an AD LDS (ADAM) instance. Recovery Manager for Active Directory will display only backups taken from that AD LDS (ADAM) instance.
 - **Site.** Provides a space for you to type the name of a site. Recovery Manager for Active Directory will display only backups taken from AD LDS (ADAM) instances located in that site.
- **Backup dates.** This option allows you to filter backups based on backup dates.
 - **From.** Select this check box to see backups that were taken starting with a specific date. To specify the date, use the list next to the check box.
 - **To.** Select this check box to see backups that were taken till a specific date. To specify the date, use the list next to the check box.

To filter backups

1. Select the **Filter backups view** check box.
2. Do the following:
 - To filter by backup sources, fill in the corresponding fields under **Backup sources**.
 - To filter by backup creation dates, specify the dates under **Backups dates**.

Properties of registered AD and AD LDS (ADAM) backups

The **Properties** dialog box for a registered Active Directory or AD LDS (ADAM) backup provides detailed information about the backup, such as the backup creation date, backup size, and a list of the system state components the backup includes.

To display the Properties dialog box for the Active Directory or AD LDS (ADAM) backup

1. In the console tree, expand the **Backups** node, and then select **Active Directory** or **AD LDS (ADAM)**.
2. In the details pane, select the desired backup, and then click **Properties** on the **Action** menu.

The **Properties** dialog box for the Active Directory or AD LDS (ADAM) backup includes the **General** and the **Components** tabs.

General tab

The **General** tab displays general information about the selected backup.

Components tab

The **Components** tab displays a list of the System State components the backup includes.

The **Backed up components** box lists the system components included in the backup. In the list, each entry includes the following fields:

- **Component.** Displays the name of the backed up component.
- **Unpacked.** Indicates whether the component is unpacked (False or True.)
- **Size in Backup.** Displays the size of a component in the backup, after data compression by Backup Agent.
- **Original Size.** Displays the size of a component on the source system, before data compression by Backup Agent.
- **Path.** Displays the path to the unpacked components, if any.

Restoring data

- [Getting started with Active Directory recovery](#)
- [Managing deleted or recycled objects](#)
- [Restoring backed up System State components](#)
- [Using granular online restore](#)
- [Restoring AD LDS \(ADAM\)](#)
- [Selectively restoring Active Directory object attributes](#)
- [Restoring objects in an application directory partition](#)
- [Restoring object quotas](#)
- [Restoring cross-domain group membership](#)
- [Performing a restore without having administrator privileges](#)
- [Reports about objects and operations](#)
- [Using complete offline restore](#)
- [Offline restore implications](#)
- [Restoring SYSVOL authoritatively](#)
- [Performing a granular restore of SYSVOL](#)
- [Recovering Group Policy](#)
- [Restoring data from third-party backups](#)
- [Using the Extract Wizard](#)
- [Restoring passwords and SID history](#)

Getting started with Active Directory recovery

This section provides important information about performing data recovery operations with Recovery Manager for Active Directory. Please read it carefully before you start using the product to restore Active Directory data.

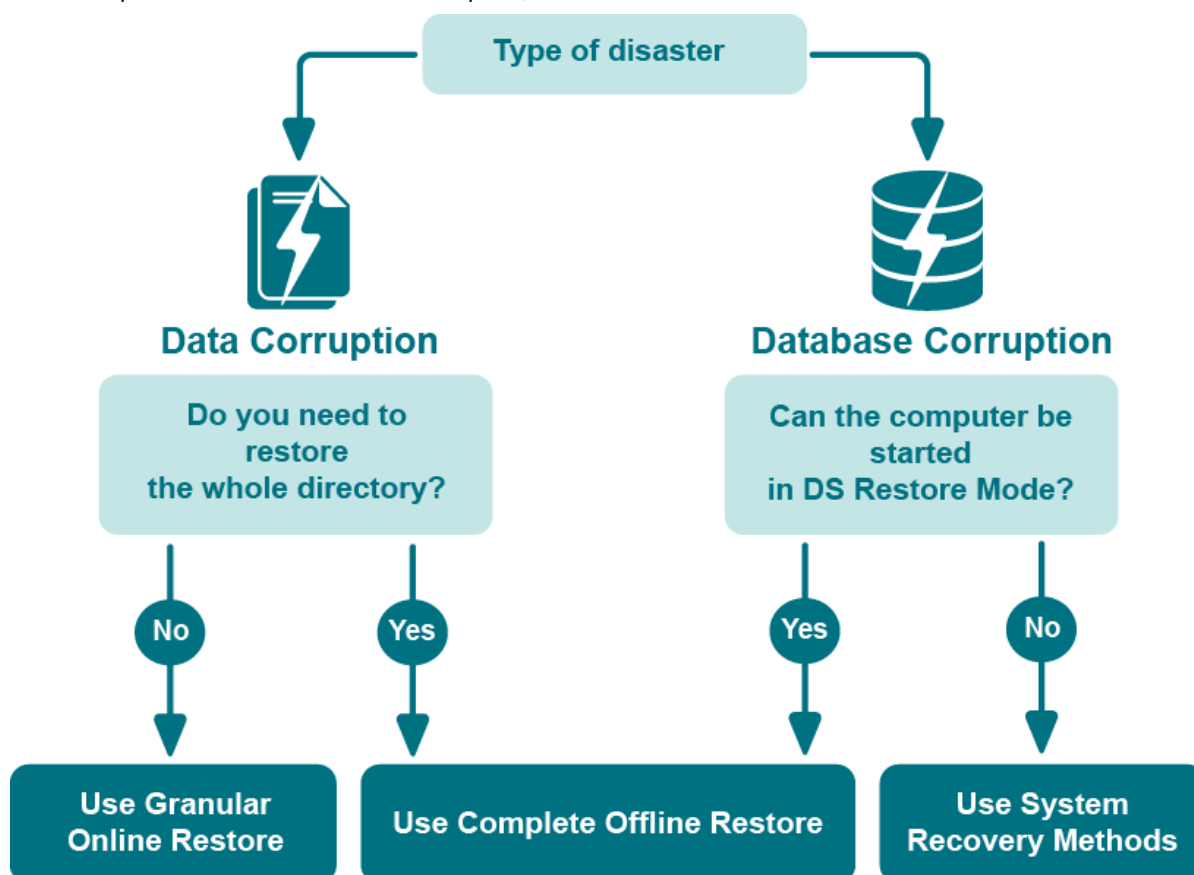
This section covers:

- [Choosing an Active Directory recovery method](#)
- [Implications of the online restore](#)
- [Using agentless or agent-based method](#)

Choosing an Active Directory recovery method

Recovery Manager for Active Directory 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.

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 for Active Directory offers two methods for restoring Active Directory object data on a domain controller: granular online restore and 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 for Active Directory 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 operation.

Implications of the online restore

This section provides important information that you should consider when using the Online Restore Wizard.

The wizard allows you to selectively restore a portion of the Active Directory domain naming context. At that, the wizard causes Active Directory to replicate this restored state of objects, overwriting the copies currently held on

all domain controllers within the domain. The restored objects and object attributes receive a version greater than the current set of directory objects. As a result, the restored objects appear to be more recent and therefore they are replicated out to the other domain controllers within the domain.

Restore the wizard performs is authoritative. With an authoritative restore, Active Directory object data reverts to the state it had when the backup was created and any updates that were made after that point are lost. For example, obsolete passwords could be restored, which may have impact on user and computer accounts.

One more issue related to authoritative restore is the impact on linked attributes, such as group memberships. For example, when you authoritatively restore a user that is currently marked as deleted (undelete a user account), in some recovery scenarios you risk possible loss of group membership information.

To ensure the correct restoration of group memberships, along with the other linked attributes, the Online Restore Wizard can force incremental replication of Active Directory. Incremental replication transfers only the changes that occurred since the last replication.

Once the wizard has undeleted some objects for which linked attributes need to be restored, it reminds you that the un-deletion must be replicated to all domain controllers for the linked attributes to be correctly represented on each domain controller. The wizard prompts you to choose whether to force the replication, skip the replication, or stop the operation.

Before making a choice, consider the following:

- [Forcing replication](#)
- [Skipping replication](#)
- [Stopping online restore](#)

Forcing replication

When you choose to force the replication, the wizard ensures that all linked attributes, such as group memberships, of the undeleted objects are correctly restored on all domain controllers.

This choice may result in considerable replication traffic, depending on the number of domain controllers in your domain. However, it is required because of the way links and deletions are dealt with in Active Directory. Before the restoration of linked attributes, the undeleted objects must be replicated to all domain controllers for the restored linked attributes to be correctly represented on each domain controller.

This requirement stems not from the wizard's implementation, but from the way in which the data is replicated in Active Directory.

Skipping replication

When you choose not to force the replication, you may risk a loss of linked attributes, such as group memberships, on replication partners after the normal Active Directory replication transfers the undeletion to all domain controllers.

For example, when you select a user to be undeleted, with the user being a member of a certain group, and choose not to have the wizard force the replication, the results of the restore on the representation of the user's group memberships may vary. These variations are based on which objects replicate first after the wizard completes the restore.

If the undeletion of the user replicates first, then the group membership information of both the group (the members it contains) and the user (the groups he or she belongs to) will be represented correctly.

If the restore of the group replicates first, the replication partners will drop the addition of the (locally) deleted user from the group membership. The only exception to this is the user's primary group, which is always represented correctly from both the user and group reference.

The wizard marks the undeleted objects so that they are replicated in a proper sequence. However, making changes to them before the replication is completed may break the proper sequence. Skip the replication enforcement if you are sure that no changes will be made to the restored objects until those objects are replicated to all domain controllers within the domain. Optionally, you may have the wizard force the incremental replication on the final step. You might also force the replication with a different tool, or wait for replication to occur on normal schedule.

In addition, you might skip the replication enforcement if you undelete objects whose deletions are not yet replicated within your domain. In that scenario, the objects in question are not marked as deleted on other domain controllers, which ensures the correct representation of linked attributes.

Stopping online restore

When you choose to stop the online restore operation, the wizard neither forces the replication nor restores linked attributes.

This choice implies that you wait until the undeleted objects are replicated to all domain controllers, and then restore those objects once more using the wizard. In that scenario, the second path of the wizard is used to restore the linked attributes on the undeleted objects. Stop the operation if the enforcement of replication in your domain is inadmissible for some reasons, but you want to be sure that linked attributes be represented correctly on all domain controllers.

Using agentless or agent-based method

When comparing or restoring Active Directory objects with the Online Restore Wizard, you can choose whether to use LDAP functions only ([Agentless method](#)) or Online Restore Agent ([Agent-based method](#)).

Note that some AD DS and AD LDS (ADAM) object attributes cannot be restored by using Recovery Manager for Active Directory. For more information on these attributes, see Quest Knowledge Base Article 59039 “[AD DS and AD LDS Object Attributes That Recovery Manager for Active Directory Cannot Restore](#)” at support.quest.com.

The following table contains performance test results of agentless and agent-based restore operations on the machine running Windows Exchange Server 2008 R2. The agent-based restore is performed by a single Restore Agent instance.

Configuration of the test lab:

Operating System	CPU	RAM,GB
Windows Server 2008 R2	2 x Intel Xeon E5-2651 v2 1,8 GHz	7,5

Performance test results:

Recovery method	Number of objects	Required time
Agent-based restore	1000	20 - 40 sec
	10000	4 - 6 min
	50000	23 - 34 min
Agentless restore	1000	40 - 70 sec
	10000	6 - 10 min
	50000	30 - 50 min

Agentless method

The method that uses LDAP functions is referred to as agentless method. The agentless method has both advantages and limitations. The use of LDAP functions makes the wizard operations less intrusive on the domain controller. Also, you can deliberately choose the target domain controller and you can perform restore and compare operations without having administrative access to the target domain controller.

However, some object attributes, such as User Password and SID History, cannot be compared or restored.

The ability to perform an online restore using the agentless method builds on the Restore Deleted Objects feature that was first introduced in Windows Server 2003. This feature extends the LDAP API to enable the restoration of deleted objects. However, this feature restores only the essential attributes required for the object's existence. Other attributes, such as those relating to membership in security and distribution groups, must be restored from a backup.

With the agentless method, you can perform a restore without having administrative access to the target domain controller. For more information, see [Performing a restore without having administrator privileges](#).

To use the agentless method

In the Online Restore Wizard, on the [Domain Access Options](#) page, make sure the **Use agentless method to access domain controller** check box is selected. This ensures that only LDAP functions are used to access the domain controller.

Agent-based method

To overcome the limitations of the agentless method, the Online Restore Wizard provides the alternative, agent-based method. With the agent-based method, you can compare and restore any objects (including deleted ones) and any attributes (including User Password and SID History). A restore can be performed on a domain controller running any operating system supported by Recovery Manager for Active Directory.

However, the agent-based method has the following drawbacks:

- The target domain controller must be the same as that from which the backup was created. No ability to choose the target domain controller for the restore and compare operations.
- The restore or compare operation is more intrusive: Online Restore Agent is installed on the domain controller when you start the compare or restore operation in the Online Restore Wizard and removed when you close the wizard.
- Domain administrator rights on the target domain controller are required.

To use the agent-based method

- In the Online Restore Wizard, on the [Domain Access Options](#) page, make sure the **Use agentless method to access domain controller** check box is cleared, so that Recovery Manager for Active Directory employs Online Restore Agent to perform the restore or compare operation.

To set a default method for compare and restore operations performed in the Online Restore Wizard

1. Select the Recovery Manager for Active Directory console tree root.
2. On the main menu, select **Actions | Settings**.

In the dialog box that opens, on the **General** tab, under **Default method for compare and restore operations**, select the preferable method, and click **OK**. You can change the set default method later when using the Online Restore Wizard.

Managing deleted or recycled objects

With Recovery Manager for Active Directory, you can perform the following tasks on deleted or recycled Active Directory objects:

- View a list of deleted and/or recycled objects in a particular Active Directory domain.
- Selectively recover deleted Active Directory objects by either undeleting (reanimating) them or restoring the objects from a backup created with Recovery Manager for Active Directory.
- To undelete (reanimate) an object, Recovery Manager for Active Directory 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.
- Recycle deleted Active Directory objects (only when Microsoft's Active Directory Recycle Bin feature is enabled in your environment).
- Recover recycled Active Directory objects from backups created with Recovery Manager for Active Directory.

In order you could selectively recover Active Directory objects, the user account under which Recovery Manager for Active Directory is running must have specific permissions. For more information on these permissions, see [Permissions required to use Recovery Manager for Active Directory](#).

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) (<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 object's deletion. During the tombstone lifetime period, you can use Recovery Manager for Active Directory to undelete (reanimate) the object or restore it from a backup created with Recovery Manager for Active Directory. 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:

- **Deleted state.** 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 object's deletion.

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

If necessary, you can use Recovery Manager for Active Directory to override the applicable deleted object lifetime setting and manually transfer specific deleted object state from "deleted" to "recycled" state. For more information, refer to [Recycling deleted objects](#).

- **Recycled state.** 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.

To manage recycled objects, you can use the Deleted Objects container provided by Recovery Manager for Active Directory. In this container, you can view a list of all recycled objects in the domain, selectively recycle deleted objects, and recover recycled objects from backups created with Recovery Manager for Active Directory.

For more information, see [Recycling deleted objects](#).

In this section:

- [Recovering deleted objects](#)
- [Recycling deleted objects](#)
- [Recovering recycled objects](#)

Recovering deleted objects

This section provides instructions on how to selectively recover deleted objects in a domain and how to recover all deleted objects in an organization unit.

To selectively recover deleted objects

1. On the Recovery Manager for Active Directory computer, start the Recovery Manager Console, then expand the appropriate console tree node nodes to locate the **Deleted Objects** container in the domain where you want to recover deleted objects.
2. If necessary, browse to select the subcontainer that includes the deleted objects you want to recover.
3. In the right pane, select the objects you want to recover. To select multiple objects, hold down CTRL, and click the objects you want to select.

To locate specific deleted objects, you can:

Table 10: Locating deleted objects

Task	Locating deleted objects
Sort objects	Click the heading of the right pane column by which you want to sort the objects. For example, you can click the heading of the Name column to sort the objects by their names.
Group objects	Point to the heading of the right pane column by which you want to group the objects, then click the down arrow button, and click Group . To ungroup the objects, repeat these actions.
Filter objects	Point to the heading of the right pane column by which you want to filter the objects, then click the down arrow button, and specify the filter criteria.
Limit the number of displayed objects	Select the Deleted Objects node in the console tree, then, from the main menu, select Action Set View Options , and specify how many recently deleted objects you want to view. You can also perform these actions on any container located in the Deleted Objects node.

Task	Locating deleted objects
View objects in a hierarchy	Select the Deleted Objects node in the console tree, then, from the main menu, select Action View as Hierarchy .
View objects in a flat list	Select the Deleted Objects node in the console tree, then, from the main menu, select Action View as Flat List .

4. From the main menu, select **Action | Recover Deleted Objects**.
5. Follow the steps in the wizard to complete the recovery operation. You can either undelete the objects or restore them from a backup created with Recovery Manager for Active Directory.

To recover all deleted objects in an organizational unit

1. On the Recovery Manager for Active Directory computer, start the Recovery Manager Console, then expand the appropriate console tree node nodes to locate the **Deleted Objects** container in the domain where you want to recover deleted objects.
2. Browse to select the organization unit in which you want to recover all deleted objects.
3. From the main menu, select **Action | Recover Deleted Objects**.
4. Follow the steps in the wizard to complete the recovery operation. You can either undelete the objects or restore them from a backup created with Recovery Manager for Active Directory.

Recycling deleted objects

In the Active Directory forest where Microsoft's Active Directory Recycle Bin is enabled, you can use Recovery Manager for Active Directory to override the applicable deleted object lifetime setting and manually change the state of a deleted object from "deleted" to "recycled". For more information about the "recycled" state, see [Managing deleted or recycled objects](#).

To manually recycle deleted objects

1. On the Recovery Manager for Active Directory computer, start the Recovery Manager Console, then expand the appropriate console tree node nodes to locate the **Deleted Objects** container in the domain where you want to recycle deleted objects.
2. If necessary, browse to select the subcontainer that includes the deleted objects you want to recycle.
3. In the right pane, select the deleted objects you want to recycle. To select multiple objects, hold down CTRL, and click the objects you want to select.

To locate specific deleted objects, you can:

Table 11: Locating deleted objects

Task	Your action
Sort deleted objects	Click the heading of the right pane column by which you want to sort the objects. For example, you can click the heading of the Name column to sort the objects by their names.
Group deleted objects	Point to the heading of the right pane column by which you want to group the objects, then click the down arrow button, and click Group . To ungroup the objects, repeat these actions.

Task	Your action
Filter deleted objects	Point to the heading of the right pane column by which you want to filter the objects, then click the down arrow button, and specify the filter criteria.
Limit the number of displayed deleted objects	Select the Deleted Objects node in the console tree, then, from the main menu, select Action Set View Options , and specify how many recently deleted objects you want to view.
View deleted objects in a hierarchy	Select the Deleted Objects node in the console tree, then, from the main menu, select Action View as Hierarchy .
View deleted objects in a flat list	Select the Deleted Objects node in the console tree, then, from the main menu, select Action View as Flat List .

4. From the main menu, select **Action | Recycle Deleted Objects**.

You can also recycle deleted objects by using cmdlets supplied with the Recovery Manager for Active Directory Management Shell.

Recovering recycled objects

With Recovery Manager for Active Directory you can only recover recycled objects by restoring them from a backup created with Recovery Manager for Active Directory. Therefore, make sure that you have at least one backup that includes the recycled objects you want to recover.

To recover recycled objects

1. On the Recovery Manager for Active Directory computer, start the Recovery Manager Console, then expand the appropriate console tree node nodes to select the **Deleted Objects** container in the domain where you want to view a list of recycled objects.
2. From the main menu, select **Action | View as Flat List**.
3. Filter the objects by the recycled state:
 - a. In the right pane, point to the heading of the **Object State** column, and then click the down arrow.
 - b. Select the **Recycled** check box and clear the **Deleted** check box.
4. In the right pane, select the recycled objects you want to recover. To select multiple objects, hold down CTRL, and click the objects you want to select.
5. From the main menu, select **Action | Recover Deleted Objects**.
6. Follow the steps in the wizard to restore the selected recycled objects from a backup created with Recovery Manager for Active Directory.

Restoring backed up System State components

Recovery Manager for Active Directory enables the backup and restoration of the following System State components on Active Directory domain controllers:

- Active Directory, including DIT Database and SYSVOL
- Registry, including all registry hives and the file NTUSER.DAT
- Certificate Services Database
- COM+ Class Registration Database
- Boot Files
- IIS Metabase
- Performance Counters
- Cluster Quorum

To restore backed up System State components

1. Start the Repair Wizard and follow the instructions in the wizard.
2. On the Computer and Backup Selection page, double-click the computer whose backup you want to use, and then double-click the backup you want to use. Select the check box next to **System State** and then click **Next**.
3. Follow the wizard to walk through the restore process.

To ensure the selected backup contains all System State components needed for the restore, browse the **System State** branch on the Computer and Backup Selection page.

With the Repair Wizard, you can restore data from System State backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec or Windows Server backup file (.vhd, .vhdx). To use a backup, on the Computer and Backup Selection page, click **Register**, and then click **Register Backup File**. The wizard catalogs the backup and adds a new entry to the list of backups.

Snapshot backups are not supported by the Repair Wizard. However, you can restore Active Directory data from such backups using the Online Restore Wizard and Group Policy Restore Wizard. The Extract Wizard also supports snapshot backups.

Restoring cluster information

When restoring the Cluster Quorum component on a cluster node, Recovery Manager for Active Directory leaves the quorum data in a folder on the node's disk, but does not restore it to the quorum disk at that time. Restoring the quorum disk requires that the cluster be stopped and restarted, which may not be necessary or desirable.

The process of restoring a single node of a cluster is straightforward: you must restore all the System State components, including Cluster Quorum, to the node, and then restart the node. This causes the node to rejoin the cluster and restores it to operation.

To restore the quorum disk, following the node restore, use the Cluster Quorum Restore tool (Clusrest.exe) provided by Microsoft.

To restore a cluster node using Recovery Manager for Active Directory

1. Start the Repair Wizard (select the console tree node, then select **Action | Repair Wizard** from the main menu). Follow the instructions in the Repair Wizard.
2. On the Computer and Backup Selection page, select the cluster node and a backup of that node. The backup must include the **Cluster Quorum** component.

3. Click **Next** and follow the instructions in the wizard to complete the restore.
4. Restart the node.

When restoring a cluster node, you must use a backup taken from that particular node. Therefore, it is important that you select a backup of the node you are restoring. We recommend creating backups of cluster physical nodes (computers) rather than a cluster itself (cluster virtual node). Otherwise, it will be difficult to identify the physical node from which the backup was taken.

To restore the quorum disk with the Clusrest tool

1. Use Recovery Manager for Active Directory to restore any node of the cluster. This deposits the quorum data on the node's disk drive. The quorum data must be placed on the disk before running the Clusrest tool.
2. On the restored node, at the command prompt, enter the following command:

```
clusrest
```

This causes the quorum disk to be restored to the state of the backup.

3. Start the Clusvc service on each of the cluster nodes. This is required because Clusrest stops the Clusvc service.

If the quorum data to be restored to the quorum disk is not found, the Clusrest tool reports FILE NOT FOUND.

The restore of a cluster node must be performed prior to running the Clusrest tool. During the restore of a node, the quorum data is placed on the node's disk in the %windir%\cluster\cluster_backup folder.

If the restored system is not part of a cluster or the quorum disk is not available, not formatted, or broken, the Clusrest tool reports ERROR_SERVICE_DOES_NOT_EXIST.

Using granular online restore

To perform granular online restore

- Start the Online Restore Wizard and follow the instructions in the wizard.

i | **NOTE:** Recovery Manager for Active Directory can also recover individual AD LDS (ADAM) objects. To restore AD LDS (ADAM) objects, use the Online Restore Wizard for AD LDS (ADAM).

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.

Granular online restore is always authoritative: it restores Active Directory object data to the state the data had when the backup was created, and any updates that were made after that point are lost. After Recovery Manager for Active Directory 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.

Online Restore Wizard overview

The wizard offers two options:

- [Compare, restore, and report changes in Active Directory.](#)
- [Compare two backups and report the differences.](#)

Compare, restore, and report changes in Active Directory

You can restore selected objects in Active Directory based on the data retrieved from an Active Directory backup. Select a backup from the list on the Backup Selection page, or click **Register** to register additional backups.

On the [Domain Access Options](#) page, you have the option to access the target domain controller using either LDAP functions only (agentless method, used by default) or Restore Agent. For the agentless method, you can select a target domain controller for the restore operation. The [Domain Access Options](#) page also allows you to specify the account under which you want the wizard to access the target domain controller.

On the Objects to Be Processed page, you can select objects by searching the backup, browsing the backup tree, or importing the file containing a list of objects' distinguished names. For the selected objects, on the Processing Options page you can specify whether to process their child objects. Also you can select attributes to be processed, or to process all attributes.

Then, the wizard offers to create comparison reports or perform a restore skipping the comparison. If you choose to perform a comparison, the wizard creates comparison reports. Then you can either proceed to restore or quit without restoring data.

If you choose to skip the comparison, the wizard performs a restore right away. The wizard processes all objects you have selected but skips the restoration of unchanged objects.

content.

Compare two backups and report the differences

You can compare objects selected in one backup with their counterparts in another backup. Only backups of the same domain controller can be compared, and the first of the selected backups must be older than the second one. After unpacking the backups, the wizard allows you to select objects from the first backup and perform a comparison as if the second backup were "live" Active Directory.

Reporting

You can use an advanced suite of ready-to-use, professionally laid-out reports for the Online Restore Wizard powered by Quest Reports Viewer or by Microsoft SQL Reporting Services. Designed to assist administrators with Active Directory change tracking and troubleshooting, these reports are based on data the wizard prepares during a compare operation. This feature requires that you have Microsoft SQL Server installed in your environment. For a list of SQL Server versions supported by Recovery Manager for Active Directory, see the Release Notes supplied with this release of the product.

Reports on a compare operation (comparison reports) allow you to see which properties of the objects being processed would change during a restore, examine the changes in detail, and decide whether to perform the restore, applying the changes.

After the wizard restores the selected objects, it creates a report to show which attributes of the restored objects have been modified by the wizard. The wizard affects an object's attribute value only if the value in Active Directory differs from that in the backup.

To view a comparison or restore operation report, click **View Report** on the Operation Results page of the wizard.

Selecting objects in the Online Restore Wizard

The Online Restore Wizard offers several ways for selecting objects: you can browse the directory tree, search for objects by name, or use an import file that specifies the objects you want to select.

To select objects in the Online Restore Wizard

1. Start the Online Restore Wizard and follow the instructions in the wizard.
2. On the Objects to Be Processed page, click **Add**, and then complete the steps related to the action you want to perform:

Table 12: Searching, browsing for, or importing objects

To do this	Complete these steps
Search for objects in the backup	1. On the menu, click Find. 2. Use the dialog box that opens to search for object. 3. Once your search completes, under Search results, select the check boxes next to the objects you want to add. 4. Click OK.
Browse for and select an object	1. On the menu, click Browse. 2. Use the dialog box that opens to browse for and select the object you want to add. 3. Click OK.
Import objects from an import file	1. On the menu, click Import. 2. Use the dialog box that opens to browse for and select the import file that specifies the objects you want to add. 3. Click OK. The import file must have the .txt format. You can specify one object per line in the import file. To specify an object in the file, use one of the following: • Distinguished name (DN) • sAMAccountName attribute value • User principal name (UPN) • Logon name When preparing an import file, you must escape reserved characters by prefixing such characters with a backslash (\). The reserved characters that must be escaped include: • ; < > \ " + ,

- space or # character at the beginning of a string
- space character at the end of a string

Other reserved characters, such as the equals sign (=) or non-UTF-8 characters, must be encoded in hexadecimal by replacing the character with a backslash followed by two hex digits.

3. To specify whether to process child objects, on the Processing Options page, under **Child objects processing**, select one of the following options:
 - **Process no child objects.** Processes only the objects you have selected
 - **Process all child objects.** Processes the objects you have selected along with all objects they contain
 - **Process child objects of selected types.** Processes the objects you have selected along with some objects they contain. You can use this option to restrict the operation scope by selecting object types. For example, you might want the wizard to process only user objects within the selected containers. Click **Select Object Types** and specify the types of child objects you want the wizard to process.
4. Follow the instructions to complete the wizard.

The following are examples of some distinguished names that include escaped characters. The first example is an organizational unit name with an embedded comma; the second example is a value containing a carriage return.

CN=Litware,OU=Docs\, Adatum,DC=Company,DC=Com

CN=Before\0DAfter,OU=Test,DC=North America,DC=Company,DC=Com

You can view attribute values of the selected object by clicking **Properties** on the Objects to Be Processed page. The **Properties** dialog box displays a list of attributes and attribute values. The **Properties** command is also available in the **Find** dialog box. To access it, right-click object names in the Search results list. You can remove selected objects from the list by clicking **Remove** or pressing DELETE.

Restoring AD LDS (ADAM)

With Recovery Manager for Active Directory, you can perform an online restore of Active Directory Lightweight Directory Services (AD LDS), previously known as Active Directory Application Mode (ADAM), by using one of the following methods:

- [Method 1: Restore an AD LDS \(ADAM\) instance from a backup created with Recovery Manager for Active Directory](#)
- [Method 2: Restore an AD LDS \(ADAM\) database from a backup created with third-party software](#)

Note that some AD LDS (ADAM) object attributes cannot be restored by using Recovery Manager for Active Directory. For more information on these attributes, see [Quest Knowledge Base Article 59039 "AD DS and AD LDS Object Attributes That Recovery Manager for Active Directory Cannot Restore"](#) at support.quest.com.

Method 1: Restore an AD LDS (ADAM) instance from a backup created with Recovery Manager for Active Directory

Complete these steps:

- [Step 1: Select a backup](#)
- [Step 2: Restore AD LDS \(ADAM\) instance](#)

Step 1: Select a backup

1. In the Recovery Manager Console tree (left pane), expand **Backups**, and select the **AD LDS (ADAM)** node.
2. In the right pane, select the backup from which you want to restore AD LDS (ADAM) instance.

If the backup is not available in the right pane, on the main menu, select **Action**, point to **Register Backup**, and then click **Register Backup File** to browse for, select, and register the backup with Recovery Manager for Active Directory.

Step 2: Restore AD LDS (ADAM) instance

1. On the main menu, select **Action | Online Restore**, and step through the Online Restore Wizard for AD LDS (ADAM).
2. On the Wizard Operation Mode page, select the **Compare, restore, and report changes in AD LDS (ADAM)** option. Click **Next**.
3. On the AD LDS (ADAM) Instance Selection page, select the AD LDS (ADAM) instance you want to restore, and click **Next**.
4. On the Backup Selection page, select the backup from which you want to restore the AD LDS (ADAM) instance, and step through the wizard to complete the restoration of the selected AD LDS (ADAM) instance.

Method 2: Restore an AD LDS (ADAM) database from a backup created with third-party software

Complete these steps:

- [Step 1: Extract and register AD LDS \(ADAM\) database](#)
- [Step 2: Restore the extracted AD LDS \(ADAM\) database](#)

Step 1: Extract and register AD LDS (ADAM) database

1. Use the third-party backup software to extract the AD LDS (ADAM) database files from the backup to an alternate location. For more information, see the documentation supplied with the backup software you

use.

2. In the Recovery Manager Console tree (left pane), expand **Backups**, and select the **AD LDS (ADAM)** node.
3. On the main menu, select **Action**, point to **Register Backup**, and then click **Register Offline AD LDS (ADAM) Database** to browse for, select, and register the .dit file and log files that belong to the AD LDS (ADAM) database you want to register with Recovery Manager for Active Directory.

Step 2: Restore the extracted AD LDS (ADAM) database

1. In the right pane, select the list entry that represents the AD LDS (ADAM) database you extracted in [Step 1: Extract and register AD LDS \(ADAM\) database](#).
2. On the main menu, select **Action | Online Restore**, and step through the Online Restore Wizard for AD LDS (ADAM).
3. On the Wizard Operation Mode page, select the **Compare, restore, report changes in AD LDS (ADAM)** option, and click **Next**.
4. On the AD LDS (ADAM) Instance Selection page, select the AD LDS (ADAM) instance you want to restore, and click **Next**.
5. On the Backup Selection page, select the list entry that represents the AD LDS (ADAM) database you extracted in [Step 1: Extract and register AD LDS \(ADAM\) database](#).
6. Step through the wizard to complete the restoration of the selected AD LDS (ADAM) instance.

Selectively restoring Active Directory object attributes

The Online Restore Wizard allows you to restore particular attributes of Active Directory objects, leaving all the other attributes intact. This feature allows you to keep the valuable changes made in Active Directory since the backup time.

Note that some AD LDS (ADAM) object attributes cannot be restored by using Recovery Manager for Active Directory. For more information on these attributes, see Quest Knowledge Base Article 59039 "[AD DS and AD LDS Object Attributes That Recovery Manager for Active Directory Cannot Restore](#)" at support.quest.com.

To select the attributes to be processed by the Online Restore Wizard

1. Start the Online Restore Wizard and follow the instructions in the wizard.
2. On the Processing Options page, click **Process no child objects**, click **Process selected attributes**, and then click **Select Attributes**.
3. In the **Select Attributes to Be Processed** dialog box, select the check boxes next to the attributes to be processed.
4. Click **Next**, and follow the instructions in the wizard to complete the operation.

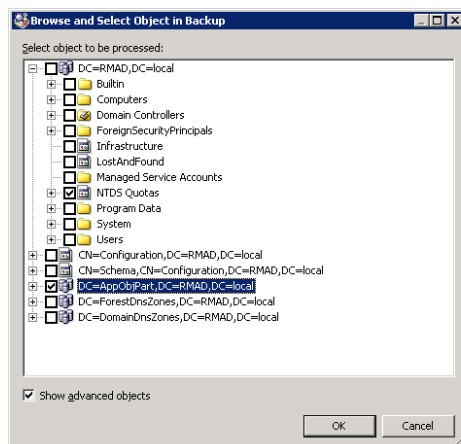
The entries in the upper part of the **Attributes** list allow you to select groups of attributes. For example, when you select **Account Information**, all account-related attributes are selected.

Restoring objects in an application directory partition

Application directory partitions are used to store application-specific data. When restoring Active Directory from a backup, Recovery Manager for Active Directory allows you to selectively restore objects and object attributes in application directory partitions, in the same way as it restores objects and attributes in domain directory partitions.

To restore objects in an application directory partition

1. Start the Online Restore Wizard and follow the instructions in the wizard.
2. On the Objects to Be Processed page, click **Add**, and then click **Find**.
3. In the **Find and Select Object in Backup** dialog box, do the following:
 - a. Select **Any type** from the **Find** list.
 - b. Click **Browse** and use the **Browse and Select Object in Backup** dialog box to select the application directory partition to search:



- c. Ensure that the **Show advanced objects** check box is selected: otherwise, the dialog box displays only the domain directory partition.
 - d. Click **OK**.
4. In the **Name** box, type the name of the objects, or part of the name.
 5. Click **Find Now**.
 6. Click **Select All** or select individual check boxes in Search results. When finished, click **OK**.
 7. Follow the instructions in the wizard to complete the operation.

NOTE: The **Find** option is used here as an example. You can also select an object by clicking **Browse**. Or, you can specify the names (DNs) of objects in a text file and open that file by clicking **Import**. If you click **Browse**, ensure that the **Show advanced objects** check box is selected. Otherwise, only the domain directory partition is displayed in the **Browse and Select Object in Backup** dialog box.

Restoring object quotas

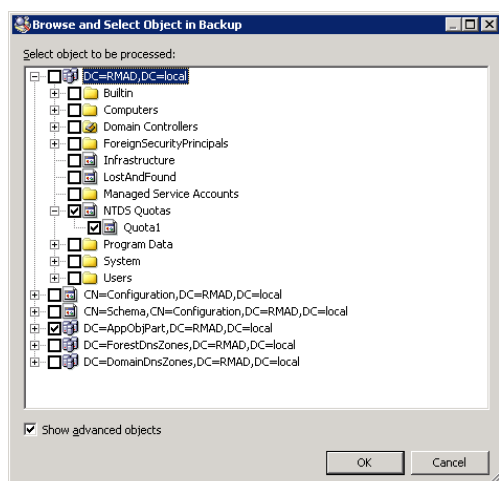
Object quotas are used to determine the number of objects that can be created in a given directory partition by a given administrator. Object quotas help prevent the denial of service situations that can occur if an administrator accidentally or intentionally creates so many objects that the domain controller runs out of storage space.

Object quotas are specified and administered separately for each directory partition. On a directory partition, object quotas can be assigned to any user or group.

Object quotas for a directory partition are stored as objects in the partition's child container called NTDS Quotas. With Recovery Manager for Active Directory, you can use the Online Restore Wizard to restore selected objects in the container NTDS Quotas, or restore the entire container NTDS Quotas.

To restore an object in the container NTDS Quotas

1. Start the Online Restore Wizard.
2. Follow the instructions in the wizard. On the **Objects to Be Processed** page, click **Add**, and then click **Browse**.
3. In the **Browse and Select Object in Backup** dialog box, expand the directory partition that contains the object quotas you want to restore, expand **NTDS Quotas**, and select the object to restore.



4. Ensure that the **Show advanced objects** check box is selected. Otherwise, the **NTDS Quotas** container will not be displayed.
5. Click **OK**, and follow the instructions in the wizard to complete the operation.

Restoring cross-domain group membership

When restoring an object, such as a user or computer, the Online Restore Wizard allows the restore of the object's membership in all groups, including those groups that reside in domains outside the object's home domain. This requires a backup that meets the following requirements:

- The backup must be taken from a domain controller that holds the Global Catalog role.
- The backup must have been created with the following option: When backing up Global Catalog servers, collect group membership information from all domains within the Active Directory forest.

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. For example, suppose a user belongs to a local group defined in a resource domain other than the user's home domain. If the restored user object were to lose its membership of that group, the user would no longer have the corresponding group permissions, and would therefore be unable to access some resources. This option is designed to overcome such issues.

To restore cross-domain group membership information

1. Start the Online Restore Wizard.
2. Follow the instructions in the wizard.
3. On the Backup Selection page, select a backup of a Global Catalog server. The backup must be created with the option **When backing up Global Catalog servers, collect group membership information from all domains within the Active Directory forest**.
4. Follow the instructions in the wizard to complete the operation.

Performing a restore without having administrator privileges

With the Online Restore Wizard, you can perform a restore without having administrative access to the target domain controller. To restore object attributes, you must only have write access to the attributes being restored.

Restoration of deleted objects requires a target domain controller running Windows Server 2003 or later. To restore a deleted object, the user account under which Recovery Manager for Active Directory runs must have sufficient permissions to selectively recover Active Directory objects. For more information about these permissions, see [Permissions required to use Recovery Manager for Active Directory](#).

To perform a restore without having administrator privileges

1. Start the Online Restore Wizard.
2. Follow the instructions in the wizard.
3. If you are going to restore deleted objects, on the [Domain Access Options](#) page ensure that the target domain controller is running Windows Server 2003 or later.
4. Follow the instructions in the wizard to complete the operation.

By default, the "Reanimate Tombstone" control access right is granted only to domain administrators. Domain administrators can grant the permission necessary to restore deleted objects to other users and groups by granting the user or group the "Reanimate Tombstone" control access right.

- **WARNING:** A security risk can be introduced by granting this permission, because it allows a user to restore an account that may have a level of access greater than that of the user. By restoring such an account, the user in effect gains control of that account. This is because the LDAP API does not restore the backed up account password, and so the user can set the initial password on the account.

Reports about objects and operations

Recovery Manager for Active Directory provides a number of reports that allow you to track changes made to Active Directory, AD LDS (ADAM), and Group Policy objects and view summary information about the compare and restore operations performed on Active Directory and AD LDS (ADAM) objects with Recovery Manager for Active Directory.

To generate and view these reports, you can use the Online Restore Wizard, the Online Restore Wizard for AD LDS (ADAM), and the Group Policy Restore Wizard.

In this section:

- [Reports about Active Directory objects](#)
- [Reports about AD LDS \(ADAM\) objects](#)
- [Reports about Group Policy objects](#)
- [Reports about who modified Active Directory objects](#)

Reports about Active Directory objects

The Online Restore Wizard provides reports that allow you to track changes of Active Directory (AD) objects by comparing the state of objects in backup and in Active Directory. You can also compare AD objects held in two backups.

You can generate and view a detailed report about a particular compare or restore operation that Recovery Manager for Active Directory performed on AD objects. Alternatively, you can generate and view a summary of all compare and restore operations performed with Recovery Manager for Active Directory on AD and AD LDS (ADAM) objects. Performing a compare operation on an AD or AD LDS (ADAM) object does not modify that object in any way.

To generate and view a report on AD objects

1. Start the Online Restore Wizard:
 - a. In the Recovery Manager Console, select the **Recovery Manager for Active Directory** console tree root.
 - b. On the main menu, select **Action | Online Restore Wizard**.
2. Step through the wizard until you are on the Wizard Operation Mode page, then do one of the following:
 - If you want to compare AD objects in a backup against those in live Active Directory or restore AD objects and view the restore operation report, select **Compare, restore, and report changes in Active Directory**.
 - If you want to compare Active Directory objects in two backups, select **Compare two backups and report the differences**.
3. Step through the wizard until you are on the Action Selection page. Select **Compare, analyze, and, optionally, restore**.
4. Step through the wizard until you are on the Reporting Options page. Select **Generate report**, then specify what kind of information you want included in the report.
5. Step through the wizard until you are on the Operation Option page. Click **View Report**.

You can use the **Expand all** or **Collapse all** element provided in the report to expand or collapse all object entries displayed in the report.

To view a summary of all compare and restore operations that Recovery Manager for Active Directory performed on AD and AD LDS (ADAM) objects, click the **View Summary Report** button at the bottom of the report window.

Reports about AD LDS (ADAM) objects

The Online Restore Wizard provides reports that allow you to track changes of Active Directory (AD) objects by comparing the state of objects in backup and in a live AD LDS (ADAM) instance. You can also compare AD LDS (ADAM) objects held in two backups.

You can generate and view a detailed report about a particular compare or restore operation performed on AD LDS (ADAM) objects with Recovery Manager for Active Directory. Alternatively, you can generate and view a summary of all compare and restore operations performed with Recovery Manager for Active Directory on AD and AD LDS (ADAM) objects. Performing a compare operation on an AD or AD LDS (ADAM) object does not modify that object in any way.

To generate and view a report on AD LDS (ADAM) objects

1. Start the Online Restore Wizard for AD LDS (ADAM):
 - a. In the Recovery Manager Console, select the **Recovery Manager for Active Directory** console tree root.
 - b. On the main menu, select **Action | Online Restore Wizard for AD LDS (ADAM)**.
2. Step through the wizard until you reach the Action Selection page. Select **Compare, analyze, and, optionally, restore**.
3. Step through the wizard until you reach the Reporting Options page. Select **Generate report**, then specify what kind of information you want in the report.
4. Step through the wizard until you reach the Operation Option page. Click **View Report**.

To view a summary report about all compare and restore operations that Recovery Manager for Active Directory performed on AD and AD LDS (ADAM) objects, click the **View Summary Report** button at the bottom of the report window.

Reports about Group Policy objects

The Group Policy Restore Wizard helps you generate comparison reports that allow you to track changes of Group Policy objects by comparing their state in a backup and in Active Directory.

To generate and view a report on Group Policy objects

1. Start the Group Policy Restore Wizard:
 - a. In the Recovery Manager Console, select the **Recovery Manager for Active Directory** console tree root.
 - b. On the main menu, select **Action | Group Policy Restore Wizard**.
2. Step through the wizard until you are on the Backup Selection page. Select the backup that includes the Group Policy objects whose state you want to compare with that in Active Directory.

