Quest Recovery Manager for Active Directory
10.3

User Guide

© 2023 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, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Updated – March 2023

Contents

Overview **10**
About Quest® Recovery Manager for Active Directory 10
Features and benefits 10
Comprehensive Active Directory® recovery options 11
AD LDS (ADAM) recovery 11
Granular selective restore 11
Integration with On Demand Recovery 11
Group Policy recovery 11
Integrity checks for Backups 12
Centralized remote administration 12
Audit of objects and operations 12
Integration with Change Auditor for Active Directory 13
Fault tolerance 13
Management Shell 13
Scheduling and automation 13
Scalability and performance 14
Technical overview 14
Creating backups 14
Backup Storage 15
Backup Agent 16
Recovering Active Directory 17
Recovering Group Policy 18
Comparison reports 19

Getting started **20**
Permissions required to use Recovery Manager for Active Directory 20
Recovery Manager Console 25
Getting and using help 27
Configuring Windows Firewall 27
Manual method 28
Automatic method 30
Using Computer Collections 31
Creating Computer Collections 32
Renaming Computer Collections 32
Modifying Computer Collection properties 32
Deleting Computer Collections 32
Specifying an access account for Backup Agent and backup storage 33
Adding domain controllers to a Computer Collection 34
Adding containers to a Computer Collection 35

Adding AD LDS (ADAM) hosts and instances to a Computer Collection 36
Removing items from a Computer Collection 37
Hybrid Recovery with On Demand Recovery 37
About the Hybrid Connector 37
TLS 1.2 for Hybrid Connector 38
What can be restored using hybrid recovery 38
Managing Recovery Manager for Active Directory configuration 43
Preparing for working with Active Directory® or AD LDS (ADAM) backups 44
How to ensure that required DLLs are available 44
Settings 44
Default properties for Computer Collections 49
Properties for an existing Computer Collection 49
Container and site properties 59
Sessions node properties 61
Forest properties 62
Domain properties 62
Domain controller properties 63
AD LDS (ADAM) partition properties 63
AD LDS (ADAM) instance properties 64
Showing or hiding AD LDS (ADAM) partitions 64
Showing or hiding domains 64
Showing or hiding sites 65
Licensing 65
Installing license key file 65
Updating license key file 66
Revoking licenses 66

Backing up data 66
Permissions required for the Backup operation 67
Managing Backup Agent 67
Installing Backup Agent automatically 68
Preinstalling Backup Agent manually 69
Discovering preinstalled Backup Agent 70
Updating Backup Agent information 70
Upgrading Backup Agent 70
Uninstalling Backup Agent 71
Removing a Backup Agent entry from the Backup Agent Management node 71
Using a least-privileged user account to back up data 71
Using Managed Service Accounts 72
Active Directory backups vs Windows System State backups 74
Creating BMR and Active Directory backups 74
Creating Active Directory® backup 75
Creating BMR backups 75
Usage of backup access credentials 78
Using the Backup Wizard 80
Retrying backup creation 81
Enabling backup encryption 81
Backing up AD LDS (ADAM) 84

Method 1: Back up AD LDS (ADAM) from the Recovery Manager Console 84
Method 2: Schedule backup creation for AD LDS (ADAM) 84
Backing up cross-domain group membership.....85
Backing up distributed file system (DFS) data 86
Backup scheduling 86
Task scheduler overview 86
Setting performance options 89
Setting advanced backup options 89
Unpacking backups.....90
Configuring default settings to unpack backups.....90
Configuring Computer Collection-specific settings to unpack backups 91
Unpacking a backup manually.....91
Deleting data unpacked from a backup 91
Using e-mail notification 92
Viewing backup creation results 93
Sessions node properties 93
Computer properties 94
Computer session properties.....94
Backups node properties.....95
Filtering backups 96
Integrity checks for Active Directory, Bare Metal, and AD LDS (ADAM) backups 98
Export List of Active Directory, Bare Metal, and AD LDS (ADAM) backups 102
Properties of registered Active Directory, Bare Metal, and AD LDS (ADAM) backups...103

Restoring data 105
Getting started with Active Directory® recovery 105
Active Directory recovery options 106
Implications of the online restore.....107
Using agentless or agent-based method.....108
Managing deleted or recycled objects 111
Recovering deleted objects 112
Recycling deleted objects.....113
Recovering recycled objects.....113
Restoring backed up Active Directory® components 114
Integration with Change Auditor for Active Directory 114
Using granular online restore.....118
Online Restore Wizard overview 119
Restoring AD LDS (ADAM) 121
Method 1: Restore an AD LDS (ADAM) instance from a backup created with Recovery Manager for Active Directory 122
Method 2: Restore an AD LDS (ADAM) database from a backup created with third-party software 122
Selectively restoring Active Directory® object attributes 123
Restoring objects in an application directory partition 124
Restoring object quotas 125
Restoring cross-domain group membership.....126
Performing a restore without having administrator privileges 126

Reports about objects and operations 127
Reports about Active Directory® objects....127
Reports about AD LDS (ADAM) objects....128
Reports about Group Policy objects....128
Data about who modified Active Directory® objects 129
Using complete offline restore 129
Repair Wizard overview....130
Offline restore implications....131
Non-authoritative restore 131
Authoritative restore 132
Restoring SYSVOL authoritatively 132
Performing a granular restore of SYSVOL....134
Recovering Group Policy 134
Group Policy Restore Wizard overview....135
Restoring data from third-party backups....135
Using the Extract Wizard....135
Creating a Windows Server® 2008 R2-based domain controller from a backup....136
Creating a Windows Server® 2012-based domain controller or higher from a backup ..137
Restoring passwords and SID history....138
Preserving passwords and SID history in object tombstones 138

Full Replication 139
Configure the full replication in Recovery Manager Console 141

Consolidating backup registration data 144
Configure replication of backup information in Recovery Manager Console 145

Monitoring Recovery Manager for Active Directory....148
Supported versions of Microsoft Operations Manager 148
Importing Management Pack....148
Rules provided in Microsoft System Center Operations Manager....149
Health dashboards....150

Using Management Shell....152
About Management Shell....152

Collecting diagnostic data for technical support 152
Step 1: Use Diagnostic Data Collector to automatically gather data 153
Step 2: Gather remaining data manually 153

Appendices....154
Frequently asked questions 154
Why do I need to restore deleted users or groups, rather than re-create them?....155
How can I restore a user or group in Active Directory®?....155
How does online restore work? 155
When an object is undeleted, what is restored from the tombstone and what is restored from the backup?....155
What's the difference between an online restore and an authoritative restore? 156

What's the difference between the agentless restore method and the agent-based restore method? 156
Can I undelete a mailbox-enabled user? 157
In the Group Policy Restore Wizard, a GPO link is shown as deleted, but the link actually exists in Active Directory. What's wrong? 157
What is a primary restore of the SYSVOL? 157
How do I change the Backup Agent port number? 157
Best practices for using Computer Collections 158
Technical characteristics 159
Typical backup creation times 159
Typical times to unpack backups 160
Typical sizes of databases 160
Best practices for creating backups 161
Develop a backup and restore plan 161
Determine which domain controllers to back up and how often 161
Methods for deploying Backup Agent 161
Retain recent backups 162
Where to store backups 162
Ports Used by Recovery Manager for Active Directory 164
Backup wizard 165
What to Back Up 166
Where to Store Backups 167
When to Back Up 167
Computer Collection Name (optional) 167
Completing the Backup Wizard 168
Online Restore Wizard 168
Wizard Operation Mode 170
Domain Selection 170
Backup Selection 171
Backup for Comparison (optional) 171
Unpacked Backups Folder Selection 172
Backup Data Preparation 172
Domain Access Options 173
Objects to Be Processed 173
Action Selection 175
Action Selection (Compare two backups) 175
Processing Options 175
Additional Options 176
Operation Start 177
Operation Progress 177
Operation Option (if the Compare, analyze, and optionally restore was selected in Action Selection dialog) 179
Objects to Be Restored 181
Where to Restore Deleted Objects 182
Operation Results 182
Completing the Online Restore Wizard 182
Online Restore Wizard for AD LDS (ADAM) 183
Wizard Operation Mode 185

AD LDS (ADAM) Instance Selection 185
Backup Selection 185
Backup for Comparison 186
Unpacked Backups Folder Selection 186
Backup Data Preparation 186
AD LDS (ADAM) Access Options 187
Objects to Be Processed 187
Action Selection 188
Processing Options 188
Additional Options 189
Operation Start 189
Operation Progress 190
Operation Option 190
Objects to Be Restored 190
Where to Restore Deleted Objects 191
Operation Results 191
Completing the Online Restore Wizard for AD LDS (ADAM) 191
Group Policy Restore Wizard 192
Domain Selection 192
Backup Selection 192
Backup Data Preparation 193
Select Domain Controller 193
Group Policy Object Selection 193
GPO Restore Options 194
Link Restore Options 194
Restore Process Start 195
Completing the Group Policy Restore Wizard 195
Repair Wizard 195
Computer and Backup Selection 196
Target Computer 197
Computer Restart 198
Primary Restore of SYSVOL 199
Restore Process Start 199
Restore Progress 199
Authoritative Restore Selections 199
Computer Restart in Normal Mode 200
Completing the Repair Wizard 200
Extract Wizard 200
Backup Selection 200
Folder Selection 201
Operation Start 201
Operation Progress 201
Completing the Extract Wizard 201
Events generated by Recovery Manager for Active Directory 201
Common Events 202
Recovery Manager Console events 202
Backup Agent events 204
Management Agent events 205

Restore Agent events 205

About us.....207

Overview

- About Quest® Recovery Manager for Active Directory
- Features and benefits
- Technical overview

About Quest® Recovery Manager for Active Directory

It is crucial for any modern business to maintain the availability of its network-computer environment at all times. Unplanned downtime caused by a disastrous event, such as a directory service malfunction, can severely disrupt the operation of a business. Therefore, business-critical infrastructures demand the ability to recover failed systems and services in the shortest possible time.

Recovery Manager for Active Directory (RMAD) employs advanced technologies to minimize the downtime caused by the corruption or improper modification of Active Directory®, Active Directory Lightweight Directory Services (AD LDS), formerly known as Active Directory Application Mode (ADAM), and Group Policy data. This product allows for automatic backup, and fast, remotely managed recovery of data stored in Active Directory®.

Recovery Manager for Active Directory (RMAD) dramatically reduces the time required to restore Active Directory®, AD LDS (ADAM), and Group Policy data. This improves the availability of corporate networks and reduces network downtime. Given that the time required to recover Active Directory® using a conventional full-backup tool is typically a few hours, Recovery Manager for Active Directory offers huge savings on time, productivity, and administrative overhead.

Features and benefits

Recovery Manager for Active Directory (RMAD) 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.

RMAD allows for quick, online recovery of data. In enterprise 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 Active Directory backups
- Active Directory®, AD LDS (ADAM), or Group Policy comparison reporting and troubleshooting

RMAD 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.

RMAD 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 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 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 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 ensures that the restored object is a member of the proper groups.

Recovery Manager for Active Directory supports granular online restore from Bare Metal Recovery (BMR) backups.

Integration with On Demand Recovery

From version 9.0, Recovery Manager for Active Directory can be integrated with On Demand Recovery 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.

Group Policy recovery

One of the key features of Recovery Manager for Active Directory (RMAD) is the ability to quickly recover individual Group Policy objects using a backup of domain controller AD components, eliminating the need for special, Group Policy-related backups. By providing straightforward, wizard-driven procedures for Group Policy restoration, RMAD 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.

Integrity checks for Backups

Recovery Manager for Active Directory supports Integrity checks for Active Directory® backups.

When a backup is created, a checksum is calculated for the backup file and saved in the backup file when the backup is registered. An integrity check recalculates the checksum and compares it to the checksum stored in the backup file.

The following statuses can be displayed after running the integrity check:

Status	Description
Passed	The newly calculated checksum value matches the previously calculated checksum stored in the backup file.
Unknown	The integrity check was not performed.
Running	The integrity check is in progress.
Failed	The backup is not accessible (wrong credentials) or may have been moved from the path.
No Checksum	The previously calculated checksum could not be read. This could be due to the backup being created by a previous version of the product. The backup also may have been damaged in such a way that the checksum was also affected.
Corrupted	The newly calculated checksum value does not match the previously calculated checksum stored in the backup file.

Centralized remote administration

Recovery Manager for Active Directory 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 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 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 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.

Integration with Change Auditor for Active Directory

To provide information on who modified particular Active Directory® objects, Recovery Manager for Active Directory integrates with Change Auditor and includes the Change Auditor data into the reports.

From version 10.0.1, Recovery Manager for Active Directory restores the deleted object(s) and restores the last change (if any) that was made to the object attributes after creating the backup, using the data from the Change Auditor database. This functionality is based on the auditing capability provided by Change Auditor 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 auditing.
You can find out more about Change Auditor for Active Directory at http://quest.com/products/changeauditor-for-active-directory.

For details about this feature, see Integration with Change Auditor for Active Directory.

Fault tolerance

Recovery Manager for Active Directory provides the following features that allow the product to continue operating without interruption in case of any failure:

- Switch from the initial Recovery Manager Console to an alternate instance of the console in case of any system failure. For more information, see Full replication.
- Consolidate backup information from multiple backup registration databases on a single Recovery Manager for Active Directory computer. For details, refer Consolidating backup registration data.

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 (RMAD) 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, RMAD relies on Task Scheduler - the Windows scheduler service. A unified graphical interface and wizard assistance provide easy access to the backup scheduling features of RMAD.

RMAD makes the creation of backups a straightforward task. Once the backup creation options and scheduling are set up, the backup creation process becomes an automatic, unattended operation.

Scalability and performance

Recovery Manager for Active Directory 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 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.

Technical overview

Recovery Manager for Active Directory performs the following functions:

- Regular backup of domain controllers' components across a network, including the Active Directory database, SYSVOL and Registry, and maintenance of one or more secure repositories containing the backed-up Active Directory 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 (RMAD) provides the facility to create backups of the Active Directory® components on domain controllers, including the Active Directory® database and Windows Server® Bare Metal Recovery (BMR) backups.

Both types of backups can be created for any Active Directory® domain controller available on the network. Backup creation is a task that can be performed on a regular basis without interrupting the operation of the domain controller.

RMAD 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.

For Active Directory® backups, it is not necessary to maintain a single, centralized repository: several repositories, perhaps based on the site topology, can make your deployment more WAN-friendly. To minimize bandwidth consumption, RMAD employs agents that compress the data to be backed up, before sending it across the network.

Backup encryption

RMAD allows backups to be encrypted and protected with a password, to prevent unauthorized access. This password is used to generate a passphrase with which the backup is encrypted.

For Active Directory® 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 RMAD 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

RMAD 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 RMAD 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 Storage

Backups created with Recovery Manager for Active Directory can be stored in multiple locations. Primary storage of backups allows for backup files to be saved on a distributed network, or on selected computers with physically restricted access. Recovery Manager considers these locations as primary storage and is referred to as Tier 1 storage.