3. Step through the wizard until you are on the Group Policy Object Selection page.
4. In the list, select the check boxes next to the Group Policy objects you want to compare, and then click **View Report**.

Note that the GPO comparison reports in the Group Policy Restore Wizard do not support providing information about certain Group Policy settings. For a list of unsupported Group Policy settings, see Quest Knowledge Base Article 12024 "[Information on Some Group Policy Settings May Be Missing from the Group Policy Object Comparison Report](https://support.quest.com/Information%20on%20Some%20Group%20Policy%20Settings%20May%20Be%20Missing%20from%20the%20Group%20Policy%20Object%20Comparison%20Report)" at support.quest.com.

Reports about who modified Active Directory objects

You can use the Recovery Manager for Active Directory reports to find out which user modified specific Active Directory objects. To provide this functionality, Recovery Manager for Active Directory requires another Quest product - ChangeAuditor for Active Directory. ChangeAuditor is designed to collect information on all critical changes occurred in Active Directory and track user and administrator activity. For more information about ChangeAuditor for Active Directory, please visit <http://quest.com/products/changeauditor-for-activedirectory>.

To provide information on who modified particular Active Directory objects, Recovery Manager for Active Directory integrates with ChangeAuditor and includes the data ChangeAuditor provides into the reports. In order to integrate, Recovery Manager for Active Directory and ChangeAuditor must be installed in the same Active Directory forest.

For a list of the ChangeAuditor for Active Directory versions with which Recovery Manager for Active Directory can integrate to provide information about the users that modified specific AD objects, see the Release Notes for this version of Recovery Manager for Active Directory.

To generate a report that shows who modified specific AD objects

1. Start the Online Restore Wizard:
 - a. In the Recovery Manager Console, select the **Recovery Manager for Active Directory** console tree root
 - b. On the main menu, select **Action | Online Restore Wizard**
2. Step through the wizard until you are on the Wizard Operation Mode page, then do one of the following:
 - If you want to compare AD objects in a backup against those in live Active Directory or restore AD objects and view the restore operation report, select **Compare, restore, and report changes in Active Directory**.
 - If you want to compare Active Directory objects in two backups, select **Compare two backups and report the differences**.
3. Step through the wizard until you are on the Action Selection page. Select **Compare, analyze, and, optionally, restore**.
4. Step through the wizard until you reach the Reporting Options page. Select **Generate report**, then specify what kind of information you want in the report.
5. Select the **Include ChangeAuditor data in reports** check box, and then specify the ChangeAuditor database you want to use.
6. Step through the wizard until you reach the Operation Option page. Click **View Report**.

The **Modified by** column in the generated report provides information on who modified particular Active Directory objects.

Using complete offline restore

i **IMPORTANT:** It is currently not possible to use the Repair Wizard to bring up a Domain Controller on identical hardware using a backup from a DC which is offline due to hardware failure. Despite being on identical hardware the operating system will contain many unique parameters. Those parameters are defined during the installation of the Operating System. Repair wizard will replace the current DIT file (with transaction logs) and the registry, however replacing the registry taken from another OS (even with similar hardware) may lead to OS instability or it may not function at all. For this reason, we do not recommend using the Repair Wizard in this situation.

To perform a complete offline restore

- Start the Repair Wizard and follow the instructions in the wizard.

The Repair Wizard enables the recovery of the whole Active Directory database on a domain controller by applying a backup that was created for that domain controller.

You can use the 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.

i **IMPORTANT:** A backup created for a given domain controller cannot be used to restore the Active Directory database to other domain controllers.

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 recommended 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. Then, Active Directory replication 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 obsolete. 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 complete offline restore. Since you cannot use the backup from the other domain controller for the 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 yet replicated to other domain controllers. 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.

Repair Wizard overview

The Repair Wizard lets you select the target domain controller and the Active Directory backup for that domain controller, and then guides you through the operation.

NOTE: You can select the domain controller where you want to restore Active Directory and then start the Repair Wizard by clicking **Repair** on the **Action** menu. As a result, the wizard only displays the backups created for that domain controller.

In the Repair Wizard, you can use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec or Windows Server backups (.vhd, .vhdx). To use a backup, on the Computer and Backup Selection window, click **Register**, and then register the backup using the **Register Backup File** or **Register Backups in Folder** item. Note that snapshot backups are not supported by the Repair Wizard. You can restore Active Directory data from such backups using the Online Restore Wizard and Group Policy Restore Wizard. The Extract Wizard also supports snapshot backups.

Active Directory restoration requires that the domain controller be restarted in Directory Services Restore Mode. At your discretion, the wizard restarts the target computer automatically or allows you to restart the target computer manually.

IMPORTANT: You will need to log on to the target computer as an Administrator after the Repair Wizard restarts it in Directory Services Restore Mode. To do this, you must use an account whose user name and password are stored in the local security account database, known as the Security Accounts Manager (SAM). You cannot use the user name and password of the Active Directory administrator.

To restart the computer in Directory Services Restore Mode

1. Restart the computer and press F8 when you are prompted to do so.
2. On the menu, choose Directory Services Restore Mode and then press ENTER.
3. If you have multiple systems installed on the computer, choose the Windows installation you are recovering, and then press ENTER. You must choose the Windows installation that was running when you launched the Repair Wizard.

After the target domain controller is restarted in Directory Services Restore Mode, the wizard restores the Active Directory database from the backup.

Optionally, the wizard allows you to mark individual objects, a subtree, or the entire directory as authoritatively restored. To mark AD objects, subtree, or the entire AD database as authoritative, Recovery Manager for Active Directory uses the capabilities provided by the **Ntdsutil.exe** tool supplied with Microsoft Windows. However, this tool included in Windows Server 2008 or higher does not support marking the entire AD database as authoritative.

The authoritatively restored objects replace existing copies of those objects on all domain controllers and prevail for the entire domain.

After the Active Directory database is restored, the target domain controller must be restarted in normal operational mode. At your discretion, the Repair Wizard restarts the target computer automatically or allows you to restart the target computer manually. The restore operation is not completed until the target domain controller is restarted in normal operational mode.

Offline restore implications

This section provides important information you should consider when recovering Active Directory with the Repair Wizard.

The wizard allows you to restore Active Directory information on a domain controller by restoring its components from a System State backup. This restores the entire Active Directory database along with the other System State components on which Active Directory depends—SYSVOL and Registry.

The wizard offers the following two options for restoring Active Directory:

- [Non-authoritative restore](#)
- [Authoritative restore](#)

Non-authoritative restore

In this section:

- [DIT database](#)
- [SYSVOL](#)

DIT database

When restored non-authoritatively, settings and entries that existed in the domain, schema, configuration, and optionally the global catalog naming contexts maintain the version number they had at the time of backup. After the restored domain controller is restarted, the Active Directory replication updates the domain controller with the changes that were made to Active Directory since the backup time.

SYSVOL

When restored non-authoritatively, the local copy of the SYSVOL that is held on the restored domain controller is updated with that of its replication partners. After the restored domain controller is restarted, it contacts its replication partners, compares SYSVOL information, and replicates the necessary changes, bringing its local copy of the SYSVOL up to date with the other domain controllers within the domain.

If the domain controller being recovered is the only functioning domain controller in the domain, a primary restore of the SYSVOL should be done. A primary restore builds a new replication service database by loading the data present under the SYSVOL onto the local domain controller. This method is the same as nonauthoritative except that the restored data is marked as the primary data.

Perform a primary restore only when all domain controllers in the domain are lost and you want to rebuild the domain from backup. Do not perform a primary restore if any other working domain controller in this domain is available. Use primary restore for the first domain controller, and then, later, use non-authoritative restore for all other domain controllers.

Authoritative restore

In this section:

- [DIT database](#)
- [SYSVOL](#)

DIT database

With the Repair Wizard, you can perform an authoritative restore of Active Directory. The wizard allows you to mark the entire Active Directory database, a single subtree, or an individual object as authoritatively restored.

To mark AD objects, subtree, or the entire AD database as authoritative, Recovery Manager for Active Directory uses the capabilities provided by the **Ntdsutil.exe** tool supplied with Microsoft Windows. However, this tool included in Windows Server 2008 or higher does not support marking the entire AD database as authoritative.

As a result, the wizard increments the version number of the attributes of all objects in the entire directory, all objects in the subtree, or the particular object to make it authoritative for the directory.

An authoritative restore can only be carried out on objects from the configuration and domain naming contexts. Authoritative restore of the schema-naming context is not supported.

SYSVOL

When performing an authoritative restore of the Active Directory database, you should also perform an authoritative restore of the SYSVOL. With the Repair Wizard, the authoritative restore of the SYSVOL does not occur automatically. To do that, you should follow the procedure outlined in the next section.

By restoring the SYSVOL authoritatively, you specify that the restored copy of SYSVOL is authoritative for the domain. As a result, the replication service replicates the local SYSVOL out to the other domain controllers within the domain.

The bandwidth associated with such replication should be considered in case of an extensive use of large Group Policy objects and logon scripts in the domain.

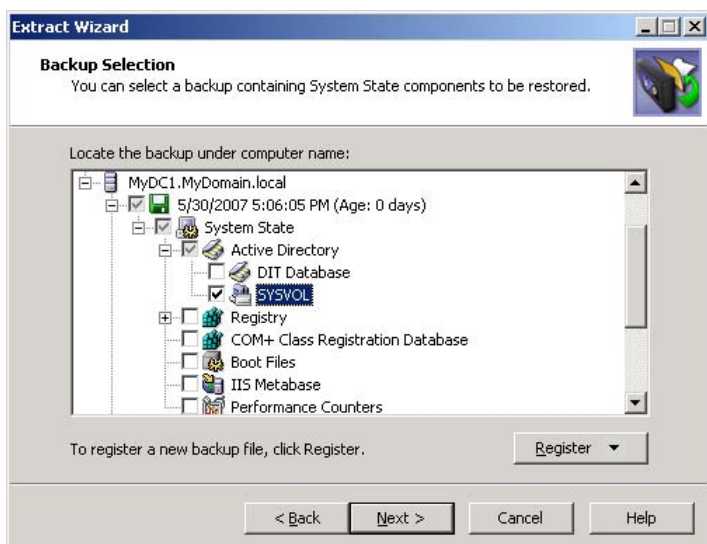
Since the Online Restore Wizard and Group Policy Restore Wizard allow you to authoritatively restore directory data with minimal effort and overhead, we recommend you to use those wizards rather than the Repair Wizard when you need to recover/undelete individual Active Directory objects and Group Policy objects.

Restoring SYSVOL authoritatively

When you have performed an authoritative restore of Active Directory using the Repair Wizard, additional steps must be taken to restore the SYSVOL authoritatively. By doing this, you are telling the other domain controllers in the domain that the SYSVOL information on the restored domain controller is authoritative. As a result, the files and folders contained under SYSVOL on the restored domain controller are replicated out to all other domain controllers in the domain.

To restore SYSVOL authoritatively

1. Use the Repair Wizard to restore Active Directory on the target domain controller.
2. After the Repair Wizard completes the restore, start the Extract Wizard.
3. Follow the instructions in the Extract Wizard.
4. On the Backup Selection page, select the SYSVOL component of the backup you want to use. The SYSVOL component is located in the **Active Directory** branch of the backup:



5. On the Folder Selection page, specify the folder for the SYSVOL data.
6. Follow the Extract Wizard to restore the SYSVOL data from the backup to the specified folder.
7. After the Extract Wizard is completed, ensure that the domain controller where you want to authoritatively restore SYSVOL is started in normal mode and the SYSVOL share is published, that is, the SYSVOL shared folder and its sub-folders are displayed in Computer Management for that domain controller.
8. Copy the restored by the Extract Wizard SYSVOL folder over the original SYSVOL folder.

When authoritatively restoring the SYSVOL, it is important that you copy SYSVOL data from the alternate location after the SYSVOL share is published.

If the computer is in a replicated domain, it can take several minutes before the SYSVOL share is published, because it needs to synchronize with its replication partners.

If there is no other functioning domain controller in the domain, a primary restore of the SYSVOL should be done. When restoring the SYSVOL, the Repair Wizard allows you to mark the SYSVOL for primary restore. A primary restore builds a new replication service database by loading the data present under SYSVOL on the local domain controller.

Given that each Group Policy object is comprised of the Group Policy Container and Group Policy Template, when a Group Policy Container is authoritatively restored by using the Repair Wizard or Online Restore Wizard, the corresponding Group Policy Template must then be authoritatively restored as part of the SYSVOL. Since selective restoration of the SYSVOL data is time-consuming and requires considerable expertise, we recommend that restoration of Group Policy objects be performed by using the Group Policy Restore Wizard, which authoritatively restores both Group Policy Containers and Group Policy Templates, and ensures that Group Policy objects are properly restored with minimal administrative overhead.

Performing a granular restore of SYSVOL

You can restore individual elements of SYSVOL authoritatively, such as specific files contained within the SYSVOL folder.

To perform a granular restore of SYSVOL

1. Start the Extract Wizard and follow the provided instructions.
2. On the Backup Selection page, select the SYSVOL component of the backup you want to use. The SYSVOL component is located in the **Active Directory** branch of the backup.
3. On the Folder Selection page, specify a folder for the SYSVOL data.
4. Follow the Extract Wizard to restore the SYSVOL data from the backup to the specified folder.
5. Ensure that the domain controller where you want to restore the individual elements of SYSVOL is started in normal mode, and the SYSVOL share is published, that is, the SYSVOL share and its sub-folders are displayed in Computer Management for that domain controller.
6. Copy the files to be restored from the Extract Wizard SYSVOL folder to the original SYSVOL folder.

i **IMPORTANT:** When authoritatively restoring the SYSVOL files, it is important that you copy SYSVOL data from the alternate location after the SYSVOL share is published. If the computer is in a replicated domain, it can take several minutes before the SYSVOL share is published, because it needs to synchronize with the replication partners.

Recovering Group Policy

With Recovery Manager for Active Directory, you can selectively restore Group Policy information from normal System State backups of domain controllers.

To restore Group Policy information

- Start the Group Policy Restore Wizard and follow the instructions in the wizard.

The Group Policy Restore Wizard helps you recover Group Policy objects and links deleted or modified since the last backup. The wizard operates in online mode and does not require restarting the domain controller. The wizard also enables the migration of Group Policy objects between domains.

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.

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.

After Recovery Manager for Active Directory completes Group Policy Restore on the target domain controller, the restored Group Policy objects and links are replicated to the other domain controllers through the normal replication process. The previously erased or modified Group Policy information is ignored during replication, because the restored data appears to be more recent.

Group Policy Restore Wizard overview

The wizard lets you choose the backup source domain and lists System State backups of domain controllers of that domain. You select a backup from the list on the Backup Selection page, or click **Register** to register additional backups. The wizard then unpacks the backup, preparing backup data for further use.

After the backup data preparation is completed, the wizard prompts you to choose the target domain controller and lists all Group Policy objects that are in the backup. To have the wizard compare the state of Group Policy

objects in the backup with their state on that domain controller, click **Compare All**. After the wizard performs the comparison, the **State in AD** column indicates a state of each object, shown as 'Different', 'Identical', or 'Deleted'. You can select the object you want the wizard to restore.

Then, the wizard prompts you to choose whether to restore policy settings in the Group Policy objects, security settings on the objects, or both, and asks about how to process links to the selected Group Policy objects.

Finally, the wizard informs you about the changes to be made to the Group Policy and allows you to start the restore process or step back to modify the restore options.

Restoring data from third-party backups

Recovery Manager for Active Directory provides for restoration of Active Directory data from backups created by other applications if these backups are stored in Microsoft Tape Format (MTF). Such backups of domain controllers' System State can be created, for example, by Windows Backup or Veritas Backup Exec. Depending on your needs, you can use the Online Restore Wizard, the Group Policy Restore Wizard, the Repair Wizard, or the Extract Wizard to restore data.

To restore data from backups created by other applications

1. Start the wizard you want to use and follow the instructions in the wizard.
2. To register a backup in the Online Restore Wizard or the Group Policy Restore Wizard, on the Backup Selection page, click **Register**, and then click one from the following items:
 - **Register Backup File**. Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf) or Windows Server backup file (.vhd, .vhdx).
 - **Register Backups in Folder**. Registers all backup files that are in the selected folder.
 - **Register Offline Active Directory Database**. Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

To register a backup in the Repair Wizard, on the Computer and Backup Selection page, click **Register**, and then click one from the above-listed items.

3. Select the newly registered backup and follow the wizard instructions to walk through the restore process.

Snapshot backups (that is, backups created using the Volume Shadow Copy service) are not supported by the Repair Wizard. By default, Veritas Backup Exec 9.0 or later uses the Volume Shadow Copy service when creating System State backups. However, you can restore Active Directory data from snapshot backups using the Online Restore Wizard and Group Policy Restore Wizard. The Extract Wizard also supports snapshot backups.

Using the Extract Wizard

The Extract Wizard allows you to restore previously backed up files to a specified folder (an alternate location). Restoring backed up files to an alternate location allows you to use the files as a standalone data source, or to replace existing files on a given computer. The wizard lets you select a backup, choose the components to be

extracted from that backup, and specify the destination folder. Then, the wizard guides you through the extract operation.

The Extract Wizard can help you to perform an authoritative restore of the SYSVOL. For more information, see [Restoring SYSVOL authoritatively](#).

Also you can use the Extract Wizard in conjunction with the Install from Media (IFM) feature of Windows to create a domain controller. IFM allows you to create an additional domain controller using a restored backup of another domain controller. The restored backup can be held on any backup media (tape, CD, or DVD) or on a shared network resource. A restored backup makes it possible to set up an additional domain controller in an existing domain without replicating the entire directory database to the new domain controller.

With the Extract Wizard, you can restore a backup of a domain controller's System State to a specified folder. Then, using the restored backup files, you can create a new domain controller, as described in the following sections:

- [Creating a Windows Server 2003-based domain controller from a backup](#)
- [Creating a Windows Server 2008-based domain controller from a backup](#)
- [Creating a Windows Server 2012-based domain controller from a backup](#)

Creating a Windows Server 2003-based domain controller from a backup

This section describes how to create a Windows Server 2003 or 2003 R2-based domain controller from a backup by using the Install from Media (IFM) feature of Windows and the Extract Wizard.

To create a Windows Server 2003-based domain controller by using IFM

1. Create a backup of a Windows Server 2003 or 2003 R2-based domain controller's System State.

Make sure you select and back up all System State components. To create a backup, you can use the [Backup Wizard](#).

2. Start the **Extract Wizard** and follow the steps in the wizard.
3. On the **Backup Selection** page, select the backup you created in step 1 of this procedure.
4. On the Folder Selection page, specify the path to the folder where you want to place the extracted backup files.
5. Follow the instructions in the wizard to complete the extract operation.
6. On the Windows Server 2003-based computer you want to designate as the new domain controller, do the following:
 - a. Click **Start**, click **Run**, type **dcpromo /adv**, and then press ENTER.
 - b. Follow the steps in the Active Directory Installation Wizard.
 - c. On the **Domain Controller Type** page, click **Additional domain controller for an existing domain**.
 - d. On the **Copying Domain Information** page, click **From these restored backup files**, and specify the location of the restored backup files created in Step 4.
 - e. Follow the instructions in the Active Directory Installation Wizard to complete the operation.

For more information on creating a domain controller by using a backup, refer to the topic “Create an additional domain controller” in Windows Server 2003 Help.

Creating a Windows Server 2008-based domain controller from a backup

This section describes how to create a Windows Server 2008 or 2008 R2-based domain controller from a backup by using the Install from Media (IFM) feature of Windows and the Extract Wizard.

To create a domain controller, complete these steps:

- [Step 1: Create and extract a backup](#)
- [Step 2: Use IFM to create a domain controller](#)

Step 1: Create and extract a backup

1. Create a backup of a Windows Server 2008 or 2008 R2-based domain controller's System State.

Make sure you select and back up all System State components. To create a backup, you can use the [Backup Wizard](#).
2. Start the Extract Wizard and follow the steps in the wizard.
3. On the **Backup Selection** page, select the backup you created in step 1 of this procedure.
4. On the **Folder Selection** page, specify the path to the folder where you want to place the extracted backup files.
5. Follow the steps in the wizard to complete the extract operation.

Step 2: Use IFM to create a domain controller

1. Make sure you install the Active Directory Domain Services server role on the Windows Server 2008 or Windows Server 2008 R2-based computer you want to designate as the new domain controller.
2. On that computer, click **Start**, click **Run**, type **dcpromo /adv**, and press ENTER.
3. On the initial page of the Active Directory Domain Services Installation Wizard, make sure you select the **Use advanced mode installation** check box.
4. Step through the wizard until you are on the **Choose a Deployment Configuration** page.
5. Click **Existing forest**, and then click **Add a domain controller to an existing domain**.
6. Click **Next**.
7. On the **Network Credentials** page, specify the account credentials you want to use.
8. Step through the wizard until you are on the **Install from Media** page.
9. Click **Replicate data from media at the following location**, and then specify the location to which you extracted the backup in [Step 1: Create and extract a backup](#).
10. Step through the wizard to complete the domain controller creation operation.

Creating a Windows Server 2012-based domain controller from a backup

This section describes how to create a Windows Server 2012 or Windows Server 2012 R2-based domain controller from a backup by using the Install from Media (IFM) feature of Windows and the Extract Wizard.

To create a domain controller, complete these steps:

- [Step 1: Create and extract a backup](#)
- [Step 2: Install AD DS on the Windows Server 2012-based computer](#)
- [Step 3: Use the Install-ADDSDomainController cmdlet to install from media](#)

Step 1: Create and extract a backup

1. Create a backup of a Windows Server 2012 or Windows Server 2012 R2-based domain controller's System State.

Make sure you select and back up all System State components. To create a backup, you can use the Backup Wizard.

2. Start the Extract Wizard and follow the steps in the wizard.
3. On the **Backup Selection** page, select the backup you created in step 1 of this procedure.
4. On the **Folder Selection** page, specify the path to the folder where you want to place the extracted backup files.
5. Follow the steps in the wizard to complete the domain controller creation extract operation.

Step 2: Install AD DS on the Windows Server 2012-based computer

On the Windows Server 2012 or Windows Server 2012 R2-based computer you want to promote to a domain controller, use Server Manager to install the Active Directory Domain Services (AD DS) role: in Server Manager, on the **Manage** menu, click **Add Roles and Features**, and then follow the steps in the wizard to install the AD DS role.

Step 3: Use the *Install-ADDSDomainController* cmdlet to install from media

Use the *Install-ADDSDomainController* cmdlet supplied with Windows PowerShell to create a new domain controller from the backup you extracted in [Step 1: Create and extract a backup](#). To specify the path to the extracted backup, use the **-InstallationMediaPath** parameter of the cmdlet.

To view detailed information about the **Install-ADDSDomainController** cmdlet, in the Windows PowerShell window, type the following:

```
Get-Help Install-ADDSDomainController -detailed
```

Restoring passwords and SID history

When undeleting an object by using the agentless method, the Online Restore Wizard employs LDAP functions along with the Restore Deleted Objects feature provided by the Windows operating system. This feature restores only the attributes preserved in the object's tombstone. The other attributes are restored from a backup. However, some attributes, such as Password and SID History cannot be written using LDAP functions, and thus cannot be restored from a backup via the agentless method.

In many situations, the inability to restore the Password attribute from a backup is not a big problem as an object's password can be reset after restoring the object. As for the SID History attribute, its restoration may be business-critical. An example is a situation where the domain from which the object was migrated is unavailable or decommissioned, and therefore SID History cannot be re-added.

To enable the restoration of these two attributes using the agentless method, the Active Directory schema may be modified so that these attributes are preserved in object tombstones. As a result, an undeleted object has the same Password and SID History as the object had when it was deleted.

As this solution requires schema modifications, it should be carefully considered. Microsoft recommends modifying or extending the schema only in extreme situations. Proceed with extreme caution, because making a mistake may render the directory service unstable, resulting in a reinstallation.

Often, organizations are reluctant to make changes to the schema because schema modifications may result in heavy replication traffic. It is not the case for the schema modifications described in this article as they do not affect the partial attribute set (PAS).

i **NOTE:** Recovery Manager for Active Directory also provides an agent-based method for restoring or undeleting objects. With the agent-based method any attributes can be restored. The agent-based method does not require any schema modifications.

Preserving passwords and SID history in object tombstones

To preserve passwords and SID history in object tombstones, complete the following steps:

- [Step 1: Make sure prerequisites are met](#)
- [Step 2: Modify the searchFlags attribute value](#)

Step 1: Make sure prerequisites are met

- You are logged on as a member of the Schema Admins group.
- Write operations to the schema are allowed.

Step 2: Modify the searchFlags attribute value

To preserve SID History in tombstones, you need to modify the **searchFlags** attribute value for the SID-History (SIDHistory) schema object.

To preserve passwords in tombstones, you need to modify the **searchFlags** attribute value for the following password-related schema objects:

- Unicode-Pwd (unicodePwd)
- DBCS-Pwd (dBCSPwd)
- Supplemental-Credentials (supplementalCredentials)
- Lm-Pwd-History (lmPwdHistory)
- Nt-Pwd-History (ntPwdHistory)

i **IMPORTANT:** The Lm-Pwd-History and Nt-Pwd-History attributes are used to store password history. For security reasons, it is recommended to restore them along with the password.

To determine the new searchFlags attribute value to be set, use the following formula:

8 + current searchFlags attribute value = new searchFlags attribute value

To modify the searchFlags attribute value

1. Use the ADSI Edit tool (Adsiedit.msc) to connect to the Schema naming context using the domain controller that holds the Schema Master FSMO role:
 - a. Start the ADSI Edit tool (Adsiedit.msc).
 - b. In the left pane of the console, right-click the **ADSI Edit** console tree root, and then on the shortcut menu click **Connect to**.
 - c. In the dialog box that opens, do the following:
 - Click **Select a well known Naming Context** option, and then select **Schema** from the list below.
 - Click **Select or type a domain controller or server** option, and then type the name of the domain controller that holds the Schema Master FSMO role.
 - d. Click **OK** to connect.
2. In the left pane of the console, expand the **Schema** container to select the container that includes the schema objects you want to modify.
3. Right-click the object you want to modify in the right pane, and then click **Properties**.
4. Enter the new **searchFlags** attribute value you determined earlier:
 - a. On the **Attribute Editor** tab, select searchFlags from the **Attributes** list, and then click the **Edit** button.
 - b. In the **Attribute Editor** box, enter the new value and click **OK**.

Fault tolerance

In complex and large environments the requirement to have a single instance of the Recovery Manager Console (and thus maintain a single backup registration database) might not be feasible. When there are two or more instances of the Recovery Manager Console deployed in your environment, each of these instances has its own dedicated backup registration database that stores information about created backups.

If necessary, you can consolidate backup information from multiple backup registration databases on a single Recovery Manager for Active Directory computer. After that, you could use the Recovery Manager Console installed on that computer to access and use the backup files created by all other Recovery Manager for Active Directory instances installed in your environment.

If you are using Recovery Manager for Active Directory Forest Edition, it is recommended to consolidate backups on the computer that hosts the Forest Recovery Console you plan to use for forest recovery operations. This will allow you to use the consolidated backups to recover domain controllers in your Active Directory forest.

Consolidating backups does not affect the backup files themselves. Rather, this operation replicates backup registration information from multiple backup registration databases into a single database, making the backups available to the Recovery Manager Console instance that uses that database.

From version 9.0, Recovery Manager for Active Directory introduces the fault tolerance feature that lets you consolidate only backup information in a single database or create a full copy of the specified master console on the local console.

This feature is based on the Recovery Manager Remote API Access service and PowerShell commands. The Recovery Manager Remote API Access service is an optional feature and must be selected when installing Recovery Manager for Active Directory Forest Edition version 9.0.1. When the fault tolerance feature is enabled, the current console connects to the Recovery Manager Remote API Access service on the remote RMAD console, then imports the data, e.g. collection information, backup schedule task information, backup information, etc.



NOTE:

- The TCP port 52132 is required for Recovery Manager Remote API Access service.
- Ensure that you have a good network performance between the consoles.
- It is recommended that you schedule the backup task and the replication task so that they do not overlap.

Full replication

The **Full** mode is used when users would like to make the local computer be a slave of the remote console (the remote console will become its master), and would not like to use any functionality of the local console, except the comparison and restore operations. They need to replicate all settings from the master console, so that the local console can fully take over the master console and perform exactly the same operations in case the master console becomes unavailable.

Which settings are replicated?

- Global settings
- Computer collection settings, including the retention policy setting
- Computer collections
- Structure of a computer collection

- Backup schedule task

i NOTE:

- If the user account is a domain user or local user, it will be changed to "SYSTEM".
- If the user account is Managed Service Account (MSA), make sure that the MSA works in the current console. Otherwise, it will be changed to "SYSTEM" too.
- All backups schedules are disabled after the replication.

- Relations between backup schedule and computer collection
- Backup information
 - Backup information only, not the backup files.
 - If the path of backup is an absolute path (e.g. "C:\backups\b1.bkf", it will be changed to the UNC path (e.g. "\\CurrentConsoleName\C\$\ backups\b1.bkf").
- Relations between backup information and computer collections

i IMPORTANT:

- Single-master mode: you can add several remote consoles to the replication list, but only one remote (master) console can be used for replication.
- All local data (collections, collection properties, etc) is completely rewritten by the data from the master console.
- After the replication, data on the slave console is read-only, but you can perform the compare and restore operations using this console.

Replication of backup information only

In the **Backups** mode, only backup information is replicated, not the backup files. Relations with computer collections are not replicated as well.

This option lets users consolidate the backup information from one or more remote consoles and use the full functionality of local and remote consoles without any impact during the backup replication. Then, users can easily perform the comparison and restore of all the consolidated backups on the local console.

i IMPORTANT:

- Multi-master mode: several remote consoles can be used simultaneously as replication sources.
- In this mode, the local console is fully functional during the backup replication.
- Local backups are merged with the backups from remote consoles.

For more information about how to configure the fault tolerance feature, see the following topics:

- [Replicating data using Recovery Manager Console](#)
- [Replicating data using PowerShell](#)

Replicating data using Recovery Manager Console

This section describes how to configure data replication using Recovery Manager Console.

To add a remote (master console for the 'Full' mode) console to the local (slave for the 'Full' mode) console and force the replication

1. Open the local Recovery Manager for Active Directory console.
2. Right-click the **Replication** node and select **Add Console**.
3. In the Add Replication Console dialog, specify a host name where the RMAD console that will be used as a replication source is installed.
4. Select one of the replication options:
 - **Replicate backups information, collections, global settings and schedule**
This option lets you create the full copy of the master console on the local console ('Full' mode).
 - **Replicate backups information only**
This option lets you replicate backup information from the replication source ('Backups' mode).
5. Supply the credentials for the replication task. These credentials will be used to connect the source console that you have just added.



NOTE:

For the 'Full' mode

- The account used for the replication task must be a member of the local **Administrators** group on the local and remote RMAD consoles.
- The account must be a member of the **Domain Users** group on each target domain.
- The account must be a member of the local **Administrators** group on the computer hosting the AD LDS (ADAM) instances.

For the 'Backups' mode

- The account used for the replication task must be a member of the local **Administrators** group on the local RMAD console.

6. Now the source console instance is added and shown in the right pane.
7. Set the console replication status to **Enabled** in the right pane.
8. To start the replication, right-click the **Replication** node and press **Replicate**. This option forces the replication for all consoles in the list, not only for the selected one .
9. To update the credentials, right-click the console instance from the list in the right pane and select **Manage Credentials**.
10. To remove the console instance from the replication console list, right-click the instance and click **Remove**.

Replication status

- If the data replication is finished successfully, the status in the console instances list is changed to "Success".

- The replication may fail with the error "Cannot connect to Recovery Manager for Active Directory on the specified computer." in the following cases:
 - If the target computer does not exist or Recovery Manager for Active Directory is not installed on the specified host.
 - If the Recovery Manager Remote API Access service is not installed or stopped
 - If you experience network connection problems
 - If the account that is used for the replication task is blocked, etc.

To create a replication schedule

1. In the Recovery Manager for Active Directory console, right-click the **Replication** node and select **Properties**.
2. In the **Replication Properties** dialog, you can create the replication schedule. For that, click **Modify...**, then click **New...** in the **Recovery Manager Replication Job** dialog to create a trigger for the schedule.
3. Make sure that the **Schedule enabled** option is selected in the **Replication Properties** dialog.
4. Provide a user account that will be used to start the replication schedule task using **Select Account...** in the **Replication Properties** dialog. Minimum requirements for the account are listed above depending on the replication mode.
5. Click **OK**.

i NOTE: You can specify the MSA account to run the replication schedule task. Note that you must add the '\$' character at the end of the account name (e.g. domain\computername\$) and leave the **Password** field blank. This account must be a member of the local Administrator group on the Recovery Manager for Active Directory machine.

Replicating data using PowerShell

This section provides information about PowerShell cmdlets that allow you to perform the data replication between multiple instances of Recovery Manager Console. To configure data replication, you have to provide credentials that have enough rights to access the replication consoles.

i NOTE:

For the 'Full' mode

- The account used for the replication task must be a member of the local **Administrators** group on the local and remote RMAD consoles.
- The account must be a member of the **Domain Users** group on each target domain.
- The account must be a member of the local **Administrators** group on the computer hosting the AD LDS (ADAM) instances.

For the 'Backups' mode

- The account used for the replication task must be a member of the local **Administrators** group on the local RMAD console.

To configure a list of remote consoles

Cmdlet	Description
Add-RMADReplicationConsole	Adds a RMAD console as a replication source. Example 1 This command adds the RMAD console on <Hostname1> to the replication console list with the Backups mode enabled. <pre>C:\>\$credential = Get-Credential C:\>Add-RMADReplicationConsole Hostname1 - AccessCredential \$credential -Mode Backup</pre> Example 2 This command adds the RMAD console on <Hostname1> to the replication console list with the Full mode enabled. <pre>C:\>Add-RMADReplicationConsole -ComputerName Hostname1 -Mode Full</pre>
Set-RMADReplicationConsole	Sets replication properties for the consoles from the replication console list: updates user credentials for connecting to a specified computer, and enables / disables the manual and scheduled replication for the console. Example 1 This command changes the credentials for accessing the console on Hostname1, and enables the replication for the console. <pre>C:\>\$credential = Get-Credential C:\>Set-RMADReplicationConsole -ComputerName Hostname1 -AccessCredential \$credential -Enabled \$true</pre> Example 2 This command changes the credentials for accessing the console with specified ID, and enables the replication for the console. <pre>C:\>Set-RMADReplicationConsole -Id 1 - AccessCredential \$credential -Enabled \$true</pre> Example 3 This command changes the credentials for accessing the console on Hostname1, and enables the replication for the console. <pre>C:\>Get-RMADReplicationConsole -ComputerName Hostname1 Set-RMADReplicationConsole - AccessCredential \$credential -Enabled \$true</pre>
Remove-RMADReplicationConsole	Removes the specified instance of RMAD console from the replication console list. Example This command removes the RMAD console on Hostname1 from the replication console list.

	C:\> Remove-RMADReplicationConsole Hostname1
Get-RMADReplicationConsole	Returns the replication console list with access credentials and the last synchronization date. Example This command gets all the RMAD consoles from the replication console list. C:\> Get-RMADReplicationConsole

To replicate the data

Cmdlet	Description and Example
Start-RMADReplication	Performs replication from other computers in the replication console list. Example 1 This command performs replication from a replication source. Start-RMADReplication Example 2 This command performs the replication as a background job. Start-RMADReplication -AsJob Example 3 This command performs replication from a replication console by its ID. Start-RMADReplication -Id 1 Example 4 This command performs replication from a replication console by its hostname. Start-RMADReplication -ComputerName ws1

To set a replication schedule

Before you set a replication schedule, create a schedule trigger using the **New-RMADSchedule** cmdlet, e.g.:
`$<schedule name> -New_RMADSchedule -Once -StartDate "8/25/2017 15:00".`

Cmdlet	Description and Example
Set-RMADReplicationSchedule	Sets or updates the existing schedule for the replication task. Example 1 This example illustrates how to replicate computers by using two replication schedules. \$credential = Get-Credential \$schedule=(New-RMADSchedule -Daily -StartDate "9/20/2013 10:00" -DaysInterval 1), (New-RMADSchedule -Daily -StartDate "9/20/2013 22:00" -DaysInterval 1) C:\PS>Set-RMADReplicationSchedule -Schedule \$schedule

	Example 2 This command updates the credentials for an existing schedule. <pre>\$credential = Get-Credential</pre> <pre>C:\PS>Set-RMADReplicationSchedule -Credential \$credential</pre>
Remove-RMADReplicationSchedule	Removes existing schedule for the specified computer. Example This command removes an existing replication schedule. <pre>Remove-RMADReplicationSchedule -ComputerName ws1</pre>
Get-RMADReplicationSchedule	Returns replication schedule information for the specified computer. Example This example illustrates how to get the replication schedule. <pre>Get-RMADReplicationSchedule -ComputerName ws1</pre>

Monitoring Recovery Manager for Active Directory

Recovery Manager for Active Directory release package contains RMAD Management Pack for Microsoft System Center Operations Manager (SCOM) that allows you to monitor the backup and restore operations performed by Recovery Manager for Active Directory. Also the Management Pack is used to check the health and availability of the Recovery Manager Console instances, Computer Collections and computers added to Computer Collections.

There are two editions of RMAD Management Packs for SCOM: Regular and Limited. By default, it is recommended to use the Regular edition of Management Pack.

Limited Management Pack contains reduced health state dashboards in comparison with the Regular edition. Only the RMAD event log is used for alert generating to reduce the computational load produced by the Management Pack.

- [Supported versions of Microsoft Operations Manager](#)
- [Importing Management Pack](#)
- [Rules provided in Microsoft System Center Operations Manager](#)
- [Health dashboards](#)

Supported versions of Microsoft Operations Manager

This Management Pack is designed for the following versions of Microsoft Operations Manager:

- Microsoft System Center Operations Manager 2012 R2
- Microsoft System Center Operations Manager 2012 SP1
- Microsoft System Center Operations Manager 2012
- Microsoft System Center Operations Manager 2007 R2
- Microsoft System Center Operations Manager 2007 SP1

Importing Management Pack

To start using the Management Pack, you need to import it into Microsoft Operations Manager as described in the example below. For more information about importing, using, and removing Management Packs, refer to the documentation supplied with your version of Microsoft Operations Manager.

To import the Management Pack into Microsoft System Center Operations Manager

1. Start System Center Operations Manager Operations Console.
2. From the main menu, select **Go | Administration**.

3. In the left pane, right-click the **Management Packs** node, and then click **Import Management Packs** on the shortcut menu.
4. On the **Select Management Packs** page, click the **Add** button, and then click **Add from disk**.
5. If you are prompted to search the online catalog for the dependencies the Management Pack may have, click **No**.
6. Browse to select the **Quest.Recovery.Manager.for.Active.Directory.mp** or **Quest.Recovery.Manager.for.Active.Directory.Limited.mp** file supplied in the Recovery Manager for Active Directory Forest Edition distribution package. When you are finished, click **Open**.
7. Click **Install** and follow the on-screen instructions to complete the Management Pack installation.

It is required to configure Recovery Manager for Active Directory 8.7 or earlier versions to start working with RMAD Management Pack for SCOM.

To configure Recovery Manager for Active Directory 8.7 or earlier versions

1. Open the Recovery Manager Console.
2. In the console tree, expand the **Computer Collections** node.
3. Right-click the Computer Collection you want to monitor by using this Management Pack, and then click **Properties** on the shortcut menu.
4. In the dialog box that opens, click the **Log** tab.
5. Make sure that you
 - Select the **Application Log** check box.
 - Select **Everything** from the **What to record** drop-down list.
 - Clear the **Create event upon warnings or errors only** check box.
6. When you are finished, click **OK** to close the dialog box.

Rules provided in Microsoft System Center Operations Manager

The next table lists the monitoring rules provided by the Management Pack in Microsoft System Center Operations Manager. The table also provides information on which of these rules are enabled or disabled by default.

Table 13: SCOM rules

Rule	Default setting
Collect Online Restore Is Starting Events (Recovery Manager Console)	Disabled
Collect Online Restore Progress - Objects Have Been Restored Successfully Events (Recovery Manager Console)	Disabled
Collect Online Restore Has Completed Events (Recovery Manager Console)	Disabled

Rule	Default setting
Collect Offline Restore Is Starting Events (Recovery Manager Console)	Disabled
Collect Offline Restore Progress - DC Restarted in Normal Mode Events (Recovery Manager Console)	Disabled
Collect Offline Restore Progress - DC Restarted in DSRM Events (Recovery Manager Console)	Disabled
Collect Offline Restore Progress - DC not Restarted in Normal Mode Events (Recovery Manager Console)	Disabled
Alert on Failed Offline Restore (Recovery Manager Console)	Enabled
Collect Offline Restore Has Failed Events (Recovery Manager Console)	Enabled
Collect Offline Restore Has Completed Successfully Events (Recovery Manager Console)	Disabled
Collect Backup Creation Has Started Events (Recovery Manager Console)	Disabled
Collect Backup Creation Has Completed with Warnings Events (Recovery Manager Console)	Disabled
Alert on Backup Creation Completed with Errors (Recovery Manager Console)	Enabled
Collect Backup Creation Has Failed Events (Recovery Manager Console)	Enabled
Collect Backup Creation Has Completed Successfully Events (Recovery Manager Console)	Disabled
Collect Online Restore Progress - Objects Have Been Restored Successfully Events (Restore Agent)	Disabled
Alert on Failed Offline Restore (Restore Agent)	Enabled
Collect Offline Restore Has Failed Events (Restore Agent)	Enabled
Collect Backup Creation Has Been Completed with Warnings Events (Backup Agent)	Disabled
Collect Backup Creation Has Started Events (Backup Agent)	Disabled
Alert on Failed Backup Creation (Backup Agent)	Enabled
Collect Backup Creation Has Failed Events (Backup Agent)	Enabled
Collect Backup Creation Has Completed Successfully Events (Backup Agent)	Disabled
Collect Information About Operations with Forest Recovery Project (Forest Recovery Console)	Disabled
Collect Forest Recovery Has Started Events (Forest Recovery Console)	Disabled
Collect Information About Forest Recovery Operation (Forest Recovery Console)	Disabled
Collect Information About Forest Recovery Operation (Forest Recovery Agent)	Disabled
Alert on Failed Forest Recovery Operation (Forest Recovery Console)	Enabled
Alert on Failed Forest Recovery Operation (Forest Recovery Agent)	Enabled
Alert on Abandoned Backup Session (Recovery Manager Console)	Enabled

Health dashboards

In the SCOM Operations console, Recovery Manager for Active Directory components are represented as three health state views (separate for each type of objects) and two multi-level diagrams. There are three types of

RMAD objects in these diagrams: Recovery Manager Console instances, Computer Collections existing in the Recovery Manager Console and Computers explicitly or implicitly added to Computer Collections. Each object has properties and health state determined by these properties.

In the multi-level diagrams **All Components in Computer Collections** and **All Recovery Manager Console Instances** under **Monitoring | Quest Recovery Manager for Active Directory**, health of upper-level components depends on the health of lower-level components.

The following table lists properties that are monitored by RMAD Management Pack for SCOM.

Table 14: RMAD object properties monitored by RMAD Management Pack

	Regular Management Pack	Limited Management Pack
Recovery Manager Console	• TargetComputer Display name of a RMAD console instance • Version Version of a RMAD console instance • IsForestEdition Indicates whether the Forest Edition of RMAD is used	• TargetComputer Display name of a RMAD console instance • Version Version of a RMAD console instance • IsForestEdition Indicates whether the Forest Edition of RMAD is used
Computer Collection	• DisplayName Display name of a computer collection • ID Computer collection ID • AgentSideBackupPath DC storage • ConsoleSideBackupPath Location of the backup storage on the RMAD Console side • CollectFEMetaData Indicates whether the RMAD Forest Edition metadata is collected • HasCollectionItems Indicates whether a computer collection has collection items	• DisplayName Display name of a computer collection • ID Computer collection ID • AgentSideBackupPath DC storage • ConsoleSideBackupPath Location of the backup storage on the RMAD Console side • CollectFEMetaData Indicates whether the RMAD Forest Edition metadata is collected • HasCollectionItems Indicates whether a computer collection has collection items
Computer	• TargetComputer Name of a domain controller • LastSessionResult Result of the last backup session • LastSessionDate Time stamp of the last backup session • BackupExists Indicates whether a backup was created in the last 30 days	• TargetComputer Name of a domain controller

The table below describes health checks that are performed by RMAD Management Pack for SCOM.

Table 15: Health checks performed by RMAD Management Pack

	Regular Management Pack	Limited Management Pack
Recovery Manager Console	Checks whether there are computer collection in the RMAD console instance.	Does not perform any checks.
Computer Collection	Checks whether a computer collection has collection items.	- Checks whether a computer collection has at least one domain controller. - There are no alerts about empty collections or collections which have no backups in the last 30 days.
Computer	- Checks whether a backup was created in the last 30 days. If there are no backups, the Management Pack generates the warning message. -OR- - Checks the result of the last backup session.	- Does not request any data about completed backups or backup sessions. - Does not check whether a backup was created in the last 30 days.

Using Management Shell

- [About Management Shell](#)
- [Installing and opening Management Shell](#)
- [Getting Help](#)

About Management Shell

The Recovery Manager for Active Directory 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 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.

Installing and opening Management Shell

This section covers:

- [Installation requirements](#)
- [Installing Management Shell](#)
- [Opening Management Shell](#)

Installation requirements

Before you install the Recovery Manager for Active Directory Management Shell, ensure that your system meets the system requirements provided in the Release Notes supplied with this release of Recovery Manager for Active Directory.

Installing Management Shell

To install Management Shell

1. Run the **Setup.exe** file included with the Recovery Manager for Active Directory Forest Edition installation package, and follow the instructions in the Setup Wizard.
2. To install Recovery Manager for Active Directory with default parameters (this includes installing the Management Shell component), click **Express**, and then follow the provided instructions to complete the Setup Wizard.

Opening Management Shell

You can open the Management Shell by using either of the following procedures. Each procedure loads the Recovery Manager for Active Directory Management Shell snap-in into Windows PowerShell. If you do not load the Recovery Manager for Active Directory Management Shell snap-in before you run a command (cmdlet) provided by that snap-in, you will receive an error.

NOTE: Recovery Manager for Active Directory Management Shell console must be started with elevated privileges. Otherwise, you will get warning messages when you execute the snap-in cmdlets.

To open the Management Shell

1. Start Windows PowerShell.

You can do so by running the **powershell** command at a command prompt (Cmd.exe).

2. At the Windows PowerShell prompt, enter the following command:

```
Add-PSSnapin Quest.RecoveryManager.AD.PowerShell
```

Alternatively, you can complete the following steps related to your version of Windows:

Table 16: Opening Management Shell

Windows 7 Windows Server 2008 or 2008 R2	A later version of Windows
1. Click Start. 2. Point to All Programs Quest Recovery Manager for Active Directory Forest Edition. 3. Click Management Shell.	On the Start screen, click the Management Shell tile.

Upon the shell start, the console may present you with a message stating that a certain file published by Quest is not trusted on your system. This security message indicates that the certificate the file is digitally signed with is not trusted on your computer, so the console requires you to enable trust for the certificate issuer before the file can be run. Press either R (Run once) or A (Always run). To prevent this message from appearing in the future, it is advisable to choose the second option (A).

Getting Help

The Recovery Manager for Active Directory Management Shell uses the Windows PowerShell help cmdlets to assist you in finding the appropriate information to accomplish your task. The following table provides some examples of how to use the **Get-Help** and **Get-Command** cmdlets to access the help information that is available for each cmdlet in the Recovery Manager for Active Directory Management Shell.

Table 17: Getting help

Command	Description
Get-Help	When you use Get-Help without any parameters, you are presented with basic instructions on how to use the help system in Windows PowerShell, including Help for the Recovery Manager for Active Directory Management Shell.
Get-Help<Cmdlet>	When you use Get-Help with the name of a cmdlet as an argument, you are presented with the help information for that cmdlet. For example, to retrieve the help information for the Get-RMADCollection cmdlet, use the following command: <pre>Get-Help Get-RMADCollection</pre>
Get-Command	Get-Command without any parameters lists all the cmdlets that are available to the shell. You can use the Get-Command cmdlet with the Format-List or Format-Table cmdlet to provide a more readable display. For example, use Get-Command Format-List to display the output in a list format. To display a list of all the Recovery Manager for Active Directory Management Shell cmdlets that are available to the shell, use the following syntax: <pre>Get-Command -PSSnapin Quest.RecoveryManager.AD.PowerShell</pre>
Get-Command<Cmdlet>	When you use Get-Command with the name of a cmdlet as an argument, you are presented with information about the parameters and other components of that cmdlet. The <Cmdlet> entry allows for wildcard character expansion. For example, to retrieve information about the cmdlets with the names ending in Member, you can use the following command: <pre>Get-Command *Member</pre>

Recovering an Active Directory forest

- [Permissions required to use Forest Recovery Console](#)
- [Forest Recovery Console](#)
- [Managing a recovery project](#)
- [Managing Forest Recovery Agent](#)
- [Rebooting domain controllers manually](#)
- [Resetting DSRM Administrator Password](#)
- [Managing the Global Catalog servers](#)
- [Managing FSMO roles](#)
- [Manage DNS Client Settings](#)
- [Configuring Windows Firewall](#)
- [Forest recovery overview](#)
- [Selectively recovering domains in a forest](#)
- [Recovering SYSVOL](#)
- [Deleting domains during recovery](#)
- [Resuming an interrupted forest recovery](#)
- [Recovering read-only domain controllers \(RODCs\)](#)
- [Checking forest health](#)
- [Collecting diagnostic data for technical support](#)

Permissions required to use Forest Recovery Console

Table 18: Minimum permissions

Task	Minimum permissions
Start and use the Forest Recovery Console	Have Read access to the Recovery Manager for Active Directory backup registration database.
Access domain controllers in the recovery project	Have either domain administrator rights or all of the following permissions: • Reanimate Tombstone control access right (or be a member of a group that has this access right).

Task	Minimum permissions
	By default, the Reanimate Tombstone control access right is only granted to domain administrators. Domain administrators can delegate the permission necessary to restore deleted objects to other users and groups by granting the user or group the Reanimate Tombstone control access right. A security risk can be introduced by delegating this permission to a user, because it allows the user to restore an account that may have a level of access greater than that of the user. By restoring such an account, the user in effect gains control of that account. This is because the LDAP API does not provide the capability to restore the backed up password, and so the user can set the initial password on the account. • Write access to each mandatory attribute that needs to be updated. • Write access to the Relative Distinguished Name (RDN) and other attributes that need to be updated. • Child-creation rights on the destination container for the object class that is to be restored. • Write access to universal and domain local groups in all domains in the forest.
Install or uninstall Forest Recovery Agent	Be a member of the local Administrators group on the target domain controller.
Check forest health if the User authentication; RID Master and GC operation option is selected on the Settings tab in the Check Forest Health dialog. For more details, refer Checking forest health.	Have either domain administrator rights or all of the following permissions on the container for the test user account: • Create/Delete user objects Applies to: This object and all descendant objects • Full Control Applies to: Descendant User objects

For information about using the Forest Recovery Console, see [Forest Recovery Console](#).

Forest Recovery Console

Recovery Manager for Active Directory Forest Edition provides a Forest Recovery Console where you can manage and monitor the recovery of the entire Active Directory forest or specific domains.

To start the Forest Recovery Console

- Complete the steps related to your version of Windows:

Table 19: Starting the Forest Recovery Console

**Windows 7
Windows Server 2008 or 2008 R2**

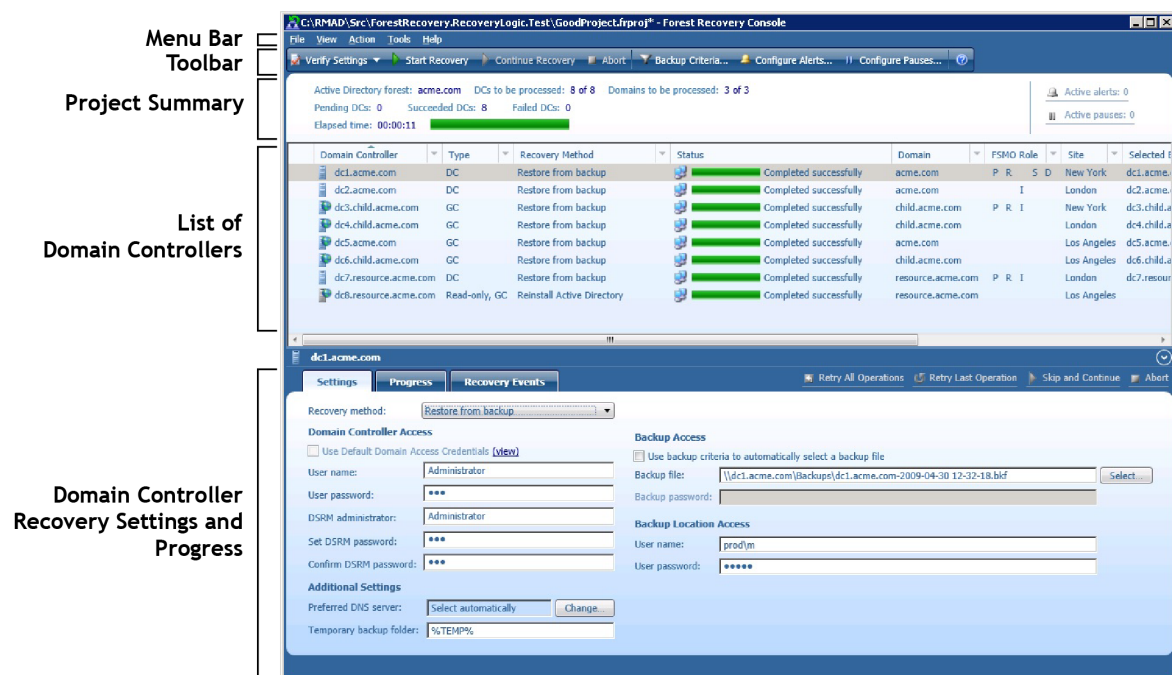
**A later version of
Windows**

1. Click **Start**.
2. Point to **All Programs | Quest | Recovery Manager for Active Directory Forest Edition**.
3. Click **Forest Recovery Console**

On the Start screen, click the **Forest Recovery Console** tile.

When opened for the first time, the Forest Recovery Console starts a wizard that helps you retrieve the Active Directory forest infrastructure information and create a recovery project for the forest. For more information, see [Managing a recovery project](#).

The Forest Recovery Console has the following elements:



Forest Recovery Console elements

Element	Description
Menu Bar	Provides commands allowing you to create, open, save, and manage a recovery project. For more information, see Managing a recovery project
Toolbar	Provides buttons for managing the current recovery project. For more information, see Toolbar .
Project Summary	Provides information about the current project and allows you to manage active recovery alerts and pauses in the project. For more information, see Project summary .
List of Domain	Provides a list of domain controllers in the current project. You can sort or filter the

Element	Description
Controllers	entries in the list by a number of criteria. For more information, see List of domain controllers .
Domain Controller Recovery Settings and Progress	Allows you to manage recovery settings and view recovery progress for the domain controllers currently selected in the list. For more information, see Domain controller recovery settings and progress .
Errors and Warnings	Displays warnings and critical errors, if any, for the recovery project. This area is located in the bottom-right corner of the Forest Recovery Console window. To view critical errors, point to the red cross. To view warnings, point to the yellow exclamation sign. The yellow exclamation sign and red cross become available only when there are any warnings or critical errors for you to view.

In this section:

- [Toolbar](#)
- [Project summary](#)
- [List of domain controllers](#)
- [Domain controller recovery settings and progress](#)
- [Configuring advanced settings](#)

For more information on permissions required to use the Forest Recovery Console and recover an Active Directory forest or specific domains, see [Permissions required to use Forest Recovery Console](#).

Toolbar

The Forest Recovery Console toolbar has the following buttons:

Table 20: Toolbar buttons

Button	Description
Verify Settings	Collects and saves the information to be used for recovery from all domain controllers in the recovery project. Then, checks the project's recovery settings against the collected information to provide you information about any inconsistencies. For more information, see Verifying recovery project settings .
Start Recovery	Starts the recovery operation on the current recovery project.
Continue Recovery	Resumes the recovery operation that was automatically suspended at a certain stage. For example, the Recovery Manager for Active Directory Forest Edition may suspend the forest recovery operation to prompt you for an action. The recovery may also be automatically suspended if the restore of a domain controller fails. For more information, see Handling failed domain controllers .
Abort	Cancels the currently running recovery or verify settings operation.
Backup Criteria	Allows you to specify backup selection criteria to automatically select a backup file for each domain controller you want to restore from backup. For more information, see Selecting backups for recovery .

Button	Description
Configure Alerts	Allows you to create, modify, or delete recovery alerts in the current project. For more information, see Using recovery alerts .
Configure Pauses	Allows you to create, modify, or delete recovery pauses in the current project. For more information, see Using recovery pauses .
Configure Schedule	Allows you to create, edit and delete a schedule for the verify settings operation.

Project summary

This area provides some basic information about the current recovery project, such as the Active Directory forest name and the number of domains and domain controllers in the forest. For a diagram that illustrates the Forest Recovery Console elements, see [Forest Recovery Console](#).

When you are running a recovery or verify settings operation, the Project Summary area provides the following elements:

Table 21: Project Summary elements

Element	Description
Active alerts	Displays the number of active recovery alerts in the recovery project. Click this link to manage active alerts and view their details. For more information, see Using recovery alerts .
Active pauses	Displays the number of active recovery pauses in the recovery project. Click this link to manage active pauses and view their details. For more information, see Using recovery pauses .

List of domain controllers

This area provides a list of all domain controllers in the current recovery project along with some basic information about each domain controller, such as domain controller name, domain, site, FSMO roles, specified recovery method, recovery pause status, and currently selected backup (if any) and its age.

You can use the list of domain controllers to perform a number of commands on the domain controllers in the recovery project.

For a diagram that illustrates the Forest Recovery Console elements, see [Forest Recovery Console](#).

In this section:

- [Filtering the list of domain controllers](#)
- [Connecting to a domain controller via RDP](#)

Filtering the list of domain controllers

To filter domain controllers in the list

1. In the list of domain controllers, point to the heading of the column by which you want to filter the domain controllers.
2. Click the down arrow next to the column heading, and specify your filter criteria.

Connecting to a domain controller via RDP

To connect to a domain controller via RDP

1. In the list of domain controllers, right-click the domain controller to which you want to connect.
2. Click **Connect via RDP** on the shortcut menu.

Domain controller recovery settings and progress

For a diagram that illustrates the Forest Recovery Console elements, see [Forest Recovery Console](#).

The Domain Controller Recovery Settings and Progress area has the **Settings** tab, the **Progress** tab, the **Recovery Events** tab, and a toolbar providing commands for managing the recovery of the domain controllers selected in the list.

In this section:

- [Settings tab](#)
- [Progress tab](#)
- [Recovery Events tab](#)

Settings tab

You can use this tab to specify recovery settings for one or more domain controllers selected in the list.



TIP: To specify recovery settings for multiple domain controllers at a time:

- Hold down CTRL, and then click to select domain controllers in the list of domain controllers.
- Use the **Settings** tab to specify recovery settings for the selected domain controllers.

The "Domain Controller Recovery Settings and Progress" area also provides the following commands for managing the recovery of domain controllers:

Table 22: Recovery-related commands

Command	Description
Retry All Operations	Retries all operations for the selected domain controllers. Before retrying all operations, you may specify a different recovery method for the domain controllers.
Retry Last Operation	Retries the last operation performed during the current session on the selected domain controllers.
Skip and Continue	Skips the error encountered for the selected domain controllers.
Abort	Cancels the recovery or verify settings operation for the domain controllers selected in the list.

The **Settings** tab has the following areas:

- **Recovery method.** Allows you to choose one of the following recovery methods for the domain controller selected in the list:

Table 23: Recovery Method

Recovery Method	Description
Restore from backup	Restores the domain controller from the backup you specify. For more information on backup selection methods, see Selecting backups for recovery. During recovery, Recovery Manager for Active Directory Forest Edition uses custom Internet Protocol security (IPSec) rules to isolate the domain controllers for which you selected this recovery method. For more information, see How does Recovery Manager for Active Directory Forest Edition isolate domain controllers during forest recovery?
Restore SYSVOL	Restores contents of the SYSVOL share on the specified domain controllers. Read-only domain controllers (RODC) will be restored as well. This method can be set only on the Recovery Mode tab of Recovery Project Settings. For details, see Recovering SYSVOL.
Reinstall Active Directory	Uninstalls Active Directory and then installs it again by using Microsoft's native tools. For domain controllers running Windows Server 2008 or earlier, this step uses the Dcpromo.exe tool. For Windows Server 2012-based domain controllers, this step uses the native Windows PowerShell cmdlets <i>Install- ADDSDomainController</i> and <i>Uninstall- ADDSDomainController</i>. After the Active Directory reinstallation is complete, the domain controller replicates Active Directory data from other domain controllers that were restored from backups in the recovery project. i NOTE: The Reinstall Active Directory recovery method removes the global catalog by default if it is present on the domain controller being recovered. If you need to reconfigure the global catalog on the domain controller during Active Directory reinstallation, select the Configure the domain controller as a global catalog server option in the Additional Settings section.
Uninstall Active Directory	Performs a forced removal of Active Directory from the domain controller and then demotes it to a member server in the domain. Domain controller's metadata is completely removed from Active Directory. NOTE: When you use this method, the local Administrator password on the target domain controller is reset to the value you specify in the Set DSRM password and Confirm DSRM password text boxes in the Forest Recovery Console.
Adjust to Active Directory changes	This option is selected automatically when the domain controller is a Global Catalog server and belongs to the excluded domain. For more details, see Selectively recovering domains in a forest. Global Catalogs of excluded domains should be adjusted to the state of recovered domains. For more information, see the description of the <i>Adjust to Active Directory Changes</i> step in Descriptions of recovery or verification steps.

Recovery Method	Description
Do not recover	Isolates and then completely removes the domain controller from its domain. Recovery Manager for Active Directory Forest Edition also removes all metadata of the domain controller from the Active Directory forest.

- **Domain Controller Access.** Allows you to specify the user name and password that will be used by Recovery Manager for Active Directory Forest Edition to access domain controllers in the domain.

This area has the following text boxes:

Table 24: Text boxes in the Domain Controller Access area

Element	Description
Use Default Domain Access Credentials	This option lets you use the default domain credentials to access domain controllers. To configure the default domain access credentials, select the option and press the view link that opens Recovery Project Settings. For more details, see Specifying recovery project settings. If the option is not selected, you can specify domain access credentials and DSRM password in the Domain Controller Access section. Otherwise, the Domain Controller Access section is not active.
• User name • User password	Allow you to specify the user name and password with which you want Recovery Manager for Active Directory Forest Edition to access the selected domain controllers in normal mode.
DSRM administrator	Allows you to specify the user name with which you want Recovery Manager for Active Directory Forest Edition to access the selected domain controllers in Directory Services Restore Mode (DSRM).
• Set DSRM password • Confirm DSRM password	Allow you to specify the DSRM password to be used by Recovery Manager for Active Directory Forest Edition during the domain controller (DC) recovery. When using these boxes, consider the current mode of the DC: • If the DC is already in DSRM mode. Use these boxes to specify the current password of the account you entered in the DSRM administrator text box. Otherwise, the DC recovery will fail. • If the DC is not in DSRM mode. Use these boxes to set a new temporary DSRM password for the account you entered in the DSRM administrator text box. Recovery Manager for Active Directory Forest Edition will use this temporary DSRM password to restart the domain controller in DSRM during the recovery. Then, Recovery Manager for Active Directory Forest Edition will replace this temporary password with the DSRM password stored in the backup you specified for the DC.
• Additional Settings	This area has the following options: • Configure the domain controller as a global catalog server Use this option if you need to reconfigure the global catalog on the domain controller during Active Directory reinstallation.

- **Preferred DNS settings.**

Allows you specify a preferred DNS server for the domain controller during its recovery. For more information, see [Assigning a preferred DNS server during recovery](#).

- **Temporary backup folder**

Here you can specify the folder on the domain controller to store temporary forest backup data.

- **Backup Access.** Allows you to select the backup file from which you want to restore the domain controller and specify other settings for accessing the backup file.

This area has the following elements:

Table 25: Elements in the Backup Access area

Element	Description
Use backup criteria to automatically select a backup file	Allows you to automatically select a backup file that meets particular criteria. To specify your criteria, click the Backup Criteria button on the toolbar.
Backup file	Displays the path and name of the currently selected backup file from which the domain controller will be restored. To manually select a backup file, make sure the Use backup criteria to automatically select a backup file check box is cleared, and then click the Select button.
Backup password	Allows you to type the password to open a password-protected backup.

- **Backup Location Access.** Allows you to enter the user name and password with which you want to access the location that holds the backup specified in the **Backup file** box. The account you specify must have Read access to that location.

Progress tab

You can use this tab to view progress of the recovery stages and steps applicable to the domain controller selected in the list. To view more information about a recovery step on this tab, point to that step, and then point to the question mark displayed next to it.

You can copy the information displayed on the **Progress** tab to the Clipboard and then paste it to another application (for example, a Microsoft Office Word file). To do so, point to the **Progress** tab, and then click the **Copy** button in the upper right corner of the tab. This copies all the information displayed on the **Progress** tab, including the current status of each recovery stage and step and any error messages displayed on the tab.

Recovery Events tab

You can use this tab to view recovery events related to the entire Active Directory forest, specific domain controllers, or both these categories of recovery events.

On this tab, you can use the following elements:

Table 26: Recovery Events tab elements

Element	Description
Show	Select a category of recovery events to view:

Element	Description
	• Forest-wide events. Shows recovery events related to the entire Active Directory forest. • Events for selected DCs. Shows recovery events related to the domain controllers selected in the list. • All events. Shows forest-wide events and events related to the domain controllers selected in the list.
Copy	Copies events in the list to Clipboard.
Export	Allows you to export events in the list to one of the following formats: • Text (Tab delimited) (*.txt) • CSV (Comma delimited) (*.csv)

Configuring advanced settings

You can change a number of advanced settings of the Forest Recovery Console. To do so, you need to modify the FRConsoleSettings.xml file that stores these advanced settings. You can find this file in the Recovery Manager for Active Directory Forest Edition installation folder (by default, this is %ProgramFiles%\Quest\Recovery Manager for Active Directory Forest Edition).

The changes you make in the FRConsoleSettings.xml file become effective right after you save the file. You do not need to restart the Forest Recovery Console.

The FRConsoleSettings.xml file includes the following XML elements you can modify:

Table 27: XML elements

XML Element	Description
SkipUnmodifiedFilesDuringRecovery	Enables or disables skipping the files that are identical on the domain controller and in the backup during restore operations. This element can take one of the following values: • TRUE. Enables skipping the files. • FALSE. Disables skipping the files.
PasswordsLength	Sets the length (in characters) for the passwords automatically generated by Recovery Manager for Active Directory Forest Edition. PasswordsSymbols Allows you to specify what symbols you want to use in the passwords automatically generated by Recovery Manager for Active Directory Forest Edition. This element can take the following values: • Latin. Specifies to use English letters. • Number. Specifies to use Arabic numerals. • Upper. Specifies to use uppercase English letters. • Lower. Specifies to use lowercase English letters. • All. Specifies to use all of the above-listed characters.

XML Element	Description
	You can specify multiple values in this element. When specifying multiple values, use a pipe () as a separator. Example: Latin Number Upper Lower
MaximumBackupAgeInDays	Specifies the maximum age (in days) of the backups to be displayed on the GUI. Backups whose age exceeds the specified value will not be displayed.
DisableSystemPauses	Do not change the value in this element. This element is for internal use only.
EnablePersistence	Enables or disables the Recovery Persistence feature. This element can take one of the following values: • TRUE. Enables the Recovery Persistence feature. • FALSE. Disables the Recovery Persistence feature.
DaysBetweenProjectUpdates	Sets the maximum number of days between the updates of a recovery project. When the specified value is exceeded for a project, the Forest Recovery Console displays a warning.
SelectDnsTimeout	Sets a timeout for the DNS server search operation performed during a forest or domain recovery. Use the format hh:mm:ss.
DiagnosticsDataPath	Specifies the default location on the Forest Recovery Console computer for storing diagnostic data gathered with the Diagnostic Data Collector.
TargetGcOccupancyLevel	Sets the global catalog partition occupancy level value to be used when advertising a rebuilt GC fast. This element can take one of the following values: • 0. No occupancy requirement. • 1. At least one read-only partition in site added by Knowledge Consistency Checker. • 2. At least one partition in site fully synchronized. • 3. All read-only partitions in site added by Knowledge Consistency Checker, at least one synchronized. • 4. All partitions in site fully synchronized. • 5. All read-only partitions in forest added by the Knowledge Consistency Checker, at least one synchronized. • 6. All partitions in forest fully synchronized.
EnsuresSingleInstance	Allows you to restrict the number of Forest Recovery Console instances that can be run simultaneously on this computer. This element can take one of the following values: • TRUE. Only one instance of Forest Recovery Console can be run at a time.

XML Element	Description
	• FALSE. The number of Forest Recovery Console instances that can be run simultaneously is unlimited.
RidPoolIncreaseValue	Specifies the value by which to raise the number of available RID pools.

If necessary, you can revert to the default values in the **FRConsoleSettings.xml** file.

To revert to the default values

1. Delete the **FRConsoleSettings.xml** file.
2. Restart the Forest Recovery Console on the computer on which you deleted the file in step 1.

Recovery Manager for Active Directory Forest Edition recreates the **FRConsoleSettings.xml** file and assigns default values to the elements in the file.

Managing a recovery project

A recovery project is where you manage the recovery of the entire Active Directory forest or specific domains. Each recovery project contains a list of domain controllers to be recovered and their recovery settings, such as recovery method and access credentials. You can specify individual recovery settings for each domain controller in a recovery project. A recovery project also has a number of project-specific settings you can modify.

Each recovery project is saved to an individual project (.frproj) file. A project (.frproj) file holds information about the contents and settings of the project and the recovery settings specified for the DCs in the project. In this section:

- [Creating a recovery project](#)
- [Opening a recovery project](#)
- [Opening a legacy recovery project](#)
- [Saving a recovery project](#)
- [Updating a recovery project](#)
- [Specifying recovery project settings](#)
- [Specifying recovery settings for a DC](#)
- [Selecting backups for recovery](#)
- [Verifying recovery project settings](#)
- [Scheduling project verification](#)
- [Using recovery alerts](#)
- [Using recovery pauses](#)
- [Copying a backup file to a new location](#)

Creating a recovery project

To create a new recovery project, you can use a New Recovery Project Wizard. This wizard helps you retrieve the Active Directory forest infrastructure information and save it in a recovery project (.frproj) file.

The wizard offers you the following methods to retrieve the forest infrastructure information:

- Retrieve the forest infrastructure information from an Active Directory backup registered with Recovery Manager for Active Directory Forest Edition.
- Connect to any available live domain controller in the forest to retrieve the forest infrastructure information.

To create a new recovery project

1. On the menu bar, select **File | New Project**.
2. On the **Retrieving the Forest Infrastructure** page of the wizard, click one of the following:
 - **Select a Backup.** Allows you to retrieve the forest infrastructure information from an Active Directory backup registered with Recovery Manager for Active Directory Forest Edition. With this option, you can only use backups stored on the computer on which you are using the Forest Recovery Console.
 - **Connect to Forest.** Allows you to connect to a live domain controller and retrieve the forest infrastructure information from the Active Directory database held on that domain controller.
3. Follow the steps in the wizard until you are on **The following forest information has been collected** page.
4. Click the **Advanced** button to specify the domains you want to include in the recovery project.
5. Click **Finish** to complete the project creation.

The title bar of the Forest Recovery Console displays the name of the project (.frproj) file you have created.

i | **NOTE:** Each recovery project must be protected with a password. When prompted, set a protection password for your project and make sure you keep the password for your records.

Opening a recovery project

To open an existing recovery project

1. On the menu bar, select **File | Open Project**.
2. Browse to select the project (.frproj) file you want to open, and then click **Open**. The title bar of the Forest Recovery Console displays the name of the project (.frproj) file you have opened.

Opening a legacy recovery project

This section describes how to open a legacy Recovery Project (.frproj) file created with Forest Recovery Console 8.2 or earlier if FIPS-compliant algorithms are enabled on the Forest Recovery Console 8.6 or later computer.

Forest Recovery Console version 8.2 or earlier used hashing and encryption algorithms incompatible with FIPS. For this reason, to open a legacy .frproj file created with Forest Recovery Console version 8.2 or earlier, you need to temporarily disable FIPS-compliant algorithms on the Forest Recovery Console 8.6 or later computer.

To open a legacy recovery project

1. On the Forest Recovery Console 8.6 or later computer, disable FIPS-compliant algorithms:
 - a. Start the Group Policy Object Editor tool (gpedit.msc).
 - b. In the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then select **Security Options**.
 - c. In the right pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
 - d. In the dialog box that opens, select **Disabled** and click **OK**.
2. Restart the computer.
3. In Forest Recovery Console 8.6 or later, open the legacy .frproj file, and then save it.

By doing so, you update the project to use FIPS-compliant algorithms.

4. Enable FIPS-compliant algorithms on the Forest Recovery Console 8.6 or later computer.

i **NOTE:** To protect its data, the Forest Recovery Console version 8.6 or later uses the SHA-1 hashing algorithm and the Triple DES encryption algorithm that are FIPS-compliant. For more information about FIPS-compliant algorithms, see Microsoft Knowledge Base article 811833 "[The effects of enabling the 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' security setting in Windows XP and in later versions of Windows](http://support.microsoft.com)" at <http://support.microsoft.com>.

Saving a recovery project

To save the changes made to a recovery project

- On the menu bar, select **File | Save Project**.

Updating a recovery project

It is recommended to regularly update your recovery project so that it reflects the changes occurred in your Active Directory forest.

To update a recovery project

1. Open the recovery project you want to update.
2. On the menu bar, click **Tools | Update Project with Changes in Active Directory**.
3. Follow the steps in the wizard to update your project.

Specifying recovery project settings

Each recovery project has a number of project-specific settings that allow you to control the various aspects of recovery. For example, you can use these settings to select how to handle the global catalog during recovery, configure balloon notifications displayed in the Forest Recovery Console, configure e-mail notification settings, select the Active Directory domains you want to recover, and enable or disable the Recovery Persistence feature that provides protection from an inadvertent shutdown of the Forest Recovery Console.

To specify the recovery project settings

1. Open or create a recovery project.
2. On the menu bar, select **Tools | Recovery Project Settings**.
3. Use the tabs described in the table below to view or modify the recovery project settings.

Table 28: Recovery project settings

Tab	Description
Recovery Mode	Displays a list of all domains in the current recovery project. On this tab, you can use the following options: • Specify which type of restore operation you want to perform: • Forest Recovery • Domain Recovery • SYSVOL Recovery • Specify the domains you want to selectively recover in the forest. For more information on how to selectively recover domains, see Selectively recovering domains in a forest. • For each domain, you can configure the domain controller where authoritative restore of SYSVOL will be performed. • You can specify default credentials to access domain controllers in the selected domain.
Global Catalog	Allows you to select how to handle the global catalog during recovery. This tab provides the following options: • Rebuild GC, advertise normally. Uses a standard Active Directory mechanism to remove and add the global catalog. By removing and then adding the global catalog you ensure that it contains no lingering objects and thus can avoid replication inconsistencies. To advertise the rebuilt global catalog servers in DNS, this option uses the existing Global Catalog Partition Occupancy level specified in the system registry. By default, a global catalog server is considered as ready to be advertised in DNS when all read-only directory partitions have been fully replicated to the new global catalog server. However, your particular forest may use a different setting. For this reason, it is recommended that you check the Catalog Partition Occupancy level specified in the system registry. If the default setting is used, then the Rebuild GC, advertise normally option is the safest and most reliable way to rebuild and advertise the global catalog during the recovery. This option rebuilds the global catalog in the entire forest regardless of how many domains you are recovering.

Tab	Description
	• Rebuild GC, advertise fast. Uses a standard Active Directory mechanism to remove and then add the global catalog. This option offers a faster way to advertise the rebuilt global catalog servers in DNS. As a result, this option can help you make a number of forest-wide services (for example, user logon and Exchange Server messaging) available to the users more quickly after the recovery. When you select this option, the rebuilt global catalog servers will be advertised in DNS without waiting for the read-only directory partitions replication to fully complete. The trade-off of using this option is that the global catalog may include some inconsistencies until the global catalog servers have received the complete information from all the other domains in the forest. This option rebuilds the global catalog only in the domains that you recover by using Recovery Manager for Active Directory Forest Edition. • Keep GC intact. Does not rebuild or change the global catalog in any way during the recovery. With this option, the global catalog servers will remain either in the state in which they were before the recovery started (this is true for the servers that are located in the domains you selected not to recover) or in the state to which they were restored from backup during the recovery. In certain situations, this option might help you avoid global catalog downtime and make some forest-wide services available to the users more quickly. However, using this option greatly increases the risk of introducing lingering objects into the global catalog, which can lead to a corrupt forest. It might happen if you use a set of backups for the domain controllers with large age difference. That is, backups may contain inconsistencies that will lead to introducing lingering object. If you use this option, it is recommended that you manually reset the global catalog to ensure it does not include inconsistencies.
Notifications	Allows you to configure balloon notifications in the Forest Recovery Console to inform you if the backups selected for recovery were created at different points in time or if your recovery project is outdated. • Age difference of selected backups exceeds <Number> hours. When selected, notifies you if the age difference of backups selected for recovery exceeds the number of hours you specify in this option. This option helps you ensure that the backups you select are created at a similar point in time and therefore hold similar Active Directory states. • Recovery project was updated more than <Number> days ago. When selected, notifies you if the current recovery project was last updated more than the number of days you specify in this option. • Forest topology has changed (only checked at console startup). When selected, causes the Forest Recovery Console to check if the forest topology information in the current recovery project is outdated. This check is performed each time the Forest Recovery Console starts up. Allows you to send e-mail notifications to specific recipients when the verification or

Tab	Description
	recovery process is completed. • Verification process is completed When the option is selected, the specified recipients will be notified that the verification process has been completed. • Recovery process is completed When the option is selected, the specified recipients will be notified that the recovery process has been completed. • E-mail address Use this text box to specify e-mail recipients.
E-mail	On this tab, you can configure e-mail notification settings. Recovery Manager for Active Directory Forest Edition will use these SMTP settings to send e-mail notification after the verification or recovery process has been completed. NOTE: SSL data encryption is not supported for email notifications. • SMTP server Specify the SMTP server for outgoing messages. • SMTP port Specify the port number that will be used to connect to your SMTP server. • Sender email address Specify the return address for your e-mail notification messages. It is recommended that you specify the e-mail address of the Recovery Manager for Active Directory administrator. • SMTP server requires authentication When the option is selected, you will be prompted to provide credentials to log on to the SMTP server. • User name Specify the account name used to log on to the SMTP server. • Password Specify the user password. • Test settings Sends a test notification message to the address specified in the Sender email address text box. Use this button to verify that the specified e-mail notification settings are valid.
Agents	On this tab, you can specify TCP ports that will be used by Forest Recovery Console to communicate with Forest Recovery Agent and Management Agent. • Connect to Management Agent using a specific TCP port. This agent is used to deploy other agents to the target server. Allows you to specify the TCP port number that will be used to connect to Management Agent installed on a target domain controller. If the option is not selected, RPC dynamic port range is used by default. • Management Agent will configure Windows Firewall exceptions. If this option is selected, Windows Firewall settings will be configured automatically for Management Agent. • Connect to Forest Recovery Agent using a specific TCP port. Allows you to specify the TCP port number that will be used to connect to Forest Recovery Agent installed on a target domain controller. If the option is not selected, RPC dynamic port range is used by default. • Forest Recovery Agent will configure Windows Firewall exceptions. If this option is selected, Windows Firewall settings will be configured automatically for Forest Recovery Agent.

Verifying recovery project settings

To ensure you can recover your Active Directory forest with minimum downtime, it is recommended that you regularly run the verify settings operation on your recovery project. When you run this operation, Recovery Manager for Active Directory Forest Edition connects to the domain controllers in the project, collects their configuration parameters, and then saves these parameters in the recovery project (.frproj) file. The verify settings operation does not modify any data in your Active Directory forest.

After the configuration parameters have been collected, Recovery Manager for Active Directory Forest Edition checks the recovery project settings against these parameters for any incompatibilities that may affect the forest recovery process. When the verify settings operation completes, you can view a report providing details about any problems found in your recovery project.

Running the verify settings operation on a regular basis allows you to promptly reveal any potential recovery problems and proactively prevent them by making appropriate adjustments to the recovery project settings.

When you run the verify settings operation, Recovery Manager for Active Directory Forest Edition collects and saves the following information from each domain controller in the project:

- IP addresses of all network adapters
- IP addresses of all DNS servers on all network adapters
- DNS names of all FSMO role holders in the Active Directory forest
- Forest Recovery Agent version installed on the domain controller (if any)
- Whether the domain controller is read-only (RODC)
- Operating system version installed on the domain controller

To verify the settings of your recovery project

1. Create or open a recovery project.
2. Specify recovery settings in the project.
3. On the toolbar, click **Verify Settings** and wait for the operation to complete.

After the verify settings operation completes, you can view a report on the operation results: from the menu bar, select **View | Report**.

Scheduling project verification

To automate running of the verify settings operation on a regular basis, you can schedule this operation for the recovery project.

i **NOTE:** You must configure email settings to receive verification results when the scheduled verification task is completed. Otherwise, the project verification on schedule will not work. For more details, see [Specifying recovery project settings](#).

To create a schedule for the verify settings operation

1. In Forest Recovery Console, create or open an existing recovery project.
2. On the toolbar, click **Configure Schedule....**
3. In the **Configure Schedule** dialog box, click **Modify....**
4. In the dialog that appears, click **New...** and configure the schedule.

5. Then you will be able to see a list of configured schedules in the **Configure Schedule** dialog. The **Enable schedule** option is selected by default.
6. To specify a user account for the project verification, click **Select account...** in the **Configure Schedule** dialog. If you skip this step, you will be prompted for a user name and password when saving the schedule. You must use the Administrator user account.
7. Click **OK** to save the schedule.

To change the project schedule settings

1. In Forest Recovery Console, open an existing recovery project.
2. On the toolbar, click **Configure Schedule...**
3. To enable or disable the schedule, use the **Enable Schedule** check box in the **Configure Schedule** dialog.
4. To change the schedule, click **Modify.....**
5. In the dialog box that opens, configure the new schedule and click **OK**.
6. To change the schedule account, click **Select account...** in the **Configure Schedule** dialog.
7. Enter new credentials, then you will be prompted for the account which is currently used for this schedule. Enter the current credential and click **OK**.
8. Click **OK** to save the changes in the **Configure Schedule** dialog. If you have not changed the account, you will be prompted for the current credentials.

To remove a schedule for the project:

1. In Forest Recovery Console, open an existing recovery project.
2. On the toolbar, click **Configure Schedule...**
3. Click **Modify....**
4. Delete all schedules and click **OK**.
5. Click **OK** in the **Configure Schedule** dialog and you will be prompted for the current schedule account.
6. Enter the current credentials and click **OK**.

Specifying recovery settings for a DC

You can set individual recovery settings for each domain controller in your recovery project. For more information about these settings, see [Domain controller recovery settings and progress](#).

To specify recovery settings for a domain controller

1. Create or open a recovery project.
2. In the list of domain controllers, select the domain controller for which you want to specify recovery settings.
3. Use the **Settings** tab to specify recovery settings.

Selecting backups for recovery

You can only restore domain controllers from backups created with Recovery Manager for Active Directory Forest Edition. The Forest Recovery Console provides the following methods for you to select backups for recovery:

- **Method 1: Automatically select backups based on your criteria.** Allows you to automatically select specific backups for multiple domain controllers according to the backup selection criteria you specify.
- **Method 2: Manually select backups.** Allows you to manually select any backup for a given domain controller in the recovery project. You can only select from backups created with Recovery Manager for Active Directory Forest Edition.

The next sections describe each of these methods.

Method 1: Automatically select backups based on your criteria

You can use the Forest Recovery Console to automatically select backups for multiple domain controllers in your recovery project. This method allows you to specify a time period, and then automatically select the latest backup created in that period for particular domain controllers in the project.

To automatically select backups

1. Specify your backup selection criteria:
 - a. Create or open a recovery project.
 - b. On the Forest Recovery Console toolbar, click **Backup Criteria**.
 - c. Select one of the following options:

Table 29: Automatic backup selection options

Option	Description
Use latest backup	Allows you to use the most recent backup registered with Recovery Manager for Active Directory Forest Edition for a given domain controller.
Use latest backup created before <Date> and after <Date>	Allows you to specify a date range and use the most recent backup from that range for a particular domain controller.
Use backups on DCs whenever possible	When this check box is selected, Recovery Manager for Active Directory Forest Edition first searches DCs to be restored for backups that meet the criteria you have specified. If no suitable backups found on the DCs, Recovery Manager for Active Directory Forest Edition will search the Forest Recovery Console computer for backups. By selecting this check box, you can avoid unnecessary backup file copying from the Forest Recovery Console to the DCs to be restored and thus speed up the recovery process.

2. When you are finished, click **OK**.
3. Specify the domain controllers for which you want to automatically select backups:
 - a. Hold down CTRL, and then click to select such domain controllers in the list of domain controllers.
 - b. Open the **Settings** tab, and then select the **Use backup criteria to automatically select a backup file** check box.

To view which backup was automatically selected for a domain controller, select that domain controller in the list, open the **Settings** tab, and see the backup file path and name in the **Backup file** box.

To manually select a different backup, clear the **Use backup criteria to automatically select a backup file** check box, and click the **Select** button to select a backup.

Method 2: Manually select backups

This method allows you to manually select any backup for a given domain controller in the recovery project. You can only select from backups registered with Recovery Manager for Active Directory.

To manually select a backup

1. Create or open a recovery project.
2. In the list of domain controllers, select the domain controller for which you want to select a backup.
3. Open the **Settings** tab, and then click the **Select** button next to the **Backup file** box to select a backup.

Using recovery alerts

Recovery alerts provide you with the real-time information about the recovery of domain controllers in your project. You can configure a recovery alert to inform you when particular domain controllers complete the recovery stage you specified in the alert settings.

For a recovery project, you can create and configure multiple alerts, each having different settings. You can also modify settings of existing alerts or delete alerts as necessary. To manage recovery alerts, click the **Configure Alerts** button on the toolbar of the Forest Recovery Console.