Primary Storage (Tier 1)

Recovery Manager for Active Directory provides options for primary storage in local and remote locations. Local storage is refers to storage on the Recovery Manager console computer, where remote storage is storage on the backed up domain controller or other remote servers on network shares. These locations are remote due to not

being on the Recovery Manager console computer. See the Local Storage tab and Remote Storage tab. For both local and remote storage locations, a primary backup path can be provided and an alternate backup path.

Primary storage is for the original backup files to be saved to the a safe location. For primary storage, the backup agent creates the backup file, compresses the data and then the file is saved to the configured storage locations. In the diagram below see line number **1** to view the process that is taken to save the backup file to primary storage locations. The RPC protocol is used to save backups files to the console computer. For saving to remote storage locations SMB protocols are used.

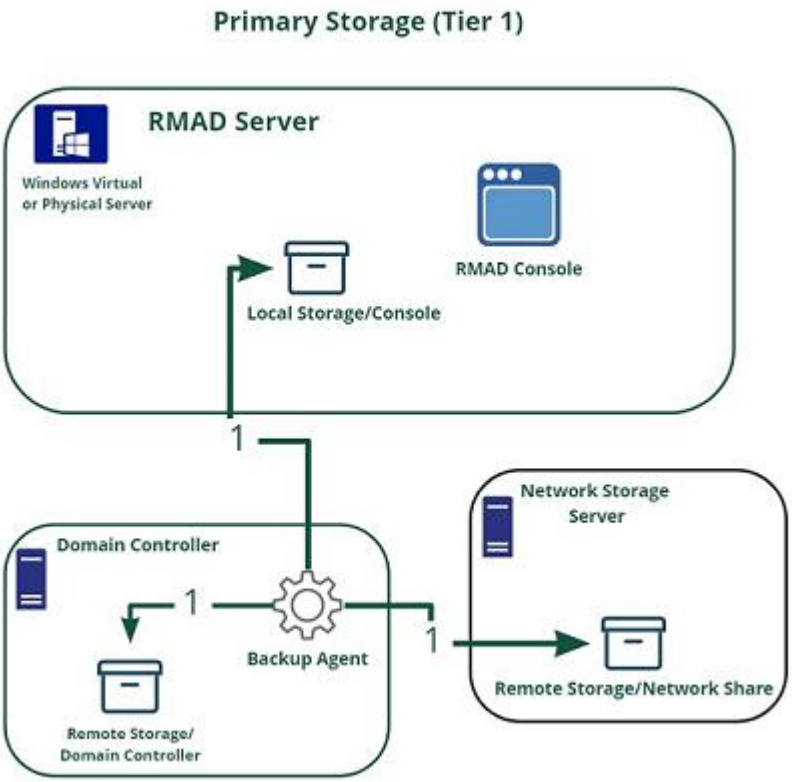


Figure: Primary Storage for Backups

The figure illustrates how Recovery Manager for Active Directory creates and saves backup files to primary storage locations.

Backup Agent

NOTE **For Recovery Manager for Active Directory 10.1 or higher**: Make sure that you use the Backup Agent version supplied with this release of Recovery Manager for Active Directory.

Recovery Manager for Active Directory 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. RMAD 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.

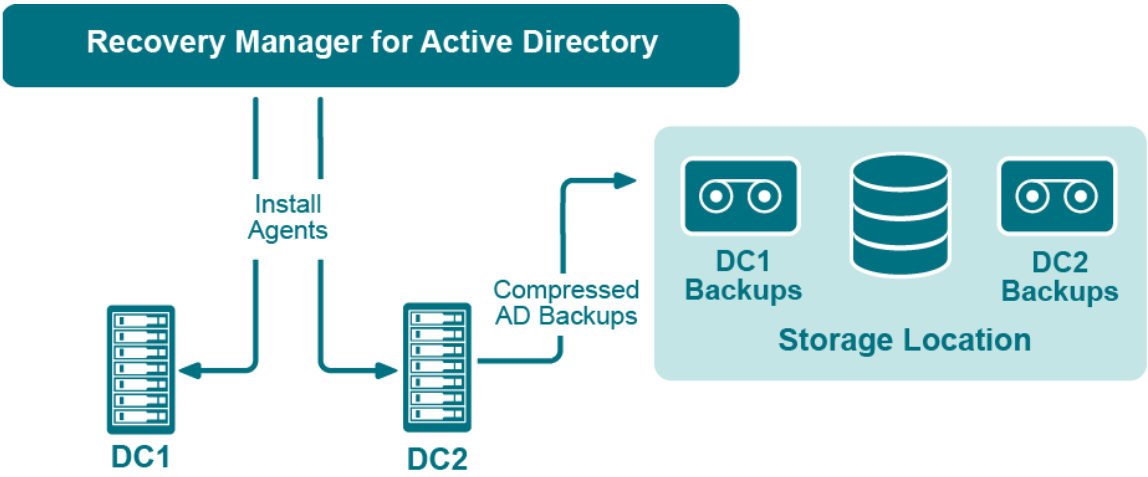


Figure: Backup Agents

The Recovery Manager for Active Directory (RMAD) employs a Backup Agent when creating backups. The Backup Agent is installed on domain controllers DC1 and DC2 and compresses the data and transfers the compressed data to 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

RMAD allows to run Backup Agent in the security context of a specific user account. Since RMAD needs administrative access to the domain controller in order to run Backup Agent, the account under which RMAD 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 RMAD 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

RMAD 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 RMAD 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 RMAD is running, solving the so-called “no trust” problem.

NOTE **For Recovery Manager for Active Directory 10.3 or higher**, the option to **Use preinstalled Backup Agent** is selected by default for all new computer collections.

Recovering Active Directory

Recovery Manager for Active Directory (RMAD) 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 RMAD should only be performed by highly trusted directory administrators.

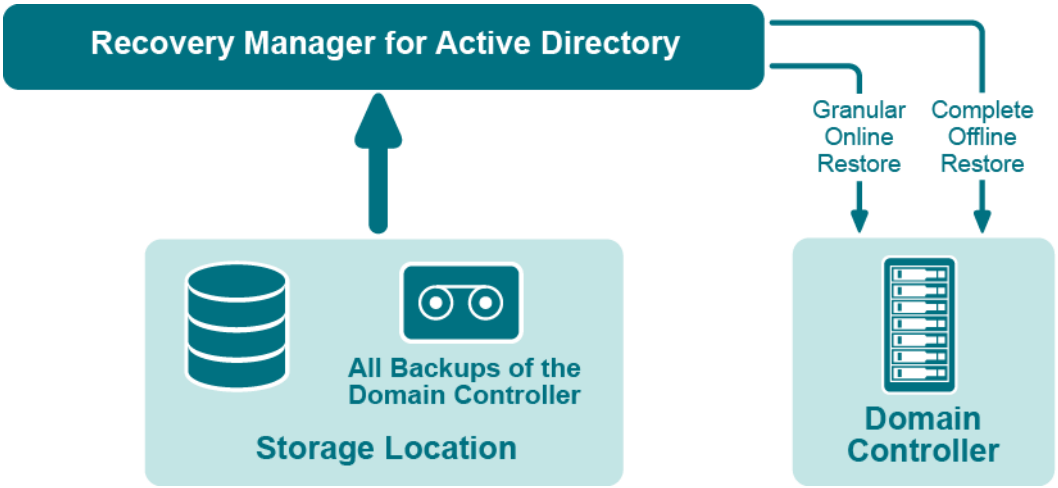


Figure: Recovering Active Directory

If certain objects are inadvertently deleted or modified in Active Directory, they can be restored from a backup of domain controller's Active Directory® components, 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 Active Directory® backup created for that domain controller. All the restore operations are administered remotely.

Recovery Manager for Active Directory 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.

Recovery Manager for Active Directory supports granular online restore from BMR backups.

Recovering Group Policy

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

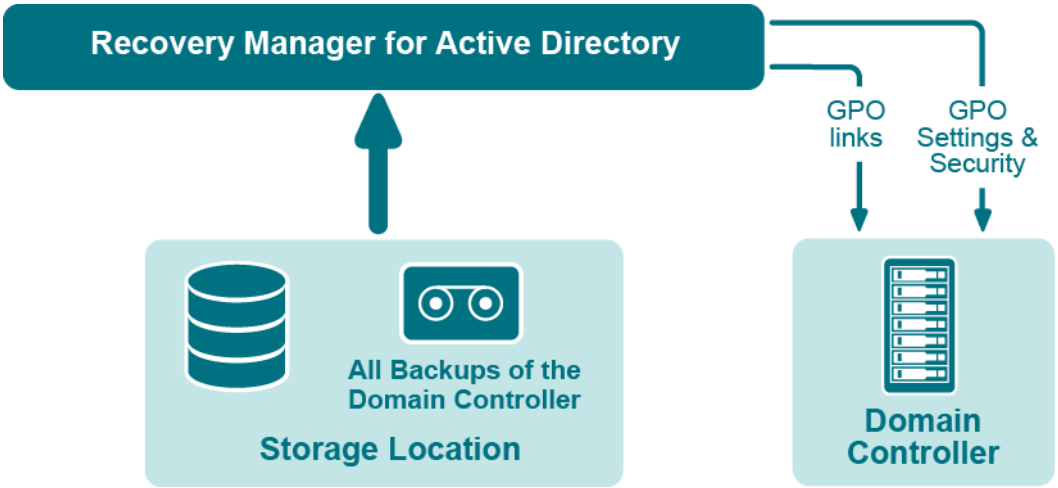


Figure: Group Policy Recovery

If specific Group Policy objects or links are inadvertently deleted or modified, they can be restored from a backup of a domain controller's Active Directory® components, without restoring the entire Active Directory®, restarting the domain controller, or affecting other objects.

Recovery Manager for Active Directory 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, RMAD 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 domain controller's Active Directory® components.

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 Active Directory® 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 (RMAD) 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.

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.

RMAD 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
- 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

NOTE From version 8.8, Recovery Manager for Active Directory (RMAD) supports environments with disabled NTLM authentication and the Protected Users Security Group.

The following user account permissions are required to perform some common tasks with RMAD.

Table 1. Backup Permissions

Action	Computer	Permissions Needed
Discover preinstalled Backup Agent instances	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Uninstall Backup Agent	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Update information displayed about Backup Agent in the Recovery Manager Console	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Automatically install Backup Agent and back up Active Directory data	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Back up Active Directory using preinstalled Backup Agent	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.

Table 2. Restore Permissions

Action	Computer	Permissions Needed
Perform a complete offline restore of Active Directory by using the Repair Wizard	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Perform a selective online restore of Active Directory objects - Agentless restore	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.
Perform a selective online restore of Active Directory objects - Agent-based restore	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Be a member of the Backup Operators group in the domain associated with the target domain controller.

Table 3. Backup and Restore AD LDS (ADAM) Permissions

Action	Computer	Permissions Needed
Automatically install Backup Agent and back up an AD LDS (ADAM) instance	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Local Administrator on computer hosting AD LDS (ADAM).

Action	Computer	Permissions Needed
Back up an AD LDS (ADAM) instance using preinstalled Backup Agent	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Local Administrator on computer hosting AD LDS (ADAM).
Restore an AD LDS (ADAM) instance	RMAD computer	**Write** permission to the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder. Local Administrator on computer hosting AD LDS (ADAM).

Table 4. RMAD cmdlets Permissions

Action	Computer	Permissions Needed
Run Recovery Manager for Active Directory cmdlets	RMAD computer	**Write** permission to the **%ProgramData%\Quest\Recovery Manager for Active Directory** folder.

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 RMAD. If during the installation you specify an existing SQL Server instance, the account with which RMAD 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 RMAD:

- Insert
- Delete
- 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

The account you use to access the target computer must be a member of the local Administrators group on that computer.

Discover preinstalled Backup Agent instances

The account used to access the target domain controllers must:

- Have the **Write** permission on the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD computer.
- Be a member of the Backup Operators group on each target domain controller.

Uninstall Backup Agent

The account used to access the target domain controllers must:

- Have the **Write** permission on the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD computer.
- Be a member of the Backup Operators group on each target domain controller.

Update information displayed about Backup Agent in the Recovery Manager Console

The account used to access the target domain controllers must:

- Have the **Write** permission on the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD computer.
- 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 the **Write** permission on the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder located on the Recovery RMAD 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 **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD 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 **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder located on the RMAD computer.

Perform a selective online restore of Active Directory objects

Agentless restore (used by default in Online Restore Wizard)

The account used to access target domain controllers must:

- Have the **Write** permission on the **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD 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.
- Replicating Directory Changes permission.

For more details, see Agentless method.

Agent-based restore

- The account used to access target domain controllers must have domain administrator rights.

For more details, see Agent-based method.

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 **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder that is located on the RMAD 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 **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder located on the RMAD 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 **%AllUsersProfile%\Quest\Recovery Manager for Active Directory** folder located on the RMAD computer.
- Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance.

Access the SQL reporting database

To access the SQL reporting database (%ProgramData%\Quest\Recovery Manager for Active Directory\DBReporting\RecoveryManager-Reporting-<host name>), the account must be assigned to db_datareader, db_datawriter roles and have rights to run all the usp_* procedures, as follows:

- usp_GetSummaryReportBody
- usp_GetSessionErrors
- usp_GetReportsList
- usp_GetReportsHeader
- usp_GetReportBody
- usp_GetReplicationHistory
- usp_GetOptionalObjects
- usp_GetOptionalAttributes
- usp_GetObjectChildren
- usp_GetObjectAttributes
- usp_GetAllObjects
- usp_GetAllChildObjects
- usp_GetAllAttributes

Run Recovery Manager for Active Directory cmdlets

Verify that the user account under which you run RMAD Management Shell console has the **Write** permission to the **%ProgramData%\Quest\Recovery Manager for Active Directory** folder. Otherwise, you will get warning messages when you run the snap-in cmdlets.