For each alert, you can select one or more domain controllers to which the alert will apply. You can configure an alert to inform you about the completion of one or more of the following recovery stages on the target domain controllers:

Table 30: Recovery stages for which you can use alerts

Recovery stage	Description
Prepare to restore from backup	During this stage, Recovery Manager for Active Directory Forest Edition verifies that the backup files you selected for recovery are available on the target domain controllers. If necessary, Recovery Manager for Active Directory Forest Edition copies the backup files that are missing. Also, Recovery Manager for Active Directory Forest Edition disables Microsoft Windows Update if it is enabled on the domain controllers.
Perform restore from	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps:

Recovery stage	Description
backup	• Detect current mode (DSRM or normal) • Reset DSRM administrator password • Restart domain controller in DSRM • Enable domain controller isolation • Disable BitLocker • Disable custom password filters • Restore data from backup • Restart domain controller in normal mode
Configure domain controller	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: • Get information about domain controller • Select preferred DNS server • Remove global catalog (if you did not specify to keep the existing global catalog) • Raise RID pool • Invalidate RID pool • Seize FSMO roles • Clean up metadata of removed domain controllers • Reset the Krbtgt password • Reset computer account passwords • Enable custom password filters • Restart domain controller in normal mode • Reset trust passwords
Make domain controller available	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: • Ensure that domain controller isolation is disabled • Clean up metadata of unrecovered domains if necessary • Change global catalog partition occupancy level • Add global catalog (if you did not specify to keep the existing global catalog) • Wait for a global catalog server to become available • Restore initial global catalog partition occupancy level • Enable the use of global catalog for user authentication • Enable BitLocker • Enable Windows Update (if it was enabled before the recovery)

Recovery stage	Description
	Remove temporary files
Uninstall Active Directory Domain Services	During this stage, Recovery Manager for Active Directory Forest Edition uninstalls Active Directory using the native tools provided by Microsoft. For domain controllers running Windows Server 2008 or earlier, Recovery Manager for Active Directory Forest Edition uses the Dcpromo.exe tool. For Windows Server 2012-based domain controllers, Recovery Manager for Active Directory Forest Edition uses the native Windows PowerShell cmdlet <i>Uninstall-ADDSDomainController</i>. Also, Recovery Manager for Active Directory Forest Edition disables Microsoft Windows Update if it is enabled on the domain controllers.
Reinstall Active Directory Domain Services	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: - Select preferred DNS server - Wait for a global catalog server to become available - Reinstall Active Directory Domain Services - Remove temporary files - Enable Windows Update (if it was enabled before the recovery)

- Remove temporary files

Uninstall Active Directory Domain Services

During this stage, Recovery Manager for Active Directory Forest Edition uninstalls Active Directory using the native tools provided by Microsoft. For domain controllers running Windows Server 2008 or earlier, Recovery Manager for Active Directory Forest Edition uses the **Dcpromo.exe** tool. For Windows Server 2012-based domain controllers, Recovery Manager for Active Directory Forest Edition uses the native Windows PowerShell cmdlet *Uninstall-ADDSDomainController*.

Also, Recovery Manager for Active Directory Forest Edition disables Microsoft Windows Update if it is enabled on the domain controllers.

Reinstall Active Directory Domain Services

During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps:

- Select preferred DNS server
- Wait for a global catalog server to become available
- Reinstall Active Directory Domain Services
- Remove temporary files
- Enable Windows Update (if it was enabled before the recovery)

In this section:

- [Creating an alert](#)
- [Viewing active alerts](#)
- [Modifying an alert](#)
- [Deleting an alert](#)

Creating an alert

To create an alert

- Create or open a recovery project.
- On the toolbar, click **Configure Alerts**.
- In the dialog box that opens, click **Create Alert**.
- Under **Alert properties**, do the following:
 - Use the **Alert name** box to type a descriptive name for the alert.
 - Use the **Alert me about completion of the specified stage** list to select a recovery stage.
 - Under the **Use this alert for domain controllers list**, click **Add**, and then select the check boxes next to the domain controllers to which you want to apply this alert. When you are finished, click **OK**.

By default, the created alert informs you when all specified domain controllers complete the selected recovery stage, regardless of whether or not the stage succeeded. To modify this behavior, complete the next steps.

- If you want to be informed when any of the domain controllers complete the recovery stage, select the **Alert me when any DC in the list completes specified stage** check box.
- If you only want to be informed about the successful completion of the stage, select the **Only alert me when specified stage is completed successfully**.

5. Click **OK** to apply your settings.

Viewing active alerts

After you start the recovery or verify settings operation on a recovery project, you can monitor active alerts in the project.

The number of currently active alerts is displayed next to the Active alerts link in the Project Summary area of the Forest Recovery Console. You can click the Active alerts link to display a list of active alerts and view the details for each active alert.

To view the details of an active alert

1. In the **Project Summary** area of the Forest Recovery Console, click the **Active alerts** link.
2. Use the **Active alerts** list to select the alert whose details you want to view.
3. Use the **Alert details** list to view the details of the selected alert.

Modifying an alert

For an existing alert, you can modify such settings as alert name, the recovery stage the alert informs you about, the list of domain controllers to which the alert applies, and the conditions when the alert becomes active.

To modify an alert

1. Open the recovery project that includes the alert you want to modify.
2. On the toolbar, click **Configure Alerts**.
3. In the dialog box that opens, use the **Alerts list** to select the alert you want to modify.
4. Under **Alert properties**, modify the alert settings as necessary.
5. When you are finished, click **OK** to apply your changes.

Deleting an alert

To delete an alert

1. Open the recovery project that includes the alert you want to delete.
2. On the toolbar, click **Configure Alerts**.
3. In the dialog box that opens, use the **Alerts list** to select the alert you want to delete.
4. Click the **Remove** button. If prompted, confirm the deletion of the alert.
5. When you are finished, click **OK** to apply your changes.

Using recovery pauses

A recovery pause allows you to suspend the recovery of one or more domain controllers right before they enter a certain recovery stage. You can then resume the recovery of the domain controllers from the point at which it was paused.

For example, recovery pauses let you temporarily suspend the recovery of particular domain controllers in order you could perform a manual action outside of Recovery Manager for Active Directory Forest Edition.

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

In your recovery project, you can use recovery pauses of the following types:

- **Manual pauses.** Allow you to pause the recovery of a domain controller at any recovery step you want. A manual recovery pause only applies to one domain controller. For more information, see [Managing manual pauses](#) on page 154.
- **Automatic pauses.** Allow you to pause the recovery of one or more domain controllers of your choice at the recovery stage you want. Once you configure and save an automatic pause, you can reuse or reconfigure it according to your needs. An automatic pause is only applicable to certain recovery stages. For more information, see [Managing automatic pauses](#) on page 154.

In this section:

- [Managing manual pauses](#)
- [Managing automatic pauses](#)
- [Monitoring active pauses](#)

Managing manual pauses

In a recovery project, you can use manual pauses to pause any recovery step of a domain controller.

In this section:

- [Creating a manual pause](#)
- [Releasing a manual pause](#)

Creating a manual pause

To create a manual pause

1. Open or create a recovery project.
2. In the list of domain controllers, right-click the domain controller whose recovery you want to pause, and then click **Pause next recovery step** on the shortcut menu.

The manual pause will activate before the next recovery step begins for the domain controller. The pause does not apply to the recovery step that is currently underway.

To view the current and the next recovery step for a domain controller, use the **Progress** tab in the **Domain Controller Recovery Settings and Progress** area.

Releasing a manual pause

To release a manual pause

1. In the list of domain controllers, right-click the domain controller on which you want to release an active manual pause.
2. On the shortcut menu, click **Resume next recovery step**.

This command is only applicable to the currently active manual pause. It is not applicable to any automatic pauses that may be active for the domain controller.

Monitoring active pauses

To monitor active pauses, you can use the List of Domain Controllers area. The domain controllers whose recovery is currently paused are labeled with the following icon:

Table 31: Active pause icon

Icon	Description
	Indicates that the recovery of the domain controller is paused. To view which recovery stage or step is now paused, click the domain controller in the list, and then open the Progress tab. The paused recovery stage or step is also labeled with the pause icon.

Managing automatic pauses

In a recovery project, you can create multiple automatic pauses, each having different settings. You can also modify the settings of existing automatic pauses or delete automatic pauses as necessary. To manage automatic pauses, click the **Configure Pauses** button on the Forest Recovery Console toolbar.

For each automatic 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 automatic pause on the domain controllers. The automatic pause becomes active when at least one domain controller specified in the pause settings reaches the recovery stage you specified.

You can configure an automatic pause to become active before one of the following recovery stages described in the next table.

Table 32: Recovery stages for which you can use automatic pauses

Recovery stage	Description
Prepare for restore from backup	During this stage, Recovery Manager for Active Directory Forest Edition verifies that the backup files you selected for recovery are available on the target domain controllers. If necessary, Recovery Manager for Active Directory Forest Edition copies the backup files that are missing.
Perform restore from backup	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: • Detect current mode (DSRM or normal) • Reset DSRM administrator password • Restart domain controller in DSRM • Enable domain controller isolation • Disable custom password filters

Recovery stage	Description
	• Disable BitLocker • Restore data from backup • Restart domain controller in normal mode
Configure domain controller	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: • Get information about domain controller • Select preferred DNS server • Remove global catalog (if you did not specify to keep the existing global catalog) • Raise RID pool • Invalidate RID pool • Seize FSMO roles • Clean up metadata of removed domain controllers • Reset the Krbtgt password • Reset computer account passwords • Enable custom password filters • Restart domain controller in normal mode • Reset trust passwords
Make domain controller available	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps: • Ensure that domain controller isolation is disabled • Clean up metadata of unrecovered domains if necessary • Change global catalog partition occupancy level • Add global catalog (if you did not specify to keep the existing global catalog) • Wait for a global catalog server to become available • Restore initial global catalog partition occupancy level • Enable the use of global catalog for user authentication • Enable BitLocker • Remove temporary files
Uninstall Active Directory Domain Services	During this stage, Recovery Manager for Active Directory Forest Edition uninstalls Active Directory using the native tools provided by Microsoft. For domain controllers running Windows Server 2008 or earlier, Recovery Manager for Active Directory Forest Edition uses the Dcpromo.exe tool. For Windows Server 2012-based domain controllers, Recovery Manager for Active Directory Forest Edition uses the native Windows PowerShell cmdlet <i>Uninstall-ADDSDomainController</i>.
Reinstall Active Directory	During this stage, Recovery Manager for Active Directory Forest Edition performs the following steps:

Recovery stage	Description
----------------	-------------

- | | |
|-----------------|--|
| Domain Services | <ul style="list-style-type: none">• Select preferred DNS server• Wait for a global catalog server to become available• Reinstall Active Directory Domain Services• Remove temporary files |
|-----------------|--|

In this section:

- [Creating an automatic pause](#)
- [Releasing an automatic pause](#)
- [Modifying an automatic pause](#)
- [Deleting an automatic pause](#)

Creating an automatic pause

To create an automatic pause

1. Create or open a recovery project.
2. On the toolbar, click **Configure Pauses**.
3. In the dialog box that opens, click **Create Pause**.
4. Under **Pause properties**, do the following:
 - a. Use the **Pause name** box to type a descriptive name for the automatic pause.
 - b. Use the **Activate pause before the specified stage** list to select a recovery stage.
 - c. Under the **Use this pause for domain controllers** list, click **Add**, and then select the check boxes next to the domain controllers to which you want to apply this pause. When you are finished, click **OK**.
5. Click **OK** to apply your settings.

Releasing an automatic pause

After you start the recovery of your project or run the verify settings operation on the project, you can monitor active pauses in the project and release active pauses as necessary. After you release an active automatic pause, all paused domain controllers to which the pause applies resume their recovery.

You can view the number of active pauses next to the **Active pauses** link in the **Project Summary** area of the Forest Recovery Console. You can click the **Active pauses** link to view the details of and selectively release active automatic pauses.

To release an active automatic pause

1. In the **Project Summary** area of the Forest Recovery Console, click the **Active pauses** link.
2. Use the **Active pauses** list to select the pause you want to release.

After you select a pause, you can view a list of domain controllers to which the pause applies and current pause status for each of these domain controllers.

3. Click the **Release** button to resume the recovery of the paused domain controllers to which the pause applies.

Modifying an automatic pause

For each automatic pause, you can modify such settings as the pause name, the recovery stage before which the pause activates, and the list of domain controllers to which the pause applies.

To modify an automatic pause

1. Open the recovery project that includes the automatic pause you want to modify.
2. On the toolbar, click **Configure Pauses**.
3. Use the **Pauses** list to select the automatic pause you want to modify.
4. Under **Pause properties**, modify the pause settings as necessary.
5. When you are finished, click **OK** to apply your changes.

Deleting an automatic pause

To delete an automatic pause

1. Open the recovery project that includes the automatic pause you want to delete.
2. On the toolbar, click **Configure Pauses**.
3. Use the **Pauses** list to select the automatic pause you want to delete.
4. Click the **Remove** button. If prompted, confirm the deletion of the pause.
5. When you are finished, click **OK** to apply your changes.

Copying a backup file to a new location

You can copy a backup file registered with Recovery Manager for Active Directory Forest Edition to a new location. This may be required to meet a specific corporate policy or to provide a faster access to the file. After you copy the file, you will need to update the recovery project settings to redirect Recovery Manager for Active Directory Forest Edition to the new location of the file.

To copy a backup to a new location

1. Copy the backup file to a new location.
2. Start the Forest Recovery Console.
3. Open the recovery project in which you want to use the backup file in its new location.
4. Use the List of Domain Controllers area to select the domain controller you plan to restore from the copied backup file.

5. Open the **Settings** tab, and then do the following:
 - a. Specify the **Restore from backup** method for the domain controller.
 - b. Clear the **Use backup criteria to automatically select a backup file** check box.
 - c. Click the **Select** button, and then use the provided list to select the backup file you copied. When finished, click **OK**.
 - d. In the **Backup file** text box, edit the backup file path to specify the new location of the file.
6. Click the **Verify Settings** button to verify the changes you have made.

Managing Forest Recovery Agent

Recovery Manager for Active Directory Forest Edition employs a Forest Recovery Agent to recover domain controllers. For this reason, it is recommended that you install Forest Recovery Agent on each domain controller you want to recover with Recovery Manager for Active Directory Forest Edition.

Recovery Manager for Active Directory Forest Edition uses the [Secure Remote Procedure Call \(RPC\) over Secure Sockets Layer \(SSL\)](#) communication logic to establish secure connection between Forest Recovery Console and the Forest Recovery Agent based on the Microsoft Secure Channel (SChannel). The process of agent installation starts with generating the Console and Agent certificates on the console side, then these certificates are deployed to the agent host. After the certificates are deployed, the both sides verify that each other has a valid certificate to provide the mutual authentication without using the domain access credentials.

If Forest Recovery Agent is not installed a domain controller in your recovery project, Recovery Manager for Active Directory Forest Edition attempts to automatically install the Forest Recovery Agent on that domain controller after you start the recovery operation on the project.

After you have upgraded the Forest Recovery Console to a new version, it is recommended that you manually upgrade the Forest Recovery Agent on each domain controller in your recovery projects to the version supplied with the new Forest Recovery Console. By doing so you ensure the Forest Recovery Console and the Forest Recovery Agent are fully compatible and can correctly communicate with each other after the upgrade.

In this section:

- [Installing or upgrading Forest Recovery Agent](#)
- [Viewing installed Forest Recovery Agent version](#)
- [Uninstalling Forest Recovery Agent](#)

Installing or upgrading Forest Recovery Agent

To deploy the Forest Recovery Agent, you can use the following methods:

Table 33: Methods to deploy Forest Recovery Agent

Automatic method	Manual method
Automatically deploys and upgrades (if required) the Forest Recovery Agent during backup of domain controllers. If this method is used, all necessary SSL certificates will be deployed as well.	Allows you to manually deploy the Forest Recovery Agent on multiple domain controllers from the Forest Recovery Console. You can use this method to upgrade the

Automatic method

To automatically install the agent

1. In the Recovery Manager Console tree, expand the **Computer Collections** node to select the Computer Collection in which you want to automatically install or update the Forest Recovery Agent.
2. On the **Action** menu, click **Properties**.
3. In the Computer Collection Properties dialog box, open the **Agent Settings** tab, and then select the **Ensure Forest Recovery agent is deployed** check box.
4. Click **OK**.

When backing up the Computer Collection, Recovery Manager for Active Directory Forest Edition will verify that an up-to-date version of the Forest Recovery Agent is installed on each domain controller in the Collection.

Note that clearing the **Ensure Forest Recovery Agent is deployed** check box does not uninstall the Forest Recovery Agent. For instructions on how to uninstall the agent, see [Uninstalling Forest Recovery Agent](#).

Manual method

Forest Recovery Agent on domain controllers after you have upgraded the Forest Recovery Console to a new version.

To manually install or upgrade the agent

1. Create or open a recovery project.
2. Use the List of Domain Controllers area to select the domain controllers on which you want to install or upgrade the agent. To select multiple domain controllers, hold down CTRL, and click the domain controllers you want to select.
3. On the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**.
4. In the dialog box that opens, click the **Install Agent** button to install or upgrade the Forest Recovery Agent on the domain controllers.

Viewing installed Forest Recovery Agent version

To view the installed Forest Recovery Agent version

1. Open the recovery project where you want to view the installed Forest Recovery Agent version.
2. Use the List of Domain Controllers area to select the domain controllers for which you want to view the installed Forest Recovery Agent version.

To select multiple domain controllers, hold down CTRL, and click the domain controllers you want to select.

3. On the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**.
4. In the dialog box that opens, use the **Agent Version** column to view the installed Forest Recovery Agent version.

It is recommended to ensure that the Forest Recovery Agent version is the same as that of the Forest Recovery Console you use.

Uninstalling Forest Recovery Agent

To uninstall the Forest Recovery Agent, you can use one the following methods:

- Uninstall the Forest Recovery Agent from the Forest Recovery Console.
- Access the target computer directly to uninstall the Forest Recovery Agent.

The latter method allows you to remove the Forest Recovery Agent from a domain controller that was demoted to member server and thus excluded from your recovery project.

To uninstall the agent from the Forest Recovery Console

1. Open the recovery project where you want to remove the Forest Recovery Agent.
2. Use the List of Domain Controllers area to select the domain controllers from which you want to remove the agent.

To select multiple domain controllers, hold down CTRL, and click the domain controllers you want to select.
3. On the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**.
4. In the dialog box that opens, click the **Uninstall Agent** button.

To uninstall the agent by accessing the computer directly

1. Log on to the computer from which you want to uninstall the Forest Recovery Agent.
2. Complete the steps related to your version of Windows Server:

Table 34: Uninstalling Forest Recovery Agent

Windows Server 2003	A later version of Windows Server
1. In Control Panel, click Add or Remove Programs. 2. In the list, select Quest Forest Recovery Agent, and then click Remove.	1. In Control Panel, click Uninstall a program. 2. In the list, select Quest Forest Recovery Agent, and then click Uninstall.

Rebooting domain controllers manually

You can use the Forest Recovery Console to selectively reboot domain controllers in the current recovery project. You can reboot domain controllers either in normal mode or Directory Services Restore Mode (DSRM).

To reboot domain controllers

1. In the List of Domain Controllers area, select the domain controllers you want to reboot.

To select multiple domain controllers, hold down CTRL, and click the domain controllers you want to select.
2. On the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**.
3. In the dialog box that opens, click the **Reboot** button, and then click one of the following:
 - **Reboot in Normal Mode**. Reboots the domain controllers in normal mode.

- **Reboot in DSRM.** Reboots the domain controllers in Directory Services Restore Mode.

Resetting DSRM Administrator Password

You can use the Forest Recovery Console to selectively reset the Directory Services Restore Mode (DSRM) administrator password on domain controllers in the current recovery project. You can reset the DSRM administrator password to the value specified in the domain controllers' recovery settings or specify a new DSRM administrator password.

To reset DSRM administrator password

1. Use the List of Domain Controllers area to select the domain controllers on which you want to reset the DSRM administrator password.

To select multiple domain controllers, hold down CTRL, and click the domain controllers you want to select.

2. On the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**.
3. In the dialog box that opens, click **More**, and then click **Reset DSRM Password**.
4. Use one of the following options:
 - **Reset password to the value in recovery settings.** Allows you to reset the DSRM administrator password to the value specified in the recovery settings for each domain controller. For more information about recovery settings, see [Domain controller recovery settings and progress](#).
 - **Reset password to this value.** Allows you to reset the DSRM administrator password to the value you type in this option.
5. When you are finished, click **Apply**.

Managing the Global Catalog servers

You can use Recovery Manager for Active Directory Forest Edition to manage the global catalog servers in your Active Directory forest before or after the recovery. For example, you can view which domain controllers currently hold the global catalog server role and manually remove or assign the global catalog server role to the domain controllers you want.

To manage the global catalog servers

1. In the Forest Recovery Console, open the recovery project in which you want to manage the global catalog servers.
2. On the menu bar, select **Tools | Manage | Global Catalog Servers**.

3. Do one of the following:
 - To assign the global catalog server role to a domain controller, select the check box in the **Global Catalog Server** column next to that domain controller.
 - To remove the global catalog server role from a domain controller, clear the check box in the **Global Catalog Server** column next to that domain controller.
 - To sort or group the domain controllers in the list by the criteria you want, right-click anywhere in the list, and then select an appropriate command from the shortcut menu.
4. When you are finished, click the **Apply** button for your changes to take effect.

i **TIP:** To avoid excessive replication traffic, it is recommended to assign one global catalog server role at a time.

Managing FSMO roles

You can use the Forest Recovery Console to view the current Flexible Single Master Operations (FSMO) role owners in your recovered Active Directory forest and manually change the FSMO role owners if necessary.

During the recovery, Recovery Manager for Active Directory Forest Edition uses an internal algorithm to automatically assign FSMO roles to the recovered domain controllers. After the recovery completes, you can view the current FSMO role owners and selectively reassign the FSMO roles if necessary.

To view and assign FSMO role owners

1. In the Forest Recovery Console, open the recovery project in which you want to view the current FSMO roles.
2. On the menu bar, select **Tools | Manage | FSMO Roles**.
3. Use the dialog box that opens to view the current FSMO role owners and reassign FSMO roles as necessary.

You can use the following elements:

Table 35: Elements you can use

Element	Description
Suggest Previous Owners	Allows you to automatically distribute FSMO roles to the domain controllers (owners) that held these roles before the recovery (that is, the owners stored in the recovery project). After you click this button, use the Assign Role To column to view or specify new role owners. If a FSMO role owner no longer exists, the most optimal existing owner will be selected for that role.
Suggest Optimal Owners	Click this button to automatically distribute FSMO roles to the most optimal existing owners in the recovered Active Directory forest.
Clear	Click this button to undo the changes you have made in the Assign Role To column. You can only use this button before you apply the changes you have made.
FSMO Roles	Lists all FSMO roles in the recovered Active Directory forest.
Current Owners	Lists the current owner of each FSMO role in the recovered Active Directory forest.

Element	Description
Assign Role To	Use this column to manually select a new owner for the corresponding FSMO role. You can also use this column to view the automatically selected new owners after you click the Suggest Prerecovery Owners or Suggest Optimal Owners button.

- When you are finished, click **Apply**.

Manage DNS Client Settings

You can use the Forest Recovery Console to view or change DNS client settings for each domain controller in your recovery project. In the DNS client settings, you can define the DNS servers used by the domain controller. You can manage DNS client settings before or after recovery of your project.

To view or change assigned DNS servers

- In the Forest Recovery Console, open the recovery project in which you want to view or change the assigned DNS servers.
- On the menu bar, select **Tools | Manage | DNS Client Settings**.
- In the dialog box that opens, use the following elements:

Table 36: Elements you can use

Element	Description
Suggest Previous Settings	Allows you to revert to the DNS client settings the domain controllers in your recovery project used before the recovery (that is, the settings stored in the recovery project).
Edit	Allows you to change the DNS client settings for the domain controller selected in the list.
Undo	Allows you to undo the changes you have made.
Apply	Applies the changes you have made.

Configuring Windows Firewall

A firewall enabled in your environment may block traffic on ports used by Recovery Manager for Active Directory Forest Edition, preventing you from backing up or restoring data. Before you start using Recovery Manager for Active Directory Forest Edition, make sure your firewall does not block traffic on ports used by Recovery Manager for Active Directory Forest Edition. For more information about these ports, see the Deployment Guide supplied with this release of Recovery Manager for Active Directory Forest Edition.

This section provides instructions on how to configure the built-in Windows Firewall enabled on Windows Server 2008- and Windows Server 2012-based domain controllers in a domain or forest you want to recover, so that Recovery Manager for Active Directory Forest Edition could recover that domain or forest. To ensure a successful recovery, create the following Windows Firewall security rules on all Windows Server 2008- and Windows Server 2012-based domain controllers in the domain or forest (leave the default values for settings not mentioned below):

Rule 1 (inbound)

- Rule type: Custom
- Program path: %SystemRoot%\System32\Svchost.exe
- Service settings: Windows Management Instrumentation (Winmgmt)
- Protocol: TCP
- Local ports: Any
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Rule 2 (inbound)

- Rule type: Custom
- Program path: System
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 445
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Rule 3 (inbound)

- Rule type: Custom
- Program path:
 - On a 32-bit system: <Product installation folder>\FRRestoreService.exe; on a 64-bit system: <Product installation folder>\FRRestoreService64.exe
 - The default product installation folder is %ProgramFiles%\Quest\ Recovery Manager for Active Directory Forest Edition.
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: RPC dynamic port range
- Remote ports: Any
- Local IP addresses: Any

- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any
- Allowed computers: Any

Rule 4 (inbound)

- Rule type: Custom
- Program path: %SystemRoot%\System32\Svchost.exe
- Service settings: Remote Procedure Call (RpcSs)
- Protocol: TCP
- Local ports: RPC dynamic port range
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, private, and public
- Allowed users: Any

For more information about RPC dynamic port range, refer to the following Microsoft Support Knowledge Base articles at <http://support.microsoft.com>:

- [How to configure RPC to use certain ports and how to help secure those ports by using IPsec](#) (article ID: 908472)
- [How to configure RPC dynamic port allocation to work with firewalls](#) (article ID: 154596)
- [The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008](#) (article ID: 929851)

Forest recovery overview

In general, a forest recovery is necessary if none of the domain controllers in the forest can function normally or if the corrupted domain controllers can spread dangerous data to other domain controllers. Some examples of forest-wide failures include:

- None of the domain controllers can replicate with its replication partner.
- Changes cannot be made to Active Directory at any domain controller.
- New domain controllers cannot be installed in any domain.
- All domain controllers have been logically corrupted or physically damaged to a point that business continuity is impossible (for instance, all business applications that depend on Active Directory are non-functional).
- A rogue administrator has compromised the Active Directory environment.

- An adversary intentionally or an administrator accidentally runs a script that spreads data corruption across the Active Directory forest.
- An adversary intentionally or an administrator accidentally extends the Active Directory schema with malicious or conflicting changes.

i **IMPORTANT:** When you encounter the symptoms of a forest-wide failure, work with Microsoft Customer Support Service to determine the cause of the failure and evaluate any possible remedies. Because of the complexity and critical nature of the forest recovery process, the recovery of the entire Active Directory forest should be viewed as a last resort. Please consult Microsoft Customer Support Service before you take a definitive decision.

Developing a custom forest recovery plan

When planning for Active Directory forest recovery, you should first have a detailed topology map of your forest. The map should list all the information about the domain controllers, such as their names, FSMO roles, backup status, and the trust relationships between them.

i **IMPORTANT:** To perform a forest recovery, an Administrator account password is required for each domain in the forest. It is a good practice to archive the Administrator account password history in a safe place.

Because of the complexity and critical nature of the forest recovery process, it is strongly recommended that Active Directory administrator observe the following rules to prevent the forest failure:

- Use only reliable and tested hardware, such as hard disks and uninterruptible power supply.
- Test any new configuration in a test lab before deploying it in your environment.
- Ensure that each domain in the forest has at least two domain controllers.
- Keep detailed logs about the health state of Active Directory on a daily basis, so that in case of a forest-wide failure the approximate time of failure can be identified.
- Regularly back up all domain controllers in the forest with Recovery Manager for Active Directory.
- Install Forest Recovery Agent on all domain controllers in the forest.
- Use the Forest Recovery Console to create a recovery project for your forest. Verify the settings of your forest recovery project on a regular basis, especially when there are membership changes to the Enterprise Admins or Domain Admins group. This helps ensure that the IT staff fully understands the forest recovery plan.

Recovery Manager for Active Directory Forest Edition allows you to restore a domain in the forest to its state at the time of the last trusted backup. Consequently, the restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted backup.
- All updates made to existing objects since the last trusted backup.
- All changes made to either the configuration partition or the schema partition in Active Directory (such as schema changes).
- Additionally, any software applications that were running on the domain controllers will need to be reinstalled on the domain controllers after the forest is recovered.

Backing up domain controllers

To restore domain controllers, you can use backups created with Recovery Manager for Active Directory or Recovery Manager for Active Directory Forest Edition. For this reason, you should back up domain controllers in the forest on a regular basis using one of these applications.

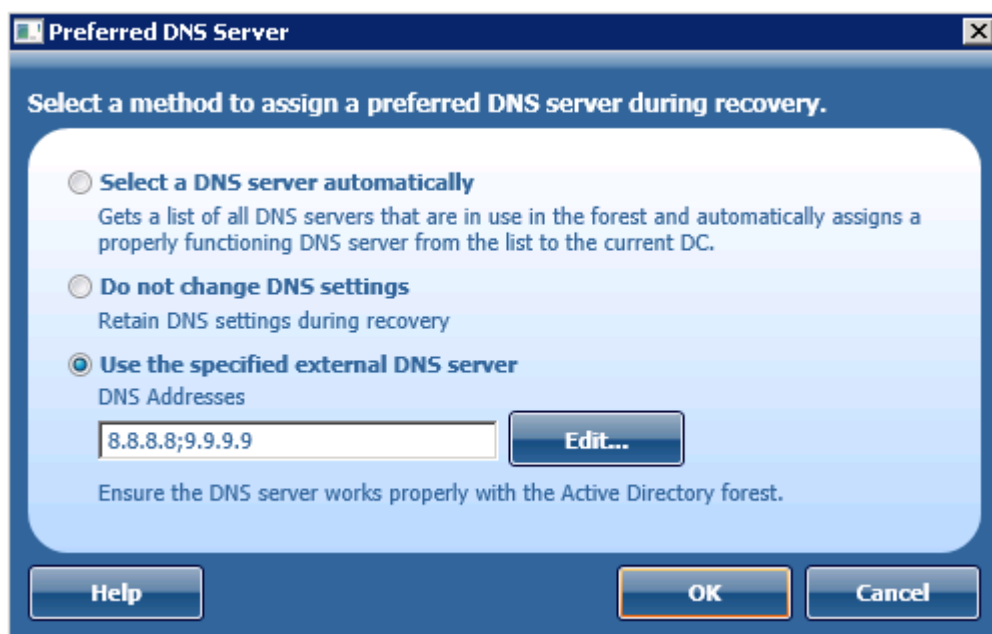
It is a good practice to create a Computer Collection that includes all domain controllers in the forest and back up the Collection each time you make changes to the forest infrastructure. Besides, you can use the Computer Collection to ensure that Forest Recovery Agent is installed on each domain controller in the Collection.

For more information about using the Forest Recovery Agent and Computer Collections, see the User Guide supplied with this release of Recovery Manager for Active Directory Forest Edition.

Assigning a preferred DNS server during recovery

Before starting a forest recovery operation, you should specify a method for selecting a preferred DNS server for each domain controller in your recovery project. You can choose one of the following DNS server selection methods:

- **Select a DNS server automatically**
Let Recovery Manager for Active Directory Forest Edition automatically select a DNS server (used by default).
- **Do not change DNS settings**
Recovery Manager for Active Directory Forest Edition retains DNS client settings during the recovery operation.
- **Use the specified external DNS server**
Specify an external DNS server manually - here you can specify one DNS address or a list of DNS servers separated by semicolons or using the **Edit** button.



For more information on how to specify a DNS server selection method, see [Domain controller recovery settings and progress](#).

When you choose to select a DNS server automatically, Recovery Manager for Active Directory Forest Edition contacts the domain controllers in the forest to get a list of all DNS servers they use. Then, Recovery Manager for Active Directory Forest Edition automatically selects a properly working DNS server from the received list and assigns that DNS server to the domain controller.

The automatic DNS selection method is recommended in the following cases:

- Your DNS is not Active Directory-integrated.
- Your DNS is Active Directory-integrated and you restore from backups the DNS servers (domain controllers) that act as primary source for each DNS zone.

i | IMPORTANT: It is not recommended to uninstall or reinstall Active Directory on the DNS servers that act as a primary source for an Active Directory-integrated DNS zone. Also, it is not recommended to remove such DNS servers from Active Directory during recovery .

The **Do not change DNS settings** option lets you retain DNS settings during recovery so you do not need to reconfigure DNS settings for each domain controller within the forest after the recovery operation is completed.

When you specify a DNS server or list of DNS servers manually, Recovery Manager for Active Directory Forest Edition first tries to assign the specified DNS server(s) to the domain controller. If the specified DNS server does not function properly or is inaccessible, Recovery Manager for Active Directory Forest Edition automatically selects a properly functioning DNS server from a list of all DNS servers that are in use in the forest.

If you want to use the manual DNS server selection method, it is recommended to make sure you have one or more external DNS servers properly configured for working with the domain controllers being recovered. All these external DNS servers must support dynamic updates and have DNS zones configured for each domain in the forest you want to recover. Make sure you specify one of these DNS servers for each domain controller in your recovery project.

Forest recovery methods

Before you choose one of the recovery methods described in this section, it is strongly recommended that you read Microsoft's best-practice paper, [Planning for Active Directory Forest Recovery](#).

This section covers the following:

- [Recovery method 1: Restore as many domain controllers from backups as possible](#)
- [Recovery method 2: Restore one domain controller from backup in each domain](#)

Recovery method 1: Restore as many domain controllers from backups as possible

To use this method, you must have recent and trusted backups for as many domain controllers 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 for Active Directory Forest Edition restores as many domain controllers as possible in each domain from the recent and trusted backups you specify. The more domain controllers you restore from backups, the faster the forest recovery operation completes.

2. Recovery Manager for Active Directory Forest Edition uses Microsoft's native tools (**Dcpromo.exe** or the *Uninstall-ADDSDomainController* and *Install-ADDSDomainController* cmdlets) to automatically reinstall Active Directory on the domain controllers for which no backups are available.
3. The domain controllers where Active Directory was reinstalled replicate AD data from the domain controllers restored from reliable backups.

Method 1 has the following advantages and limitations:

Table 37: Recovery method 1: Advantages and limitations

Advantages	Limitations
• Fast recovery of the entire forest. Since most domain controllers are simultaneously restored from backups, the forest recovery operation completes faster than in Method 2. • 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 domain controllers fails. • This method allows you to retain the original forest infrastructure. Since many domain controllers are restored from backups, the recovered forest is close to its original prefailure condition.	• The risk of reintroducing corrupted or unwanted data is higher than in Method 2. Because of the large number of backups used in this method, there is no guarantee that corrupted or unwanted data from the backups will not be reintroduced into the recovered forest.

For a step-by-step procedure on how to perform a forest recovery, [Overview of steps to recover a forest](#)

Recovery method 2: Restore one domain controller from backup in each domain

This recovery method is recommended by Microsoft in the Planning for Active Directory Forest Recovery paper. To use this method, you must have a recent and trusted backup for one domain controller 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, recovering a forest using this method includes the following stages:

1. Recovery Manager for Active Directory Forest Edition restores one domain controller in each domain from the recent and trusted backup you specify.
2. Recovery Manager for Active Directory Forest Edition uses Microsoft's native tools (**Dcpromo.exe** or the *Uninstall-ADDSDomainController* and *Install-ADDSDomainController* cmdlets) to automatically reinstall Active Directory on the domain controllers for which no backups are available.
3. The domain controllers on which Active Directory was reinstalled replicate Active Directory data from the domain controllers restored from reliable backups.

Method 2 has the following advantages and limitations:

Table 38: Recovery method 2: Advantages and limitations

Advantages	Limitations
• Recommended by Microsoft. This recovery method is recommended in the Microsoft's bestpractice paper, Planning for Active Directory Forest Recovery. • Safer, healthier recovery 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 they do not include any corrupted or unwanted data.	• Forest recovery may require 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 domain controller. A successful restore of one domain controller from backup is required before Active Directory can be reinstalled on all other domain controllers in the domain. • The original forest infrastructure is not retained. Because Active Directory is reinstalled on most domain controllers in the forest, the forest infrastructure cannot be restored to its exact pre-failure state.

For a step-by-step procedure on how to perform a forest recovery, [Overview of steps to recover a forest](#)

Deciding which backups to use

To restore domain controllers from backups, use the backups that were taken a few days before the occurrence of the failure. In general, you have 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 re-introducing dangerous data into the restored forest.

It is strongly recommended that you keep detailed logs about the health state of Active Directory on a daily basis, so that in case of a forest-wide failure you could identify an approximate time of the failure.

For more information on the methods you can use to select backups for recovery, see [Selecting backups for recovery](#).

Running custom scripts while recovering a forest

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

Recovery Manager for Active Directory Forest Edition is supplied with a Microsoft Windows Script (.wsf) file serving as a template where you can insert your custom scripts written in the VBScript or JScript language. The file name is ConsoleSideScripting.wsf, and you can find it in the Recovery Manager for Active Directory Forest Edition installation folder (by default, this is %ProgramFiles%\Quest\Recovery Manager for Active Directory Forest Edition).

The .wsf file has a number of XML elements where you can insert your scripts. Each XML element in the .wsf file provides a description explaining when the script inserted that element will run. Depending on where you inserted your script, it will run:

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

To configure Recovery Manager for Active Directory Forest Edition to automatically run your scripts

1. Locate the file ConsoleSideScripting.wsf in the Recovery Manager for Active Directory Forest Edition installation folder, and open the file in a text editor.
2. In the file, read the descriptions provided for the XML elements to identify the ones where you want to insert your script, then insert your script as appropriate.

Overview of steps to recover a forest

To recover your Active Directory forest

1. Open the recovery project you created for your environment.
For more information, see [Opening a recovery project](#).
2. Use the Active Directory logs to determine the forest failure date.
3. Select appropriate backups for the domain controllers in your project. Make sure you use backups that were created before the point in time when the forest failure occurred.
For more information on how to select backups for the recovery, see [Selecting backups for recovery](#).
4. Verify the settings specified in your recovery project.
For more information, see [Specifying recovery project settings](#).
5. Verify the recovery settings specified for each domain controller in your recovery project:
 - a. Use the list of domain controllers in the Forest Recovery Console to select the domain controller whose settings you want to verify.
 - b. Open the **Settings** tab, and then verify the specified recovery settings. If necessary, adjust the settings as needed.
 - c. Repeat these steps for each domain controller in the project.
 For more information about forest recovery methods, see [Forest recovery methods](#).
6. On the toolbar, click **Start Recovery** to start the recovery operation on your project.

i **IMPORTANT:** Before starting a forest recovery, the settings verification must be successfully passed. For more information, see [Verifying recovery project settings](#).

Viewing forest recovery progress

While performing a forest recovery operation, you can use the Forest Recovery Console to monitor the recovery progress of each domain controller in the project.

To view the recovery progress for a domain controller

1. In the Forest Recovery Console, use the list of domain controllers to select the domain controller whose recovery progress you want to view.
2. Open the **Progress** tab to view the recovery operation progress.

Viewing recovery plan

Before you start recovering your Active Directory forest, you can generate and view a recovery plan for the recovery project. The recovery plan reflects the settings specified in your recovery project. For example, you can generate and view the recovery plan after making some changes to the recovery project settings to identify whether these changes will have the effect you want.

Recovery project plan shows the details of each Active Directory domain and site included in your recovery project, such as the total number of domain controllers, the number of domain controllers to be recovered, and the number of domain controllers to be removed from Active Directory during the recovery.

For each domain controller, the recovery plan shows the following:

- Currently selected recovery method.
- DNS servers used by the domain controller before the recovery.
- Current FSMO roles.
- Whether or not the domain controller to be recovered is a global catalog server.
- Applicable recovery alerts and pauses.

To view recovery plan

1. Start the Forest Recovery Console.
2. On the menu bar, click **View | Recovery Plan**.

To view detailed information about a particular recovery method (that is, the recovery stages and steps the related domain controllers will go through), click the name of that method.

You can use the toolbar in the report window to print or export the recovery plan to a preferred format.

Viewing a report about forest recovery or verify settings operation

Upon the completion of a forest recovery or verify settings operation, you can view a report on that operation.

To view a report

- On the menu bar, click **View | Report**.

You can use the toolbar in the report window to print or export the report to a preferred format.

Handling failed domain controllers

It is recommended that you investigate the failure reason for each domain controller whose recovery has failed. For example, make sure the failed domain controller is connected to the network and the recovery settings specified for that domain controller are correct.

In some cases, the Forest Recovery Console may prompt you to perform a certain action to resolve the issue encountered during the domain controllers recovery. If you are not prompted for action, you can perform the next steps.

To select an action for a failed domain controller

1. In the List of Domain Controllers area, right-click the failed domain controller.
2. Select one of the following actions from the shortcut menu:

Table 39: Actions applicable to failed domain controllers

Action	Description
Retry All Operations	Allows you to rerun all recovery steps on the domain controller you selected. This action is recommended when you change the recovery method for the failed domain
Retry Last Operation	Allows you to rerun the failed recovery step on the domain controller you selected. This action is recommended when you manually fixed the issue that had caused the recovery step to fail.
Skip and Continue	Allows you to skip the current failed recovery step for the domain controller you selected and continue the domain controller's recovery. This action is recommended only if you have manually completed the failed recovery step on the domain controller.

Adding a domain controller to a running recovery operation

There may be a situation where you want to add a domain controller that is not being recovered to the running forest recovery operation. You can do so without stopping the forest recovery operation.

To add a domain controller to a running recovery operation

1. In the list of domain controllers, select the domain controller you want to add to the currently running recovery operation.
2. Use the **Settings** tab to specify recovery settings for the domain controller.
3. Right-click the domain controller, and then click **Retry All Operations**.

Selectively recovering domains in a forest

You can use Recovery Manager for Active Directory Forest Edition to selectively recover domains in an Active Directory forest. You can use this method if you have identified the domains that include dangerous or

unwanted data and want to selectively recover them. Before you proceed with such a selective recovery, make absolutely sure no dangerous or unwanted data is replicated to the domains you do not plan to recover.

i IMPORTANT:

- You cannot selectively recover domains and delete domains at the same time. During recovery, use only one of these two features. For more information about deleting domains, see [Deleting domains during recovery](#)
- The **Adjust to Active Directory changes** recovery method is performed automatically on Global Catalogs of excluded domains. In case of full reset of Global Catalog, the replication of Global Catalog data may require additional time. For more details, see the description of the **Adjust to Active directory Changes** recovery method [here](#).

Step 1: Select domains to recover

In this step, select the domains you want to recover in your recovery project. This step presumes that you have already created a recovery project for your forest. For more information on how to create a recovery project, see [Creating a recovery project](#).

To select domains

1. Open the recovery project where you want to select domains to recover.
2. On the menu bar, click **Tools | Recovery Project Settings**.
3. Open the **Recovery Mode** tab.
4. In the **Recovery scope** drop-down list, select **Domain Recovery**.
5. Select the check boxes next to the domains you want to recover.
6. Optionally, you can specify default credentials to access domain controllers in the selected domains.
7. Click **OK**.

The recovery of the domains you selected may affect computers in other domains. These computers will be displayed in your recovery project.

Step 2: Specify recovery settings for domain controllers

To specify recovery settings for DCs

1. In the list of domain controllers, select the domain controller whose recovery settings you want to specify.
2. Open the **Settings** tab to specify the recovery settings.
3. Repeat these steps for other domain controllers in the project.

For more information, see [Domain controller recovery settings and progress](#).

Step 3: Start recovery

To start the recovery

- On the toolbar, click **Start Recovery**.

Recovering SYSVOL

Recovery Manager for Active Directory Forest Edition supports authoritative restore of SYSVOL on the selected domain controllers. Authoritative SYSVOL restores are used in case of critical situations such as divergence of data in the content of the SYSVOL share.