Recovery Manager Console

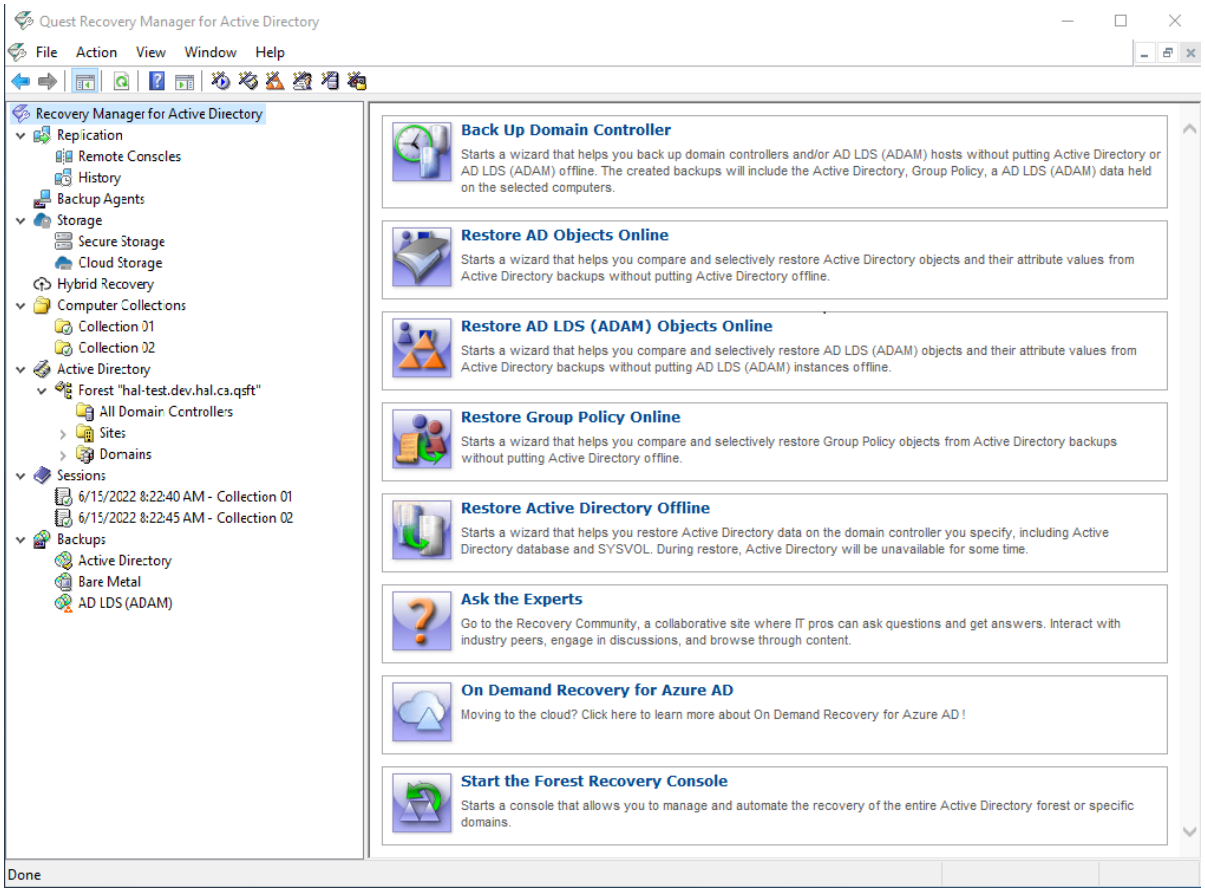
Recovery Manager for Active Directory (RMAD) includes an MMC snap-in (also known as the Recovery Manager Console) to ensure intuitive operation and close integration with the Windows® operating system.

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 object search in a backup during the online restore operation may fail.

To start the Recovery Manager Console

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 Full replication and Consolidating backup registration data.
- **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 RMAD. 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, AD LDS (ADAM) backups registered in the backup registration database of RMAD. 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.

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 (RMAD), preventing you from backing up or restoring data. Before you start using RMAD, make sure your firewall does not block traffic on ports used by RMAD.

This section provides instructions on how to configure built-in Windows Firewall on a the domain controllers to be backed up, so that RMAD could back up data on that computer.

The section covers the following methods:

- Manual method
- Automatic method

Manual method

For each of the following agents, you must create the specified firewall rules to allow traffic on ports used by RMAD. For descriptions of each firewall rule, see the table below.

Backup Agent:

- If you have a preinstalled Backup Agent, create Rule 3 and specify **BackupAgent64.exe** in the **Program path** parameter.
- If you have an automatic Backup Agent installation, create Rule 3 and specify **ErdAgent.exe** instead of <backup agent> in the **Program path** parameter.
- If you use the specified Backup Agent port, you need to configure Rule 1 and Rule 3. In Rule 3, specify <specific TCP port> for the Backup Agent in the **Local ports** parameter.
- If you use the RPC dynamic port range for the Backup Agent, configure Rule 1, Rule 2, and Rule 3. In Rule 3, specify the <RPC dynamic port range> for the Backup Agent in the **Local ports** parameter.

Online Restore Agent:

- Configure Rule 4 and specify **OnlineRestoreAdapter.exe** in the **Program path** parameter.
- If you use the specified Online Restore Agent port, configure Rule 1 and Rule 4. In Rule 4, specify <specific TCP port> for the Online Restore Agent in the **Local ports** parameter.
- If the RPC dynamic port range is used for the Online Restore Agent , configure Rule 1, Rule 2, and Rule 4. In Rule 4, specify <RPC dynamic port range> for the Online Restore Agent in the **Local ports** parameter.

Offline Restore Agent:

- Configure Rule 5 and specify **RstAgent.exe** in the **Program path** parameter.
- If you use the specified Offline Restore Agent port, you need to configure Rule 1 and Rule 5. In Rule 5, specify <specific TCP port> for the Offline Restore Agent in the **Local ports** parameter.
- If you use the RPC dynamic port range for the Offline Restore Agent , configure Rule 1, Rule 2, and Rule 5. In Rule 5, specify <RPC dynamic port range> for the Offline Restore Agent in the **Local ports** parameter.

Management Agent:

- Configure Rule 6 and specify the **ManagementAgent.exe** in the **Program path** parameter.
- If you use the specified Backup Agent port, configure Rule 1 and Rule 6. In Rule 6, specify <specific TCP port> for the Management Agent in the **Local ports** parameter.
- If you use the RPC dynamic port range for the Management Agent, configure Rule 1, Rule 2, and Rule 6. In Rule 6, specify <RPC dynamic port range> for the Management Agent in the **Local ports** parameter.

The following list describes the settings for each firewall rule. Any setting not described in this list can be left as the default value.

Rule 1

- 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

PowerShell for the Rule 1 settings: *New-NetFirewallRule -DisplayName "Rule 1" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort 445 -Protocol TCP -Program System*

Rule 2

- 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

PowerShell for the Rule 2 settings: *New-NetFirewallRule -DisplayName "Rule 2" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort RPCEPMap -Protocol TCP -Program "%SystemRoot%\System32\Svchost.exe" -Service RpcSs*

Rule 3

- Rule Type: Custom
- Program Path: %SystemRoot%\RecoveryManagerAD\BackupAgent64.exe or %SystemRoot%RecoveryManagerAD\ErdAgent.exe
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: RPC dynamic port range/specified 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

PowerShell for the Rule 3 settings: *New-NetFirewallRule -DisplayName "Rule 3" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "%SystemRoot%\RecoveryManagerAD\BackupAgent64.exe"*

Note: If the Backup Agent uses a specific TCP port then specify the TCP port in the LocalPort parameter. If the RPC dynamic port range is used then specify the RPC dynamic port range in the LocalPort parameter

Rule 4

- Rule Type: Custom
- Program Path: C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRestoreService64.exe"
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 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

PowerShell for the Rule 4 settings: *New-NetFirewallRule -DisplayName "Rule 4" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRestoreService64.exe"*

Note: If the Online Restore Agent uses a specific TCP port then specify the TCP port in the LocalPort parameter. If the RPC dynamic port range is used then specify the RPC dynamic port range in the LocalPort parameter.

Rule 5

- Rule Type: Custom
- Program Path: %SystemRoot%\RecoveryManagerAD\RstAgent.exe
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 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

PowerShell for the Rule 5 settings: *New-NetFirewallRule -DisplayName "Rule 5" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "**- Program Path**: "%SystemRoot%\RecoveryManagerAD\RstAgent.exe"" "*

Note: If the Offline Restore Agent uses a specific TCP port then specify the TCP port in the LocalPort parameter. If the RPC dynamic port range is used then specify the RPC dynamic port range in the LocalPort parameter.

Rule 6

- Rule Type: Custom
- Program Path: %SystemRoot%\RecoveryManagerAD\ManagementAgent.exe
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 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

PowerShell for the Rule 6 settings: *New-NetFirewallRule -DisplayName "Rule 6" -Group RMAD -Enabled True -Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "%SystemRoot%\RecoveryManagerAD\ManagementAgent.exe"*

Note: If the Management Agent uses a specific TCP port then specify the TCP port in the LocalPort parameter. If the RPC dynamic port range is used then specify the RPC dynamic port range in the LocalPort parameter.

NOTE For more information on RPC dynamic port range, refer to the following Microsoft Support Knowledge Base articles at https://support.microsoft.com:
How to configure RPC to use certain ports and how to help secure those ports by using IPsec
How to configure RPC dynamic port allocation to work with firewalls
The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008

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, Management Agent.

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.
- You can automatically configure Windows Firewall settings for Backup Agent using the Computer Collection properties in Recovery Manager Console:
    - 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.
    - From the main menu, select **Action | Properties**.
    - In the dialog box that opens, go to the **Agent Settings** tab.
    - 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.
    - Select the **Automatically configure Windows Firewall** check box, and click **OK**

RMAD 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 and backup file storages
- 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 storage

For each Computer Collection (applicable to all domain controllers within a 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. The account is used for the following operations:
  - backup creation
  - discover Backup Agent instances or update Backup Agent information
  - install, upgrade or uninstall Backup Agent instances
- 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 *Remote Storage tab* section in Properties for an existing Computer Collection.

These credentials are also used to connect to Active Directory® in the following cases:

- Show or refresh the content of collections that contain containers
- Operate on collections that contain container-items
- This account is used for backup unpacking only if no account is configured on the Remote Storage tab

For example: modifying an exclusion list for a container; installing the Backup Agent from a collection menu, collecting diagnostic data, etc.

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** 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 storages, and global catalog servers.
5. When finished, click **OK**.

NOTE Recovery Manager for Active Directory has deprecated support for a group managed service account (gMSA) to be specified as the account to connect to the backup agent for manually triggered backups. Managed service accounts will continue to be supported for scheduled backup tasks. In accordance with Microsoft®, it is recommended to not use a group managed service account (gMSA) for interactively initiated network connections such as Recovery Manager for Active Directory manually triggered backups. To enforce this recommendation and to address the vulnerability CVE-2023-21524 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21524), Microsoft has limited the usages of managed service accounts with a Windows Update. By removing support for a gMSA to connect to the backup agent, this ensures an attacker does not exploit the RMAD backup agent to perform actions or access resources over the network. To utilize the benefits and security provided by a group managed service account (gMSA), we highly recommend that a gMSA account is used for the scheduled backup task. See Setting user account for scheduled tasks

You can also specify a separate account that will be used to access the backup storage on the **Remote Storage** tab.

If no access account is specified on the **Agent** tab and no scheduled tasks exist for the Computer Collection, Recovery Manager for Active Directory (RMAD) 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, RMAD 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.

NOTE The scheduled task account is not used to access the Remote Storage from the agent side. The agent uses a local system account on a domain controller for this operation.

For additional information about the account requirements, please refer Permissions required for the Backup operation.

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 selected Computer Collection

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

To add domain controllers to a Computer Collection

1. Browse the console tree select and expand **Active Directory**, expand **Domains** then expand the domain and 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 or right click the select domain controllers, 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**.

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 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 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**.

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 .

Alternatively, you can add containers to a Computer Collection using the following procedure

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**.

NOTE Also 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.

To view and modify an exclusion list for a container

This option lets you specify an explicit list of the domain controllers that will not be included in the backup.

1. In the Recovery Manager Console tree, select the Computer Collection that holds the container.
2. In the details pane, right-click the container and select **Properties**.
3. In the Properties dialog box, click **Modify**.

4. Select domain controllers that you want to exclude from the **Available domain controllers** list and click **Add**.
5. Click **OK**.

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:
   - In the AD LDS (ADAM) host box, type the full DNS name of the host to which you want to connect.
   - In the **Port number** box, type the port number used by AD LDS (ADAM).
   - 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) 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.

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**.

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.

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**.

Hybrid Recovery with On Demand Recovery

Recovery Manager for Active Directory integration with On Demand Recovery enables the restoration and undelete of on-premises objects that are synchronized with Azure Active Directory.

About the Hybrid Connector

The Hybrid Connector Windows service establishes a secure connection to the On Demand Recovery online service enabling simultaneous restoration of both on-premises and online objects.

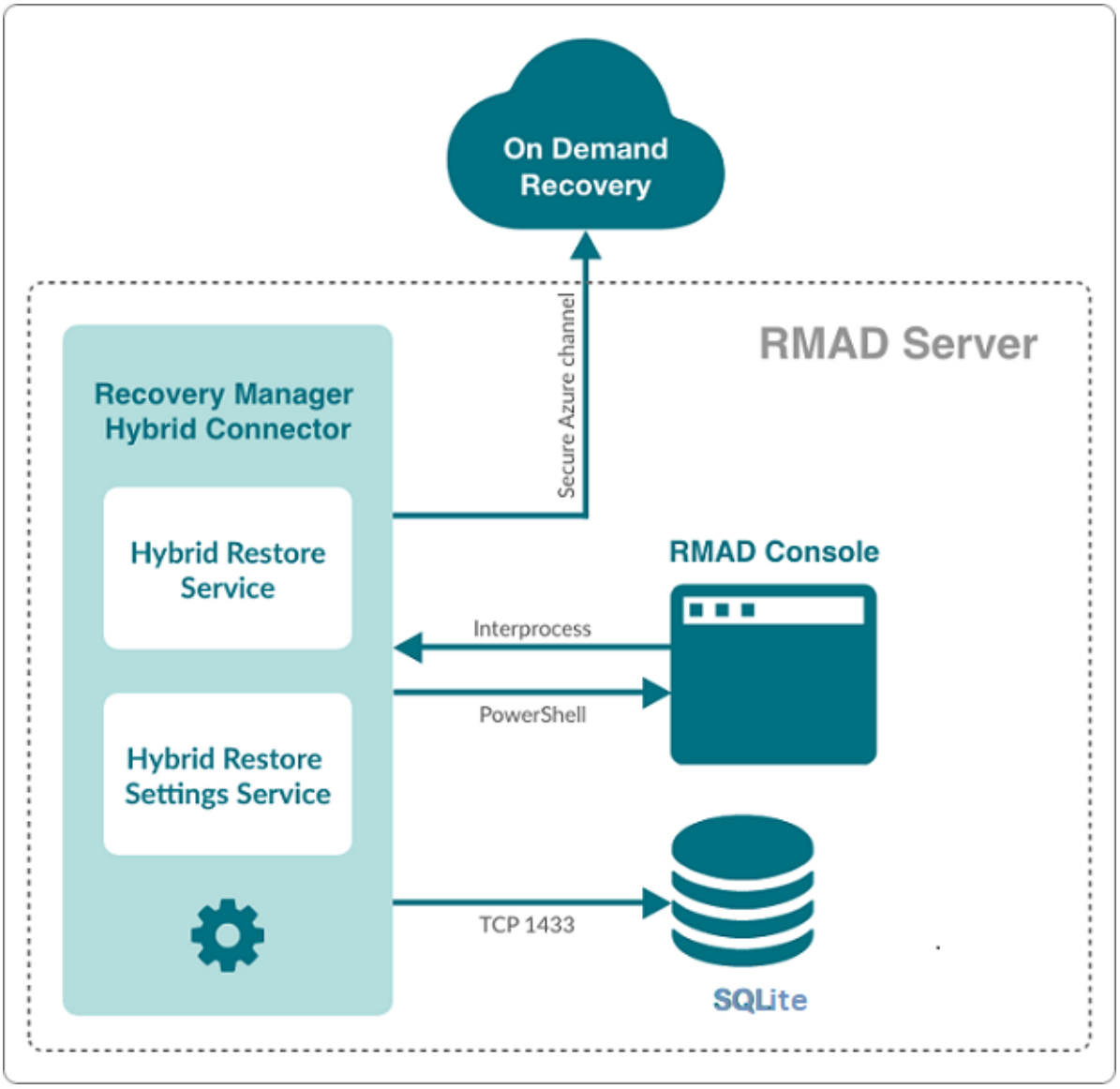


Figure: Simplified architectural Hybrid services block diagram

TLS 1.2 for Hybrid Connector

The TLSv1.2 protocol is enforced for the Hybrid Connection Service when communicating with On Demand Recovery.

What can be restored using hybrid recovery

- On-premises groups
- Microsoft 365® licenses (assignedLicenses property for cloud users) and cloud group membership
- Deleted on-premises users and groups
- Service principals' appRoleAssignments to on-premises users
- appRoleAssignments to non-Microsoft 365® groups (used for SSO and App Roles)

- Directory roles: Global administrator, Exchange administrator, Compliance administrator
- Other cloud-only properties: such as Block sign in, Authentication contact information, Minors and Consent
- Multifactor authentication (MFA) settings if a customer uses cloud MFA
- Azure® application custom attributes (schema extension attributes)
- Conditional access policies
- Inactive mailboxes of permanently deleted users; the Federated Domain scenario is also supported.

Important Considerations

To restore on-premises objects, On Demand Recovery uses attribute values from the RMAD backup that is closest in time but older than the cloud backup unpacked in the On Demand Recovery user interface. If the closest on-premises backup is 24 hours older than the cloud backup, you will receive the warning message.

By default, the search of the closest in time on-premises backup is performed among the backups that were unpacked in RMAD. You can use the **Use unpack and encrypted backups for restore operations** option on Hybrid Recovery settings of RMAD – in this case, the on-premises backup will be unpacked automatically during the restore operation.

On Demand Recovery shows only on-premises attributes synchronized with the cloud and cloud-only attributes for the selected object when you click **Browse** in the Restore Objects dialog. On-premises only attributes are not included in this list. To restore on-premises only attributes, you must select the **Restore all attributes** option in the Restore Objects dialog.

After the hybrid restore operation, On Demand Recovery forces Azure AD Connect synchronization to push on-premises changes to the cloud and wait until it completes the synchronization. Restore events can be used to track steps of Azure AD Connect synchronization, such as export and import.

To restore 'member' or 'memberOf' attributes for an object, restore the group from the **Unpacked Objects** view. Restoring of group memberships from the **Differences** report is not supported in hybrid environments.

Hybrid restore from the **Differences** report uses attribute values from the on-premises backup. These values may be different from the corresponding values shown in the **Differences** report.

On Demand Recovery supports one hybrid connection per On Demand organization. If you need to manage multiple hybrid tenants, create a separate On Demand organization for each Hybrid Azure AD tenant.

On Demand Recovery restores Back Link attributes: 'memberOf' (the back link for the 'member' attribute) and 'directReports' (the back link for the 'manager' attribute). These attributes can be selected along with all other attributes when you click **Browse** in the Restore Objects dialog.

Separate Microsoft Azure Relay service is used for each hybrid connection (one per On Demand organization). On Demand Recovery creates WCF Relay per On Demand organization. No changes to On-Premises Firewall settings are required.

On Demand Recovery users can restore objects from all on-premises domains and forests that are synchronized with the Azure AD tenant. Also, in Recovery Manager, you need to add domain controllers for every domain that will be restored and specify the account under which the restore operation will be performed.

Required Permissions

Depending on which kind of restore operation (agent-based or agentless) you are going to perform in a hybrid configuration, the account under which you want the selected Recovery Manager for Active Directory instance to recover data in the domain must meet the corresponding requirements. For details about account permissions for agent-based and agentless restore, see Permissions required to use Recovery Manager for Active Directory.

To push an Azure® synchronization, the specified account must be a member of the ADSyncOperators group on the Azure® Active Directory® synchronization server. This account must also be able to run remote PowerShell commands against the server.

How to disable hybrid integration on the Web Portal

If hybrid integration is configured on the Web Portal it must be disabled prior to configuring hybrid integration from the Recovery Manager for AD (RMAD) console. Failure to do so may result in a failed online restoration.

Follow the steps below to fully disable hybrid integration on the Web Portal.

1. Logon to Web Portal
2. Select the “Configuration” tab at the top
3. Expand the “Portal Settings” expander
4. Click on the “Configure On Demand” button
5. Remove the checkmark from the “Enable integration” checkbox
6. Click “OK” to save and close the dialog
7. Open the Windows “Services” application
8. Find the Windows service “Quest Recovery Manager Portal” from the list
9. Right click on the service and select “Stop”
10. Once the service has been stopped it can then be re-enabled if desired

Web Portal and Recovery Manager for Active Directory (RMAD) version compatibility

To continue using the Web Portal with newer versions of the RMAD console some configuration changes must be made.

For instructions on how to make the necessary configuration changes follow the steps below.

1. Navigate to the installation directory of the Web Portal (the default installation location is C:\Program Files (x86)\Quest\Recovery Manager Portal)
2. Open the file **EnterprisePortalSettings.xml**
3. Inside the **GeneralSettings** element find the property **VersionValidationMode**. If this property is not present one will have to be created
4. Change the value of the **VersionValidationMode** to **None**

Below is a sample of what the configuration should look like once the changes have been made.

```
<GeneralSettings>
    <add key="VersionValidationMode" value="None" />
    Other configuration values…
</GeneralSettings>
```

NOTE Recovery Manager for Active Directory 10.3 no longer uses SQL Server® for Hybrid configuration. After upgrade to 10.3, it will be required to re-enter credentials for each domain listed under Discovered Domains. Previous versions of RMAD used SQL Server® and a database, **RecoveryMgrHybridRestore**, was created which contained the Hybrid information. This database can be deleted as it is no longer used.

PowerShell Remoting and Hybrid Connector

If Azure AD Connect (ADSync) is installed on a system or DC and not on the RMAD Console, **PowerShell remoting** must be enabled on the remote machine. If PowerShell remoting is not enabled, an Access Denied error will occur in the RMAD console when configuring Azure AD Connect settings:

- **The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set to Stop (dc1.rmad.local) Connecting to remote server dc1.rmad.local faied with the following error message. Access is denied. For more information see the about_Reomte_Troubleshooting Help topic.**

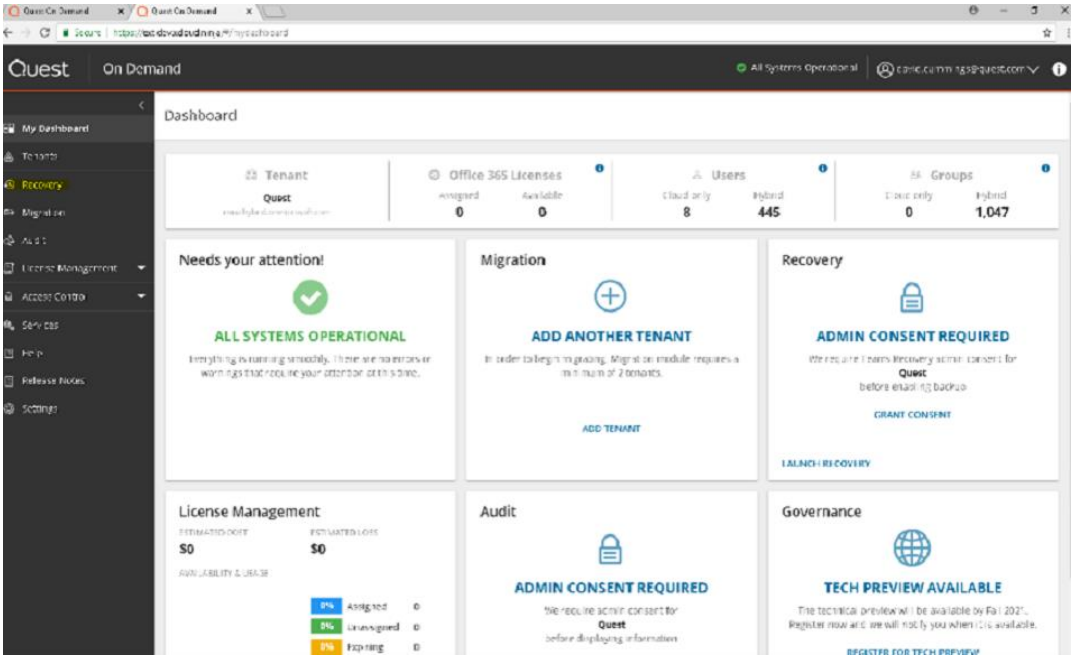
Error is recorded in Portal log similar to the following:

- **Incorrect AAD Connect settings: System.Management.Automation.ActionPreferenceStopException: The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set to Stop: [dc1] Connecting to remote server dc1 failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.**

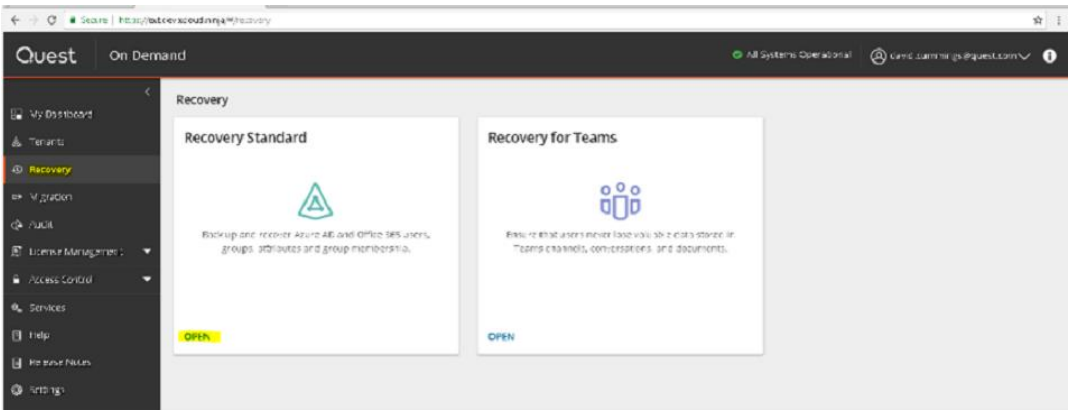
Configure Hybrid Recovery

1. From within the RMAD Console, select the **Hybrid Recovery** node from the tree on the left.
2. Select the **Enable integration with On Demand Recovery** checkbox to enable a secure connection to the online On Demand Recovery service.
3. Enter the **On Demand Recovery Settings** using the following procedure:

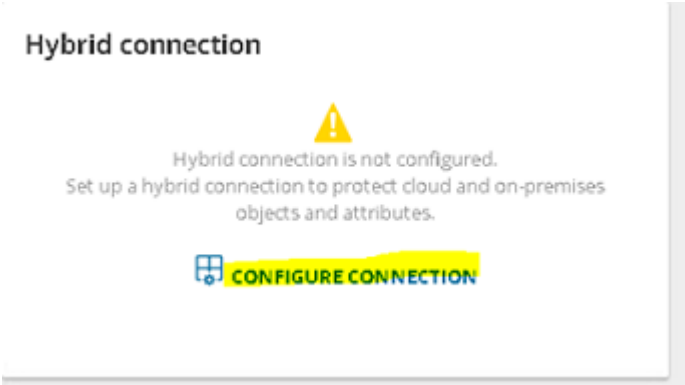
    - Navigate to the On Demand Recovery online dashboard and select the **Recovery** menu option from the left-hand side (highlighted in yellow in the image below)



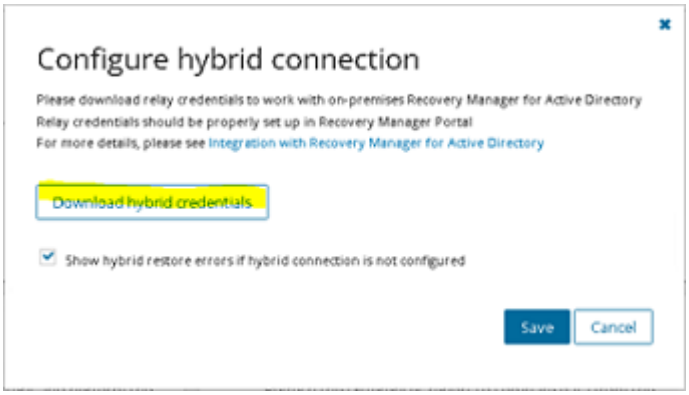
    - Click **OPEN** under the **Recovery Standard** panel



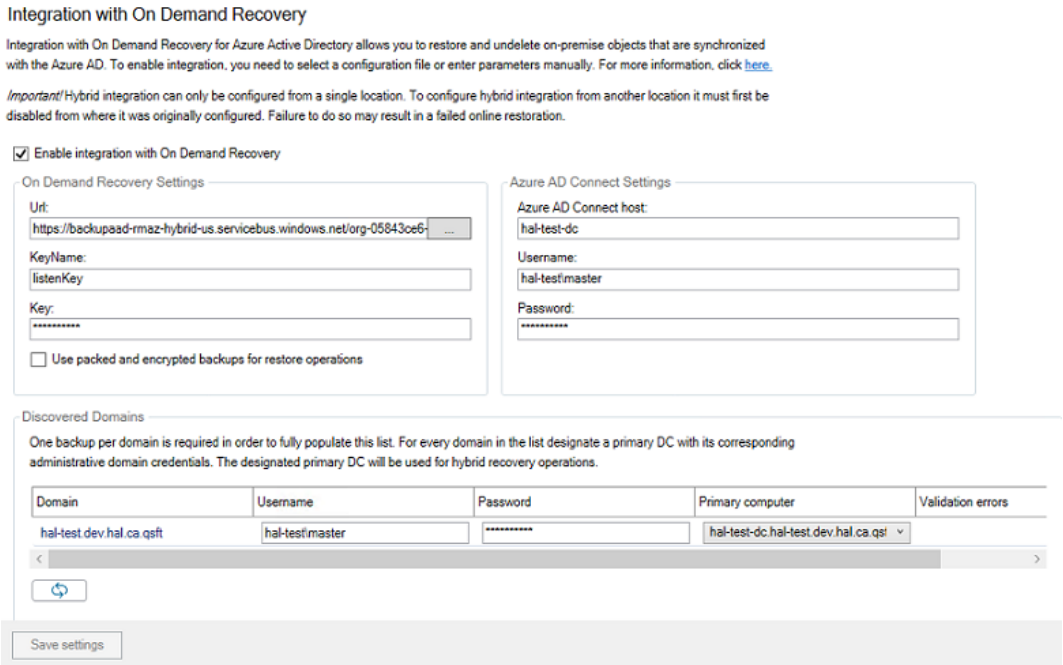
    - Click **CONFIGURE CONNECTION** under the **Hybrid Connection** panel. This will bring up the hybrid connection dialog.



- Click the **Download hybrid credentials** button on the dialog to download the required connection credentials. This file will be used to configure the **On Demand Recovery Settings** in the Recovery Manager for Active Directory console.



- From the Hybrid Recovery node on the Recovery Manager for Active Directory console, click on the ellipses (…) button located inside of the **Url** text box. This will bring up the Windows file dialog. Navigate to the location where the hybrid credentials file was saved (in the previous step) and select **Open**. This will automatically populate all the required fields under the **On Demand Recovery Settings**.