NOTE:

- If you have very large backups and the backup data is stored on a remote computer (not on domain controllers), you do not need to specify the backups for non-authoritative domain controllers in Forest Recovery Console to restore the SYSVOL data. When the backup is not selected, the SYSVOL data is replicated from the authoritative domain controller by the replication service. In this case, the full backup information is not copied to the domain controller that saves the disk space.
- Along with the SYSVOL restore, Recovery for Active Directory Forest Edition allows you to perform the [non-authoritative restore of RODCs](#) using the **Restore SYSVOL** recovery method.

To restore the SYSVOL folder from backup, perform the following steps

1. Open your recovery project where the authoritative restore of SYSVOL will be performed.
2. On the menu bar, click **Tools | Recovery Project Settings**.
3. Open the **Recovery Mode** tab.
4. In the **Recovery scope** drop-down list, select **SYSVOL Recovery**. If the **SYSVOL Recovery** scope is selected, the **Restore SYSVOL** method is set on the **Settings** tab in the [domain controller recovery settings](#) and cannot be changed.
5. Select the check boxes next to the domains you want to recover and specify a domain controller for each domain to perform the authoritative restore. If the domain controller is not specified, it will be selected automatically. For more information, see [How does Recovery Manager for Active Directory Forest Edition select a DC for an authoritative \(primary\) restore of SYSVOL during forest recovery](#).
6. Optionally, you can specify default credentials to access domain controllers in the selected domains.
7. Click **OK**.

Deleting domains during recovery

When recovering an Active Directory forest, you can use Recovery Manager for Active Directory Forest Edition to selectively delete particular domains from the forest being recovered. You may need to delete domains when, for example, the account you use to recover an Active Directory forest does not have sufficient permissions to access and recover some domains in the forest. In this case, you may want to sacrifice these domains and recover the forest without them.

i | **IMPORTANT:**

- You cannot selectively recover domains and delete domains at the same time. During recovery, use only one of these two features. For more information about selectively recovering domains, see [Selectively recovering domains in a forest](#).
- You cannot delete the root domain of the forest being recovered.

To delete a domain from the forest being recovered, you need to set the recovery method for all DCs in that domain to **Do not recover**. Then, after you run the recovery operation, Recovery Manager for Active Directory Forest Edition does the following:

- Deletes the domain's partition.
- Cleans up metadata of all DCs in the domain from the forest.

To delete a domain while recovering an Active Directory forest

1. In the Forest Recovery Console, open or create a recovery project.
2. Set the recovery method for all DCs in the domain you want to delete to **Do not recover**:
 - a. Select a DC in the list.
 - b. On the **Settings** tab, from the **Recovery method** list, select **Do not recover**.
3. Specify other settings for your recovery project as appropriate, and then click **Start Recovery** on the toolbar.

Resuming an interrupted forest recovery

Recovery Manager for Active Directory Forest Edition provides the Fault Tolerance feature that allows you to resume the last forest recovery operation in case it was unexpectedly interrupted by one of these events:

- You close the Forest Recovery Console while the forest recovery operation is still running.
- The Forest Recovery Console unexpectedly shuts down partway through the forest recovery operation.
- The computer running the Forest Recovery Console powers off while the forest recovery operation is still running.

i | **IMPORTANT:** The Fault Tolerance feature does not allow you to resume a forest recovery operation you canceled from the Forest Recovery Console (for example, by clicking the **Abort** button).

When the Fault Tolerance feature is enabled, it constantly saves the current forest recovery operation state to a dedicated SQL Server database named **ForestRecovery-Persistence**. Each time you start the Forest Recovery Console, a check is performed to see whether the last forest recovery operation was interrupted by any of the events listed earlier in this section. If that is true, the Forest Recovery Console prompts you to resume the forest recovery from the point at which it was interrupted.

In case you choose not to resume an interrupted forest recovery operation and select the **Delete last recovery session data** option in the Resume Recovery wizard, the saved session state will be permanently deleted from the **ForestRecovery-Persistence** database.

Permissions required to access the ForestRecovery-Persistence database

- Add an account that is used to access the **ForestRecovery-Persistence** database as the Security Login in SQL Server Management Studio. The **public** role will be automatically granted to the user account on the **Server Roles** tab of **Login Properties**.
- Add users mapped to this Login and assign the **db_datareader** role on the **User Mapping** page of the **Login Properties** to use the account as the Forest Recovery project reader.
- Explicitly grant the **Execute** right on the **Permissions** tab of the **ForestRecovery-Persistence** database **Properties**. This permits to use the account for the **Restore** operation.

For the Fault Tolerance feature, all involved console instances must have the same SSL certificate that is used to communicate with Forest Recovery Agents without using the domain access credentials.

To share the SSL certificate between console instances

1. Open or create a recovery project in Forest Recovery Console.
2. On the menu bar, select **Tools | Fault Tolerance**.
3. Click **Export certificates...** and specify the certificate file location and access credentials.
4. Save the certificate file.
5. Then, launch another instance of Forest Recovery Console.

i **IMPORTANT:** Before you import the certificate file, you must uninstall Forest Recovery Agents on all domain controllers that were processed via this console, if any. For that, on the menu bar, select **Tools | Manage | Forest Recovery Agent or DCs**. In the dialog box that opens, select all domain controller and click the **Uninstall Agent** button.

6. On the menu bar, select **Tools | Fault Tolerance | Import certificates...**, specify the certificate file and click **Open**.
7. Reinstall the agents if they were uninstalled.
8. For security reasons, remove the certificate file from your computer after the Fault Tolerance feature will be configured.

To modify the fault tolerance settings for a recovery project

1. In Forest Recovery Console, select **Tools | Fault Tolerance | Settings** from the toolbar.
2. In the **Fault Tolerance Settings** dialog, use the following options:

Table 40: Recovery persistence settings

Option	Description
Enable fault tolerance	Allows you to enable or disable the Fault Tolerance feature by selecting or clearing this check box.
SQL Server name and instance	Allows you to specify the SQL Server instance in which you want to store the current forest recovery operation state. To specify a SQL Server instance, use the format <code><SQLServerName>/<Instance></code> . The forest recovery operation state is saved to a SQL Server database named ForestRecovery-Persistence. If the ForestRecovery-Persistence database does not exist in the SQL Server instance you specify, it will be created there. If the ForestRecovery-Persistence database already exists in the SQL Server instance you specify, the data in that database will not be erased until you start a new forest recovery

Option	Description
	operation. Until that moment, you can resume the interrupted forest recovery operation whose state is held in the specified ForestRecovery-Persistence database.
Authentication method	Allows you to select a method for authenticating on the specified SQL Server. • Use Windows authentication. Allows you to authenticate with the user account under which the Forest Recovery Console is currently running. • Use SQL authentication. Allows you to authenticate with the user name and password specified in this option. This authentication method is recommended when Recovery Manager for Active Directory Forest Edition uses the ForestRecovery-Persistence database that is hosted on an external SQL Server computer and not on the Recovery
List of consoles	Shows the list of Forest Recovery Consoles configured to support the Fault Tolerance feature.

Recovering read-only domain controllers (RODCs)

Recovery Manager for Active Directory Forest Edition does not support recovering read-only domain controllers (RODCs) from backups.

The full list of recovery methods that can be applied to the RODCs in your recovery project:

- Restore SYSVOL
This method allows you to perform the non-authoritative restore of RODCs
- Reinstall Active Directory on the RODCs
- Uninstall Active Directory from the RODCs.
- Do not recover the RODCs.

For more information on selecting a recovery method for a domain controller in the current recovery project, see [Domain controller recovery settings and progress](#)

Checking forest health

The Forest Recovery Console provides a tool that allows you to check the health of your forest. You can use the tool to run tests to ensure that domain controllers, Active Directory replication, domain trusts, user authentication, RID Master, and global catalog are working properly in your Active Directory forest.

The Forest Recovery Console automatically prompts you to check the forest health after the forest recovery has succeeded, so that you could ensure the forest works exactly the way you want. If necessary, you can manually run a health check on your forest at any time before or after the forest recovery operation.

What does Recovery Manager for Active Directory Forest Edition check?

Items to check	Description
----------------	-------------

Domain controllers	• Verifies that every domain controller in a forest is accessible and running using the LDAP bind request to the directory root (RootDSE) of a domain controller. • Checks that Forest Recovery Agents are installed on domain controllers and accessible using the RPC call to get information about agents and domain controller states.
Active Directory replication	• Forces the replication for one random object on every replication partner for every partition of a domain controller using the replicateSingleObject operation.
Domain trusts	• Checks that all trust relationships between domains configured in Active Directory forest are fully established.
User authentication; RID Master and GC operation	• Verifies that a user account is created in the default or specified container on each domain controller. Then, LDAP authentication is performed using this account to check that the Global Catalog server is available for the domain controller.

To run a forest health check

1. Open your recovery project.
2. In the Forest Recovery Console, from the main menu, select **Tools | Diagnose | Check Forest Health**.
3. In the dialog box that opens, on the **Settings** tab, select the check boxes next to the items whose health you want to check.
4. When finished, click the **Check Health** button.

When the check health operation completes, use the **Details** tab to view information about the health of the selected items.

If you select the **User authentication; RID Master and GC operation** option on the **Settings** tab, you can specify a container for the test user account on the domain controller.

For the list of required permissions, see <http://documents.quest.com/recovery-manager-for-ad-forest-edition/8.8/deployment-guide/permissions-required-to-use-forest-recovery-console>.

To specify a container for the test user account

1. Close the Forest Recovery console.
2. Open the project (.frproj) file that was created by the Console and edit the '<Domains>' section, as shown in the following example.
You can specify different containers for different domains.

```
<Domains>
<Domain DomainName="rmad.local" HealthCheckContainer="OU=test1" />
<Domain DomainName="second.rmad.local" HealthCheckContainer="OU=test2" />
</Domains>
```

To specify the same container for different domains, you can use the asterisk wildcard (*), for example:

```
<Domains>
```

```
<Domain DomainName="" HealthCheckContainer="OU=test1" />
</Domains>
```

You should specify the relative container distinguished name for the **HealthCheckContainer** attribute. For example, if the full DN of the container is *OU=test1,DC=rmad,DC=local*, specify the DN name as *OU=test1*.

Collecting diagnostic data for technical support

There may be a situation where technical support requests you to gather and supply diagnostic data from your computer collection. For this purpose, you can use a special tool provided in the Forest Recovery Console. This tool is called Diagnostic Data Collector.

i **NOTE:** From version 8.7, the diagnostic data can be collected for the Recovery Manager Console as well. For more details, refer the *Collecting diagnostic data for technical support* section in [Recovery Manager for Active Directory User Guide](#).

When gathering diagnostic data, the Diagnostic Data Collector collects the following:

- **From Forest Recovery Console machine**
 - Collects the data saved in the current Recovery Project (.frproj) file, except for the passwords stored in that file.
 - Collects the Forest Recovery Console log
 - Collects the Recovery Manager for Active Directory Forest Edition event logs
 - .mdb database files
 - Recovery Manager for Active Directory Forest Edition configuration files
- **From Domain Controller**
 - Collects Backup and Restore agent logs
 - Collects system event logs
 - Windows debug logs
 - Runs Microsoft Netdiag, Dcdiag, Nltest, Msiinfo32 and Repadmin tools (in diagnostic mode only), and then collects the output provided by these tools. The tools are started by **Collectdcddata.cmd** and you can modify the list of collected logs.

To gather diagnostic data for your recovery project by using the Diagnostic Data Collector, you need to complete the following steps:

- **Step 1: Use Diagnostic Data Collector to automatically gather data.** In this step, you use the Diagnostic Data Collector to automatically gather diagnostic data from each domain controller in your recovery project and save the data to the folder you specify. You can perform this step regardless of whether or not a recovery operation is currently running on the recovery project. If this step completes successfully for all domain controllers, Step 2 is not needed.

- [Step 2: Gather remaining data manually](#). You need to perform this step only for those domain controllers from which you could not successfully collect data in Step 1. In Step 2, you copy several files supplied with Recovery Manager for Active Directory to the target domain controller, and then run one of the copied files. As a result, diagnostic data is collected from the domain controller and saved to a new folder created in the location from which you ran the file.

The next sections provide instructions on how to complete each of these steps.

Step 1: Use Diagnostic Data Collector to automatically gather data

To automatically gather diagnostic data

1. In the Forest Recovery Console, open the recovery project for which you want to collect diagnostic data.
2. Make sure you specify credentials to access each domain controller in the project. To check whether you specified access credentials for a particular domain controller, do the following:
 - a. Select that domain controller in the list of domain controllers.
 - b. Open the **Settings** tab.
 - c. Make sure you specify the correct credentials in the **Domain Controller Access** option.

The Forest Recovery Console will use the specified credentials to access the domain controller and gather diagnostic data from it.

3. From the menu bar, select **Tools | Diagnose | Collect Diagnostic Data**.
4. Use the **Drop folder** text box to specify the local or UNC path to the folder where you want to save the diagnostic data to be collected. The collected data is saved to a .zip, e.g. **CollectedLogs_10_20_2015 07_23_25.zip**
5. You can change credentials to access the domain controllers that were specified on the step 2.
6. Select the **Delete collected logs from domain controllers** option to delete collected RMAD\RMADFE logs from domain controllers.
7. Click the **Collect** button and wait for the operation to complete.

If you successfully collected data from all the domain controllers in this step, you can submit the .zip file to Quest technical support. Otherwise, complete [Step 2: Gather remaining data manually](#).

Step 2: Gather remaining data manually

Perform the next steps for each domain controller from which you could not successfully collect data in [Step 1: Use Diagnostic Data Collector to automatically gather data](#).

To gather diagnostic data manually

1. Create a temporary folder on the local disk of the target domain controller.
2. Copy **Collectdcdata.cmd** from the Recovery Manager for Active Directory Forest Edition installation folder to the folder you created in step 1 of this procedure.
3. Run the **Collectdcdata.cmd** file in the location to which you copied it and wait for the script to complete.

The collected diagnostic data is saved to the CollectedData folder created in the location where you ran the **Collectdcdata.cmd** file.

4. Rename the CollectedData folder so that its name reflects the name of the domain controller from which you collected data.
5. Add the folder to the .zip file created in [Step 1: Use Diagnostic Data Collector to automatically gather data](#).

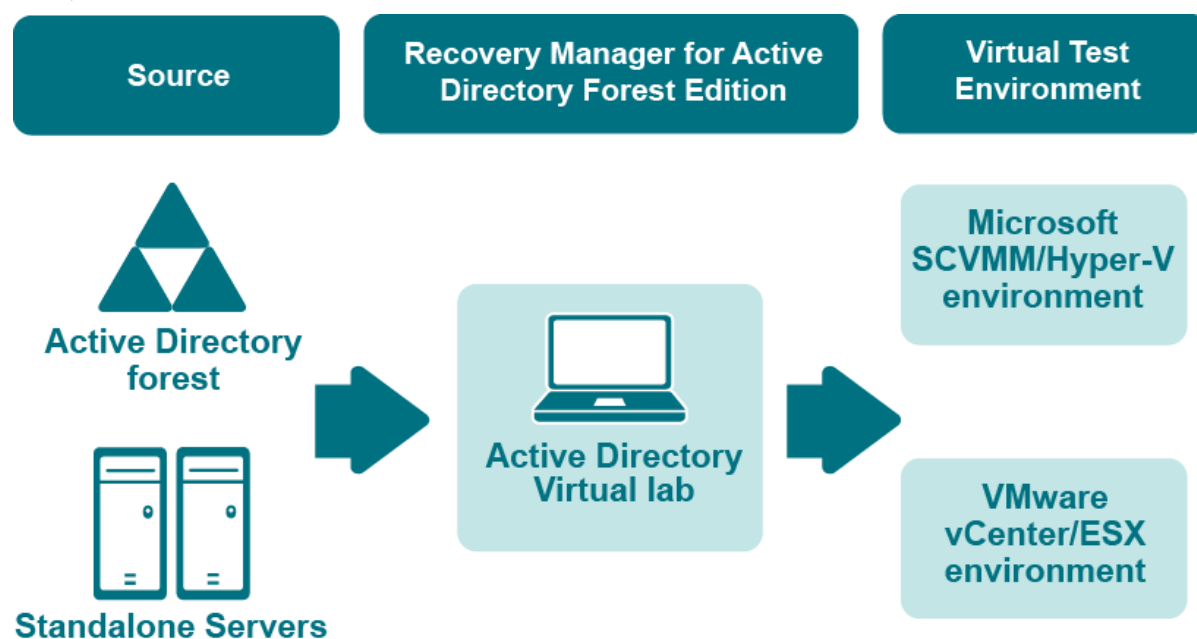
Now you can submit the .zip file to Quest technical support.

Creating virtual test environments

- [About Active Directory Virtual Lab](#)
- [Permissions](#)
- [Communication ports](#)
- [Deployment](#)
- [User interface](#)
- [How to create a virtual test environment](#)

About Active Directory Virtual Lab

The Active Directory Virtual Lab is a component of Recovery Manager for Active Directory Forest Edition that helps you create virtual test environments from an Active Directory forest. You can use the created test environments to design and evaluate Active Directory disaster recovery scenarios, test planned Active Directory changes before deploying them to production, train your staff to perform Active Directory-related tasks, and more.



When creating virtual machines from the source computers, the Active Directory Virtual Lab uses third-party virtualization software, such as Microsoft System Center Virtual Machine Manager (SCVMM), VMware ESX, or VMware vCenter. For a full list of supported virtualization software, see the *System Requirements* section in the *Recovery Manager for Active Directory Forest Edition Release Notes*.

You can create virtual machines that maintain all the data available on the source computers, including Active Directory, installed programs, and files. To manage the created virtual test environment, you need to use the native tools provided by the virtualization software with which the Active Directory Virtual Lab created the virtual machines in the test environment.

To create a virtual test environment from an Active Directory forest, you first need to select the source computers (domain controllers or standalone servers) you want to include in the test environment, configure settings to create a virtual machine from each source computer, and then have the Active Directory Virtual Lab create the test environment for you.

For instructions on creating a virtual test environment, see [How to create a virtual test environment](#).

Permissions

This section lists the permissions required to create a virtual test environment by using the Active Directory Virtual Lab.

Table 41: Required permissions

Task	Minimum permissions
Install and use Active Directory Virtual Lab.	Be a member of the local Administrators group.
Create a virtual machine from a source computer. NOTE: This includes access to the source computer, Forest Recovery Agent installation, and virtualization agent installation.	
Create a virtual test environment using Microsoft SCVMM.	Have the Delegated Administrator role on the Microsoft SCVMM server. Be a member of the local Administrators group on the target Hyper-V host.
Create a virtual test environment using VMware vCenter/ESX.	VMware vCenter/ESX server: - Datastore - Allocate Space - Browse Datastore - Network - Assign Network - Resource - Assign Virtual Machine To Resource Pool - Profile-driven storage - Profile-driven storage view NOTE: This permission must be assigned to the vCenter Server root level. - Virtual Machine - Configuration - Guest Operations

Task	Minimum permissions
	- Interaction - Configure CD Media - Device Connection - Power Off - Power On - VMware Tools Install - Inventory - Provisioning - Allow Disk Access - Allow Read-Only Disk Access - Customize - Modify Customization Specifications - Read Customization Specifications To install Converter Standalone agent, use built-in Administrator account to connect to the source machine or disable User Access Control (UAC) on the source machine.

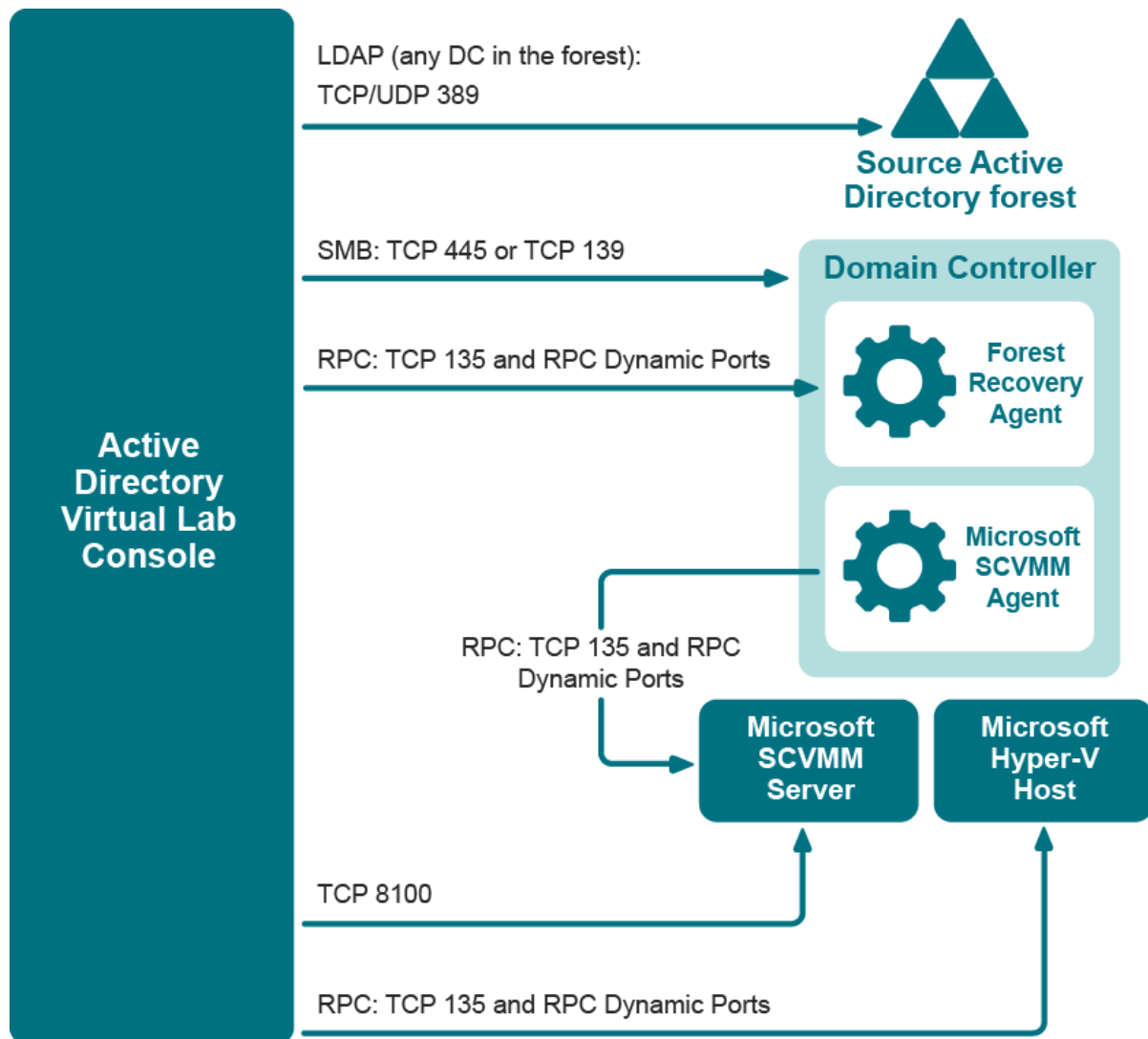
Communication ports

This section provides information about the communication ports required to create a virtual test environment with the Active Directory Virtual Lab.

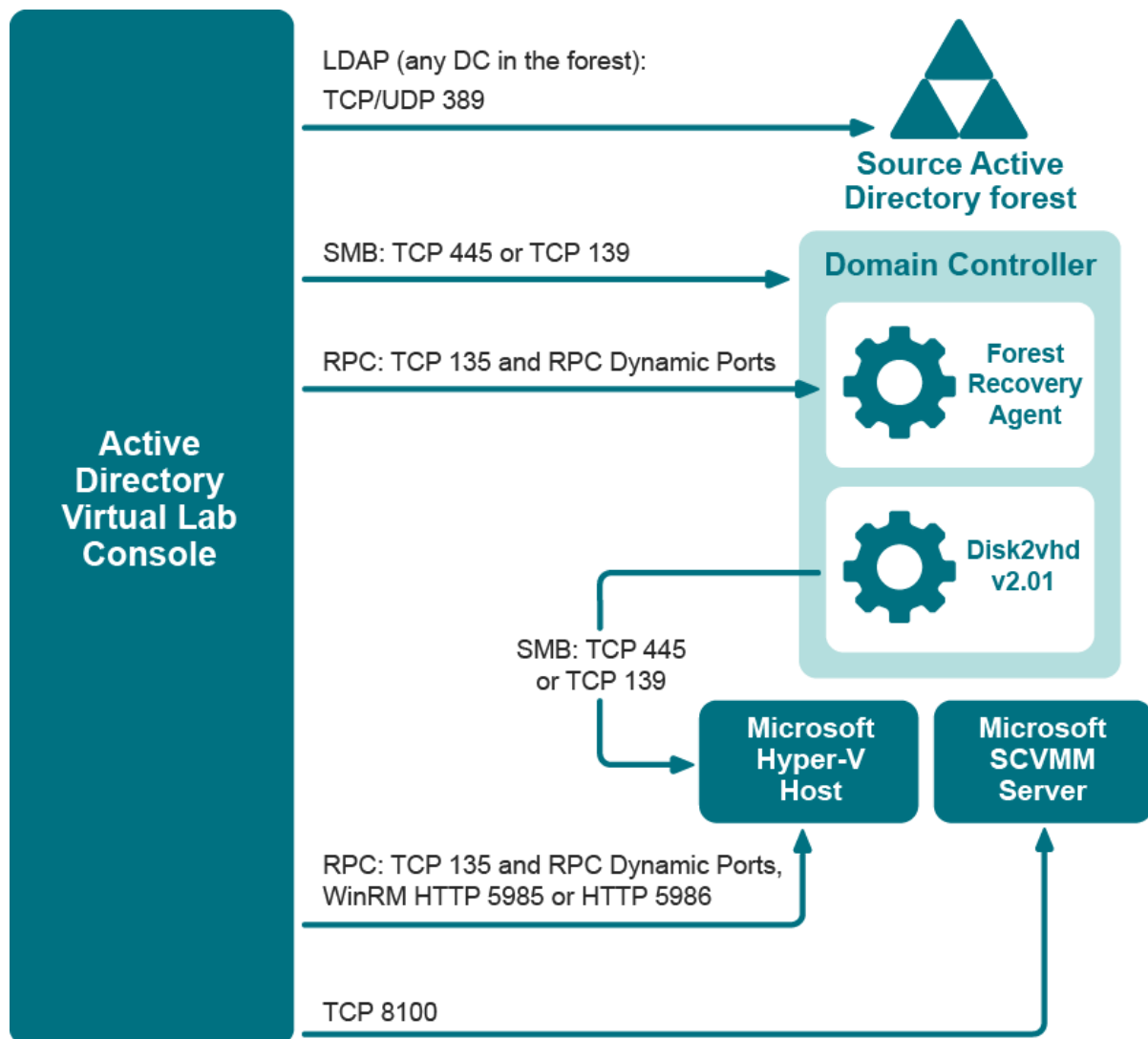
In this section:

- [Microsoft SCVMM Environment](#)
- [Microsoft SCVMM 2012 R2 Environment](#)
- [VMware Environment](#)

Microsoft SCVMM 2012 or 2012 SP1 Environment



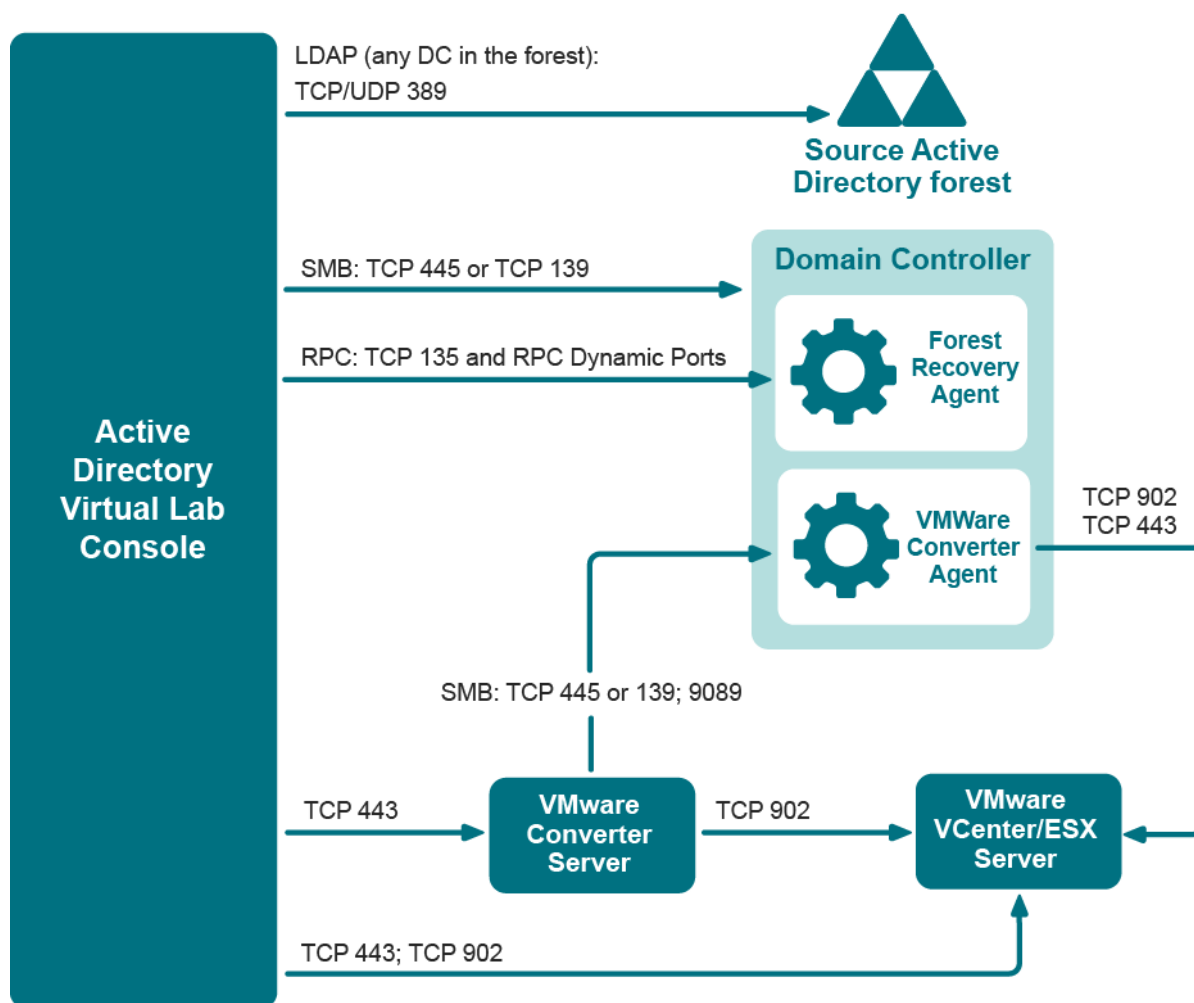
Microsoft SCVMM 2012 R2 or 2016 Environment



VMware Environment

i NOTE:

- To successfully setup the VMware vCenter Converter Agent you should provide network connections via DNS between all members of the conversion process: domain controller, VMware Converter Server, Recovery Manager Console and VMware vCenter/ESX Server.
- To install Converter Agent, use built-in Administrator account to connect to the source machine or disable User Access Control (UAC) on the source machine.



Deployment

By default, the Active Directory Virtual Lab is automatically installed when you install Recovery Manager for Active Directory Forest Edition. If necessary, you can exclude the Active Directory Virtual Lab from installation or uninstall it.

IMPORTANT: To create virtual test environments, the Active Directory Virtual Lab requires third-party virtualization software. Make sure you have supported virtualization software installed and accessible to the Active Directory Virtual Lab. For a list of supported virtualization software, see the System Requirements section in the *Recovery Manager for Active Directory Forest Edition Release Notes*.

To exclude Active Directory Virtual Lab from installation

- Start the Recovery Manager for Active Directory Forest Edition Setup Wizard and use the **Custom** option to select the features you want to install.

To uninstall Active Directory Virtual Lab

1. Open the list of installed programs (**appwiz.cpl**).
2. In the list, select the **Recovery Manager for Active Directory Forest Edition** entry, and then click the **Change** button.
3. Follow the steps in the Setup Wizard to change the installation so as to uninstall the Active Directory Virtual Lab feature.

User interface

The graphical user interface where you can manage the creation of a virtual test environment is called the Active Directory Virtual Lab console.

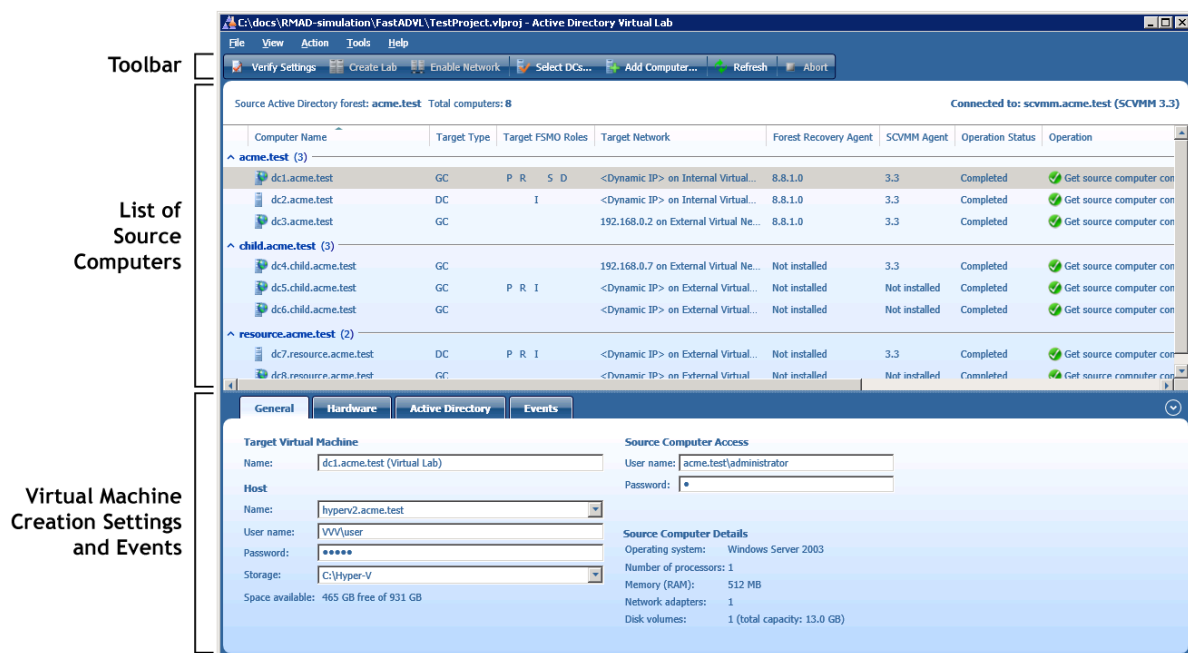
To start the Active Directory Virtual Lab console

- Use the steps provided for your version of Windows:

Table 42: Starting the Active Directory Virtual Lab console

Windows Vista Windows 7 Windows Server 2008 or 2008 R2	A later version of Windows
1. Click Start. 2. Point to All Programs Quest Recovery Manager for Active Directory Forest Edition. 3. Click Active Directory Virtual Lab.	On the Apps screen (Windows logo key + Q), locate and click the Active Directory Virtual Lab tile.

The Active Directory Virtual Lab console has the following areas:



In this section:

- [Toolbar](#)
- [List of source computers](#)
- [Virtual machine creation settings and events](#)
- [Virtual lab project default settings](#)

Toolbar

This area provides the following buttons:

- **Verify Settings.** Starts the verification of the virtual machine creation settings specified for each source production computer. If any issues are found, you are prompted to resolve them.
- **Create Lab.** Starts the virtual test environment creation using the specified settings. This button only becomes available after you have successfully verified the virtual machine creation settings.
- **Enable Network.** Use this option to manually enable network adapters in the created test environment.
- **Select DCs.** Opens a dialog box you can use to select source domain controllers for which to create virtual machines in your virtual test environment. The source domain controllers you have already selected are displayed in the **List of Source Computers**.
- **Add Computer.** Opens a dialog box you can use to specify a source standalone server from which to create a virtual machine in your virtual test environment. The source standalone servers you have already specified are displayed in the **List of Source Computers**.

For example, you can use the **Add computer** button to add DNS servers not integrated into Active Directory, Exchange Servers, or the current computer on which you are using Recovery Manager for Active Directory Forest Edition.

- **Refresh.** Refreshes the information displayed in the Active Directory Virtual Lab console.

List of source computers

Lists the source computers for which the Active Directory Virtual Lab creates virtual machines in your virtual test environment using the settings configured on the **General**, **Hardware**, and **Active Directory** tabs.

Virtual machine creation settings and events

Provides tabs on which you can configure settings to create a virtual machine from the selected source computer. You can also view events generated by the Active Directory Virtual Lab during the virtual machine creation.

This area provides the following tabs:

- [General tab](#)
- [Hardware tab](#)
- [Active Directory tab](#)
- [Events tab](#)

General tab

Provides the following elements:

- **Target Virtual Machine**
 - **Name.** Use the Name text box to type a name for the virtual machine to be created from the source computer.
- **Infrastructure** Specify the virtual host and location on the host where you want to place the virtual machine.
 - **Storage Policy.** For VMware vCenter 6.5 and later, ADVL allows a user to select a storage policy which will be applied to the target virtual machine. The selected policy will be applied to the virtual machine files in the VM Home directory and all virtual disks. When the selected storage policy has encryption as part of its configuration, the target virtual machine will be encrypted.
 - **Host name.** Specify the host where you want to place the virtual machine.
(VMware only) When you have a cluster in the VMware vCenter configuration, the cluster name will be shown in the list instead of cluster hosts when the Distributed Resource Scheduler (DRS) feature is enabled and DRS automation level is Partially or Fully Automated.
If DRS cluster is selected, you should specify the shared storage for the managed hosts in the **Storage** option.
 - **User name and Password .** (SCVMM only) Type access credentials for connecting to the selected virtual host. The account whose credentials you specify must have sufficient permissions on the target host. For more information, see [Permissions](#).
 - **VM folder.** (VMware only). Select the folder in which you want to place the target virtual machine.
 - **Storage.** Select a storage in which to place the virtual machine files. You should specify the shared storage if you use VMware DRS cluster. Otherwise, the DRS feature will not work.
- **Source Computer Access.** Use the User name and Password text boxes to type access credentials for connecting to the source computer. The account you specify must have sufficient permissions on the source computer. For more information, see [Permissions](#).

- **Source Computer Details.** View detailed information about the source computer selected in the **List of Source Computers**.

Hardware tab

Provides the following elements:

General

- **Number of processors.** Specify the number of processors you want to have on the target virtual machine.
- **Memory (RAM).** Set the amount of random access memory you want to allocate to the target virtual machine.

Network adapters. Select the number of network adapters you want to have on the target virtual machine. When you are done, in the list below this option, configure TCP/IP settings for each adapter (to get started, in the **IP Address** column, click <Dynamic IP>).

Disk Volumes. Select the disk volumes you want to virtualize and add to the target virtual machine. For VMware vCenter 5.0 and later, you can specify the provisioning type for the target virtual disks. By default, "Thin Provision" is used. To specify Thick Provision Lazy Zeroed for the disk, select the check box in the **Thick Provision** column in the **Disk Volumes** section. For more details about the type of disk provisioning, refer [here](#).

Active Directory tab

If the source computer is a domain controller, this area provides the following elements:

- **FSMO Roles.** Allows you to configure FSMO roles for the virtual machine to be created. To add new FSMO roles, select the check boxes next to those roles.
- **Global Catalog.** Select the check box in this option if you want the virtual machine to act as a Global Catalog server in the virtual test environment.

Events tab

View the events generated by the Active Directory Virtual Lab for the source computer selected in the **List of Source Computers**.

Virtual lab project default settings

Each virtual lab project has a number of default settings. Initially, you configure these settings in the wizard that helps you create new virtual lab project. For each virtual lab project, you can view or modify these default project settings.

To view or modify the default project settings

1. In the Active Directory Virtual Lab console, open the virtual lab project whose settings you want to modify.
2. From the main menu, select **Tools | Project Settings**.

In the dialog box that opens, use the following tabs:

- **Source Forest.** View or change access credentials for connecting to the source Active Directory forest from which to create your virtual test environment.
- **Virtualization.** View or change access credentials for connecting to the third-party virtualization software with which to create virtual machines in your virtual test environment.
- **Host.** View or change the virtual host and storage where to place the target virtual machines. You can also view the amount of space available in the currently selected storage.
- **Hardware.** View or change the default parameters for creating target virtual machines, such as the number of processors, amount of RAM, number of network adapters, and network settings.

Default parameters set on the **Host** and **Hardware** tabs are used to populate options in the [Virtual machine creation settings and events area](#) for each new source computer you add to the virtual lab project.

How to create a virtual test environment

This section lists considerations, precautions, and provides step-by-step instructions for creating a new virtual test environment.

In this section:

- [Considerations](#)
- [Precautions](#)
- [Step-by-step instructions](#)

Considerations

This section describes the various aspects you should consider before creating a new virtual test environment or opening an existing virtual lab project.

In this section:

- [Isolated virtual network and DNS](#)
- [Virtualization agent behavior](#)
- [Working with SCVMM 2012 R2 or higher](#)
- [Forest Recovery Agent is required](#)
- [Opening a legacy virtual lab project](#)

Isolated virtual network and DNS

This section provides some considerations and recommendations for using an isolated virtual network for your virtual test environment.

- **Add a DNS server to your virtual test environment.** Ensure your virtual test environment has a properly configured DNS server. Add a source DNS server computer to your virtual lab project at Step 2: Add source computers to virtual lab project, so that the Active Directory Virtual Lab creates a virtual

machine for the DNS server in your test environment.

- **Initially, use one DNS server per domain that hosts its DNS zone.** We recommend that in [Step 3: Modify virtual machine creation settings](#) you specify the same DNS server for all target virtual machines in that domain. This does not mean that you should not add multiple DNS servers to your virtual test environment. You can add them, but initially configure the target virtual machines to use only one of the added DNS servers. After you start your virtual test environment and Active Directory replication completes then you can reconfigure the target virtual machines to use other DNS servers you have added.
- **AD and DNS may be interdependent at startup.** In case with Active Directory-integrated DNS, you should consider the fact that Active Directory and DNS are interdependent at startup. That is, when you start virtual machines in the virtual test environment, Active Directory waits for DNS to become available. In turn, DNS cannot start without Active Directory. However, there's a timeout programmed in Active Directory, and after some time of waiting Active Directory starts without DNS, and this will make DNS work too.
- **Invalid resource records in DNS.** If DNS in the virtual test environment is the exact copy of the source DNS and you excluded some source computers from the virtual test environment, there may be left some invalid resource records in DNS referring to those excluded computers. To eliminate the invalid resource records from DNS, recreate the primary forward lookup zones in your virtual test environment. As for invalid resource records in the reverse lookup zones, you can recreate or delete these zones because they are not vital for Active Directory.

Virtualization agent behavior

To create virtual machines, the virtualization software supported by the Active Directory Virtual Lab needs to install its virtualization agent on the source computers.

i | **NOTE:** If you work with Microsoft SCVMM 2012 R2, use the Disk2vhd utility instead of virtualization agent. For more details, see [Working with SCVMM 2012 R2](#).

If you use Microsoft SCVMM, it automatically removes its virtualization agent from the source computers after the virtualization completes. However, in case with VMware vCenter or ESX, the virtualization agent remains on the source computers after the virtualization. You can uninstall the agent manually by using a shortcut menu command on the source computers in the Active Directory Virtual Lab console.