4. Enter in the Azure AD Connect host and its associated credentials under **Azure AD Connector Settings**. The values entered depends on where Azure AD Connect is installed.

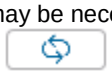
   NOTE: If Azure AD Connect is currently installed on the same server as the Recovery Manager for Active Directory console, then these fields can be left blank.

   Azure AD connector Host: Enter in the host name or IP address of the system where Azure AD Connect is installed.

   - **Username:** Enter in the domain username for this server. This account should have the necessary permissions listed under the **Required Permissions** section.
   - **Password:** Enter in the domain password for this server.

5. Enter in the domain username, password and primary computer for each domain listed under Discovered Domains. The designated primary computer will be used for hybrid recovery operations.

   The domains listed under **Discovered Domains** are pulled from backups; this means to fully populate this list at least one backup per domain is required.

   After performing a backup, it may be necessary to manually refresh this list which can be done by clicking on the refresh button ,  .

6. Once all configuration has been entered click on the Save settings button located at the bottom of the screen

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 (RMAD) requires specific dynamic link libraries (DLLs) supplied with the Windows operating system. In case RMAD 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 RMAD 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 RMAD computer.

How to ensure that required DLLs are available

Requirements

Operating system on the Recovery Manager for Active Directory computer

NOTE The OS version on the domain controller cannot be higher than the OS version on the Recovery Manager Console machine. For the list of supported OS, see Release Notes.

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
- Registering Application for Exchange Online Email Notifications
- 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 the Active Directory node**. Use this box to type the maximum number of objects (default 2000) that you want to be 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 that you can select, see Using the agentless or agent-based method.
- **Change Auditor (CA)**
    - **Include Change Auditor "Who" data in reports**. Includes 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 Change Auditor for Active Directory installed in the home Active Directory forest of RMAD.
    - **Include subsequent changes from CA on deleted objects**. When this option is selected, Recovery Manager for Active Directory restores the deleted object(s) and continuously restores the last change (if any) that was made to the object attributes after creating the backup, using data from the Change Auditor database.
    - **Database**. Allows you to specify the name of Change Auditor database.

      To specify the CA database server, instance, port, and name, use the following format: <Server Name>\<Instance Name>,<Port>\<Database Name>. **Example:** testserver.domain.com\testinstance,1432\ChangeAuditorDB

      For details about the Change Auditor-related options, see Integration with Change Auditor for Active Directory.
- **Default Active Directory connection**
    - **Use Secure Sockets Layer (SSL) to encrypt the connection**. Allows you to use LDAP over SSL when accessing the AD forests. This selection affects all the LDAP connections in RMAD and sets the default value for this check box in the other dialogs where it is displayed.

NOTE You must reopen the Forest Recovery console after updating the **Use Secure Socket Layer (SSL) to encrypt the connection** setting for the changes to take effect.

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 (default 3) 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 RMAD to keep (default 7 days) the backups unpacked by the wizards.
- **Unpacked backups folder**. Provides a space for you to specify the path to the folder (default C:\ProgramData\Quest\Recovery Manager for Active Directory\Unpacked) where you want RMAD 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.

E-mail tab

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

This tab provides the following options:

- **Service Type** Select SMTP Authentication or Exchange OAuth2 for Microsoft 365 Exchange Online.
- **SMTP Authentication**
- To set up email notifications for Exchange, specify the following for SMTP Authentication:
  - **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 (default port for SMTP is 25) 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 RMAD 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.
  - **Use Secure Sockets Layer (SSL) to encrypt the connection**. Allows you to use SSL when accessing the e-mail server.
- **Exchange OAuth2 Authentication**
- To set up email notifications for Microsoft 365 Exchange Online, you need to register Recovery Manager for Active Directory with Azure Active Directory. For steps to create and manage your Azure Active Directory application see Registering Recovery Manager for Microsoft 365 Exchange Online Email Notifications.
  - **From address**. Provides a space for you to specify the return address for your email notification messages. It is recommended that you specify the e-mail address of the RMAD administrator.
  - **Application (client) ID**. Provide the application (client) ID for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.

- **Directory (tenant) ID**. Provide the directory (tenant) ID for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.
- **Certificate Thumprint**. Provide the certificate thumbprint for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.

- **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.

Registering Recovery Manager Application for Exchange Online Email Notifications

To use email notifications using Microsoft 365 Exchange Online, you need to register Recovery Manager for Active Directory with Azure Active Directory. During the registration process, the required variables are generated. These variables are used when you configure OAuth2 authentication.

To register an application for Microsoft 365 Exchange Online through Azure Active Directory

- Log into the Azure Active Directory portal (https://portal.azure.com) with your global administrator user account.
- In the Microsoft Azure dashboard, go to **Azure Active Directory | App Registrations**, and click **New Registration**.
- Enter a name for the application.
- Under Supported account types, select **Accounts in this organizational directory only (Single tenant)** for the accounts that can access the application API.

  IMPORTANT: It is highly recommended that the application does not have access to all mailboxes. For more information about how to limit the application access to all mailboxes see the article Limiting application permissions to specific Exchange Online mailboxes.
- Leave the **Redirect URI (optional)** field empty.
- Click **Register**.
- On the **Overview** tab, go to View API Permissions. Click **Add a permission**, click **Microsoft Graph | Application Permissions** and add the **Mail.ReadWrite** and **Mail.Send** permissions. See Microsoft documentation for details on limiting permissions to specific Exchange Online mailboxes. (Note: The **Enforce approver account validation** option found when configuring email notifications will not function if you select to follow the Microsoft article to restrict access to a single mailbox.)
- Click **Add Permission**.
- On the **API Permission** tab, under **Grant consent**, click **Grant admin consent** for tenant name.
- Click **Yes** to confirm.
- On the preview screen, click **Overview**, and note the application ID and the directory ID. (You will need these values when setting up OAuth authentication.)
- Go to **Azure Active Directory - Roles and administrators** and assign the **Exchange Administrator** role for the application you created in previous steps.
- The Azure Active Directory application requires a certificate for authentication. Go to **Certificates & secrets**, select **Upload Certificate** and upload the required file.

Recovery Manager for Active Directory requires the certificate to be copied to the machine where the Recovery Manager console is installed. The certificate should be stored in the local certificate store.

To import the certificate on the console machine:

- Open the **Certificate Import Wizard**
- Select **Local machine** for **Store location**. Click **Next**.
- Select **Place all certificates in the following store**, click **Browse** and select the **Personal** store. Click **Next**
- After the certificate is imported to the store, obtain and save the certificate thumbprint. The certificate thumbprint wil be needed when setting up OAuth authentication.

NOTE Once OAuth2 authentication is set up, Recovery Manager for Active Directory saves the Application (client) ID, Directory (tenant) ID, and Certificate thumbprint in the registry. It is located in the registry path: "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active Directory\Options\Email".

Logging tab

On this tab, you can configure diagnostic logging to write detailed information about the activity of RMAD to log files.

This tab provides the following options:

- **Use diagnostic logging**. Select this check box to enable diagnostic logging in RMAD. Diagnostic logging produces a set of log files detailing the activity of RMAD.

CAUTION **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 RMAD on your server.**

- **Log files location**. Specifies the location where to create the log files. The default location is C:\ProgramData\Quest\Recovery Manager for Active Directory\Logs.
- **Create a new set of log files**. Use this list to define how often (default Daily) 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:

Backup Agent

- **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.

Online Restore Agent

- **Automatically configure Windows Firewall** If this option is selected, Windows Firewall settings will be configured automatically for the operations performed by Online Restore Agent.
- **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.

Offline Restore Agent

- **Automatically configure Windows Firewall** If this option is selected, Windows Firewall settings will be configured automatically for the operations performed by Offline Restore Agent.

- **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.

Management Agent

- **Automatically configure Windows Firewall** If this option is selected, Windows Firewall settings will be configured automatically for the operations performed by Management 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.

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 additional 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 the **Action** menu and click **Collection Defaults** or right click on **Computer Collections** node and **Collection Defaults**.

The fields 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. Each Computer Collections can have unique settings.

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

- Backup tab
- Local Storage tab

- Remote Storage tab
- Agent tab
- Schedule tab
- Alerts tab
- Performance tab
- Advanced tab
- Unpacked Backups tab

Backup tab

On this tab, you can use the following elements:

- **Backup type**. There are two backup types available:
  - **Active Directory (Standard)**. Select this option to create a standard Active Directory backup.
  - **Bare Metal Recovery (Full)**. Select this option to create Bare Metal Recovery Backup. The storage for BMR backups is specified on the **Remote Storage** tab. Bare Metal backups require Recovery Manager for Active Directory Disaster Recovery Edition license.
- **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.
- **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%.

Local Storage tab

NOTE Options on this tab are not supported for BMR backups. BMR backups must be saved to remote storage locations and are configured on the **Remote Storage** tab.

This tab includes the following elements:

- **Save Backups on the Recovery Manager console computer**. Select this check box to save backup files on the Recovery Manager for Active Directory (RMAD) computer. Enter the location for backup files in the **Primary Backup Path** box. If you specify a UNC share, backup files will be streamed to that share via the RMAD computer.
- **Primary Backup Path**. 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%\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 **Primary Backup Path**.
- **Additional backup path (optional)**. Select this checkbox to store a copy of each backup in an additional location.
- **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 **Additional backup path(optional)**.

  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.
- **For each computer, delete all backups except the last <Number>**. Select this check box to retain a number of backups for each computer. Specify the number of backups to maintain. It is recommended to configure a backup retention policy to maintain backups created in the last two weeks. If you create backups on a daily basis specify 14 to maintain backups for each domain controller for two weeks.

  This check box can be selected only when RMAD stores backups separately. To ensure that RMAD does so, add the %DATETIME% expression to the path or file name in the **Backup file name format** box.

IMPORTANT When the backup is triggered and a specified backup path is not available, no backup is created. The backup creation session will fail.

Remote Storage tab

This tab includes the following elements:

- **Save backups on the backed up DC 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. 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** tab.
- **Primary Backup path:**. Use the provided space to specify format for paths and names of 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%`.
- **Expression**. Click this button to specify path and file name notations in **Backup path** or **Alternative backup path (optional)**. 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 **Backup path** or **Alternative backup path (optional)**.
- **Additional backup path (optional)**.

IMPORTANT According to the Forest Recovery best practices, the RMAD Active Directory® backup should be stored on a domain controller. At the same time, the **Additional backup path** option allows you to store the same Active Directory® backup on remote backup storage. This can be useful if the DC is destroyed and you want to restore it from a BMR backup and the latest Active Directory® backup. The retention policy is applied to both backup paths. So, if you set it to 10, and you have both paths configured - it means that there will be 5 backups on DC and 5 backups on the remote storage.

- **Use the following account to access the backup storage:**. Allows you to explicitly specify a user account that will be used to access the backup storage. This option lets you work with network shares from different security realms, such as Azure® Files or Linux shares.

NOTE The backup storage account is used to access all remote storage backup locations. Currently, separate access accounts are not supported.

- **For each computer, delete all backups except the last:**. Select this check box to retain a number of backups for each computer. Specify the number of backups to maintain. It is recommended to configure a backup retention policy to maintain backups created in the last two weeks . If you create backups on a daily basis specify 14 to maintain backups for each domain controller for two weeks.

  This check box can be selected only when RMAD stores backups separately. To ensure that RMAD does so, add the %DATETIME% expression to the path or file name in the **Backup file name format** box.

IMPORTANT When the backup is triggered and any specified backup path is not available, no backup is created. The backup creation session will fail

Secondary Storage tab

NOTE All Secondary Storage functionality require a Recovery Manager for Active Directory Disaster Recovery Edition license. The tab will be disabled if license is not available.

This tab includes the following elements:

- **Enable a Secure Storage server**. Select this check box to enable a Secure Storage server for a backup. After creation and saving of backup to primary storage locations, a copy of the backup will be saved to the Secure Storage server.
- Select the radio button below **Enable a Secure Storage server** to choose the primary storage location for the backup file to be copied from. Select **Copy backup from remote storage location to the selected Secure Storage server** to pull the backup file from the remote storage location. Select **Copy backup from local storage location to the selected Secure Storage server** to pull backup file from the local storage location. If using both local and remote storage options for primary storage, the recommendation is to configure your Secure Storage server to communicate with the primary storage location closest for optimal network performance.
- **Copy backup from remote storage location to the selected Secure Storage server**. Select the DNS name or IP address of a Secure Storage host.
- **Copy backup from local storage location to the selected Secure Storage server**. Select the DNS name or IP address of a Secure Storage host.
- **Enable Cloud Storage and select Cloud Storage locations**. Select this checkbox to enable Cloud Storage. After creation and saving of backup to primary storage locations, a copy of the backup will be made to the configured Cloud storage locations.
- Select the checkbox for each registered Cloud Storage location to be used for this backup.

NOTE Computer collections can also be selected on the Cloud Storage node.

Access Credentials For Reading Data

IMPORTANT Access credentials are required for reading backups on primary storage to copy to Secure Storage and Cloud Storage. There may be some cases where credentials have to be specified for both remote and local storage based on the types of primary and secondary storage configured for the computer collection.

- **An account to read data from remote storage location**. Select an account that has read permission to the remote storage location. This account will be used to read the backup from the **remote** storage location and copy to all secondary storage locations. The Secure Storage agent on the Secure Storage server and the Recovery Manager Cloud Upload service on the Recovery Manager console, use this account. If an account is incorrect and does not have the proper permissions, the copy of the backup to secondary storage will fail.
- **An account to read data from local storage location**. Select an account that has read permission to the local storage location. This account will be used to read the backup from the **local** storage location and copy to all secondary storage locations. The Secure Storage agent on the Secure Storage server and the Recovery Manager Cloud Upload service on the Recovery Manager console, use this account. If an account is incorrect and does not have the proper permissions, the copy of the backup to secondary storage will fail.

Agent tab

NOTE **For Recovery Manager for Active Directory (RMAD) 10.1 or higher**: Make sure that you use the Backup Agent version supplied with this release of Recovery Manager for Active Directory.

The **Agent** tab is used to specify settings for Backup Agent.

The elements of the Agent tab are defined as follows:

NOTE You can configure Recovery Manager for Active Directory (RMAD) to back up data in an Active Directory® domain under a least-privileged user account and create a group named RMAD Backup Operators that will automatically grant the necessary permissions to back up data. See Using a least-privileged user account to backup data

- **Use the following account to access Backup Agent**. Allows you to explicitly specify a user account under which you want the Recovery Manager Console to access Backup Agent. When this check box is cleared, the Recovery Manager Console uses the account under which it is running to access Backup Agent. To explicitly specify a user account, select this check box, and then click **Select Account** to specify the account credentials.

NOTE Recovery Manager for Active Directory has deprecated support for a group managed service account (gMSA) to be specified as the account to connect to the backup agent for manually triggered backups. Managed service accounts will continue to be supported for scheduled backup tasks. In accordance with Microsoft®, it is recommended to not use a group managed service account (gMSA) for interactively initiated network connections such as Recovery Manager for Active Directory manually triggered backups. To enforce this recommendation and to address the vulnerability CVE-2023-21524 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21524), Microsoft has limited the usages of managed service accounts with a Windows Update. By removing support for a gMSA to connect to the backup agent, this ensures an attacker does not exploit the RMAD backup agent to perform actions or access resources over the network. To utilize the benefits and security provided by a group managed service account (gMSA), we highly recommend that a gMSA account is used for the scheduled backup task. See Setting user account for scheduled tasks

- **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.

NOTE It is highly recommended and best practice to use a preinstalled backup agent. With preinstalled backup agents, Recovery Manager for Active Directory does not have to store highly privileged domain admin credentials for agent installation, thus increasing security of the product installation.

> For Recovery Manager for Active Directory 10.3 or higher this option is selected by default for all new computer collections.

When the check box **Use preinstalled Backup Agent** is selected the product will have the following behavior:

- RMAD backs up only those computers where the Backup Agent is preinstalled manually.
- RMAD does not automatically install the Backup Agent on the computers in the Computer Collection.
- RMAD automatically installs the Backup Agent before backing up a computer where the agent is not preinstalled manually.
- 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, RMAD will use that agent to back up data on the computer. RMAD 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 RMAD automatically configure Windows Firewall on target Windows Server® 2008-based or Windows Server® 2012-based DCs, so that RMAD can back up these DCs.

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 alert settings for the given Computer Collection.

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, More that one address can be entered, separated by a semicolon or a comma.
- **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.

- **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.
- **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.
- **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.

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:

- **Limit maximum backup time** This option limits the maximum backup session time.
- **Limit maximum DC backup time** This option limits the maximum backup session time for a single DC.

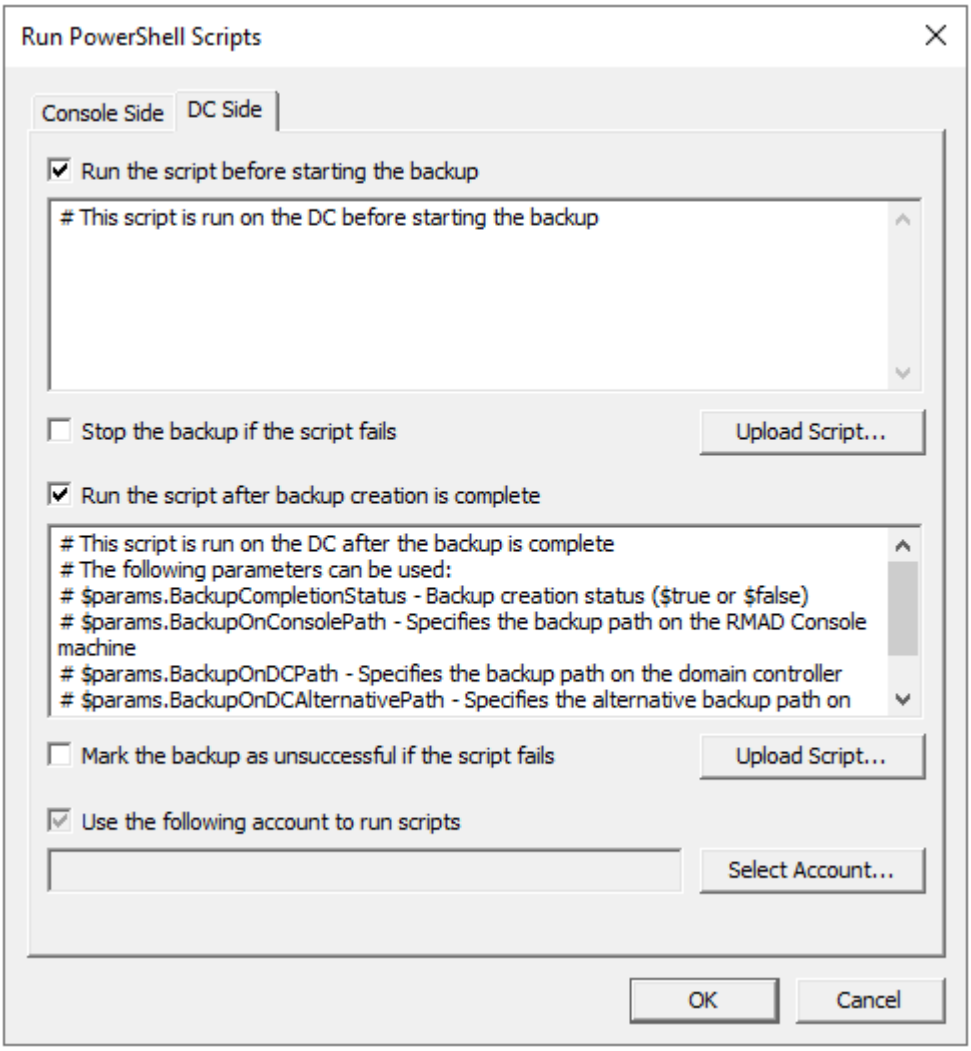
- **Run Scripts** This option allows you to customize your environment by running PowerShell® scripts before and/or after creating a backup. Custom scripts can be launched either on the Recovery Manager for Active Directory Console machine or on the domain controller side.
- **Diagnostic Logging** Specify the logging setting for the Recovery Manager and Backup Agents for all domain controllers in the collection.
- **When backing up Global Catalog servers, collect group membership information from all domains within the Active Directory forest** Set by default, this option will collect group membership information from all domains within the Active Directory forest when backing up servers containing the Global Catalog.
- **Perform integrity check after scheduled backup** Set by default, this option performs an integrity check when scheduled backups have completed. You can also check previous backups ranging from 1 to 100 sessions (28 is the default).

Advanced Scripts

- **Run Scripts**

  In the Run PowerShell® Scripts dialog, the following options can be specified:

  - **Run the script before starting the backup** - Launches specified PowerShell® scripts before the backup creation process is started.
  - **Stop the backup if the script fails** - Stops the backup process if the script cannot be run without errors.
  - **Run the script after backup creation is complete** - Launches specified PowerShell® scripts after backup is created.
  - **Mark the backup as unsuccessful if the script fails** - If the script fails, the backup process will be shown as failed with error in the RMAD console.
  - **Upload Script** - Using this option you can upload an existing PowerShell® script file (.ps1). After the script is uploaded, the contents of the script will be displayed in the dialog and you can edit it if necessary.
  - **Use the following account to run scripts** and **Select Account** - Here you can select an account under which the scripts will be running. For the "Console scripts", by default, the account under which the console is launched will be used. For the "DC scripts", there is no default value, and the user has to select an account. Otherwise, the settings will not be saved.



NOTE If the script is run on a domain controller, we strongly recommend using an account with the minimum rights required only to perform the actions specified in the script.

The "Console scripts" are launched only once for each run of backup creation on the console machine. The "DC scripts" are run on each DC for which the backup is created. If the "script for DC" fails, the corresponding DC will have an error or warning. If the "console script" fails, then all DCs for which the backup process was started will have an error or warning.

Recovery Manager for Active Directory provides an option to set the maximum timeout during which a script can run (the default value is 60 seconds). To change this value, set the **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active Directory\Options\ScriptExecTimeoutInSeconds (DWORD)** registry key to <required value>.

Failed script can lead to both Warning and Error results. It depends on the specified settings:

Option Name	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Run the script before starting the backup	✓	✓		
Stop the backup if the script fails	✕	✓		
Run the script after backup creation is complete			✓	✓
Mark the backup as unsuccessful if the script fails			✕	✓

Option Name	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Result	Warning	Error	Warning	Error

Script security

Running scripts can be dangerous - especially on a domain controller. Recovery Manager includes the following security measures for scripts:

- Scripts are stored in the Recovery Manager database in an encrypted form.
- Scripts are sent from the Recovery Manager console to the Backup Agent using a secure RPC channel.
- Scripts are run in memory and no temporary files are created on the disk. When running scripts, the **-EncodedCommand** parameter of PowerShell.exe is used.
- For scripts run on the domain controller, specifying a custom account under which the script will run is required. Using an account with minimum rights is recommended.
- All scripts have a timeout when running. If the timeout is exceeded, the script will be forcibly stopped.
- The result of the script running is recorded in the Windows Event Log.

Advanced Logging

- **Diagnostic logging** Specify the logging setting for the Recovery Manager and Backup Agents for all domain controllers in the collection.

  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**

- **Creating a new set of log files** Specify the creation of new logs for Recovery Manager and Backup Agents for all controllers in the collection.

  Edit HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Recovery Manager for Active Directory\Diagnostics

  Modify or create REG_SZ registry value called **LogRotationInterval**

  The following options are available:

  - **Never** - Never create new logs
  - **Daily** - Create new logs daily.
  - **Weekly** - Create new logs weekly.
  - **Monthly** - Create new logs monthly.

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) instance**s 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, complete the following steps:
    - 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.
    - Select the **Use Secure Socket Layer (SSL) to encrypt the connection** check box to use LDAP over SSL when connecting to the forest. The default value for this option is determined by the same setting in the RMAD Settings dialog; however, you can change the setting here for this particular connection.
    - 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.
- **Tombstone Lifetime**. Displays the number of days before a deleted object is removed from directory services.
- **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 (RMAD) 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, RMAD 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, RMAD 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 RMAD 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.

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 (RMAD) 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 RMAD 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
- Using Managed Service Accounts
- Active Directory backups vs Windows System State backups
- Creating BMR and Active Directory 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
- 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.

Minimum permissions required for the Backup operation

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 to 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 (RMAD) 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 RMAD.

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 RMAD in one of the following ways:

- **Use preinstalled Backup Agent only**. When configured this way, RMAD 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, RMAD will use preinstalled Backup Agent if it is present on the target computer. If the Backup Agent is missing, RMAD 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

NOTE **For Recovery Manager for Active Directory 10.1 or higher**: Make sure that you use the Backup Agent version supplied with this release of Recovery Manager for Active Directory.

You can configure Recovery Manager for Active Directory (RMAD) 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, RMAD will automatically install the Backup Agent before backing up a computer where the agent is not preinstalled. When the backup operation completes, RMAD will remove the automatically installed Backup Agent.

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

For RMAD to automatically install the Backup Agent, the user account under which RMAD accesses the target Computer Collection must have specific permissions. For more information, see Permissions required to use Recovery Manager for Active Directory.

NOTE **Check that the Administrative Share Admin$ exists and is accessible on the target domain controller to perform the remote agent installation.**

- Windows Server automatically creates Administrative Shares. If the automatic creation of shares was disabled (Microsoft KB Article 954422), re-enable the automatic shares creation.
- Check that Administrative Shares are accessible. For details, see Shared Folders in Microsoft documentation.

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

To preinstall Backup Agent on all computers in a Computer Collection, perform the following steps:

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

To selectively preinstall Backup Agent on computers in a Computer Collection, perform the following steps:

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

To perform a silent installation of the Backup Agent, perform the following steps:

1. Copy the **Backupagent.msi** file supplied in the RMAD 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: `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 RMAD 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, RMAD 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, RMAD 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, RMAD 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 (RMAD) 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 RMAD.

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 RMAD.

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 RMAD.

   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 saves the group SID in the registry. Then the Backup Agent uses this group SID to check that the user account is a member of the **RMAD Backup Operators** group.

   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.

Using Managed Service Accounts

Recovery Manager for Active Directory (RMAD) supports MSA/gMSA accounts for:

- Scheduled backups - the account can be specified for scheduled tasks in the Computer Collection properties on the **Schedule** tab or in Task Scheduler.
- Scheduled replication tasks (Fault Tolerance)
- For PowerShell® scripts launched from the domain controller side before and/or after creating a backup. (Scripts run from the Recovery Manager for Active Directory console are not supported)

NOTE Recovery Manager for Active Directory has deprecated support for a group managed service account (gMSA) to be specified as the account to connect to the backup agent for manually triggered backups. Managed service accounts will continue to be supported for scheduled backup tasks. In accordance with Microsoft®, it is recommended to not use a group managed service account (gMSA) for interactively initiated network connections such as Recovery Manager for Active Directory manually triggered backups. To enforce this recommendation and to address the vulnerability CVE-2023-21524 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21524), Microsoft has limited the usages of managed service accounts with a Windows Update. By removing support for a gMSA to connect to the backup agent, this ensures an attacker does not exploit the RMAD backup agent to perform actions or access resources over the network. To utilize the benefits and security provided by a group managed service account (gMSA), we highly recommend that a gMSA account is used for the scheduled backup task. See Setting user account for scheduled tasks

MSA/gMSA account requirements:

- You can use Managed Service Account (in Windows Server® 2008 or higher) or Group Managed Service Account (in 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/gMSA account must be a member of the local Administrator group on the RMAD machine.

How to create a Group Managed Service Accounts (gMSA)

Although the following instructions will configure gMSA accounts in your Active Directory® Forest, we recommend you first review the Microsoft® article: Getting Started with Group Managed Service Accounts

NOTE Even with the `-EffectiveImmediately` switch shown below, you **must wait 10 hours** after issuing this command before continuing. This ensures that the key has replicated throughout the domain so that all domain controllers can generate a password for your gMSA account.

1. If you have never used gMSA accounts before, you must prepare Active Directory® by creating a KDS Root Key with one of the following PowerShell® commands on a domain controller:

   In production, issue the command:

   ```
   Add-KdsRootKey -EffectiveImmediately
   ```

   In a test lab with minimal domain controllers, it's safe to issue this command:

   ```
   Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
   ```

   Run this command once in each Domain of the Forest.

   NOTE: For more information, see Create the Key Distribution Services KDS Root Key and this Microsoft Blog post.

2. (Optional) If you plan to use the same gMSA account on more than one host (for example, you have more than one RMAD server), then it may be easier to create a group for the hosts you plan to use it on. We suggest a Domain-Local Security group for this purpose. The following PowerShell® commands will create the group in the default **Users** container, then add your RMAD server as a member:

   ```
   Add-ADGroupMember -Identity <GroupName> -Members <RMADServer$>
   ```

   Repeat the command above for each RMAD server you want to use the gMSA account.

   NOTE: If you use a group, then you must either restart the host(s) you added as members or run the command `klist purge -li 0x3e7` on each host before performing step 4 below. This is to refresh the computer's Kerberos ticket so it will include the new group SID in its NT Token.

3. Create the gMSA account using the following PowerShell command:

   ```
   New-ADServiceAccount -Name <gMSAName> -DNSHost <gMSAName.domain> -
   PrincipalsAllowedToRetrieveManagedPassword <AccountName>
   ```

   Where:

   - `<gMSAName>` is the name of your gMSA account. For example: "gMSABackup"
   - `<gMSAName.domain>` is the gMSA account followed by the domain. For example: "gMSABackup.contoso.com"
   - `<AccountName>` is either `<RMADServer$>`, or the group name you created in step 2 above.

NOTE: If using remote storage for backups, the account for each domain controller being backed up, needs to be added to the "PrincipalsAllowedToRetrieveManagedPassword" property for the gMSA account. Use the following command:
SetADServiceAccount -Identity `<gMSAName>` -PrincipalsAllowedToRetreiveManagedPassword `<AccountName>`.