Working with SCVMM 2012 R2 or higher

To create virtual test environment using Microsoft SCVMM 2012 R2 or higher, you need to install the Disk2vhd utility on the source computers instead of virtualization agent using Active Directory Virtual Lab console. This tool creates Virtual Hard Disk (VHD) versions of physical disks.

To configure ADVL to work with SCVMM 2012 R2 or higher

1. Download Disk2vhd v2.01 [here](#).
2. Unpack **Disk2vhd.zip** and save **disk2vhd.exe** to the folder of your choice on the computer where the Active Directory Virtual Lab console is installed.
3. Run the utility and accept the License Agreement.
4. In the Active Directory Virtual Lab console, select **Tools | Configure** and specify the path to the Disk2vhd utility.

i | **NOTE:** Do not remove the Disk2vhd utility. Otherwise, the ADVL console cannot deploy the utility on the source machine.

Forest Recovery Agent is required

Forest Recovery Agent must be installed on the source computers. This is the same Forest Recovery Agent that is used by Recovery Manager for Active Directory Forest Edition to recover domain controllers. Forest Recovery Agent also plays a vital part in the virtual test environment creation. For example, it is used to clean up metadata, seize FSMO roles, and validate that guest OS tools are installed on the virtual machines created in the lab.

For this reason, before creating a virtual test environment, you need to ensure that each source computer has the current Forest Recovery Agent version installed. To do so, you can use the Active Directory Virtual Lab console.

When you click the **Verify Settings** button in *Step 4: Verify virtual machine creation settings* in [Step-by-step instructions](#), the Active Directory Virtual Lab checks and displays the Forest Recovery Agent version installed on the source computers in your project. If the current version of the agent is not installed, the Active Directory Virtual Lab displays a warning. If you ignore this warning, the current agent version will be automatically installed on the source computers during the virtual test environment creation.

Alternatively, you can use the Active Directory Virtual Lab console to manually install or update the Forest Recovery Agent: just select the appropriate shortcut menu command on the source computers in the virtual lab project.

Opening a legacy virtual lab project

This section describes how to open a legacy Virtual Lab Project (.vlproj) file created with the Active Directory Virtual Lab 8.5 if FIPS-compliant algorithms are enabled on the Active Directory Virtual Lab 8.6 or later computer.

The Active Directory Virtual Lab 8.5 uses hashing and encryption algorithms incompatible with FIPS. For this reason, to open a legacy .vlproj file created with the Active Directory Virtual Lab 8.5, you need to temporarily disable FIPS-compliant algorithms on the Active Directory Virtual Lab 8.6 or later computer.

To open a legacy project

1. On the Active Directory Virtual Lab 8.6 or later computer, disable FIPS-compliant algorithms:
 - a. Start the Group Policy Object Editor tool (gpedit.msc).
 - b. In the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then select **Security Options**.
 - c. In the right pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
 - d. In the dialog box that opens, select **Disabled** and click **OK**.
2. Restart the computer.
3. Start the Active Directory Virtual Lab 8.6 or later console, open the legacy .vlproj file, and then save it. By doing so, you update the project to use FIPS-compliant algorithms.
4. Enable FIPS-compliant algorithms on the Active Directory Virtual Lab 8.6 or later computer.

i **NOTE:** To protect its data, the Active Directory Virtual Lab 8.6 or later uses the SHA-1 hashing algorithm and the Triple DES encryption algorithm that are FIPS-compliant. For more information about FIPS-compliant algorithms, see Microsoft Knowledge Base article 811833 "[The effects of enabling the 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' security setting in Windows XP and in later versions of Windows](http://support.microsoft.com)" at <http://support.microsoft.com>.

Precautions

Please consider the following precautions before creating a virtual test environment:

- Virtual test environments created by the Active Directory Virtual Lab can only be used for testing, training, or evaluation purposes. Never restore or copy any data from your virtual test environments to the production Active Directory.
- Ensure your virtual test environment is properly isolated from the source Active Directory forest. Otherwise, the source forest may be seriously damaged after you enable the network adapters in the newly-created virtual test environment.

Step-by-step instructions

To create a virtual test environment from an Active Directory forest, complete these steps:

- [Step 1: Create a virtual lab project](#)
- [Step 2: Add source computers to virtual lab project](#)
- [Step 3: Modify virtual machine creation settings](#)
- [Step 4: Verify virtual machine creation settings](#)
- [Step 5: Start virtual test environment creation](#)
- [Step 6: Enable network adapters](#)

Step 1: Create a virtual lab project

To create a virtual lab project

- Start the Active Directory Virtual Lab console.

After the console opens, a wizard starts automatically to guide you through the virtual lab project creation.

Alternatively, if you have the Active Directory Virtual Lab console already open, from the main menu, select **File | New Project**, and then follow the steps in the wizard.

When creating a virtual lab project, you are prompted to specify the following:

- Third-party virtualization software with which to create virtual machines from the source computers.

The virtualization software must be preinstalled in your environment and be accessible to the Active Directory Virtual Lab. For the privileges required to use the virtualization software, see [Permissions](#).

- Source Active Directory forest from which to create your virtual test environment.
- Default hardware settings for creating virtual machines from source computers in the virtual lab project.

If necessary, later you can modify these default settings for each virtual machine to be created.

- A Virtual Lab Project (*.vlproj) file to save your project. You can reuse the settings stored in the .vlproj file to create more virtual test environments in the future.

Step 2: Add source computers to virtual lab project

Once you have created a virtual lab project, you need to populate it with the source computers from which to create virtual machines in your virtual test environment. The source computers can be physical or virtual domain controllers or standalone servers. The source computers added to your virtual lab project are displayed in the [List of source computers](#) area.

To add domain controllers to your project

1. In the Active Directory Virtual Lab console, click the **Select DC** button.

In the dialog box that opens, wait until the Active Directory Virtual Lab retrieves information about all domain controllers in the source Active Directory forest.

2. Select the check boxes next to the domain controllers for which you want to create virtual machines.

If you do not want specific domains in your virtual test environment, leave the check boxes cleared for all domain controllers in those domains. As a result, the Active Directory Virtual lab excludes these domains from the virtual test environment by cleaning up their metadata.

3. When you are finished, click **OK**.

i **NOTE:** We recommend that you select one target domain controller in each domain that hosts AD integrated DNS zone as a primary DNS server and set its target IP address as a DNS server for all other target virtual machines in this domain. The corresponding source domain controller should be the DNS server as well. When all target virtual machines have been created, they have a network interface card (NIC) configured according to the ADVL project settings. During the Enable Network operation, the Primary DNS servers are restarted and IP addresses are updated for all other virtual machines in this domain. After the updated DNS data will be replicated to domain controllers in other domains, other DNS servers in these domains should work as well.

To add a standalone server to your project

1. In the Active Directory Virtual Lab console, click the **Add computer** button.

2. In the dialog box that opens, use the following elements:

- **Computer name.** Type the fully qualified domain name (FQDN), NetBIOS name, or IP address of the source standalone server you want to add.
- **User name.** Type the user name of the account with which you want to access the source standalone server.
- **Password.** Type the password that matches the user name you have specified in the **User name** text box.

For information on the permissions the account you specify must have on the source computer, see [Permissions](#).

3. Click **OK** to add the standalone server to the virtual lab project.

To remove a source computer from your project

- In the **List of Source Computers** area, right-click the computer you want to remove from your project, and then click **Remove** on the shortcut menu.

Step 3: Modify virtual machine creation settings

By default, the virtual machine creation settings for each source computer in your virtual lab project are populated with the default values you have configured when creating the project (see [Virtual lab project default settings](#)).

If necessary, you can modify the virtual machine creation settings for each source computer in the project.

To modify the virtual machine creation settings

1. In the **List of Source Computers**, click to select the source computer.
2. Use the following tabs to modify the virtual machine creation settings as necessary:
 - **General** tab
 - **Hardware** tab
 - **Active Directory** tab

For more information about the options you can use on these tabs, see [Virtual machine creation settings and events](#).

To configure a setting for multiple source computers at once, select those computers in the **List of Source Computers** (hold down CTRL and click the computers in the list), and then configure the setting you want on the above-listed tabs.

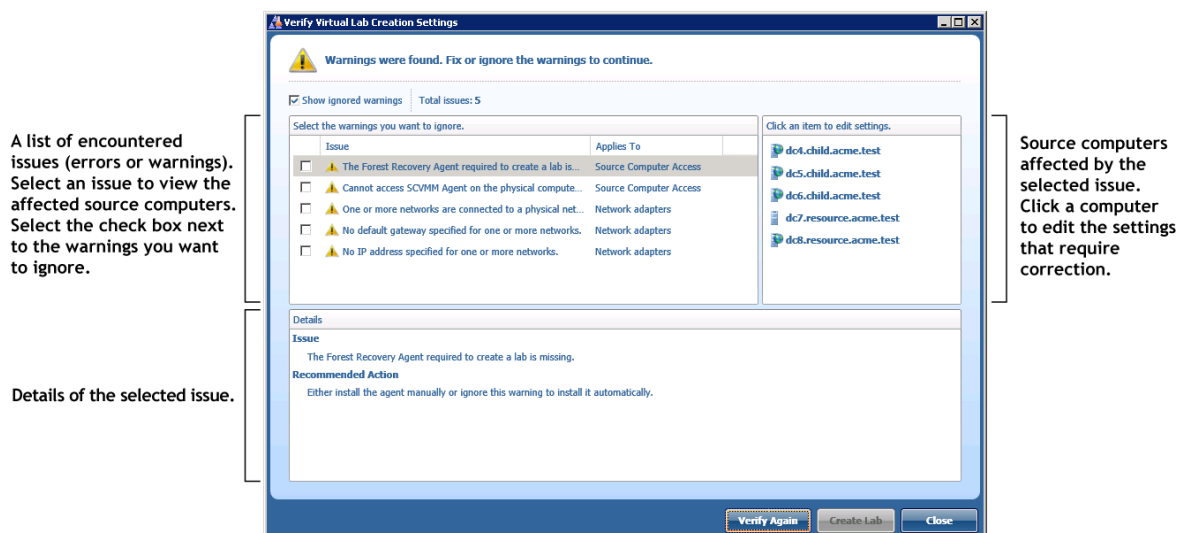
Step 4: Verify virtual machine creation settings

In this step, you verify the virtual machine creation settings specified for each source computer to ensure they are correct. If any issues are found, you are prompted to fix them. You cannot proceed with the virtual test environment creation until you resolve all errors encountered during the verification. Also, you must resolve or ignore the encountered warnings, if any.

To verify the settings in your project

- In the Active Directory Virtual Lab console, click the **Verify Settings** button and wait for the verification to complete.

Once the verification completes, you can view its results in a dialog box that opens automatically. If any issues are found during the verification, this dialog box looks similar to the following:



After resolving or ignoring the issues found, click the **Verify Again** button in this dialog box to re-run the verification operation on the virtual lab project. If the issues have been resolved successfully, the **Create Lab** button becomes available and you can proceed with the virtual lab creation.

Step 5: Start virtual test environment creation

To start the virtual environment creation

- In the Verify Virtual Lab Creation Settings dialog box, click the **Create Lab** button.

Alternatively, you can click the **Create Lab** button on the Toolbar in the Active Directory Virtual Lab console.

To view the virtual machine creation progress for a source computer, select that computer in the List of source computers, and then click the **Events** tab.

NOTE: If the creation of a virtual machine fails, we recommend that you retry the last operation on the source computer: In the **List of Source Computers**, right-click the source computer, and then click **Retry Last Operation**.

In the created virtual test environment, all network adapters are disabled to prevent possible conflicts with the source Active Directory forest. Before enabling network adapters, ensure your virtual test environment is properly isolated from the source forest.

Persistence of the ADVL console

This feature is supported only for Microsoft SCVMM 2012 R2 and VMware environments.

If you close the ADVL console during the creation of the virtual environment, the session can be resumed if it was interrupted on the following steps (see the **Events** tab):

- Convert source machine to virtual machine
- Wait for other virtual machines to be created

To resume the creation of the virtual environment, reopen the ADVL project.

Step 6: Enable network adapters

After the virtual test environment has been successfully created, the Active Directory Virtual Console automatically displays a dialog box that prompts you to enable network adapters in the created test environment. In that dialog box, click **Enable** if you want to enable the network adapters now or click **Cancel** if you want to enable them manually later.

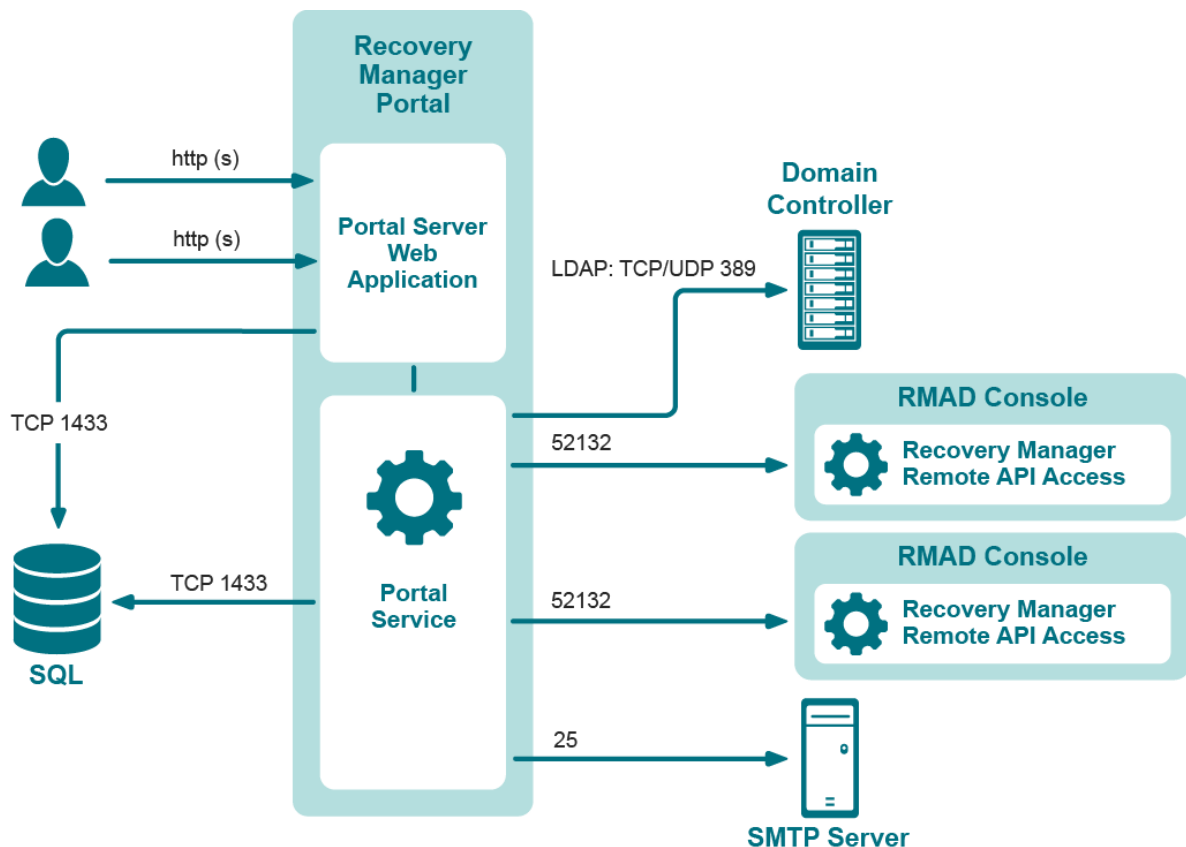
Using Recovery Manager for Active Directory Web Interface

- [About Recovery Manager Portal](#)
- [Installing Recovery Manager Portal](#)
- [Connecting to Recovery Manager Portal](#)
- [Administering Recovery Manager Portal](#)
- [Viewing health summary for Recovery Manager for Active Directory instances](#)
- [Viewing backup creation history](#)
- [Recovering data using Recovery Manager Portal](#)

About Recovery Manager Portal

The Recovery Manager Portal implements a Web interface that allows you to do the following:

- Access the search and restore functionality of Recovery Manager for Active Directory via a Web browser.
- Delegate permissions to restore or undelete Active Directory objects to specific users or groups in your Active Directory forest.
- Monitor the health of Recovery Manager for Active Directory instances deployed in your environment.
- View a history of backups created by a specific Recovery Manager for Active Directory instance.



The Recovery Manager Portal enables intranet users to use a Web browser to access the search and restore functionality provided by Recovery Manager for Active Directory. Through the Recovery Manager Portal, the users can search for and restore objects from the unpacked Active Directory backups created with Recovery Manager for Active Directory. You can configure the Recovery Manager Portal to work with multiple instances of Recovery Manager for Active Directory.

To access a Recovery Manager for Active Directory instance, the Recovery Manager Portal requires a service called the Recovery Manager Remote API Access. This service is supplied with Recovery Manager for Active Directory and must be installed and running on each computer hosting the Recovery Manager for Active Directory instances whose Active Directory backups you want to make available to the Recovery Manager Portal users.

Installing Recovery Manager Portal

You can install the Recovery Manager Portal on any domain-joined computer, including the one where Recovery Manager for Active Directory is installed. To install the Recovery Manager Portal, you must be a local administrator on the target computer.

To install the Recovery Manager Portal

1. Ensure the computer on which you plan to install the Recovery Manager Portal meets the system requirements in the Recovery Manager for Active Directory Forest Edition Release Notes.

2. Run the **RecoveryManagerPortal.exe** file supplied with the Recovery Manager for Active Directory Forest Edition installation package.
3. From version 8.7, the Recovery Manager Portal can be run under the Managed Service Account (MSA). If you specify the MSA account, add the '\$' character at the end of the account name (e.g. domain\computername\$) and leave the **Password** field blank (on the **Specify Web Site Settings** step of the wizard).

i NOTE:

- The MSA account must be a member of the local Administrator group on the Recovery Manager for Active Directory machine.
 - In case of MSA account, Recovery Manager Portal supports only Windows authentication to access the SQL Server databases.
4. Follow the steps in the wizard to complete the portal installation.
Take note of the Web site and virtual directory you specify in the wizard, because they make up the URL at which users can access the Recovery Manager Portal, as follows:
`http://<WebSite>/<VirtualDirectory>`
 5. After you complete the Setup Wizard, finalize the installation by logging off and then logging back on to the Recovery Manager Computer.

Once you have installed the Recovery Manager Portal, you need to configure it for working with the Recovery Manager for Active Directory instances deployed in your environment. For details, see [Configuring portal for working with Recovery Manager for Active Directory](#).

Connecting to Recovery Manager Portal

Before connecting to the Recovery Manager Portal for the first time, log out, and then log back on to the computer where you have installed the Recovery Manager Portal.

To connect to the Recovery Manager Portal

- Start your Web browser, and then go to the following URL:

`http://<WebSite>/<VirtualDirectory>/`

Substitute the Web site and virtual directory names specified during the Recovery Manager Portal installation for the <WebSite> and <VirtualDirectory> placeholders.

For example, if the Recovery Manager Portal site is installed on the computer named **Comp** to the virtual directory **RecoveryManagerPortal** in the default Web site, to access the Recovery Manager Portal, you need to go to **`http://Comp/RecoveryManagerPortal`**.

Administering Recovery Manager Portal

This section describes how to perform administrative tasks in the Recovery Manager Portal. To perform these tasks, you must access the Recovery Manager Portal using the account under which you installed the portal. For more information, see [Assigning roles to portal users](#).

In this section:

- [Configuring portal for working with Recovery Manager for Active Directory](#)
- [Modifying recovery settings for domains](#)
- [Assigning roles to portal users](#)
- [Delegating restore or undelete permissions](#)
- [Configuring e-mail notification](#)
- [How Recovery Manager Portal recovers data](#)

Configuring portal for working with Recovery Manager for Active Directory

To restore Active Directory data, the Recovery Manager Portal relies on unpacked backups created by the Recovery Manager for Active Directory instances deployed in your environment. For this reason, you need to configure the Recovery Manager for Active Directory instances to create unpacked backups for the domain controllers you want. Then, configure the Recovery Manager Portal to work with those instances.

Note that the Recovery Manager Portal can only work with Recovery Manager for Active Directory version 8.6 or higher, so make sure to install or upgrade to that Recovery Manager for Active Directory version.

To configure the Recovery Manager Portal for working with Recovery Manager for Active Directory, complete the following steps:

- [Step 1: Install Recovery Manager Remote API Access Service](#)
- [Step 2: Configure Recovery Manager for Active Directory](#)
- [Step 3: Add Recovery Manager for Active Directory instances](#)
- [Step 4: Configure recovery settings for Active Directory domains](#)

Step 1: Install Recovery Manager Remote API Access Service

To access a Recovery Manager for Active Directory instance, the Recovery Manager Portal requires the **Recovery Manager Remote API Access** service to be installed and running on the Recovery Manager for Active Directory computer. This service enables the following Recovery Manager for Active Directory features: integration with Recovery Manager Portal, RMAD console fault tolerance and support for hybrid environment.

The **Recovery Manager Remote API Access** service is an optional feature and you must select this component when installing Recovery Manager for Active Directory Forest Edition version 9.0.1. To check if this service is installed and running, you can use the Services tool (services.msc). If the service is not installed, complete the next steps to install it.

To install the Recovery Manager Remote API Access service

1. Open the list of installed programs (appwiz.cpl).
2. In the list of installed programs, locate and select Recovery Manager for Active Directory Forest Edition.
3. At the top of the list, click **Change**.
4. Step through the wizard until you are on the **Change, repair, or remove installation** page.
5. Click the **Change** button, and then select the **Recovery Manager Remote API Access** feature for installation.
6. Follow the steps to complete the wizard.

Step 2: Configure Recovery Manager for Active Directory

In this step, you need to configure the Recovery Manager for Active Directory instances for working with the Recovery Manager Portal.

To configure a Recovery Manager for Active Directory instance

1. In each Active Directory domain, choose one domain controller whose backups the Recovery Manager Portal will use for recovery operations.
2. In the appropriate instance of Recovery Manager for Active Directory, create a separate Computer Collection for each domain controller you have chosen.
3. Add the domain controllers to their individual Computer Collections.
4. Configure backup settings for these Computer Collections:

- **Specify to unpack backups.** For instructions, see [Configuring Computer Collection-specific settings to unpack backups](#).

This is required because the Recovery Manager Portal can only restore data from unpacked backups.

- **Configure a retention policy for the unpacked backups.** For instructions, see *Unpacked Backups* tab in [Properties for an existing Computer Collection](#).

The number of retained unpacked backups determines the number of available backup states to which you can restore Active Directory objects in the Recovery Manager Portal.

Step 3: Add Recovery Manager for Active Directory instances

In the Recovery Manager Portal, add the Recovery Manager for Active Directory instances you have configured in the previous step. By adding the instances, you make the unpacked backups they create available in the Recovery Manager Portal.

To add a Recovery Manager for Active Directory instance

1. Connect to the Recovery Manager Portal with your Web browser.

Use the user account under which you installed the Recovery Manager Portal. By default, this account has all necessary permissions to modify the portal configuration.

2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Recovery Manager for Active Directory Instances**.
4. Click the **Add instance** button.
5. Use the following options in the dialog box that opens:
 - **Computer**. Type the fully qualified domain name (FQDN) of the computer that hosts the Recovery Manager for Active Directory instance.
 - **Access the computer using**. Type the user name and password of the account with which you want to access the specified computer. The account must be a local administrator on the target computer.
6. When finished, click **OK**.

Step 4: Configure recovery settings for Active Directory domains

To configure recovery settings

1. In the Recovery Manager Portal, open the **Configuration** tab.
 2. Expand **Active Directory Domains**.
 3. Click a domain, and then do the following in the dialog box that opens:
 - **Recovery Manager for Active Directory**. Select the instance you have configured to back up a domain controller in the selected domain.
 - **Backups of selected DC**. Select the domain controller you have added to the Computer Collection in [Step 2: Configure Recovery Manager for Active Directory](#).
 - **Access the domain using**. Specify the account under which you want the selected Recovery Manager for Active Directory instance to recover data in the domain.
- i** **NOTE:** If you leave the **User name** and **Password** text boxes blank, the account specified in [Step 3: Add Recovery Manager for Active Directory instances](#) (**Access the computer using** option) is used by default. If a collection contains domain controllers from other domains or forests, Recovery Manager Portal should be able to read Active Directory schema for all domains included in the collection. For that, you need to specify the access credentials for these domains.
4. When finished, click **OK**.

Modifying recovery settings for domains

For each Active Directory domain available in the Recovery Manager Portal, you can specify the domaincontroller whose unpacked backups you want to use for recovering data in the Recovery Manager Portal, and the Recovery Manager for Active Directory instance you want to use for data recovery operations.

To configure recovery settings

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Active Directory Domains**.

4. Click the domain for which you want to configure the recovery settings.
5. In the dialog box that opens, use the following options:
 - **Recovery Manager for Active Directory.** Select the Recovery Manager for Active Directory instance you want to use to recover data in the domain.
 - **Backups of selected DC.** Select the domain controller whose backups you want to use to recover data in the entire domain.
 - **User name and password.** Type the credentials of the user account under which you want to restore data in the domain.
 - **Grant restore rights to all domain admins.** Select this check box if you want to delegate the rights to restore or undelete data to all accounts in the Domain Admins group. For more information about delegation, see [Delegating restore or undelete permissions](#).

Assigning roles to portal users

You can assign specific roles to the Recovery Manager Portal users. A role assigned to a user defines the Recovery Manager Portal user interface elements and functionality available to that user. You can only assign portal roles by using the account under which the Recovery Manager Portal was installed. By default, this account is granted all portal roles.

To assign portal roles, you can use local security groups existing on the computer where the Recovery Manager Portal is installed. By adding or removing members in these groups you can define the scope of authority for a portal user and the operations that the user can perform in the Recovery Manager Portal.

The local security groups are as follows:

- **Recovery Manager Portal - Configuration Admins.** Members in this group have permissions to modify the Recovery Manager Portal configuration and delegate restore permissions to other Recovery Manager Portal users.
- **Recovery Manager Portal - Recovery Operators.** Members in this group have permissions to restore or undelete Active Directory objects by using the Recovery Manager Portal.
- **Recovery Manager Portal - Undelete Operators.** Members in this group have permissions to undelete Active Directory objects by using the Recovery Manager Portal.
- **Recovery Manager Portal - Monitoring Operators.** Members in this group can view the health summary and backup creation history for the Recovery Manager for Active Directory instances with which the portal is configured to work.

Delegating restore or undelete permissions

You can delegate permissions to restore or undelete objects in specific Active Directory containers to the users or groups of your choice. These users or groups must reside in the Active Directory forest where the Recovery Manager Portal is installed and be assigned an appropriate portal role. For more information about portal roles, see [Assigning roles to portal users](#).

To delegate restore permissions, you also must have a specific role in the Recovery Manager Portal. For details, see [Assigning roles to portal users](#).

To delegate permissions

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Active Directory Domains**.
4. Click the name of the domain that includes the containers on which you want to delegate permissions.
5. Click **Configure a list of delegates**, and then expand the domain entry.
6. Click the container on which you want to delegate permissions.
7. Add delegates to the **Users or groups** list.
8. Below the list, select the operations you want to grant or deny to the added users or groups.
9. When you are finished, click **OK**. If necessary, repeat steps 6-9 for other containers in the domain.

Configuring e-mail notification

You can configure the Recovery Manager Portal to send notification e-mails to specific recipients when the health state of any Recovery Manager for Active Directory instance with which the Recovery Manager Portal is configured to work changes from healthy to unhealthy or vice versa.

To configure e-mail notification

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Portal Settings**, and then click **E-mail notification**.
4. Use the following options in the dialog box that opens:
 - **Outgoing SMTP server**. Type the fully qualified domain name (FQDN) or IP address of the SMTP server you want to use for sending notification e-mails.
 - **SMTP port**. Type the number of the port on which you want to connect to the server.
 - **Sender e-mail address**. Type the e-mail address you want to display in the **From** field of all notification e-mail messages.
 - **Notification recipients**. Here you can specify a list of notification recipients. To specify multiple values, use semicolon as the separator.
5. **User name and password**. Type the user name and password of the user account you want to use to send notification e-mails from the SMTP server. The account must have the appropriate permissions.
6. When you are finished, click **OK** to apply your settings.

How Recovery Manager Portal recovers data

Please consider the following behavior of the Recovery Manager Portal:

- By default, the permissions to restore or undelete objects in an Active Directory domain are only granted to the members of the Domain Admins group in that domain. However, you can delegate the restore or undelete permissions to the portal users you want. For more information, see [Delegating restore or](#)

[undelete permissions](#).

- By default, the Recovery Manager Portal uses the agent-based method for all search and restore operations, regardless of the settings configured on the Recovery Manager for Active Directory instance used to perform these operations. For more information about the agent-based method, see *Agent-based method* in [Using agentless or agent-based method](#). You can change the portal settings to use the agentless method.

To use the agentless method

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Portal Settings**, and then select the **Use agentless method for all search and restore operations** check box.

To undelete an Active Directory object, the Recovery Manager Portal uses Microsoft's Active Directory Recycle Bin feature if it is enabled in the target forest. If this feature is unavailable, the Recovery Manager Portal restores the object from the latest available unpacked backup that includes the object before its deletion.

Integrating with On Demand Recovery for Azure Active Directory

You can use On Demand Recovery for Azure Active Directory to restore on-premises objects that are synchronized with cloud.

What can be restored using the hybrid configuration

- On-premises object attributes that were synchronized with the cloud
- On-premises groups
- Office 365 licenses (assignedLicenses property for cloud users) and cloud group membership
- Deleted on-premises users and groups

i **IMPORTANT:** To configure the hybrid connection, outbound HTTPS (port 443) should be opened in the firewall on the machine where Recovery Manager Portal is installed.

To enable integration with the cloud

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Portal Settings** and click **On Demand integration...**
4. In the On Demand integration dialog, select **Enable integration** check box and specify Relay URL and credentials. To get these parameters, please go to Recovery for Azure Active Directory and perform the following steps:
 - a. On the **Dashboard** screen, click **Create hybrid connection**.
 - b. In the Create hybrid connection dialog, click **Download hybrid credentials** to download a configuration file with Relay credentials.
 - c. Save the file to the folder of your choice.

- d. Go back to the On Demand integration dialog, click **Choose file** and select the configuration file. For security reasons, you should remove this file from your computer after the credentials will be specified in Recovery Manager Portal.

NOTE: Azure AD Connect synchronization occurs automatically after the restore operation. But Recovery for Azure Active Directory has the ability to force synchronization cycle and requires credentials for the machine where Azure AD Connect is installed.

5. Specify Azure AD Connect host name and credentials. If Azure AD Connect and Recovery Manager Portal are installed on the same machine, leave the fields blank.

For more information about integration with Recovery for Azure Active Directory, please see the [Integration with Recovery Manager for Active Directory](#) section in the On Demand product documentation.

Viewing health summary for Recovery Manager for Active Directory instances

You can view the health summary for the Recovery Manager for Active Directory instances with which the portal is configured to work. To view the health summary, you must be assigned a specific role in the Recovery Manager Portal. For more information, see [Assigning roles to portal users](#).

To view the health summary

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Monitoring** tab.
3. Expand the **Health Summary** node to view the health summary.

Viewing backup creation history

You can view backup creation history for a particular instance of the Recovery Manager for Active Directory with which the Recovery Manager Portal is configured to work. To view backup creation history, you must be assigned a specific role in the Recovery Manager Portal. For more information, see [Assigning roles to portal users](#).

The backup creation history displays the date when a particular backup was created, the backup operation duration, and the size of the created backup. You can also view the name of the computer hosting the Recovery Manager for Active Directory instance that created the backup, the name of backed up Computer Collection and backed up computer.

To view backup creation history

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Monitoring** tab.
3. Expand the **Backup Creation History** node.

You can use the provided search box to find a specific entry in the list.

Recovering data using Recovery Manager Portal

In this section:

- [Restoring objects from a backup](#)
- [Undeleting objects](#)

Restoring objects from a backup

To restore objects from a backup, you must be assigned a specific role in the Recovery Manager Portal. For more

information, see [Assigning roles to portal users](#).

To restore objects

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Recovery** tab.
3. Click **Restore objects**.
4. Follow the steps in the wizard to find and restore the objects you want.

Undeleting objects

To undelete objects, you must be assigned a specific role in the Recovery Manager Portal. For more information, see [Assigning roles to portal users](#).

To undelete objects

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Recovery** tab.
3. Click **Undelete objects**.
4. Follow the steps in the wizard to find and undelete the objects you want

Appendices

- [Frequently asked questions](#)
- [Best practices for creating backups for forest recovery](#)
- [Best practices for recovering a forest](#)
- [Descriptions of recovery or verification steps](#)
- [Backup Wizard](#)
- [Online Restore Wizard](#)
- [Online Restore Wizard for AD LDS \(ADAM\)](#)
- [Group Policy Restore Wizard](#)
- [Repair Wizard](#)
- [Extract Wizard](#)
- [Events generated by Recovery Manager for Active Directory](#)

Frequently asked questions

- [Why do I need to restore deleted users or groups, rather than re-create them?](#)
- [How can I restore a user or group in Active Directory?](#)
- [How does online restore work?](#)
- [When an object is undeleted, what is restored from the tombstone and what is restored from the backup?](#)
- [What's the difference between an online restore and an authoritative restore?](#)
- [What's the difference between the agentless restore method and the agent-based restore method?](#)
- [Can I undelete a mailbox-enabled user?](#)
- [In the Group Policy Restore Wizard, a GPO link is shown as deleted, but the link actually exists in Active Directory. What's wrong?](#)
- [What is a primary restore of the SYSVOL?](#)
- [How do I change the Backup Agent port number?](#)

Why do I need to restore deleted users or groups, rather than re-create them?

Each user account or security group is uniquely identified with a SID (Security ID) and a GUID (Global Unique ID). If a user or group has been deleted, and is then re-created with the same name, the SID and GUID of the newly created user or group will differ from those of the deleted object. As a result, the new user or group loses all permissions, profile settings, and all other settings associated with the old SID and GUID.

When you restore a deleted user or group from a backup, the restored user or group will have the same SID and GUID as the deleted object, and will have all the settings associated with that SID and GUID.

How can I restore a user or group in Active Directory?

You can restore individual objects using the Online Restore feature of Recovery Manager for Active Directory. Alternatively, you can restore the entire Active Directory database, and then select individual objects for authoritative restore.

While Recovery Manager for Active Directory supports both methods, online restore is the recommended option as it is faster and simpler. The online restore method allows you to easily restore individual directory objects and object attributes without restarting domain controllers and putting Active Directory offline, thus achieving near-zero downtime.

How does online restore work?

The Recovery Manager for Active Directory online restore method facilitates the restoration of objects and objects attribute values, without putting Active Directory offline. The product can:

- Recover deleted objects with all their attributes and links by using the functionality provided by Microsoft's Active Directory Recycle Bin feature.
- Convert the tombstones into regular objects before applying the attribute values held in the backup.

In the latter scenario, Active Directory retains the object's tombstone for a specified configurable period of time (tombstone lifetime) in order to enable Active Directory replication to propagate the deletion. An object can only be undeleted if its tombstone exists. After applying the backed-up attribute values, the online restore process adjusts replication-related properties of the restored objects, so that Active Directory replication propagates the restored data to all domain controllers. Optionally, online restore can force replication of the restored data to decrease propagation delay.

When an object is undeleted, what is restored from the tombstone and what is restored from the backup?

When Microsoft's Active Directory Recycle Bin feature is enabled in the Active Directory forest, Recovery Manager for Active Directory can use the functionality provided by Microsoft's Active Directory Recycle Bin feature to undelete the object with all its attributes and links to the state the object was in immediately before deletion. No backups required in this recovery scenario.

In other recovery scenarios, when Microsoft's Active Directory Recycle Bin feature is disabled or not supported, Recovery Manager for Active Directory first restores all the attributes preserved in the object's tombstone. The remaining attributes are then restored from backup. If the backed-up value of an attribute differs from the value restored from the tombstone, then the backed-up value is restored. As a result, after the recovery operation completes, the restored object has the same attribute values, group memberships, and security descriptor as it had when the backup was created.

It is possible to determine which attributes are preserved in object tombstones by analyzing the AD schema. In such attributes, the third bit in the searchFlags property is set to 1. You can therefore enumerate these attributes using a filter that contains a matching rule such as the following:

```
searchFlags:1.2.840.113556.1.4.803:=8
```

What's the difference between an online restore and an authoritative restore?

An online restore is authoritative meaning that Active Directory replication updates all domain controllers with the restored data. However, online restore includes some additional functions. This method is designed to overcome the limitations inherent in a normal authoritative restore performed using native Windows tools. These limitations are as follows:

- Domain controllers must be restarted in Directory Services Restore mode, and the entire Active Directory database must be restored.
- When restoring an object, you must restore all attributes, which may overwrite valuable data stored in the object.
- When restoring a container, you must restore the entire sub-tree rooted in that container. There is no ability to restore only child objects of certain types.
- To restore an object's linked attributes, you need to restore both the object, and all objects to which the linked attributes refer; for example, if you only restore a deleted user, the user's group memberships are not restored.
- It is not possible to select individual objects for restore based on changes that occurred in Active Directory since backup creation.

To overcome these limitations, the online restore method includes the following capabilities:

- Selective restoration of objects without putting Active Directory offline, and without restoring the entire Active Directory database.
- Selective restoration of attribute values in directory objects; this allows you to specify exactly what object data should be restored.
- Selective restoration of child objects by object type. This allows you, for example, to restore only those users in a certain container and leave other child objects intact.
- Unattended restoration of linked attributes, such as the Member Of attribute. For example, when you undelete a user with online restore, the user's group memberships are also restored.
- Comparison of a backup with Active Directory, or with another backup, to facilitate Active Directory change tracking and troubleshooting: this allows you to select precisely the objects that should be restored.

What's the difference between the agentless restore method and the agent-based restore method?

Recovery Manager for Active Directory provides two different methods of restoring objects online. A check box in the Online Restore Wizard allows you to specify which method to use. The agentless method uses Microsoft Tombstone Reanimation interface, first made available in Windows Server 2003, to undelete the object and then re-applies all attributes that are not stored in the object's tombstone from the backup using ADSI calls. This method requires that the target domain controller be running Windows Server 2003 or later. Since the Tombstone Reanimation interface was not available in pre-Windows Server 2003 versions of the Windows operating system, the agent-based method provided online restore capabilities by placing the object's tombstone and attributes from backup into the Active Directory database.

Aside from operating system support, there are some additional differences between the two methods. The agentless and agent-based methods require different permissions to run. For example, the agentless method supports delegated permissions as outlined in the User Guide. The agentless method may not restore some attributes, depending on the operating system and service pack level, namely user passwords and SIDHistory, as these attributes cannot be set using ADSI. In order to restore these attributes using the agentless method, you can configure the Active Directory schema to store these attributes in the object tombstone as described in the User Guide.

Can I undelete a mailbox-enabled user?

Yes, you can undelete mailbox-enabled users with the online restore function of Recovery Manager for Active Directory. When you undelete a mailbox-enabled user within the mailbox retention period, the user's access to the mailbox is also restored.

After a user is deleted, the Exchange Server retains the user's mailbox for a specified period, before permanently deleting the mailbox. If the mailbox retention period has expired, the mailbox access associated with the undeleted user is not recovered. Recovery Manager for Active Directory cannot restore mailboxes that have been permanently deleted.

In the Group Policy Restore Wizard, a GPO link is shown as deleted, but the link actually exists in Active Directory. What's wrong?

If a link's No Override option or Disabled option has been changed, Recovery Manager for Active Directory treats the link as having been deleted, and assumes that a new link was created with new options. This behavior is by design.

What is a primary restore of the SYSVOL?

A primary restore is intended to recover the initial member of the SYSVOL replica set, only when the entire replica set has been lost. A primary restore should therefore not be used if there are two or more operational domain controllers in the domain. If there are other members in the replica set with which the restored SYSVOL can synchronize, a primary restore should not be performed, as it disrupts the replication of SYSVOL data.

For more information about primary restore, see the Microsoft article "Authoritative, Primary, and Normal Restores" at <http://technet.microsoft.com>.

How do I change the Backup Agent port number?

Recovery Manager for Active Directory uses a TCP port to communicate with Backup Agent installed on the target domain controllers to be backed up. To change the Backup Agent port number, perform the following procedures.

On each target domain controller to be backed up, perform the following steps:

1. Start Registry Editor (Regedit.exe), and then locate the registry key:

HKLM\SYSTEM\CurrentControlSet\Services\ErdAgent

2. In the details pane, double-click the **ImagePath** value, and in the **Value data** text box, specify the port number in the following way:

%SystemRoot%\RecoveryManagerAD\ErdAgent.exe -I -P:3899

In this example, Backup Agent will use port 3899. When finished, click **OK**.

3. Close Registry Editor.
4. Restart the Backup Agent service.

Start the Recovery Manager for Active Directory Console (snap-in), and then perform the following steps:

1. In the console tree, select the node Recovery Manager for Active Directory, and then on the **Action** menu, click **Settings**.
2. On the **Ports** tab, select the **Connect to Backup Agent using a specific TCP port** check box, and then specify the port number in the **Port** text box.
3. Click **OK** to close the **Recovery Manager for Active Directory Properties** dialog box.

i | IMPORTANT: If you are using a firewall, the specified TCP port must be opened. You must specify the same port number for all target domain controllers to be backed up.

How does Recovery Manager for Active Directory Forest Edition select a DC for an authoritative (primary) restore of SYSVOL during forest recovery?

When recovering an Active Directory forest, Recovery Manager for Active Directory Forest Edition automatically selects a DC in each domain to perform an authoritative (primary) restore of the SYSVOL folder. To select such a DC, Recovery Manager for Active Directory Forest Edition uses a number of predefined criteria listed in this section. These criteria are listed in the order they are applied by Recovery Manager for Active Directory Forest Edition. If no DC meets the first criteria in the list, Recovery Manager for Active Directory Forest Edition tries to apply the next criteria. Recovery Manager for Active Directory Forest Edition keeps going through the list of criteria, from top to bottom, until it finds a suitable DC.

Criteria used to determine if a DC is suitable for an authoritative (primary) restore of the SYSVOL (in the order of priority):

1. DC is the primary domain controller (PDC) emulator master
2. DC is the domain naming master or schema master in the forest.
3. DC is the RID master in the domain.
4. DC is a DNS server in the domain.
5. DC resides in the largest Active Directory site (as compared to other DCs in the domain).

How does Recovery Manager for Active Directory Forest Edition isolate domain controllers during forest recovery?

The overall success of a domain or forest recovery operation very much depends on the domain controllers being restored from backups. Not only it is important to ensure these domain controllers are restored from recent and trusted backups, it is also necessary to temporarily isolate these domain controllers to guarantee that no dangerous or unwanted data will be replicated to them from their replication partners during the recovery. Recovery Manager for Active Directory Forest Edition isolates domain controllers by creating a service dependency and using custom Internet Protocol security (IPSec) rules.

Before isolating the domain controllers being restored from backups, Recovery Manager for Active Directory Forest Edition backs up the IPSec settings existing in your environment to revert to these settings later.

Then, at the recovery step named **Enable domain controller isolation**, Recovery Manager for Active Directory Forest Edition does the following:

1. Establishes a dependency between the IPsec Policy Agent (PolicyAgent) service and the Active Directory Domain Services (NTDS) service. As a result, the Active Directory Domain Services service cannot start until the IPsec Policy Agent service starts.
2. Activates a number of custom IPSec rules defined in the `IsolateDC.bat` file.