4. After the gMSA account is created, you must install it on each host it will be used on (for example; on your RMAD server). Do this by running the following PowerShell® command on each host:

```
Install-ADServiceAccount -Identity <gMSAName>
```

5. (Optional) You can test that the gMSA account can be used by running the following PowerShell® command on each host where you installed the gMSA account:

   ```
   Test-ADServiceAccount <gMSAName>
   ```

   A result of **True** shows the gMSA account is ready to be used.

For more details, see Getting Started with Group Managed Service Accounts.

Active Directory backups vs Windows System State backups

The Active Directory and Windows System State backups are very similar. The key components that Recovery Manager for Active Directory (RMAD) backs up as part of the AD system state are the Registry, the NTDS.dit file, and SYSVOL.

What differences do they have?

- Windows System State backup is a full backup of the Windows operating system; Active Directory® backup contains only pieces of Active Directory® that allow you to restore the domain controller on a clean operating system.
- Windows System State backups contain more components - not all of these components are necessary for Active Directory recovery, e.g. IIS Metabase, Cluster Services, etc.
- Windows System State backup may contain viruses in the components of the operating system.
- Windows System State backups are larger than Active Directory® backups.

For the list of Windows System State backup components, see Microsoft documentation.

RMAD enables the backup and restoration of the following Active Directory® components on domain controllers:

- DIT Database
- SYSVOL
- Registry, including all registry hives and the file NTUSER.DAT

RMAD Disaster Recovery Edition also supports Bare Metal Recovery (BMR) backups. With BMR backups, you can completely rebuild the server if necessary.

Creating BMR and Active Directory backups

Recovery Manager for Active Directory (RMAD) allows you to create backups of system-specific data known as the Active Directory® and BMR backups. Note that RMAD creates Active Directory® backups for Active Directory® domain controllers only.

NOTE If you are going to store backups on the Recovery Manager Console machine, check that the Administrative Share "DriveLetter$" exists and is accessible on this host. Otherwise, the backup operation will fail. For more information, see Installing Backup Agent automatically.

You can use Computer Collections to create backups for multiple computers. For more information, see Using Computer Collections.

- Creating Active Directory backup

- Creating BMR backup
- Usage of backup access credentials

Creating Active Directory® backup

NOTE When the backup is triggered and any specified backup path is not available, no backup is created, neither in the remote storage nor in the local storage. The backup creation session will fail.

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.

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.

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.

Creating BMR backups

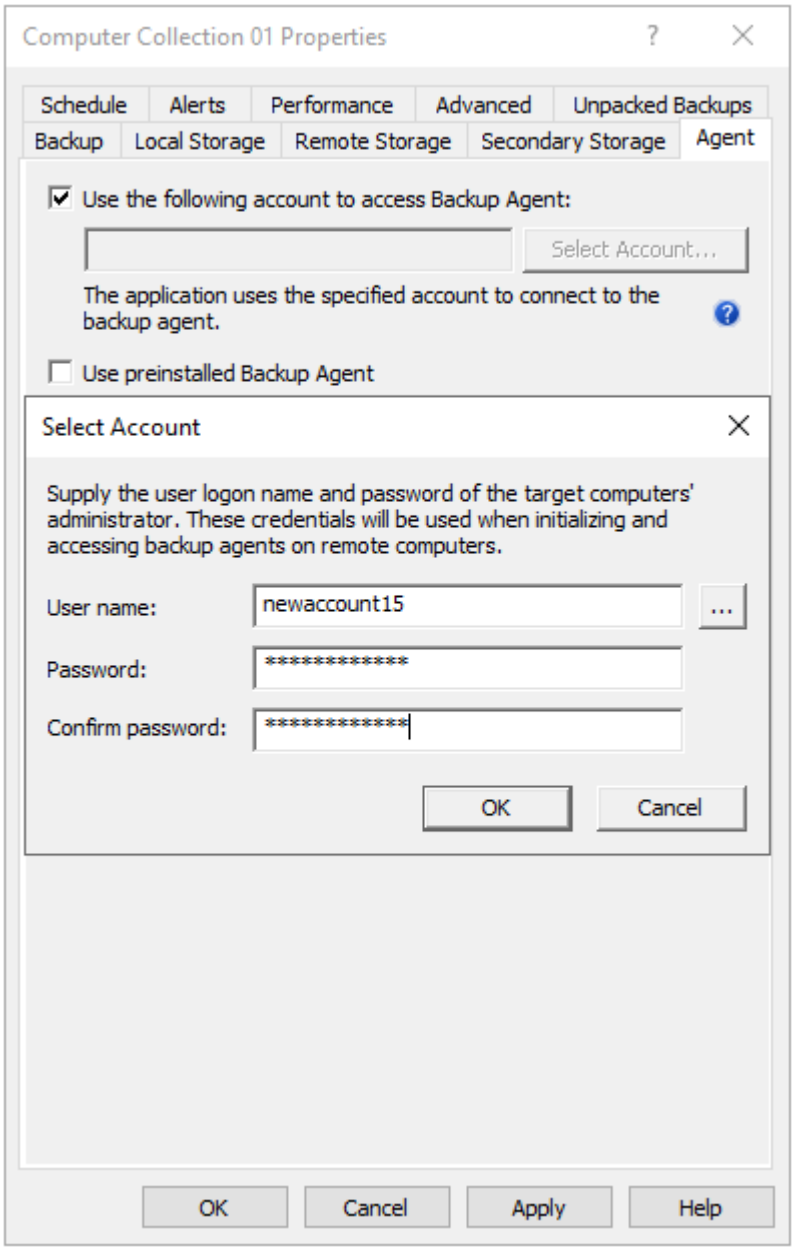
- This feature is supported only for Windows Server 2008 R2 or higher domain controllers.
- Active Directory® does not allow using a backup whose age exceeds the Active Directory® tombstone lifetime (default is 180 days). But if there is a RMAD BMR backup that is older than 180 days and a more recent Active Directory® backup, you can successfully perform the restore operation.
- Cache and reuse the extracted WinRe images for BMR, which will reduce failures while creating ISO images from backup.
  Locate the extracted Windows imaging file WimRe.wim under \ProgramData\Cache\WinRe\10.0 folder on the RMAD machine.

- If the process of creating a Windows Server 2008 R2 BMR backup completes with the error like "The sector size of the physical disk on which the virtual disk resides is not supported.", make sure that the disk sector size on the target machine (NAS device or similar) is equal to 512 bytes.

For instance, NetApp® ONTAP® operating system uses the following command: `vserver cifs options modify -file-system-sector-size 512`.

To create a BMR backup

1. Create a computer collection.
2. Right-click the computer collection, and then click **Properties** to open the **Computer Collection Properties** dialog box.
3. On the **Agent** tab, select the option **Use the following account to access Backup Agent** and specify account credentials. In RMAD, this account is used both to connect to the Backup Agent and to access the backup storage if you do not specify a separate account for the backup share on the **Remote Storage** tab. For more details, see Usage of backup access credentials.



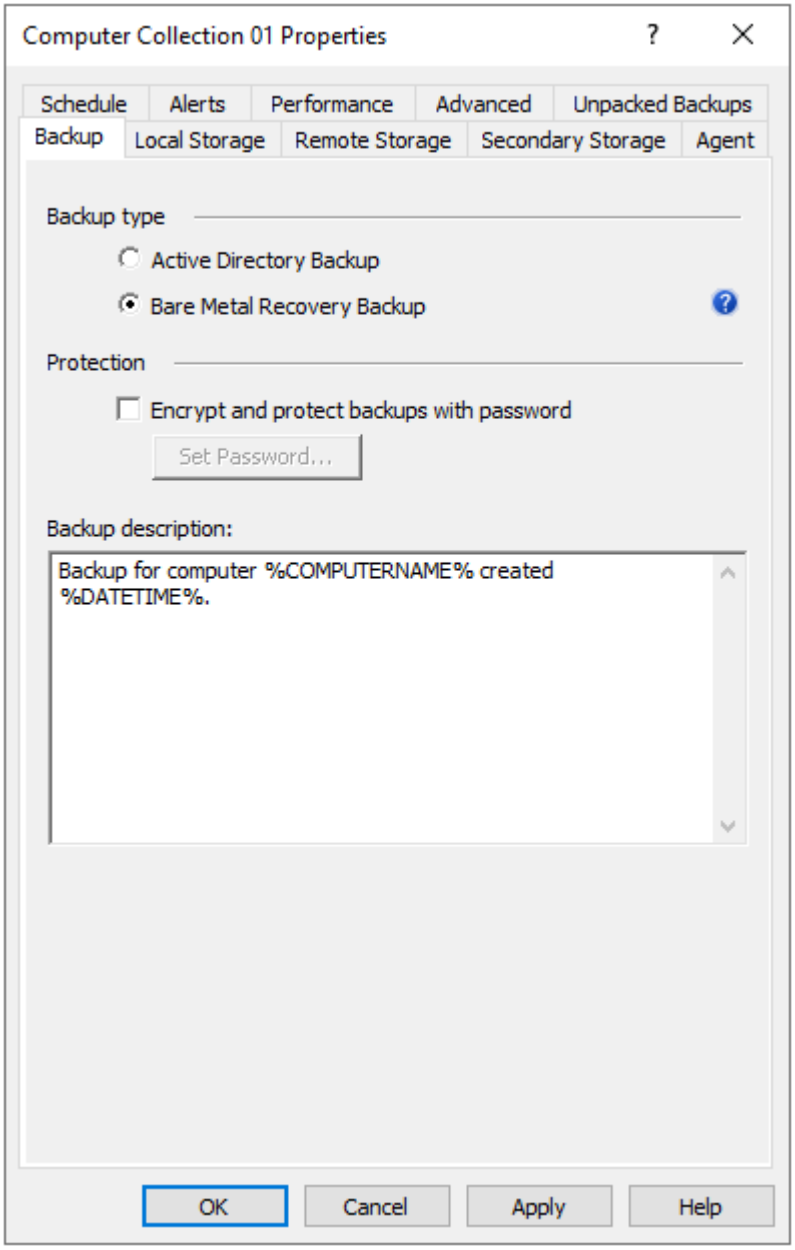
4. On the **Remote Storage** tab, select the option **Save backups on the backed up DC or a UNC share** and enter the backup path. You need to specify path to the SMB share in the following format

(`%DATETIME%` variable is required):
`\\RemoteHost\ShareName\%COMPUTERNAME%\%DATETIME%`.

5. On the **Backup** tab, select the **Bare Metal Recovery** backup type. Now only system critical volumes are included in the BMR backup by default. For information on how to include additional volumes into a BMR backup, see below in this article.

   Select the **Encrypt and protect backups with password** option to encrypt BMR backups and protect them with a password (**Recommended**). This password is used to generate a passphrase with which the backup is encrypted. The password cannot be used directly to unlock the backup container *.vhd(x) file.

   IMPORTANT: If a customer restores encrypted volumes from a backup, the volumes are restored as unencrypted.



6. Right-click the collection node and click **Create Backup**.

Including additional volumes to a BMR backup

By default, only the system critical volumes are included in the BMR backup. This includes Operating System volumes and live Active Directory volumes (database, logs, sysvol), but would not include any volumes that does

not contain these critical components. If you had an additional volume where you stored system state backups, or even RMAD Active Directory backups, then this volume would not be included in the BMR backup.

To include additional volume on several domain controllers

1. Create the following registry key on the selected domain controller, or check if the key already exists in the directory:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Recovery Manager for Active Directory`

2. Add the following string value under this registry key:

   Name: `WindowsBackupCommandLine`

   Data: `wbadmin start backup -allcritical -quiet -backuptarget:"%s" -include:E:,G:`

   Where "E:,G:" - drives that will be included into the BMR backup.

To include additional volume on all domain controllers

On the Recovery Manager Console machine, add the new string value under both these registry keys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Recovery Manager for Active Directory`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Quest\Recovery Manager for Active Directory`

  Name: `WindowsBackupCommandLine`

  Data: `wbadmin start backup -allcritical -quiet -backuptarget:"%s" -include:E:,G:`

  Where "E:,G:" - drives that will be included into the BMR backup.

Usage of backup access credentials

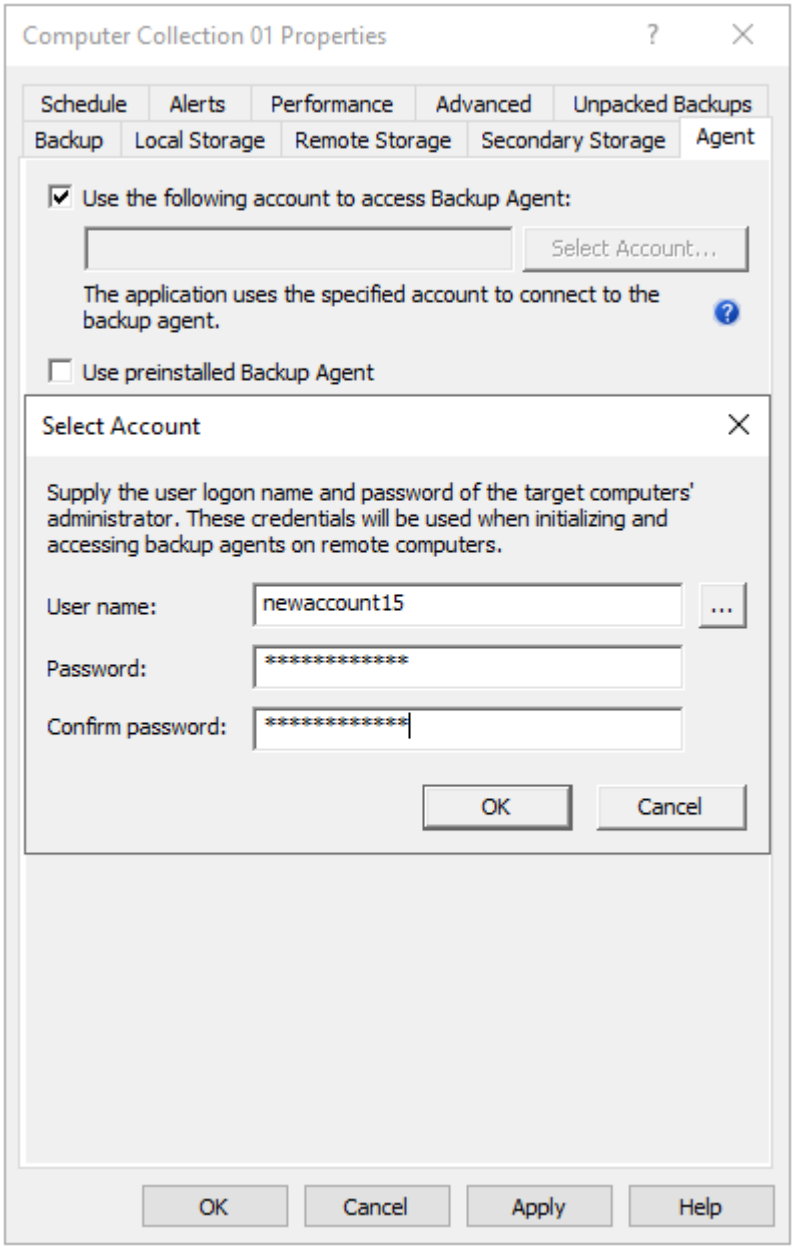
Recovery Manager for Active Directory (RMAD) uses the same credentials to access backup files on the remote share and to connect to Backup Agent. These credentials are specified on the **Agent Settings** tab of the collection properties (option "**Use the following account to access Backup Agent**").