The **IsolateDC.bat** file is located in the Recovery Manager for Active Directory Forest Edition installation folder (by default, this is `%ProgramFiles%\Quest\Recovery Manager for Active Directory Forest Edition`). The IPSec rules defined in the `IsolateDC.bat` file block all IP traffic between the domain controllers and their replication partners, except for the IP traffic generated by the following tools/services:

- Remote Desktop Connection client
- Ping command
- File sharing services
- Domain Naming System

These IPSec rules also apply to the IP traffic from the domain controllers to the Forest Recovery Console computer. Traffic from the Forest Recovery Console computer to the domain controllers is not affected by these IPSec rules.

i **NOTE:** You can edit the **IsolateDC.bat** file to define the IPSec rules that become active during recovery. However, we cannot guarantee that problems that may occur if you incorrectly edit the **IsolateDC.bat** file can be solved. Edit the **IsolateDC.bat** file at your own risk.

At the recovery step named **Ensure that domain controller isolation is disabled**, Recovery Manager for Active Directory Forest Edition removes the dependency between the Active Directory Domain Services service and the NTDS service and uses the **UnisolateDC.bat** file to revert to the pre-recovery IPSec settings.

The **UnisolateDC.bat** file is located in the Recovery Manager for Active Directory Forest Edition installation folder (by default, this is `%ProgramFiles%\Quest\Recovery Manager for Active Directory Forest Edition`).

How does Recovery Manager for Active Directory Forest Edition select a DC to add the global catalog during forest recovery?

When recovering an Active Directory forest, Recovery Manager for Active Directory Forest Edition adds the global catalog to the DCs that acted as global catalog servers before the recovery, provided that these DCs were successfully restored from backup.

If none of DCs that acted as global catalog servers before the recovery were successfully restored from backup, Recovery Manager for Active Directory Forest Edition adds the global catalog to the DC which was assigned the schema master role during the recovery.

Best practices for creating backups for forest recovery

- [How many instances of the Recovery Manager Console to deploy?](#)
- [How many domain controllers to back up?](#)
- [How many domain controllers to back up at once?](#)
- [What data to back up?](#)
- [Using data compression](#)
- [Using unpacked backups](#)

How many instances of the Recovery Manager Console to deploy?

To recover your Active Directory forest with the Forest Recovery Console, you can only use backups created with the Recovery Manager Console. In simple environments, it is advisable to have only one Recovery Manager Console deployed. However, this may not be possible in large distributed environments that spread across different physical locations connected by slow links. In this case, you can deploy several instances of the Recovery Manager Console in each main physical location to back up domain controllers there.

You can also deploy several instances of the Recovery Manager Console if you want to

- Delegate the right to back up individual Active Directory objects and perform online restores to other administrators in your environment, without delegating the right to run forest recovery operations.
- Back up and restore individual Active Directory objects using backup and restore strategy and schedule specific to those objects.

How many domain controllers to back up?

This depends on the forest recovery method you choose for your environment. For more information about these methods, see [Forest recovery methods](#).

The decision on how many domain controllers to back up (and, therefore, which method to use for forest recovery) depends on the factors like

- The overall number of domain controllers in Active Directory
- The size of Active Directory database

With a large number (50+) of domain controllers in the domain and significant size (over 1 GB) of the Active Directory database, it may not be feasible to fully back up system state of all domain controllers in the domain due to storage limitations or time constraints. In this case, you can back up only some of the domain controllers.

A good practice is to back up at least two domain controllers in each domain in the forest. It is recommended to back up the domain controllers that are DNS servers and FSMO role holders.

How many domain controllers to back up at once?

The Recovery Manager Console allows you to group the computers you want to back up into computer collections, each collection having its own backup creation parameters and schedule.

All computers in a computer collection are backed up simultaneously. The backup creation process may be a resource-consuming task if the number of computers in a collection is more than 10. Therefore, it is recommended that you back up only one computer collection at a time. Also, it is not recommended to have more than 10 domain controllers in a single computer collection.

What data to back up?

All of the domain controller backups that you plan to use for forest recovery must include the following System State components:

- Active Directory (SYSVOL and DIT database)
- System registry

To make sure you back up the above components, go to the System State tab in the **Properties** dialog box for the computer collection you want to back up to check that these System State components will be backed up.

On the same tab, make sure you specify to collect forest recovery metadata and group membership information from all domains within the Active Directory forest. However, if the backup creation operation takes a significant time to complete, you may disable collecting group membership information from all domains within the forest. For more information about the **Properties** dialog box for a computer collection, see the User Guide supplied with this release of Recovery Manager for Active Directory Forest Edition.

To streamline the creation of Active Directory backups, you can follow these best practices:

- Avoid using groups with cross-domain membership in Active Directory as much as possible. To reveal such groups, you can use an Active Directory reporting tool such as Quest Reporter.
- If you cannot avoid using groups with cross-domain membership, make sure you have a procedure in place to back up and restore these groups manually. For example, you can do so by using such command line tools as Ldifde or Csvde provided by Microsoft.

Using data compression

For each computer collection you can specify the data compression method to be used in backup creation operations. To ensure both a reasonable backup time and a reasonable compressed backup size, it is recommended that you use either Fast or Normal compression method. For more information on how to specify a data compression method for a computer collection, see the User Guide supplied with this release of Recovery Manager for Active Directory Forest Edition.

Using unpacked backups

Recovery Manager for Active Directory Forest Edition can keep unpacked Active Directory backups in the location you specify in order to reuse them for subsequent online restore operations. The use of unpacked backups helps to significantly accelerate the backup data preparation stage of an online restore operation.

Although the use of unpacked backups is helpful for online restores of individual Active Directory objects, this approach is not recommended for forest recovery because in this case the entire Active Directory database is unpacked on each domain controller you restore from backup, which can be a lengthy process.

It is recommended that you configure Recovery Manager to not unpack the Active Directory backups you plan to use for forest recovery. For more information on how to do it, see the User Guide supplied with this release of Recovery Manager for Active Directory Forest Edition.

Best practices for recovering a forest

- [How many Instances of the Forest Recovery Console to deploy?](#)
- [Where to Install the Forest Recovery Console?](#)
- [Backing up the Recovery Manager for Active Directory Forest Edition configuration](#)

How many Instances of the Forest Recovery Console to deploy?

The Forest Recovery Console must have access to the Recovery Manager for Active Directory Forest Edition backup registration database containing information about all backups of the domain controllers in the forest. To meet this requirement, you must deploy the Forest Recovery Console on the same computer that hosts the Recovery Manager Console used to create backups of the domain controllers.

You can easily meet this requirement in simple and relatively small environments where you have a single instance of the Recovery Manager Console deployed. However, in complex and large environments the requirement to have a single instance of the Recovery Manager Console (and thus maintain a single forest-wide backup registration catalog) might not be feasible.

For more information on how to consolidate backups created by different instances of Recovery Manager for Active Directory Forest Edition deployed in your environment, see [Consolidating backups from different backup registration databases](#).

Where to Install the Forest Recovery Console?

The best practice is to install the Forest Recovery Console on a standalone computer. This allows you to avoid situations where a corruption in Active Directory prevents you from using the Forest Recovery Console. Keeping the Forest Recovery Console computer in a demilitarized zone (DMZ) and not in a domain will help you to prevent any negative consequences of logical corruption in Active Directory, should it occur.

Backing up the Recovery Manager for Active Directory Forest Edition configuration

It is recommended to regularly back up the Recovery Manager for Active Directory Forest Edition configuration, so that you could quickly reinstall the product and restore its configuration to the last backed up state in case Recovery Manager for Active Directory Forest Edition becomes inoperable due to a failure. All the Recovery Manager for Active Directory Forest Edition configuration data is held in the following location on the Recovery Manager for Active Directory Forest Edition computer:

%AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory The Recovery Manager Console saves its configuration data in the following files:

- **Erdiskad.mdb**. Contains the Recovery Manager Console configuration data, such as computer collections and backup creation sessions.
- **Backups.mdb**. Contains the backup registration database that stores information about created Active Directory and ADAM backups.

As a rule, the overall size of these .mdb files does not exceed 10 MB.

The Forest Recovery Console saves all its configuration data in the Forest Recovery Project (.frproj) file.

Descriptions of recovery or verification steps

The next table describes the steps you may encounter in the Recovery Plan or on the **Progress** tab in the Forest Recovery Console while running a restore or verify settings operation.

Table 43: Recovery or verification steps

Step	Description
Add global catalog	Adds the global catalog to the DC if: • The global catalog was removed from the DC during the recovery. • The recovery project settings specify to rebuild the global catalog. If no global catalog servers were successfully restored from backup, the global catalog is added to the DC that was assigned the Schema Master role during the recovery.
Change global catalog partition occupancy level	Sets the appropriate global catalog partition occupancy level to advertise the global catalog servers in DNS according to the recovery project settings. For

Step	Description
	more information on advertising the global catalog servers, see Specifying recovery project settings .
Clean up metadata of removed domain controllers	Removes metadata of all domain controllers that were not restored from backup. This includes the domain controllers whose restore from backup has failed and those for which a recovery method other than Restore from backup has been selected.
Clean up metadata for domains that were not restored if necessary	Cleans up metadata of the domains in which no DCs were successfully restored from backup or for which you specified to not recover any DCs.
Check if BitLocker is enabled	Checks whether BitLocker Drive Encryption is enabled on the DC. Gets the BitLocker configuration if BitLocker is enabled.
Check if domain controller is read-only	Checks whether the DC is read-only (RODC).
Check if computer is a domain controller	Checks if the computer is a domain controller to ensure that restore from backup is possible.
Copy the backup file to domain controller, if there is one	If a backup was configured, then copies the backup file specified in the DC recovery settings to the DC. If there was no backup configured, this step will be skipped.
Detect current mode (DSRM or normal)	Checks whether the DC is in normal mode or DSRM.
Disable BitLocker	Disables BitLocker Drive Encryption if it is enabled on the DC.
Disable custom filters for passwords	Disables any third-party custom password filters enabled on the DC. This step is required to ensure the filters do not block any password reset operations during the recovery.
Disable Windows Update	Disables Microsoft Windows Update on the DC for the duration of the recovery to prevent the installation of updates and possible reboots of the DC.
Enable BitLocker	Enables BitLocker Drive Encryption if it was disabled on the domain controller earlier in the recovery process.
Enable custom filters for passwords	Enables the third-party custom password filters that were disabled on the DC earlier in the recovery process.
Enable domain controller isolation	Uses IPsec policies to restrict all traffic on the DC except for the following: • Network traffic to/from the Forest Recovery Console • Incoming RDP traffic • Incoming and outgoing ICMP traffic • Incoming and outgoing DNS traffic • File share access traffic • Internal TCP traffic This step does not delete any existing IPsec policies. If the DC is running Windows Server 2008 or later, this step sets certain additional parameters to avoid AD DS being unavailable until the replication of a

Step	Description
	writable directory partition has completed.
Enable the use of global catalog for user authentication	Enables the use of the global catalog for user logon validation.
Enable Windows Update	Re-enables Microsoft Windows Update on the DC.
Ensure global catalog is available	Performs all necessary operations to ensure a global catalog server is available in the forest and functioning properly.
Ensure that the SYSVOL share is available	Checks that the SYSVOL share is available on the DC.
Ensure that domain controller isolation is disabled	Disables any IPsec policies that were enabled during the recovery. Enables the IPsec policies that were in effect before the recovery started. If the DC is running Windows Server 2008 or later, this step sets certain additional parameters. These parameters require a DC that restarts and holds operations master roles to have successful AD DS replication with its known replica partners before it advertises itself as DC.
Ensure that Forest Recovery Agent is installed and running	Checks the installed version of Forest Recovery Agent. If necessary, installs the agent or upgrades it to the version supplied with the Forest Recovery Console you are using.
Get information about domain controller	Collects the following information from the DC: • IP addresses of all network adapters • IP addresses of all DNS servers on all network adapters • DNS names of all FSMO role holders in the forest • Installed Forest Recovery Agent version (if any) • Whether the current DC is a RODC • Operating system version
Get replication data from the DC	Collects replication data from the DC. The collected data will be used later to determine if lingering objects are present.
Raise RID pool	Raises the value of available RID pools by the value specified in the Forest Recovery Console configuration file (100,000 by default).
Invalidate RID pool	Invalidates the current RID pool. This operation reverts the restored domain controller from re-issuing RIDs from the RID pool that was assigned at the time the backup was created.
Reinstall Active Directory Domain Services	Installs Active Directory Domain Services (AD DS) on the computer. Restarts the computer after the AD DS installation completes.
Adjust to Active Directory changes	Global Catalogs from excluded domains are adjusted to the state of recovered domains. This step involves the Repadmin tool. If particular changes performed by the Repadmin tool do not succeed, then the Global Catalog on this domain controller will be reset.
Remove global catalog	Removes the global catalog from the DC.

Step	Description
Remove global catalog if necessary	Removes the global catalog from the DC if necessary, provided that the DC is a global catalog server.
Remove temporary files	Deletes the backup file from the DC if the file was copied to the DC during the recovery.
Reset computer account passwords	Resets computer account passwords twice to an automatically generated value. The passwords are reset for the current DC and all other DCs in the project. By default, the automatically generated password value includes 12 characters: at least one lower-case English letter, one upper-case English letter, one digit, and one non-alphanumeric character.
Reset DSRM administrator password	Resets the DSRM administrator password to the value specified in the DC recovery settings.
Reset global catalog	Removes the global catalog from the DC if all of the following is true: • The DC is a global catalog server • You selected an option in the recovery project settings to rebuild the global catalog to ensure no lingering objects are present. Then, adds the global catalog back to the DC.
Reset the Krbtgt password	Resets the Krbtgt password twice to an automatically generated value. By default, the automatically generated password value includes 12 characters: at least one lower-case English letter, one upper-case English letter, one digit, and one non-alphanumeric character.
Reset trust passwords	Resets the trust passwords twice to an automatically generated value. By default, the automatically generated password value includes 12 characters: at least one lower-case English letter, one upper-case English letter, one digit, and one non-alphanumeric character. This operation is performed for all implicit and explicit trusts between this domain and all other trusted domains in the forest. Trust passwords for any external trusts are not reset.
Restart domain controller in DSRM if necessary	If DSRM is not the current mode, restarts the domain controller in DSRM and resets the DSRM password.
Restart domain controller in DSRM if necessary	Restarts the DC in DSRM if it is not the current mode.
Restart domain controller in normal mode	Restarts the DC in normal mode for the changes to take effect. When performing this step on a DC restored from backup, Recovery Manager for Active Directory Forest Edition also resets the user password to the value specified in the DC recovery settings. This password reset overwrites the old password restored from backup.
Restore data from backup, if there is one	Restores the Active Directory database (.dit file), SYSVOL, and system registry entries from the backup specified in the DC recovery settings. Disables the use of global catalog for user logon validation. This allows users other than the built-in Administrator to log on during the recovery.
Restore initial global	Sets the global catalog partition occupancy level to the value that existed before

Step	Description
catalog partition occupancy level	the recovery. For more information on the recovery project settings that may cause Recovery Manager for Active Directory Forest Edition to change the global catalog partition occupancy level during recovery, see Specifying recovery project settings .
Run pre-recovery checks	If the Restore from backup or SYSVOL Restore recovery method is selected for the DC, this step checks that: • The DSRM password specified in the DC recovery settings meets the password complexity criteria. • The backup file specified in the DC recovery settings is accessible (mandatory requirement for domain or forest recovery). • There is a sufficient amount of free disk space on the DC to accommodate the backup file (mandatory requirement for domain or forest recovery). • A preferred DNS server is specified for the DC in the recovery settings. If this is true, then this step checks the validity of the DNS server. If either Reinstall Active Directory or Uninstall Active Directory recovery method is selected for the DC, this step checks that: • The DSRM password specified in the DC recovery settings meets the password complexity criteria. • A preferred DNS server is specified for the DC in the recovery settings. If this is true, then this step checks the validity of the DNS server.
Seize FSMO roles	Seizes FSMO roles for the DCs automatically selected for each role.
Select preferred DNS server	Selects a properly functioning DNS server for all network adapters on the DC. This step uses the following order of priority to select a DNS server: 1. Preferred DNS server specified in the DC recovery settings. 2. Primary and alternate DNS servers that were selected for the DC before the recovery. 3. DNS servers selected for other DCs in the same domain. 4. All other DNS servers in the forest. AD-integrated DNS servers hosted on DCs that were not successfully restored from backup are excluded from the list of possible DNS servers.
Save start types of Windows services	Save start types of Windows services that can be changed during recovery.
Uninstall Active Directory Domain Services	Demotes the DC to a member server joined to the workgroup named WORKGROUP. Resets the local Administrator password to the value specified in the Set DSRM password option in the DC recovery settings.
Wait for a global catalog server to become available	Waits for at least one global catalog server to become available in the forest. This step may take a significant time to complete.

Backup wizard

The Backup Wizard helps you create backups of domain controllers' System State, including Active Directory and Group Policy data. With this wizard you can select domain controllers whose System State is to be backed up, specify where to store backups, run backup immediately or schedule it for later, view and modify backup options, such as what System State components are to be backed up.

The wizard has the following steps:

- [What to Back Up](#)
- [Where to Store Backups](#)
- [When to Back Up](#)
- [Computer Collection Name \(optional\)](#)
- [Completing the Backup Wizard](#)

What to Back Up

Use this page to select computers whose system state you want the wizard to back up. You can back up selected computers or computers that reside in a specific container.

- **Selected objects.** The Selected objects list includes the names and descriptions of computers and containers the wizard will process. You can modify the list using the **Add** and **Remove** buttons.
- **Add.** When you click **Add**, the wizard presents you with these commands:
 - **Domain Controller.** Selects and adds domain controllers by name.
 - **Container.** Selects and adds a container. The wizard will back up all computers that are in that container.
 - **AD LDS (ADAM) Host.** Selects and adds AD LDS (ADAM) hosts by name.
 - **Import Computers.** Use a text file, one computer name per line, to add computers to the list.
- **Remove.** Removes the selected entries from the Selected objects list.

To add a computer by name

1. Click **Add** and then click **Add Computer**.
2. In the **Select Computers** dialog box, supply the name of the computer you want to add to the list.

With the **Select Computers** dialog box, you can select multiple computers. The **Select Computers** dialog box only allows you to add computers by computer account name. If you want to add computers by IP address, DNS name, or NetBIOS name, use an import file.

To add computers using an import file

1. Create a text file that contains computer names, one name per line.
2. Click **Add** and then click **Import Computers**.
3. Use the **Open** dialog box to locate and open the text file.

To add a container

1. Click **Add** and then click **Add Container**.
2. In the **Domain** box, select or type the DNS name of a domain. If you typed the DNS name, click **Connect** to refresh the tree in the **Containers** box.
3. In the **Containers** box, select the container to add.

If you select computers or containers before starting the Backup Wizard, the **Selected objects** list includes the objects you have selected.

Where to Store Backups

Use this page to specify the path and name format for backup files.

- **Backup file path and name format.** Provides a space for you to specify format for paths and names of .bkf files where you want the wizard to store backups. You can use UNC names to store backups in a shared network folder. The path format may include optional expressions that enable the automatic creation of subfolders. The file name format may also include expressions. For example, you might specify C:\DIRNAME\%COMPUTERNAME%\%DATETIME%.

As a result, backups for different computers will be saved in separate subfolders named by a computer name. In addition, the file name of each backup will be composed of the date and time of the backup creation.

- **Expression.** Click this button to specify optional path and file name notations in **Backup file path and name format**. You can choose the following expressions:
 - **Default backup storage (%BACKUPS%).** Path to the default backup storage folder. Unless modified during the installation of Recovery Manager for Active Directory Forest Edition, it points to the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory Forest Edition\Backups.
 - **Domain (%DOMAIN%).** Name of the home domain of the computer being backed up.
 - **Computer name (%COMPUTERNAME%).** Name of the computer being backed up.
 - **Date and Time (%DATETIME%).** Date and time of the backup creation.
- **Browse.** Click this button to locate the folder where backups are to be stored.
- **Sample path and file name matching the specified format.** This box displays an example of the path and file name that matches the format string supplied in **Backup file path and name format**.

When to Back Up

Use this page to specify whether to run the backup job immediately after finishing the wizard or schedule the backup job for later.

- **Now.** Select this option if you want to run the backup job immediately after you close the wizard.
- **Create and retain Computer Collection for the selected computers.** Select this check box if you want the wizard to create a Computer Collection that includes all objects you have selected on the **What to Back Up** page. Normally, if you select the Now option, the wizard does not create a Computer Collection.

- **Later (configure backup scheduling).** Select this option if you want to schedule the backup job.
- **Schedules for the backup creation task.** This box displays a list of schedules for the backup job. To add and remove schedules, click the **Change** button next to this box.
- **Change.** Click this button to modify the Schedules for the backup creation task list. In the dialog box that appears on the screen, select the **Show multiple schedules** check box and specify new schedules or delete existing schedules.
- **User account under which the scheduled task will run.** This box identifies the user account under which Task Scheduler will perform the backup job. To change the user account, click the **Change** button next to this box.

Computer Collection Name (optional)

Use this page to provide the name for a new Computer Collection created by the wizard. This page appears after you select either of these options on the When to Back Up page: **Create and retain Computer Collection for the selected computers** or **Later (configure backup scheduling)**.

- **Collection name.** In the **Collection name** box, the wizard displays the default name for the new Computer Collection. You can modify the name. After you complete the wizard, the new Computer Collection is created and it includes all objects you have selected on the What to Back Up page.

Completing the Backup Wizard

Use this page to view and modify additional backup creation and logging settings.

- **Advanced.** When you click **Advanced**, the wizard displays the **Properties** dialog box, which is similar to that described in [Properties for an existing Computer Collection](#). The wizard creates backups using the settings you can view and modify in the **Properties** dialog box. The wizard also uses these settings when creating a new Computer Collection. By default, the wizard uses the default settings for Computer Collections you can view and modify with the **Collection Defaults** command. The **Collection Defaults** command appears on the Action menu when you select the **Computer Collections** node in the Recovery Manager Console tree.
- **Finish.** Closes the wizard and starts or schedules the backup job

Online Restore Wizard

The Online Restore Wizard helps you recover Active Directory objects deleted or modified since the backup. With this wizard you can selectively restore individual directory objects and object attributes from an Active Directory backup, compare a backup with Active Directory, compare two backups taken from the same domain controller. The wizard has the following steps:

- [Wizard Operation Mode](#)
- [Domain Selection](#)
- [Backup Selection](#)
- [Backup for Comparison \(optional\)](#)
- [Unpacked Backups Folder Selection](#)

- [Backup Data Preparation](#)
- [Domain Access Options](#)
- [Objects to Be Processed](#)
- [Operation Selection](#)
- [Processing Options](#)
- [Reporting Options](#)
- [Operation Start](#)
- [Operation Progress](#)
- [Operation Option](#)
- [Objects to Be Restored](#)
- [Where to Restore Deleted Objects](#)
- [Operation Results](#)
- [Completing the Online Restore Wizard](#)

Wizard Operation Mode

Use this page to choose whether to perform a restore along with reporting changes or only compare two Active Directory backups taken from the same domain controller.

- **Compare, restore, and report changes in Active Directory.** With this option, the wizard performs per-attribute comparison of selected objects between a backup and Active Directory, and allows you to proceed to the object restore.
- **Compare two backups and report the differences.** With this option, the wizard performs per-attribute comparison of selected objects between two Active Directory backups taken from the same domain controller.

Domain Selection

Use this page to view a list of domains for which Active Directory backups are available in Recovery Manager for Active Directory and select the domain where you want the wizard to restore Active Directory objects.

- **Domains.** Displays a list of domains for which Active Directory backups are available in Recovery Manager for Active Directory. From the list, select the domain where you want the wizard to restore Active Directory objects, and then click **Next**. In the next step, the wizard lists available backups of domain controllers for that domain.
- **Register.** The **Domains** list only includes the domains for which Active Directory backups are registered in the backups registration database. To perform a restore to another domain, click **Register**, and then click one of the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf) or Windows Server backup file (.vhd, .vhdx).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline Active Directory Database.** Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

Backup Selection

Use this page to view a list of Active Directory backups that are registered in the Recovery Manager for Active Directory backup registration database for the selected domain, if any, and select a backup.

- **Registered backups.** Lists registered Active Directory backups for the selected domain, if any. From this list, select the backup you want the wizard to use, and then click **Next**. In the list, each entry includes the following fields:
 - **Backup Age.** Indicates how old the backup is. Active Directory does not allow using a backup whose age exceeds the Active Directory tombstone lifetime (default is 60 days).
 - **Created.** Displays the date when the backup was created.
 - **DC.** Displays the computer name of the domain controller; the backup contains directory object data retrieved from that domain controller.
 - **Media.** Displays the path and name of the backup file.

The list only includes the backups that are registered in the Recovery Manager for Active Directory backup registration database. Recovery Manager for Active Directory allows you to use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec. To use a backup of this kind, click **Register**.

- **Register.** To register additional backups, click **Register**, and then click one of the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf) or Windows Server backup file (.vhd, .vhdx).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline Active Directory Database.** Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

Backup for Comparison (optional)

Use this page to select a backup to compare with the previously selected one. This window appears after you select the Compare two backups and report the differences option on the Wizard Operation Mode page.

- **Registered backups.** Provides a list of registered Active Directory backups for the selected domain. In the list, each entry includes the following fields:
 - **Backup Age.** Indicates how old the backup is. Active Directory does not allow using a backup whose age exceeds the Active Directory tombstone lifetime.
 - **Created.** Displays the date when the backup was created.
 - **DC.** Displays the computer name of the domain controller; the backup contains directory object data retrieved from that domain controller. The wizard will connect to the domain controller that corresponds to the entry you have selected.
 - **Media.** Displays the path and name of the backup file.
- **Register.** To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf) or Windows Server backup file (.vhd, .vhdx).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.

- **Register Offline Active Directory Database.** Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

Only backups of the same domain controller can be compared. The first of the selected backups must be older than the second one.

Unpacked Backups Folder Selection

Use this page to optionally change the folder where Recovery Manager for Active Directory will unpack the selected backup.

- **Path to store unpacked backups.** Displays the path to the folder currently used to keep unpacked backups. Each unpacked backup will be saved in a separate subfolder of that folder. To leave that path unchanged, click **Next**. To specify other path, type the path to a new folder or click **Browse** to select it. When finished, click **Next**.

Your changes will not affect the default settings for unpacked backups.

Backup Data Preparation

This page enables you to view the progress of the backup extraction. To stop the unpack process, click Cancel. You can also have the wizard keep the extracted data for future use.

- **Keep extracted data after completing the wizard.** When this check box is selected, the wizard saves the extracted DIT database in a temporary folder, so you can reuse this information for subsequent starts of the Online Restore Wizard, Online Restore Wizard for AD LDS (ADAM), or Group Policy Restore Wizard. The temporary folder is specified using the **Unpacked Backups** tab in the **Recovery Manager for Active Directory Properties** dialog box. When this check box is cleared, the extracted data is erased when you close the wizard. Because the unpacking process is a lengthy operation, you should not close the wizard unless you are sure that no additional objects need to be compared or restored within the current session.

Domain Access Options

Use this page to specify a way the target domain to be accessed.

- **Use agentless method to access domain controller**
When selected, ensures that only LDAP functions are used to access the domain controller. When you leave this check box cleared, the restore is performed using Restore Agent. For more details about agentless or agent-based method, refer [Using agentless or agent-based method](#).
- **Target domain controller**
Displays the DNS name of the target domain controller for the restore operation. By default, the wizard uses the domain controller from which the backup was created. To choose the target domain controller, click **Browse**, and then complete the **Select Domain Controller** dialog box.
- **Account used to access the target domain controller**
Displays the user account with which Recovery Manager for Active Directory will access the target domain controller. By default, the wizard accesses the domain controller with the account under which Recovery Manager for Active Directory is running. To choose a different account, click **Change**, and then complete the **Select Account** dialog box.

- **Automatically configure Windows Firewall**

When selected, the Windows Firewall settings will be configured automatically for the online restore operation.

Objects to Be Processed

Use this page to select Active Directory objects to be processed.

- **Objects.** Lists the objects the wizard will process. The **Name** column displays the object's distinguished name.
- **Add.** Adds objects to the **Objects** list. Click this button, and then, on the shortcut menu, click **Find**, **Browse**, or **Import** to specify the objects you want to add.
- **Remove.** Removes selected objects from the **Objects** list.
- **Properties.** Displays the **Properties** dialog box, allowing you to view the attribute values of objects you select from the **Objects** list.

To add objects to the Objects list

- Click **Add**, and then complete the steps related to the action you want to perform:

Table 44: Adding objects to the Object list

To do this	Complete these steps
Search for objects in the backup	1. On the menu, click Find. 2. Use the dialog box that opens to search for object. 3. Once your search completes, under Search results, select the check boxes next to the objects you want to add. 4. Click OK.
Browse for and select an object	1. On the menu, click Browse. 2. Use the dialog box that opens to browse for and select the object you want to add. 3. Click OK.
Import objects from an import file	1. On the menu, click Import. 2. Use the dialog box that opens to browse for and select the import file that specifies the objects you want to add. 3. Click OK. The import file must have the .txt format. You can specify one object per line in the import file. To specify an object in the file, use one of the following: • Distinguished name (DN) • sAMAccountName attribute value • User principal name (UPN) • Logon name

To do this	Complete these steps
	When preparing an import file, you must escape reserved characters by prefixing such characters with a backslash (\). The reserved characters that must be escaped include: • ; < > \ " + , • space or # character at the beginning of a string • space character at the end of a string Other reserved characters, such as the equals sign (=) or non- UTF-8 characters, must be encoded in hexadecimal by replacing the character with a backslash followed by two hex digits.

To view values of the object attributes

- Select an object from the **Objects** list, and then click **Properties**.

The wizard displays the **Properties** dialog box. The **Attributes** box inside the **Properties** dialog box lists attributes of the selected object and displays the values each attribute has in the backup and in Active Directory. The elements of the **Properties** dialog box are defined as follows:

- **Show changed attributes only.** When selected, the **Attributes** list displays only the attributes that have been changed since the time the backup was created.
- **Show all possible attributes.** When selected, the **Attributes** list displays all possible attributes of the selected object.
- **Include attributes with empty values.** When selected, the **Attributes** list includes the attributes that have empty values.

In the **Attributes** list, each entry includes the following fields:

- **Attribute.** Displays the LDAP display name of an attribute. When the value in the backup differs from the value in Active Directory, the attribute is labeled with a red exclamation sign icon. Otherwise, it is labeled with a green tick icon.
- **Value in Backup.** Displays the value the attribute has in the backup.
- **Value in Active Directory.** Displays the value the attribute has in Active Directory, if the object exists in Active Directory.

Operation Selection

Use this page to specify what you want to do with the objects you selected.

- **Compare, analyze, and, optionally, restore.** With this option, the wizard performs per-attribute comparison of selected objects between a backup and Active Directory, and allows you to proceed to the object restore.
- **Restore (skip compare analysis).** This option allows you to proceed to the restore of the objects specified on the previous page of the wizard.

Processing Options

Use this page to specify whether to process the objects' child objects and how to process object attributes.

- **Child objects processing.** In this area, you can use the following elements:
 - **Process no child objects.** Processes only the selected objects.
 - **Process all child objects.** Processes the selected objects and all their child objects.
 - **Process child objects of selected types.** Processes the selected objects and their child objects of the types you specify using the **Select Object Types** button.
 - **Select Object Types.** Allows you to select the child object types to be processed. For more information, see [Select Object Types](#).
- **Attribute-level processing.** In this area, you can use the following elements:
 - **Process all attributes.** Processes all object attributes. When performing a restore with this option, the wizard only restores the attributes that were modified since the backup time. The wizard does not affect other attributes.
 - **Process selected attributes.** Processes selected object attributes. Use the **Select Attributes** button to specify the attributes to be processed. You can process selected attributes only if child objects are not selected for processing.
 - **Select Attributes.** Allows you to specify what object attributes the wizard will process. For more information, see [Select Attributes to Be Processed](#).

Select Object Types

The **Select Object Types** dialog box enables you to specify types of child objects you want the wizard to process.

- **Object types.** Lists types of the child objects for the selected container. In the list, select the check boxes next to the object types you want the wizard to process. When finished, click **OK**.
- **Show all object types.** When selected, causes the **Object types** list to display the advanced object types.

Select Attributes to Be Processed

The **Select Attributes to Be Processed** dialog box allows you to select attributes of the specified directory object. The Online Restore Wizard will process only the attributes you select in this dialog box.

- **Attributes.** Lists attributes of the directory object you selected. In the list, select check boxes next to attribute names. When finished, click **OK**. The entries in the upper part of the **Attributes** list allow you to select groups of attributes. For example, when you select **Address Information**, all attributes relating to the user addresses are selected.
- **Show all possible attributes.** When selected, causes the **Attributes** list to display all attributes of the selected object.
- **Clear all.** Clears all check boxes in the **Attributes** list.

Reporting Options

Use this page to specify whether or not you want to generate a comparison or restore report and what information you want to include in the report.

- **Generate report.** When this check box is selected, the wizard generates a report based on the settings you have specified.
- **Report changed objects only.** When this check box is selected, the comparison report includes information about only the objects that have been changed since the time of the backup, and the restore report includes information only about the objects that the wizard has modified or undeleted during the restore.
- **Report changed attributes only.** When this check box is selected, the comparison report includes information about only the object attributes that have been changed since the time of the backup, and the restore report includes information only about the object attributes the wizard has modified during the restore.
- **Include ChangeAuditor data in reports.** When this check box is selected, the comparison report includes the information on users who modified certain Active Directory objects. To use this option, you must have ChangeAuditor for Active Directory installed in the home Active Directory forest of Recovery Manager for Active Directory.
- **ChangeAuditor database.** Allows you to specify the ChangeAuditor database from which you want to retrieve data about users who modified Active Directory objects.

Operation Start

This page enables you to review settings you have specified in the previous steps of the wizard. To start the operation, click **Next**. To change the wizard settings, click **Back**.

Operation Progress

This page shows the progress of the operation and lets you see a summary of the comparison results or a summary of changes made to Active Directory during the restore process.

- **Objects total.** The number of objects the wizard has processed.
- **Different objects/Restored objects.** Different objects shows the number of compared objects for which the wizard has detected differences. Restored objects shows the number of objects the wizard has restored in Active Directory.
- **Errors occurred.** The number of errors the wizard has encountered during the operation. Use the **Export errors...** button to save the error data in CSV format.

Password Settings

This dialog box enables you to specify the password and password settings for the user account you restore using the Online Restore Wizard.

The dialog box has the following elements:

- **Specify the new password.** Select this option if you want to set a new password for the user account to be restored.
 - **New password.** Provides a space for you to type a case-sensitive password up to 127 characters.
 - **Confirm new password.** Provides a space for you to retype the password to confirm the spelling.
- **Leave the password unchanged.** Select this option if you want to leave the user password unchanged. When you select this option, the restored user account can be disabled if its password does not meet the password policy requirements.
- **Additional options.** Select this check box to specify additional settings for user password.
 - **Disable user account.** Select this check box to disable the user account.
 - **User must change password at next logon.** Select this check box to require users to change their passwords the next time they log on.
- **Apply these settings to all restored users.** Select this check box to apply the specified password settings for all user accounts to be restored from the selected backup.

Operation Option

Use this page to analyze comparison reports and proceed to restore after the comparison was made.

- **View Report.** Click to view comparison reports. The report is viewed and managed with Quest Reports Viewer or with Microsoft SQL Server Reporting Services. The application used for generating, managing and viewing the reports was specified while installing Recovery Manager for Active Directory.
- **Proceed to restore.** To proceed to a restore of the selected objects, select this check box and then click **Next**. To quit the wizard without performing a restore, leave this check box cleared and then click **Next**.

Objects to Be Restored

Use this page to view values of object attributes and select Active Directory objects to be restored.

- **Objects.** Lists the objects the wizard will process. The **Objects** list includes only the objects for which the comparison has detected differences. The **Name** column displays the object's distinguished name.
- **Properties.** Displays the **Properties** dialog box, allowing you to view the attribute values of objects you select from the **Objects** list.
- **Select All.** Selects all objects from the **Objects** list.
- **Clear All.** Clears all check boxes under **Objects**.

To select objects to be restored

- Select check boxes in the **Objects** list, and then click **Next**.

You can use the drop-down list to filter objects in the Objects list. You can also select and deselect all objects by clicking the **Select All** and **Clear All** buttons.

To view values of the object attributes

- Select an object from the **Objects** list, and then click **Properties**.

The wizard displays the **Properties** dialog box. The **Attributes** box inside the **Properties** dialog box lists attributes of the selected object and displays the values each attribute has in the backup and in Active Directory. The elements of the **Properties** dialog box are defined as follows:

- **Show changed attributes only.** When selected, the **Attributes** list displays only the attributes that have been changed since the time the backup was created.
- **Show all possible attributes.** When selected, the **Attributes** list displays all attributes of the selected object.
- **Include attributes with empty values.** When selected, the **Attributes** list displays the attributes that have empty values.

In the **Attributes** list, each entry includes the following fields:

- **Attribute.** Displays the LDAP display name of an attribute.
- **Value in Backup.** Displays the value the attribute has in the backup.
- **Value in Active Directory.** Displays the value the attribute has in Active Directory, if the object exists in Active Directory.

Where to Restore Deleted Objects

Use this page to specify a container where to restore the objects selected on the previous page of the wizard.

- **Restore deleted objects to their original containers (default).** With this option, the wizard restores the selected objects to their original container.
- **Specify a destination container for restoration of deleted objects.** This option allows you specify the destination container for restoration of the deleted objects. Select that container with the **Browse** button. If you select the **Show advanced objects** option in the **Browse and Select a Container** dialog, the objects can be restored to the containers that reside in the Configuration and Schema directory partitions.

Operation Results

Use this page to view or save the restore report. Click **View Report** to view comparison reports. The report is viewed and managed with Quest Reports Viewer or with Microsoft SQL Server Reporting Services. The application used for generating, managing and viewing the reports was specified while installing Recovery Manager for Active Directory.

Completing the Online Restore Wizard

This is the final page of the wizard. Click **Back** to select and compare/restore additional objects or click **Finish** to close the Online Restore Wizard. After you select a backup on the Backup Selection page, the wizard prepares temporary data, unpacking the backup. This is a lengthy operation. The prepared data is erased when you close the wizard, unless you have selected the **Keep extracted data after completing the wizard** check box on the Backup Data Preparation page.

Online Restore Wizard for AD LDS (ADAM)

The Online Restore Wizard for AD LDS (ADAM) helps you recover AD LDS (ADAM) objects deleted or modified since the backup. With this wizard you can selectively restore individual directory objects and object attributes from an Active Directory backup, compare a backup with Active Directory, and compare two backups taken from the same domain controller. The wizard has the following steps:

- [Wizard Operation Mode](#)
- [AD LDS \(ADAM\) Instance Selection](#)
- [Backup Selection](#)
- [Backup for Comparison](#)
- [Unpacked Backups Folder Selection](#)
- [Backup Data Preparation](#)
- [AD LDS \(ADAM\) Access Options](#)
- [Objects to Be Processed](#)
- [Processing Options](#)
- [Reporting Options](#)
- [Operation Start](#)
- [Operation Progress](#)
- [Operation Option](#)
- [Objects to Be Restored](#)
- [Operation Results](#)
- [Completing the Online Restore Wizard for AD LDS \(ADAM\)](#)

Wizard Operation Mode

Use this page to choose whether to perform restore and report changes or only compare two AD LDS (ADAM) backups taken from the same AD LDS (ADAM) instance.

- **Compare, restore, and report changes in AD LDS (ADAM).** With this option, the wizard performs per-attribute comparison of selected objects between the backup and AD LDS (ADAM), and allows you to proceed to the object restore.
- **Compare two backups and report the differences.** With this option, the wizard performs per-attribute comparison of selected objects between two AD LDS (ADAM) backups taken from the same AD LDS (ADAM) instance.

AD LDS (ADAM) Instance Selection

Use this page to view a list of AD LDS (ADAM) instances for which backups are available in Recovery Manager for Active Directory and select the instance where you want the wizard to restore AD LDS (ADAM) objects.

- **AD LDS (ADAM) instances.** Lists AD LDS (ADAM) instances for which backups are available in Recovery Manager for Active Directory. From the list, select the instance where you want the wizard to restore AD LDS (ADAM) objects, and then click Next. In the next step, the wizard lists available backups for this instance.
- **Register.** The AD LDS (ADAM) instances list only includes the instances for which backups are registered in the Recovery Manager for Active Directory configuration database.

To perform a restore to another AD LDS (ADAM) instance

- Click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline AD LDS (ADAM) Database.** Registers AD LDS (ADAM) database (adamntds.dit file) unpacked from a backup created with third-party backup tools.

Backup Selection

Use this page to view a list of backups that are registered in the Recovery Manager for Active Directory configuration database for the selected AD LDS (ADAM) instance, if any, and select a backup.

- **Registered backups.** Lists registered backups for the selected AD LDS (ADAM) instance, if any. From this list, select the backup you want the wizard to use, and then click **Next**. In the list, each entry includes the following fields:
 - **Backup Age.** Indicates how old the backup is. Active Directory does not allow using a backup whose age exceeds the Active Directory tombstone lifetime.
 - **Created.** Displays the date when the backup was created.
 - **Media.** Displays the path and name of the backup file.

The list only includes the backups that are registered in the Recovery Manager for Active Directory configuration database. In the Online Restore Wizard, you can also use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec. To use a backup of this kind, select **Register**.

- **Register.** To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline AD LDS (ADAM) Database.** Registers AD LDS (ADAM) database (adamntds.dit file) unpacked from a backup created with third-party backup tools.

Backup for Comparison

Use this page to select a backup to compare with the previously selected one. This window appears after you select the **Compare two backups and report the differences** option in the Wizard Operation Mode window.

- **Registered backups.** Provides a list of registered AD LDS (ADAM) backups for the selected AD LDS (ADAM) instance. In the list, each entry includes the following fields:

- **Backup Age.** Indicates how old the backup is. Active Directory does not allow using a backup whose age exceeds the Active Directory tombstone lifetime.
- **Created.** Displays the date when the backup was created.
- **Media.** Displays the path and name of the backup file.
- **Register.** To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline AD LDS (ADAM) Database.** Registers AD LDS (ADAM) database (adamntds.dit file) unpacked from a backup created with third-party backup tools.

Only backups of the same AD LDS (ADAM) instance can be compared. The first of the selected backups must be older than the second one.

Unpacked Backups Folder Selection

Use this page to optionally change the folder where Recovery Manager for Active Directory will unpack the selected backup. The **Path to store unpacked backups** box displays the path to the folder currently used to keep unpacked backups. Each unpacked backup will be saved in a separate subfolder of that folder. To leave that path unchanged, click **Next**. To specify other path, type the path to a new folder or click **Browse** to select it. When finished, click **Next**. Your changes will not affect the default settings for unpacked backups.

Backup Data Preparation

This page enables you to view the progress of the backup extraction. To stop the unpack process, click **Cancel**. You can also have the wizard keep the extracted data for future use. When the **Keep extracted data after completing the wizard** check box is selected, the wizard saves the extracted DIT database in a temporary folder, so you can reuse this information for subsequent starts of the Online Restore Wizard or Group Policy Restore Wizard. The temporary folder is specified using the **General** tab of the **Unpacked Backups Policy** dialog box. When this check box is cleared, the extracted data is erased when you close the wizard. Because the unpacking process is a lengthy operation, you should not close the wizard unless you are sure that no additional objects need to be compared or restored within the current session.

AD LDS (ADAM) Access Options

This page allows you to specify the target AD LDS (ADAM) instance and account used to access that instance.

- **Target AD LDS (ADAM) instance.** Displays the name of the AD LDS (ADAM) instance for the restore operation. By default, the wizard uses the AD LDS (ADAM) instance from which the backup was created. To specify a different instance, click **Browse**, and then complete the **Select AD LDS (ADAM) Instance** dialog box.
- **Browse.** Opens the **Select AD LDS (ADAM) Instance** dialog box that allows you to select the target AD LDS (ADAM) instance for the restore operation.
- **Port number.** Displays the port number used by AD LDS (ADAM).

- **Account used to access the AD LDS (ADAM) instance.** Displays the user account used to access the target AD LDS (ADAM) instance. To specify a different account or a different AD LDS (ADAM) instance to connect to, click **Change**.
- **Change.** Opens the **Connect to AD LDS (ADAM)** dialog box that allows you to specify the target AD LDS (ADAM) instance and the user account used to connect to that instance.

Objects to Be Processed

Use this window to select AD LDS (ADAM) objects to be processed.

- **Objects.** Lists the objects the wizard will process. The **Name** column displays the object's distinguished name.
- **Add.** Adds objects to the **Objects** list. Click this button, and then, on the shortcut menu, click **Find**, **Browse**, or **Import** to specify the objects you want to add.
- **Remove.** Removes selected objects from the **Objects** list.
- **Properties.** Displays the **Properties** dialog box, allowing you to view the attribute values of objects you select from the **Objects** list.

To add objects to the Objects list

1. Click **Add**, and then do one of the following:
 - On the shortcut menu, click **Find** and use the **Find and Select Objects in Backup** dialog box to search for objects in the backup. Under Search results, select objects by selecting check boxes next to object names.
 - On the shortcut menu, click **Browse** and use the **Browse and Select Object in Backup** dialog box to browse the directory tree and select an object.
 - On the shortcut menu, click **Import** and use the **Open** dialog box to locate and open the import file that contains distinguished names (DN) of the objects you want to add. Import files are text files that contain one DN per line. When preparing an import file for selecting objects, you must escape reserved characters by prefixing such characters with a backslash (\) in DN strings. The reserved characters that must be escaped include semicolon (;), right and left angle brackets (<, >), backslash (\), double quote ("), plus sign (+), comma (,), space or # character at the beginning of a string, and space character at the end of a string.
2. When finished, click **OK** to close the dialog box.

To view values of the object attributes

- Select an object from the **Objects** list, and then click **Properties**.

The wizard displays the **Properties** dialog box. The **Attributes** box inside the **Properties** dialog box lists attributes of the selected object and displays the values each attribute has in the backup and in Active Directory. The elements of the **Properties** dialog box are defined as follows:

- **Show changed attributes only.** When selected, the **Attributes** list displays only the attributes that have been changed since the time the backup was created.
- **Show all possible attributes.** When selected, the **Attributes** list displays all possible attributes of the selected object.

- **Include attributes with empty values.** When selected, the **Attributes** list displays only the attributes that have non-empty values.

In the **Attributes** list, each entry includes the following fields:

- **Attribute.** Displays the LDAP display name of an attribute. When the value in the backup differs from the value in AD LDS (ADAM), the attribute is labeled with a red exclamation sign icon. Otherwise, it is labeled with a green tick icon.
- **Value in Backup.** Displays the value the attribute has in the backup.
- **Value in Active Directory.** Displays the value the attribute has in AD LDS (ADAM), if the object exists in AD LDS (ADAM).

Processing Options

Use this page to select the operation option, to specify whether to process the objects' child objects, and how to process object attributes.

- **Operation option.** In this area, you can use the following elements:
 - **Compare, analyze and, optionally, restore.** Compares the selected objects with their counterparts in AD LDS (ADAM).
 - **Restore (skip compare analysis).** Skips compare operation and restores the selected objects without creating and analyzing comparison reports.
 - **Restore the selected objects.** Appears if you proceed to restore after performing the comparison. Restores objects selected in the **Objects to Be Restored** window.
- **Child objects processing.** In this area, you can use the following elements:
 - **Process no child objects.** Processes only the selected objects.
 - **Process all child objects.** Processes the selected objects and all their child objects.
 - **Process child objects of selected types.** Processes the selected objects and their child objects of the types you specify using the **Select Object Types** button.
 - **Select Object Types.** Displays the **Select Object Types** dialog box that allows you to select the child object types to be processed.
- **Attribute-level processing.** In this area, you can use the following elements:
 - **Process all attributes.** Processes all object attributes. When performing a restore with this option, the wizard only restores the attributes that were modified since the backup time. The wizard does not affect other attributes.
 - **Process selected attributes.** Processes selected object attributes. Use the **Select Attributes** button to specify the attributes to be processed. You can process selected attributes only if child objects are not selected for processing.
 - **Select Attributes.** Displays the **Select Attributes to Be Processed** dialog box that allows you to specify what object attributes the wizard will process.

Reporting Options

Use this page to specify whether or not you want to generate a comparison or restore report and what information you want in the report.

- **Generate report.** When this check box is selected, the wizard generates a report based on the settings you have specified.
- **Report changed objects only.** When this check box is selected, the comparison report includes information about only the objects that have been changed since the time of the backup, and the restore report includes information only about the objects that the wizard has modified or undeleted during the restore.
- **Report changed attributes only.** When this check box is selected, the comparison report includes information about only the object attributes that have been changed since the time of the backup, and the restore report includes information only about the object attributes the wizard has modified during the restore.

Operation Start

This page enables you to review settings you have specified in the previous steps of the wizard. To start the operation, click **Next**. To change the wizard settings, click **Back**.

Operation Progress

This page shows the progress of the operation and lets you see a summary of the comparison results or a summary of changes made to AD LDS (ADAM) during the restore process.

- **Objects total.** The number of objects the wizard has processed.
- **Different objects/Restored objects.** Different objects shows the number of compared objects for which the wizard has detected differences. **Restored objects** shows the number of objects the wizard has restored in AD LDS (ADAM).
- **Errors occurred.** The number of errors the wizard has encountered during the operation.

Operation Option

Use this page to analyze comparison reports and proceed to restore after the comparison was made.

- **View Report.** Click to view comparison reports. The report is viewed and managed with Quest Reports Viewer or with Microsoft SQL Server Reporting Services. The application used for generating, managing and viewing the reports was specified while installing Recovery Manager for Active Directory.
- **Proceed to restore.** To proceed to a restore of the selected objects, select this check box and then click **Next**. To quit the wizard without performing a restore, leave this check box cleared and then click **Next**.

Objects to Be Restored

Use this page to view values of object attributes and select AD LDS (ADAM) objects to be restored.

- **Objects.** Lists the objects the wizard will process. The **Objects** list includes only the objects for which the comparison has detected differences. The **Name** column displays the object's distinguished name.
- **Properties.** Displays the **Properties** dialog box, allowing you to view the attribute values of objects you select from the **Objects** list.

- **Select All.** Selects all objects from the **Objects** list.
- **Clear All.** Clears all check boxes under **Objects**.

To select objects to be restored

- Select check boxes in the **Objects** list, and then click **Next**.

You can use the drop-down list to filter objects in the **Objects** list. You can also select and deselect all objects by clicking the **Select All** and **Clear All** buttons.

To view values of the object attributes

- Select an object from the **Objects** list, and then click **Properties**.

The wizard displays the **Properties** dialog box. The **Attributes** box inside the **Properties** dialog box lists attributes of the selected object and displays the values each attribute has in the backup and in AD LDS (ADAM). The elements of the **Properties** dialog box are defined as follows:

- **Show changed attributes only.** When selected, the **Attributes** list displays only the attributes that have been changed since the time the backup was created.
- **Show all possible attributes.** When selected, the **Attributes** list displays all attributes of the selected object.
- **Show non-empty attributes only.** When selected, the **Attributes** list displays only the attributes that have non-empty values.

In the **Attributes** list, each entry includes the following fields:

- **Attribute.** Displays the LDAP display name of an attribute.
- **Value in Backup.** Displays the value the attribute has in the backup.
- **Value in Active Directory.** Displays the value the attribute has in Active Directory, if the object exists in Active Directory.

Operation Results

Use this page to view or save the restore report. Click **View Report** to view comparison reports. The report is viewed and managed with Quest Reports Viewer or with Microsoft SQL Server Reporting Services. The application used for generating, managing and viewing the reports was specified while installing Recovery Manager for Active Directory.

Completing the Online Restore Wizard for AD LDS (ADAM)

This is the final page of the wizard. Click **Back** to select and compare/restore additional objects or click **Finish** to close the wizard. After you select a backup on the Backup Selection page, the wizard prepares temporary data, unpacking the backup. This is a lengthy operation. The prepared data is erased when you close the wizard, unless you have selected the **Keep extracted data after completing the wizard** check box on the Backup Data Preparation page.

Group Policy Restore Wizard

The Group Policy Restore Wizard helps you restore selected Group Policy objects, security settings on Group Policy objects, and links to Group Policy objects. With this wizard you can compare the state of Group Policy objects in backup with their state in Active Directory and restore Group Policy information from an Active Directory backup to the backup source domain. The wizard has the following steps:

- [Backup Source Domain](#)
- [Backup Selection](#)
- [Unpacked Backups Folder Selection](#)
- [Backup Data Preparation](#)
- [Target Domain Controller](#)
- [Group Policy Object Selection](#)
- [GPO Restore Options](#)
- [Link Restore Options](#)
- [Restore Process Start](#)
- [Completing the Group Policy Restore Wizard](#)

Backup Source Domain

Use this page to view a list of domains for which Active Directory backups are available in Recovery Manager for Active Directory and select the domain where you want the wizard to restore Active Directory objects.

- **Domains.** Displays a list of domains for which Active Directory backups are available in Recovery Manager for Active Directory. From the list, select the domain where you want the wizard to restore Active Directory objects, and then click **Next**. In the next step, the wizard lists available backups of domain controllers for that domain.
- **Register.** The **Domains** list only includes the domains for which Active Directory backups are registered in the backups registration database.

To perform a restore to another domain

- Click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline Active Directory Database.** Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

Backup Selection

Use this window to view a list of Active Directory backups that are registered in the Recovery Manager for Active Directory configuration database for the selected domain, if any, and select a backup.

- **Registered backups.** Provides a list of registered Active Directory backups for the selected domain. In the list, select the backup from which you want to select Group Policy objects, and then click **Next**. In the list, each entry includes the following fields:
 - **Backup Age.** Indicates how old the backup is. Active Directory does not allow using a backup whose age exceeds the Active Directory tombstone lifetime (default is 60 days).
 - **Created.** Displays the date when the backup was created.
 - **DC.** Displays the computer name of the domain controller; the backup contains directory object data retrieved from that domain controller.
 - **Media.** Displays the path and name of the backup file.
- **Register.** To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.
 - **Register Offline Active Directory Database.** Registers Active Directory database (ntds.dit file) unpacked from a backup created with third-party backup tools.

In the Group Policy Restore Wizard, you can use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec.

Unpacked Backups Folder Selection

Use this window to optionally change the folder where Recovery Manager for Active Directory will unpack the selected backup. The **Path to store unpacked backups** box displays the path to the folder currently used to keep unpacked backups. Each unpacked backup will be saved in a separate subfolder of that folder. To leave that path unchanged, click **Next**. To specify other path, type the path to a new folder or click **Browse** to select it. When finished, click **Next**. Your changes will not affect the default settings for unpacked backups.

Backup Data Preparation

This page enables you to view the progress of the backup extraction. To stop the unpack process, click **Cancel**. You can also have the wizard keep the extracted data for future use. **When the Keep extracted data after completing the wizard** check box is selected, the wizard saves the extracted DIT database in a temporary folder, so you can reuse this information for subsequent starts of the Online Restore Wizard, Online Restore Wizard for AD LDS (ADAM), or Group Policy Restore Wizard. The temporary folder is specified using the **Unpacked Backups** tab in the **Recovery Manager for Active Directory Properties** dialog box. When this check box is cleared, the extracted data is erased when you close the wizard. Because the unpacking process is a lengthy operation, you should not close the wizard unless you are sure that no additional objects need to be compared or restored within the current session.

Target Domain Controller

Use this page to view a list of the domain controllers available for the target domain you specified on the Operation Target Domain page, and to select the domain controller the wizard will use to restore Group Policy information.

- **Use domain controller with the Operations Master token for the PDC emulator.** Restores Group Policy information to the primary domain controller emulator Operations Master (default option). It is strongly recommended that all changes to the Group Policy information be made on a single domain controller, such as the primary domain controller emulator Operations Master, since using the same domain controller for all Group Policy operations ensures that no data loss occurs.
- **Use a different domain controller.** Restores Group Policy information to the domain controller you can select from the list under Select one of the available domain controllers.
- **Select one of the available domain controllers.** Lists the domain controllers available for the domain specified.

Group Policy Object Selection

Use this page to select Group Policy objects to be restored. This page also allows you to view the comparison report for the selected Group Policy objects.

- **Group Policy Objects available for restore.** Lists the objects the wizard will process. The **Name** column displays the object's distinguished name. In the list, each entry includes the State in AD column indicating the state of the Group Policy object in Active Directory in comparison with that in the backup. Initially, for all entries, the **State in AD** column indicates 'Not compared'. To have the wizard compare the state of Group Policy objects in Active Directory with that in the backup, click **Compare All**.

The comparison may be a lengthy operation, depending on the number of Group Policy objects. You may skip this operation or select individual GPOs to be compared and click **Compare**.

- **Compare All.** Compares the Group Policy objects state and then modifies the Group Policy Object Selection page, allowing you to view the state of each Group Policy object available for restore. In the **Group Policy Objects available for restore** list, each entry is labeled with one of the following icons:
 -  - the object differs from that in the backup—the State in AD field indicates 'Different'.
 -  - the object is the same as that in the backup—the State in AD field indicates 'Identical'.
 -  - the object is currently deleted but still exists in the backup—the State in AD field indicates 'Deleted'.
- **Compare.** Compares the state of the selected Group Policy objects and then displays the comparison results on the Group Policy Object Selection page. In the Group Policy Objects available for restore list, the entries that correspond to the selected Group Policy objects are labeled with one of the following icons:
 -  - the object differs from that in the backup—the State in AD field indicates 'Different'.
 -  - the object is the same as that in the backup—the State in AD field indicates 'Identical'.
 -  - the object is currently deleted but still exists in the backup—the State in AD field indicates 'Deleted'.
- **View Report.** Click this button to view the comparison report for the GPOs you select from the **Group Policy Objects available for restore** list.

To select Group Policy objects to be restored

- In the list under **Group Policy Objects available for restore**, select check boxes next to Group Policy objects, and then click **Next** to proceed with the wizard.

GPO Restore Options

Use this page to choose whether to restore policy settings, security settings, or both.

- **Restore policy settings in Group Policy Object.** If the Group Policy object has been modified since the time the backup was created, restores all policy settings to the state they had at the time of the backup. If the Group Policy object has been deleted, creates a new object with the same name and policy settings as the backed up object.
- **Restore security settings on Group Policy Object.** Restores all security information on the Group Policy object. As a result, all users and security groups have the same access permissions on the object as they had when the backup was created.

Link Restore Options

Use this page to restore links to the Group Policy object to the state they had at the time of the backup. As a result, the object is used by the same sites, domains, and organizational units that used it at the time when the backup was created.

- **Action.** Allows you to specify the link restore options. You can replace the existing links in your domain with those from the backup or leave the existing links intact. In addition, you can merge the backed up links with those that currently exist in the domain.
- **Group Policy object links at the time the backup was created.** Provides a list of sites, domains, and organizational units that used the selected Group Policy object at the backup time.

If you have selected several GPOs on the Group Policy Object Selection page, this list is not displayed. In the list, each entry includes the following fields:

- **Link.** Displays the full distinguished name of directory objects to which the Group Policy object was linked at the backup time.
- **State in AD.** Indicates the current state of the link in Active Directory (shown as Present or Deleted)
- **No Override.** Indicates whether the link was set to No Override (shown as Yes or No), so that Group Policy objects linked at a lower level of Active Directory could not override that policy
- **Disabled.** Indicates whether that link was set to Disabled (shown as Yes or No), which prevented the Group Policy object from applying to the site, domain, or organizational unit

To specify the link restore options

1. From the **Action** list, select one of the following:
 - **Restore the backed up snapshot of links.** The wizard replaces the existing links to the Group Policy object with the links taken from the backup (those listed under Group Policy object links at the time the backup was created).

- **Merge the backed up links with the existing links.** The wizard restores the listed links, remaining the existing links intact.
 - **Make no changes to links.** The wizard does not restore links, nor does it make changes to the existing links.
2. When finished, click **Next**. Note that clicking **Next** does not actually start the restore process, only allowing you to review your restore options.

Restore Process Start

This page enables you to review settings you have specified in the previous steps of the wizard. To start the operation, click **Next**. To review or change your settings, click **Back**.

Completing the Group Policy Restore Wizard

This is the final page of the wizard. Click **Back** to select and restore additional Group Policy objects or click **Finish** to close the Group Policy Restore Wizard. After you select a backup on the Backup Selection page, the wizard prepares temporary data, unpacking the backup. This is a lengthy operation. The prepared data is erased when you close the wizard, unless you have selected the **Keep extracted data after completing the wizard** check box on the Backup Data Preparation page.

Repair Wizard

The Repair Wizard helps you restore the System State on a domain controller, including the Active Directory database and SYSVOL. With this wizard you can select a System State backup, select Active Directory objects for authoritative restore, and perform a primary restore of SYSVOL.

The wizard has the following pages:

- [Computer and Backup Selection](#)
- [Target Computer](#)
- [Computer Restart](#)
- [Primary Restore of SYSVOL](#)
- [Restore Process Start](#)
- [Restore Progress](#)
- [Authoritative Restore Selections](#)
- [Computer Restart in Normal Mode](#)
- [Completing the Repair Wizard](#)

Computer and Backup Selection

Use this page to view a list of computers for which backups are available and to select a backup to perform a restore. The list of computers in the window depends on how the wizard was started. If you select a computer

and then start the wizard using the Action menu, the list includes only the selected computer. Otherwise, it includes all computers.

- **Locate the backup under computer name.** Provides a list of computers for which backups are available and allows you to select a backup to perform a restore. To ensure the selected backup contains all System State components needed for the restore, browse the **System State** branch in the Computer and Backup Selection window. For the selected computer, the window lists all backups that are available in Recovery Manager for Active Directory. A backup entry includes the date and time when the backup was created, and displays the backup age in days. The list only includes the backups that are registered in the Recovery Manager for Active Directory configuration database.
- **Register.** To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File.** Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf).
 - **Register Backups in Folder.** Registers all backup files that are in the selected folder.

In the Repair Wizard, you can use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec. However, snapshot backups are not supported by the Repair Wizard. You can restore Active Directory data from such backups using the Online Restore Wizard and Group Policy Restore Wizard. The Extract Wizard also supports snapshot backups.

To select a backup

Double-click the computer whose backup you want to use, and then double-click the backup you want to use. Select the check box next to **System State** and then click **Next**.

Target Computer

Use this page to view where the System State data will be restored.

- **Restore System State data on the computer.** Displays the computer name where the System State data will be restored.
- **Change.** Click **Change** to change the target computer, and then complete the **Change Target Computer** dialog box. In the **Computer name** box, type the NetBIOS name, DNS name, or IP address of the computer where you want to perform a restore.

A restore on a computer different from the backup source can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall the system.

- **Next.** Click **Next** to connect to the target computer. No backup data is transferred at this stage.

Computer Restart

Use this page to specify how to restart the target computer in Directory Services Restore Mode.

- **Manual restart.** With this option, you must restart the target computer manually.
- **Automatic restart.** Restarts the target computer remotely, using the startup parameters shown in the Boot option box. If you want to apply different startup parameters, use Manual restart. When performing the automatic restart, the wizard modifies the Computer Restart page, allowing you to abort the shutdown, if necessary.
- **Boot option.** When you select the Automatic restart option, displays the startup parameters used to restart the target computer remotely. If you want to apply different startup parameters, use Manual restart.

To restart the computer in Directory Services Restore Mode manually

1. Restart the computer, and press F8 when you are prompted to do so.
2. On the menu, choose **Directory Services Restore Mode**, and then press ENTER.
3. If you have multiple systems installed on the computer, choose the system installation you are recovering, and then press ENTER. You must choose the same installation as the one that was started when you launched the Repair Wizard.

To abort the computer shutdown

- Click **Abort Shutdown**.

The Abort Shutdown button is available only during a 40-second grace period. The process of restarting the domain controller in Directory Services Restore Mode can take several minutes. The **Current Status** box allows you to examine the progress of the restart.

After the domain controller is started in Directory Services Restore Mode, the wizard displays the **Select Account** dialog box. You must specify the password of the Directory Service Restore Mode Administrator.

In the **Select Account** dialog box, you must supply the account name and password of the target computer local administrator (Directory Services Restore Mode Administrator). You must use the credentials of an account that is stored in the local security account (SAM) database. You cannot use the name and password of an Active Directory administrator. This is because Active Directory is offline, and account verification cannot occur. Rather, the SAM accounts database is used to control access to Active Directory on the local computer while Active Directory is offline.

Primary Restore of SYSVOL

Use this page to specify whether to perform a primary restore of SYSVOL. This window appears if the wizard fails to access the SYSVOL share on any domain controller within the domain.

The **Perform a primary restore of the SYSVOL** check box forces the wizard to perform a primary restore of SYSVOL.

To restore the SYSVOL data as the primary data

- Select the check box in the Primary Restore of SYSVOL window.

If the domain controller being recovered is the only functioning domain controller in the domain, the SYSVOL data must be restored as the primary data. As a result, a new replication service database is created by loading the data present under the SYSVOL on the local domain controller. A primary restore is the same as non-authoritative except that the restored SYSVOL is marked as Primary.

Only use this option when the SYSVOL data is lost on all the domain controllers in the domain. Do not select the **Perform a primary restore of the SYSVOL** check box if the SYSVOL shares exist on other operational domain controllers in the domain. This option is only intended for disaster recovery cases when all members of the SYSVOL replica set are lost. Setting a member as initial master when it has other members from which to synchronize may result in breaking the replication of the SYSVOL share.

Restore Process Start

This page provides an overview of the settings you have specified in the previous steps of the wizard. To start the operation, click **Next**. To review or change your settings, click **Back**.

Restore Progress

This page shows the progress of the operation. You can stop the operation by clicking **Cancel**.

Clicking the **Cancel** button when the restore is in progress can result in serious, unexpected consequences that can prevent the system from starting and require that you reinstall the system.

Authoritative Restore Selections

Use this page to mark individual Active Directory (AD) objects, a subtree, or the entire AD database as authoritatively restored. To mark AD objects, subtree, or the entire AD database as authoritative, Recovery Manager for Active Directory uses the capabilities provided by the **Ntdsutil.exe** tool supplied with Microsoft Windows. However, this tool included in Windows Server 2008 or higher does not support marking the entire AD database as authoritative.

- **Mark no objects as authoritatively restored.** Marks no restored objects as authoritative.
- **Mark the entire directory as authoritatively restored.** Marks the entire Active Directory database (both the domain and configuration naming contexts held by the domain controller) as authoritative. The schema cannot be authoritatively restored.
- **Mark a subtree or individual object as authoritatively restored.** Marks an individual object or a container along with all the objects it contains (a subtree) as authoritative. The object or container is defined by specifying its distinguished name in the **Distinguished name** box.

An authoritative restore is an advanced operation that affects the entire domain. Try to avoid using authoritative restore unless you realize all of its implications. With the Repair Wizard, the authoritative restore of the SYSVOL does not occur automatically after an authoritative restore of Active Directory, additional steps are required. For more information, see [Restoring SYSVOL authoritatively](#).

Computer Restart in Normal Mode

Use this page to specify how to restart the target computer in normal mode. Restarting the target domain controller in normal mode is required for the Active Directory restore to complete.

- **Let me restart computer later.** With this option, you must restart the target computer manually.
- **Restart the computer now.** Restarts the target computer remotely, using the boot option specified in the Boot option box. If you want to apply different startup parameters, restart the computer manually.

Completing the Repair Wizard

Use this page to view the operation results.

- **View Log.** Shows the restore results log. The purpose of the log is to facilitate troubleshooting.
- **Finish.** Click **Finish** to close the Repair Wizard.

To open the log file

- On the Completing the Repair Wizard page, click **View Log**. The log includes the following entries:
 - **Operation**. Type of the restore operation.
 - **Backup**. The path and name of the backup file.
 - **Created**. Date and time of the backup creation.
 - **Operation Started**. Date and time when the wizard started the restore.
 - **DIT Database restore started**. Under this entry you can view a list of files the wizard has restored.
 - **Operation completed**. Date and time when the wizard completed the restore.

The wizard saves the log file in the following folder: %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory\Repair.

Extract Wizard

The Extract Wizard helps you restore data from a backup to a specified folder. With this wizard, you can select the System State components you want to extract from the computer's backup and specify the destination folder for the extracted files.

The wizard has the following steps:

- [Backup Selection](#)
- [Folder Selection](#)
- [Operation Start](#)
- [Operation Progress](#)
- [Completing the Extract Wizard](#)

Backup Selection

Use this page to view a list of computers for which backups are available and to select a backup and System State components in the backup.

- **Locate the backup under computer name**. Provides a list of computers for which backups are available and allows you to select a backup to perform a restore. For the selected computer, the window lists all backups that are available in Recovery Manager for Active Directory. A backup entry includes the date and time when the backup was created, and displays the backup age in days. By selecting check boxes under a backup entry, you can extract individual components of the System State. The list only includes the backups that are registered in the Recovery Manager for Active Directory configuration database.
- **Register**. To register additional backups, click **Register**, and then click one from the following items:
 - **Register Backup File**. Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf) or Windows Server backup (.vhd, .vhdx).
 - **Register Backups in Folder**. Registers all backup files that are in the selected folder.

In the Extract Wizard, you can use backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas Backup Exec.

To select a backup

- Click the computer whose backup you want to use, double-click the backup you want to use, and select check boxes next to component names.

Folder Selection

Use this page to specify the folder where the wizard will restore the selected System State components.

- **Folder where to place the extracted files.** Provides a space for you to type the path to the folder where the wizard will place the extracted files.
- **Browse.** Click **Browse** to locate the folder on your computer or network.

Operation Start

This page provides an overview of the settings you have specified. Click **Back** to review or change your settings or click **Next** to start the operation.

Operation Progress

This page shows the operation progress. Wait while the wizard completes the operation.

Completing the Extract Wizard

This is the final page of the wizard. Click **Finish** to close the Extract Wizard.

Events generated by Recovery Manager for Active Directory

This section describes the events recorded by Recovery Manager for Active Directory to Recovery Manager for Active Directory log. Events can be logged both on the target domain controller and on the Recovery Manager for Active Directory computer.

- [Common Events](#)
- [Recovery Manager Console events](#)
- [Backup Agent events](#)
- [Management Agent events](#)
- [Restore Agent events](#)
- [Recovery Manager Portal events](#)
- [Forest Recovery Agent events](#)

- [Forest Recovery Console events](#)
- [AD Virtual Lab events](#)

Common Events

Table 45: Common events for agents

Event ID	Event type	Description
10000	Error	Failed to initialize the application log file. Error code: %22
10001	Error	An unexpected exception occurred. Error code: %22
4707	Information	Windows Firewall rule was added. Rule name: %27 Rule description: %28 Application name: %29 Service name: %30 Protocol: %31 Local ports: %32
4708	Error	An error occurred while configuring Windows Firewall. Error code: %22 Error text: %23
4709	Information	Windows Firewall rule %27 was removed.

Table 46: Common events for all components

Event ID	Event type	Description
10020	Error	An unhandled exception occurred in the function: %1. A crash dump file will be generated.
10021	Error	An unexpected exception occurred. Error code: %22 File location: %86
10022	Error	An unhandled exception occurred in the function: %85. A crash dump file will be generated.
10023	Error	Failed to generate the crash dump file. Error code: %22 Stage: %87 File location: %86
10024	Error	Crash dump file was generated successfully. File location: %86.

Recovery Manager Console events

Table 47: Recovery Console events

Event ID	Event type	Description
2100	Information	The backup session was finished successfully. Collection: %35 Scheduled: %36
2101	Error	The backup session was finished with errors. See previous events for details. Collection: %35 Scheduled: %36
2102	Warning	The backup session was finished with warnings. See previous events for details. Collection: %35 Scheduled: %36
2110	Information	The backup session was started. Collection: %35 Scheduled: %36 PID: %39
2111	Error	Error during backup. Target DC: %6 Collection: %35 Error text: %23 Error code: %22
2112	Error	Error during backup. Target host: %70 AD LDS instance name: %34 Collection: %35 Error text: %23 Error code: %22
2113	Warning	Warning during backup. Target DC: %6 Collection: %35 Warning text: %23 Warning code: %22
2114	Warning	Warning during backup. Target host: %70 AD LDS instance name: %34 Collection: %35 Warning text: %23 Warning code: %22

Event ID	Event type	Description
2120	Information	Domain controller %6 was restarted in Directory Services Restore Mode.
2121	Information	Computer %6 restart was initiated after the restore operation.
2122	Information	Computer %6 restart was not requested after the restore operation. Manual restart is required.
2130	Information	The Backup agent was successfully installed on %6. Account: %1 Port: %40
2131	Error	The Backup agent cannot be installed on %6. Description: %23
2135	Information	The Backup agent was successfully uninstalled from %6. Account: %1
2136	Error	The Backup agent cannot be uninstalled from %6. Description: %23
2150	Information	The online restore process was started. AD LDS instance name: %34 Restore method: %42 User: %1 Backed up DC: %43 Backup date: %13 Backup file: %12 Backup type: %41
2152	Information	The online restore process was successfully completed. AD LDS instance name: %34 Total number of the restored objects: %44
2160	Information	The online restore process was started. Target DC: %6 Restore method: %42 User: %1 Backed up DC: %43 Backup date: %13 Backup file: %12 Backup type: %41
2161	Information	The following objects were restored: %45
2162	Information	The online restore process was successfully completed. Target DC: %6 Total number of the restored objects: %44
2170	Information	The GPO restore operation was started. Target DC: %6

Event ID	Event type	Description
		Backup date: %13 Backup file: %12 Backup type: %41 GPOs list: <GPOs list>
2171	Information	The GPO restore operation was completed. Target DC: %6
2172	Error	The GPO restore operation failed. Target DC: %6 Description: %23
2180	Information	The offline restore process was started. Target DC: %6 Backup date: %13 Backup file: %12 Backup type: %41 Components to restore: %33
2181	Information	The offline restore process was successfully completed. Target DC: %6
2182	Error	The offline restore process failed.\n Target DC: %6 Description: %23
2200	Information	The backup was registered. Backup file: %12 Backup type: '%41'
2201	Information	The backup was deleted. Backup file: %12 Backup type: %41
2202	Warning	The session %92 was abandoned. Collection: %35 Scheduled: %36 Started: %93
2203	Error	The %9 object was not restored. %rReason:%23. Error text: %23 ObjectDN: %9
2204	Error	The online restore process was completed with errors. See previous events. Total number of the restored objects: %8 Total number of the failed objects: %7 restoredCount: %8 failedCount: %7

Event ID	Event type	Description
10003	Information	Console connected to '%89' on '%91' using authentication service '%90'.

Backup Agent events

Table 48: Backup Agent events

Event ID	Event type	Description
4701	Information	The backup of the %25 component was started. Instance name of the component: '%71'
4702	Information	The backup of the component %25 was successfully finished. Instance name of the component: '%71' Time spent: %26
4710	Information	The backup process was initiated by %1 from %24 for the following components: %33
4711	Information	The backup process was successfully completed. Backup path: %12
4712	Error	The backup process failed. Error text: %23
4713	Information	Preparing components for backup.
4714	Information	The preparation of components for backup was finished. Time spent: %26
4717	Information, Warning (depends on a component)	The component '%25' will not be backed up. Reason: %35
4718	Warning	The backup process was finished with warnings. Backup path: %12
4719	Information	The collection of cross-domain group membership information from %50 was started.
4720	Information	The collection of cross-domain group membership information from %50 was finished. Time spent: %26
4721	Warning	The collection of cross-domain group membership information from %50 was failed. Error text: %23 Time spent: %26

Management Agent events

Management Agent is used to deploy Backup Agent, Offline Restore Agent and Forest Recovery Agent. The agent logs events related to agent management operations, e. g. agent installation, uninstallation and upgrade.

Table 49: Management Agent events

Event ID	Event type	Description
4000	Information	The installation of the product "%78" was requested. MSI path: %75 Version: %62 Parameters: %76
4001	Information	The installation of the product %78 was finished with code %77
4002	Information	The upgrade of the product "%78" was requested. MSI path: %75 Parameters: %76 Current version: %79 New version: %62 Installed product code: %80 New product code: %81 Installed product upgrade code: %82 New product upgrade code: %83
4003	Information	The product %78 cannot be upgraded because the same version of the product is already installed.
4004	Information	The upgrade of the product %78 was finished with code %77.
4005	Information	The uninstallation of the product %78 was requested.
4006	Information	The uninstallation of the product %78 was finished with code %77.
4007	Warning	The product %78 cannot be uninstalled because the product does not exist on this computer.
4008	Error	An error occurred during the %3 operation. Error text: %23

Restore Agent events

Table 50: Restore Agent events

Event ID	Event type	Description
7001	Information	Online restore process was started. Source computer: %59 User: %1
7002	Information	The following objects were restored.

Event ID	Event type	Description
		%45
7003	Information	The online restore process was completed. Total number of the restored objects: %7
10002	Information	%89 started using authentication service %90.

Recovery Manager Portal events

Table 51: Recovery Manager Portal events

Event ID	Event type	Description
9000	Information	The %9 object was restored to %10. Initiated by %1
9001	Error	The %9 object was not restored to %10. Reason: %4 Initiated by %1
9002	Information	The batch restore operation was started. Number of objects: %7 Backup date: %13 RMAD console: %5 Domain controller: %6 Attributes to restore: %21 Initiated by %1
9003	Information	The batch restore operation was successfully finished. Number of restored objects: %7 Initiated by %1
9004	Error	The batch restore operation failed. Initiated by %1
9005	Warning	The batch restore operation partially completed. %8 out of %7 objects were successfully restored. Initiated by %1
9006	Information	The %9 object was successfully undeleted. Initiated by %1
9007	Error	The %9 object undelete operation failed. Reason: %4 Initiated by %1
9008	Information	The batch undelete operation was started.

Event ID	Event type	Description
		Number of objects: %7 RMAD console: %5 Domain controller: %6 Initiated by %1
9009	Information	The batch undelete operation was finished. Number of undeleted objects: %7 Initiated by %1
9010	Error	The batch undelete operation failed. Initiated by %1
9011	Warning	The batch undelete operation was partially completed.%8 out of %7 objects were successfully undeleted. Initiated by %1
9012	Information	The search operation was started. Search string: %14 Initiated by %1
9013	Information	The search operation was finished. Search string: %14 Number of found objects: %7.
9014	Error	The search operation was failed. Search string: %14 Reason: %4
9015	Information	The search operation was cancelled. Search string: %14
9016	Information	Delegation setting for %20 was changed. Resource: %19 Operation: %18 Access: %73 Initiated by %1
9017	Information	Delegation setting for %20 was deleted. Resource: %19 Operation: %18 Initiated by %1
9018	Information	Recovery Portal configuration was changed. Server: %74. Administrator: %66 Operation: %18 Initiated by %1

Forest Recovery Agent events

Table 52: Forest Recovery Agent events

Event ID	Event type	Description
1600	Information	Resetting the passwords for domain controllers.
1601	Information	Resetting the Kerberos password.
1604	Information	Removing metadata and the domain controllers that have not been restored.
1608	Information	Starting the Active Directory reinstallation...
1609	Information	The computer is being rebooted in Directory Services Restore mode.
1610	Information	The computer is being rebooted in the Normal mode.
1611	Information	The domain controller demotion was started.
1626	Error	The Active Directory reinstallation failed. Details: %1
1627	Error	The supplied backup protection password is invalid.
1628	Error	The domain controller demotion failed. Details: %1
1645	Error	The supplied DSRM password does not meet the password complexity requirements.
1646	Error	The specified DNS server was not available.
1647	Error	DC was restarted in the wrong mode (Normal). The required mode is DSRM.
1648	Error	DC was restarted in the wrong mode (DSRM). The required mode is Normal.
1649	Information	Invalidating the RID pool.
3101	Error	Cannot access the backup file %12.
3102	Information	DNS configuration completed with addresses %48.
3103	Error	Cannot prepare the backup file %12. Details: %23.
3104	Information	Removing the domain %50.
3105	Error	Cannot remove the domain %50. Details: %23
3106	Information	Domain Controller unisolation was started.
3107	Information	Domain Controller isolation was started.
3108	Information	Disabling the Windows Update service.
3109	Information	Enabling the Windows Update service.
3110	Information	Seizing FSMO roles %51.
3111	Information	The RID pool value was increased from %54 to %55.
3112	Information	Stopping the service %52.
3113	Information	Starting the test operation.

Event ID	Event type	Description
		Backup path: %12. Preferred DNS servers:%48. Temp storage: %49.
3114	Information	Preparing the backup file. Backup path: %12. Preferred DNS servers:%48. Temp storage: %49.
3115	Information	Restoring from a backup %12.
3116	Error	Forest Recovery Agent installation failed. Details: %23.
3117	Error	Cannot access the temporary backup folder %49. Details: %23.
3118	Information	Operation %3 execution was started.
3119	Information	Operation %3 was completed successfully.
3120	Error	Operation %3 failed. Details: %23.
3121	Error	The operation %3 was canceled by the user.
3122	Information	Specifying the DNS server settings. Preferred DNS Servers: %48, alternate DNS servers: %61.
3123	Error	The test operation failed. See previous events for details.
3124	Information	Disabling the Global Catalog server for the domain controller %6
3125	Information	Enabling the Global Catalog server for the domain controller %6
3126	Information	Disabling the Global Catalog server for this domain controller.
3127	Information	Enabling the Global Catalog server for this domain controller.
3128	Information	Resetting the trusts passwords for the domain %50.
3129	Information	Resetting the password for the domain controller %6.
3130	Information	DSRM password was set successfully.
3131	Error	Cannot delete the copied backup file %12. Details: %23.
3132	Error	Cannot delete the IPsec backup file %12. Details: %23.
3133	Error	The specified DNS servers %48 are not available.
3134	Information	Current IpSec rules were backed up to %12.
3135	Information	Starting the Active Directory reinstallation. Administrator name: %66, replication source domain controller:%6, replica domain DNS name:%64, site name:%65, enable GC after install: %67
3136	Information	BitLocker drive encryption was successfully disabled for volume %72.
3137	Error	Cannot disable BitLocker drive encryption for volume %72. Details: %23.
3138	Information	BitLocker drive encryption was successfully enabled for volume %72.

Event ID	Event type	Description
3139	Error	Cannot enable BitLocker drive encryption for volume %72. Details: %23.
3140	Information	Custom password filters were successfully enabled.
3141	Error	Cannot enable custom password filters. Details: %23.
3142	Information	Custom password filters were disabled successfully.
3143	Error	Cannot disable custom password filters. Details: %23.
3144	Information	Metadata for the domain controller %6 was successfully removed.
3145	Information	Metadata removing for the domain controller %6 completed with warnings: %38.
3146	Error	Cannot set the DSRM password. Details: %23.
3147	Information	Password for the krbtgt account was reset successfully.
3148	Error	Cannot reset the password for the krbtgt account. Details: %23.
3149	Error	Cannot validate the backup file. Details: %23.
3150	Information	The test operation was successfully completed.
3151	Information	The Active Directory reinstallation successfully completed.
3152	Information	The domain controller was successfully demoted.
3153	Information	Resetting the passwords for trusts.
3154	Information	Set service %52 start type to %88.
3155	Error	Cannot change start type for service %52. Details: %23.
10002	Informational	%89 started using authentication service %90.

Forest Recovery Console events

Table 53: Forest Recovery Console events

Event ID	Event type	Description
5000	Informational	Forest Recovery project was created: %56.
5001	Informational	Forest Recovery project was updated: %56.
5002	Informational	Recovery project validation was started: %56. Method %63.
5003	Informational	Forest Recovery project %56 was successfully validated. Domain Controller: %6
5005	Error	Forest Recovery project %56 validation failed. See previous events for details.
5006	Error	Forest Recovery operation failed: %18.

Event ID	Event type	Description
		Domain Controller: %6, Details: %23
5007	Informational	The recovery process was started using the following method: %63 Domain Controller: %6, Backup file: %12, Forest Recovery project %56
5008	Informational	Recovery process was finished. Domain Controller: %6, Forest Recovery project %56
5010	Error	Recovery process failed. See previous events for details. Domain Controller: %6, Forest Recovery project %56.
5011	Informational	Operation: %18 was canceled, Domain Controller %6.
5012	Informational	Operation: %18 was retried, Domain Controller %6.
5013	Informational	Operation: %18 was paused, Domain Controller %6.
5014	Informational	Operation %18 was unpaused, Domain Controller %6.
5015	Informational	%18, Domain Controller: %6.
5016	Informational	Forest Recovery Agent operation: %18 was finished successfully. Domain Controller %6, Version: %62
5017	Error	Forest Recovery Agent operation failed: %18 Domain Controller %6, Version: %62
5018	Informational	Health check was started. Active Directory Forest: %75, Forest Recovery Project %56
5019	Informational	Health check was completed successfully. Active Directory Forest: %75, Forest Recovery Project %56
5020	Error	Health check was failed. Domain Controller %6, Details: %23

Event ID	Event type	Description
5021	Error	Scheduled project operation failed to start. Project: %56 Operation: %18 Details: %23
5022	Informational	The recovery process was resumed by the Forest Recovery Console instance %95. The original console instance where the recovery process was initiated: %94 .
10003	Informational	Console connected to %89 on %91 using authentication service %90.

AD Virtual Lab events

Table 54: Active Directory Virtual Lab events

Event ID	Event type	Description
6100	Information	New Virtual Lab Project was created: Project: %56
6101	Information	Virtual Lab Project was changed: Project: %56
6102	Information	Virtual Lab Project successfully connected to %57 hypervisor. Address: %58 User: %66 Project: %56
6103	Error	Virtual Lab Project cannot connect to %57 hypervisor. Address: %58 User: %66 Error: %23 Project: %56
6104	Information	Source machine was added to the Virtual Lab Project. Machine: %59 Project: %56
6105	Information	Source machine was removed from the Virtual Lab Project. Machine: %59 Project: %56
6110	Information	Forest Recovery Agent was installed on %59.
6111	Error	Forest Recovery Agent installation failed on %59: %23
6112	Information	Forest Recovery Agent was uninstalled on %59.
6113	Error	Forest Recovery Agent uninstallation failed on %59: %23
6114	Information	VMware agent was installed on %59.
6115	Error	VMware agent installation failed on %59: %23

Event ID	Event type	Description
6116	Information	VMware agent was uninstalled on %59.
6117	Error	VMware agent uninstallation failed on %59: %23
6118	Information	SCVMM agent/Disk2Vhd tool was installed on %59.
6119	Error	SCVMM agent/Disk2Vhd tool installation failed on %59: %23
6120	Information	SCVMM agent/Disk2Vhd tool was uninstalled on %59.
6121	Error	SCVMM agent/Disk2Vhd tool uninstallation failed on %59: %23
6201	Information	Virtual Lab project settings were successfully verified. Project: %56
6202	Error	Virtual Lab project settings verification failed: Error(s): %37 Warning(s): %38 Project: %56
6203	Warning	Virtual Lab project settings verification was finished with warning(s): %38 Project: %56
6299	Warning	Virtual Lab project settings verification was finished with warning(s) but it was ignored. Then the lab creation was started. Project: %56
6300	Information	Virtual Lab project lab creation was started. Project: %56
6301	Error	Virtual Lab project lab creation failed. Failed targets: %37 Project: %56
6302	Error	Virtual machine creation failed. Machine: %59 Error: %23
6303	Information	Virtual Lab creation was successfully finished. Created targets: %68 Project: %56
6304	Warning	Virtual machine creation was interrupted by a user. Machine: %59
6401	Informational	Virtual machine network was enabled. Machine: %59
6402	Error	Enabling virtual machine network failed. Machine: %59 Error: %23

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product