If you need to specify a separate account to access the backup storage, use the option **Use the following account to access the backup storage** on the **Remote Storage** tab.

When no credentials are specified in the collection properties, the Recovery Manager Console uses the account under which it is running to access the backup storage and Backup Agent.

To specify separate credentials to access the remote backup location and Backup Agent

1. Create a computer collection in RMAD Console.
2. Right-click the computer collection, and then click **Properties** to open the **Computer Collection Properties** dialog box.
3. On the **Agent Settings** tab, select the option **Use the following account to access Backup Agent** and specify account credentials.

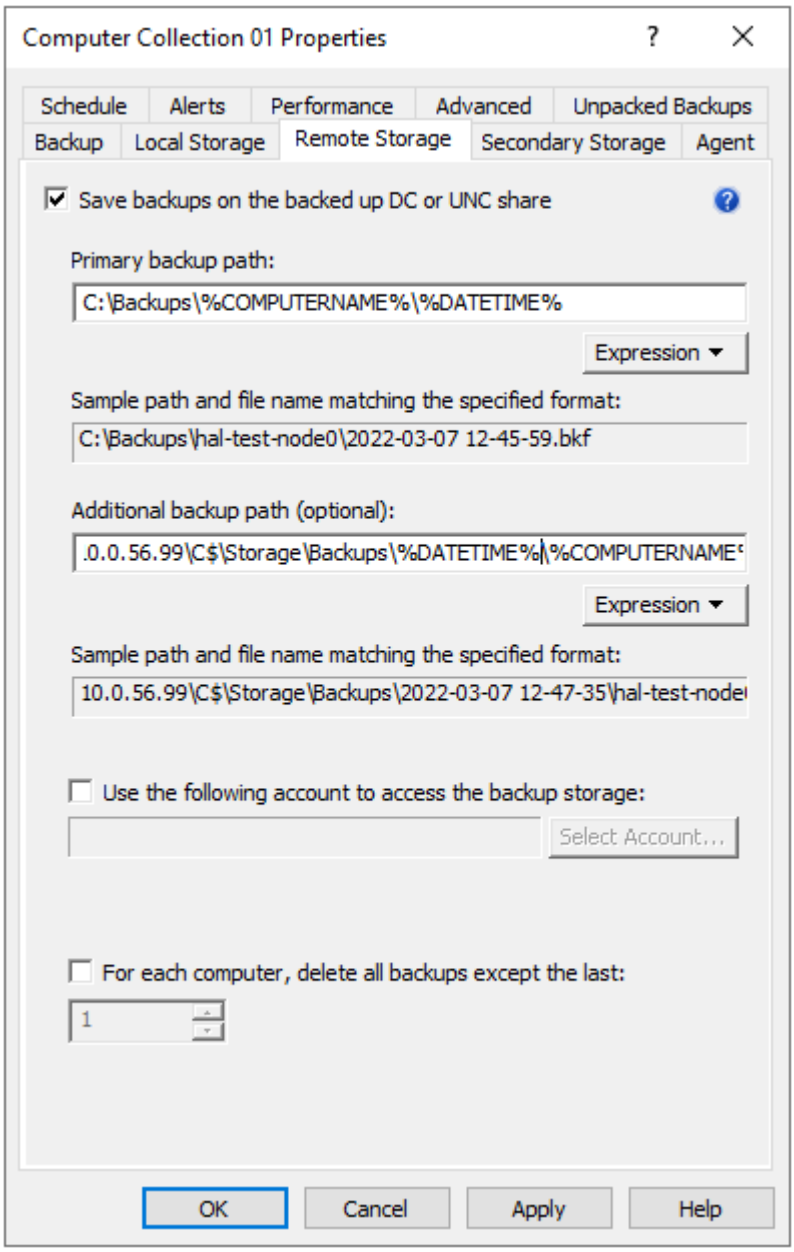


4. On the **Remote Storage** tab, select the option **Save backups on the DC being backed up or a UNC share** and enter the backup path. You need to specify path to the remote share in the following format (%DATETIME% variable is required): `\\<share name>\<backup folder>\%COMPUTERNAME%\%DATETIME%`

   IMPORTANT: According to the Forest Recovery best practices, the RMAD Active Directory® backup should be stored on a domain controller. At the same time, the **Alternative backup path** option allows you to store the same Active Directory® backup on remote backup storage. This can be useful if the DC is destroyed and you want to restore it from a BMR backup and the latest Active Directory® backup. The retention policy is applied to both backup paths. So, if you set it to 10, and you have both paths configured - it means that there will be 5 backups on DC and 5 backups on the remote storage.

5. To specify a separate account for the backup storage, select the **Use the following account to access the backup storage** option and specify account credentials.

NOTE This account is used to access both backup locations. Currently, separate access accounts are not supported.



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 (RMAD) 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 RMAD asks you to type the password.

Active Directory backup encryption:

- RMAD uses Microsoft's implementation of the AES 256 algorithm from RSA, Inc. (Microsoft RSA Base Provider), with the maximal (normally, 128-bit) cipher strength.
- If you specify DC storage, UNC share or secure storage server for encrypted backups (**Remote Storage** tab): A Backup Agent writes a backup directly to the storage to an encrypted temporary file. This temporary file is local or remote depending on the storage type. Data is encrypted in memory during a backup process. When the backup is done, the temporary file is renamed to the *.bkf file.
- If you specify a local storage for encrypted backups (**Local Storage** tab): A Backup Agent writes a backup via RPC connection to the storage on the Recovery Manager Console machine, data is encrypted in memory.

Bare Metal Recovery (BMR) backup encryption:

- The specified password is used to generate a passphrase with which the backup is encrypted. The password cannot be used directly to unlock the backup container *.vhd(x) file.
- RMAD uses a virtual hard disk encrypted with BitLocker® as a container for the backup (256-bit AES encryption). Only backup volume is encrypted on the VHD disk.
- Data is encrypted in transport by the BitLocker® engine on the DC being backed up.

NOTE

- Backup encryption does not depend on Active Directory® in any way.
- RMAD does not send unencrypted data over the wire.

The BitLocker® Drive Encryption feature should be installed on all backed up domain controllers and on the Forest Recovery Console machine to support encrypted BMR backups. But note that the BitLocker® feature does not encrypt DC drives automatically.

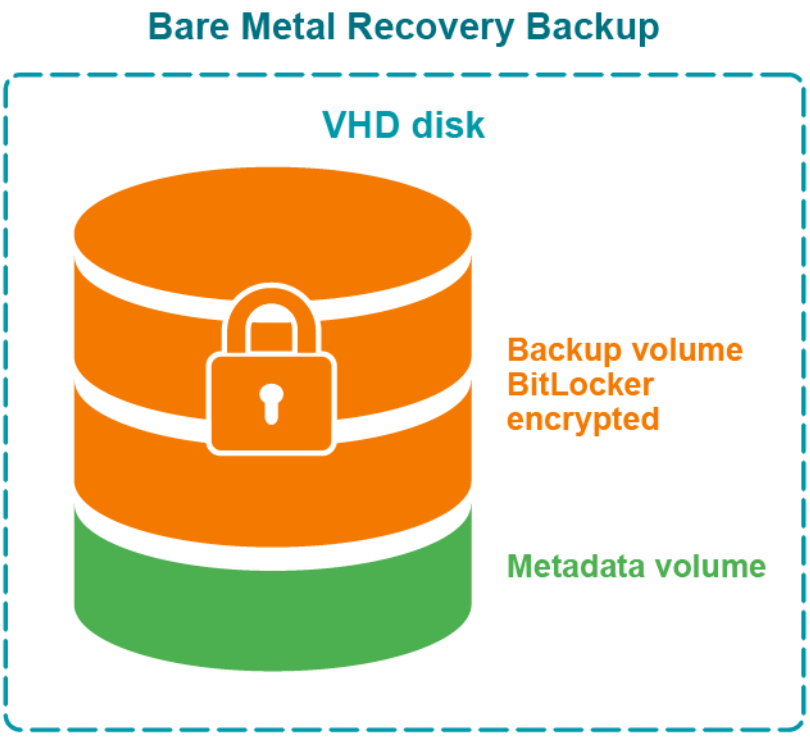


Figure: Encrypted BMR backup

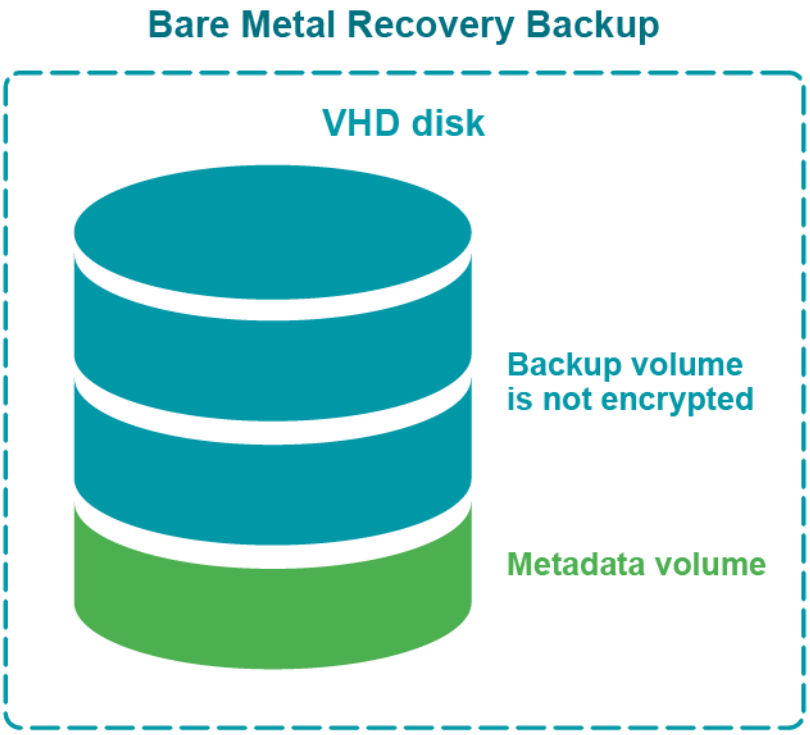


Figure: Not encrypted BMR backup

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 (RMAD) 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 **Advanced** 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 **Completing the Backup Wizard** page of the wizard.
2. In the **Properties** dialog box, click the **Advanced** tab.
3. On the **Advanced** 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 RMAD 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, RMAD 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.

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

Backup scheduling

In RMAD, 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, RMAD 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, RMAD runs as if that user started it.

The user account under which RMAD is running when creating backups must

- Belong to the Administrators local group on the RMAD 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 RMAD 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 RMAD, 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 run under a particular user account. When scheduling backup creation, you need to specify a user account that has administrator privileges on the RMAD 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 (in Windows Server® 2008 or higher) or Group Managed Service Account (in Windows Server® 2012 or higher) can be specified for scheduled tasks in the Computer Collection properties on the **Schedule** tab or in Task Scheduler.

MSA and gMSA requirements:

- Add the $ character at the end of the account name (e.g. domain\computername$) and leave the **Password** field blank.
- The MSA or gMSA account must be a member of the local Administrator group on the RMAD machine.

For details on how to create a gMSA account, see Using Managed Service Accounts.

Requirements towards the user account

Account specified explicitly

In this scenario, the account under which you run your scheduled backup creation task must:

- Belong to the local Administrators group on the RMAD computer.
- Have the “Log on as a batch job” user right on the RMAD computer. This right is granted to the local Administrators group by default.

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

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 RMAD computer and on each serviced computer that hosts the data you plan to back up by using the scheduled backup creation task.
- Have the “Log on as a batch job” user right on the RMAD 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 RMAD to access the serviced computers using a user account different from that under which the scheduled task is being run.

By doing so, you can access the serviced computers located in domains that have no trust relationships established with the domain where RMAD 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, RMAD 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 RMAD services in parallel when creating backups. The default setting is 10 computers. Increasing this number can speed backup creation. However, when RMAD 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.

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, RMAD 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**, **Local Storage**, **Remote Storage**, 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 **Local Storage** or **Remote Storage** tab. To have Recovery Manager for Active Directory store copies of backups in an additional location, select the **Additional backup path(optional)** 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.
3. In the **Properties** dialog box, click the **Advanced** tab. To limit the maximum backup session time, select the checkbox **Limit maximum backup time** or **Limit maximum DC backup time** and specify the time.
4. In the **Properties** dialog box, click the **Agent** tab, and then do the following:
   - To have Recovery Manager for Active Directory initialize Backup Agent using a different account, select the **Access back p 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 RMAD 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.

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.

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 (RMAD) 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:
    - Select the **E-mail notification** check box.
    - In the **To text** box, specify the recipient's e-mail address. More that one address can be entered, separated by a semicolon or a comma.
    - Use the **What to record** list to select what sort of information you want to be included in the notification e-mail message.
    - 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:

- **Service Type** Select SMTP Authentication or Exchange OAuth2 for Microsoft 365 Exchange Online.
- **SMTP Authentication**
    - **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 (default port for SMTP is 25) 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 RMAD 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.

    - **Use Secure Sockets Layer (SSL) to encrypt the connection**. Allows you to use SSL when accessing the e-mail server.

- **Exchange OAuth2 Authentication**
- To set up email notifications for Microsoft 365 Exchange Online, you need to register Recovery Manager for Active Directory with Azure Active Directory. For steps to create and manage your Azure Active Directory application see Registering Application for Microsoft 365 Exchange Online Email Notifications.
    - **From address**. Provides a space for you to specify the return address for your email notification messages. It is recommended that you specify the e-mail address of the RMAD administrator.
    - **Application (client) ID**. Provide the application (client) ID for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.
    - **Directory (tenant) ID**. Provide the directory (tenant) ID for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.
    - **Certificate Thumprint**. Provide the certificate thumbprint for the Azure Active Directory application created for Recovery Manager for Active Directory email notifications.
- **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.

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 specify an e-mail address and 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.
3. The **Properties** dialog box for a backup creation session includes the Progress tab and the General tab.

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.

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.

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.
4. 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 RMAD 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 Active Directory® 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.

Backups node properties

The **Backups** node in the console tree allows you to view a list of backups registered in the RMAD 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 Bare Metal backups

NOTE This option requires Recovery Manager for Active Directory Disaster Recovery Edition. Contact your account representative for more information.

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

To view a list of AD LDS (ADAM) backups

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

You can also register additional backups.

To register additional backups

Active Directory

1. In the console tree, right-click the **Backups** node then right-click the **Active Directory** node.
2. On the shortcut menu, click on **Register Backup**, and then click one of the following commands:

- **Register Backup File**. Registers a Microsoft Tape Format (MTF)-compliant backup file (.bkf). You must specify the path and name for the file to register.
- **Register Backups in Folder**. Registers all MTF-compliant backup files (.bkf) 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.

Bare Metal

NOTE This option requires Recovery Manager for Active Directory Disaster Recovery Edition. Contact your account representative for more information.

1. In the console tree, right-click the **Backups** node then right-click the **Bare Metal** 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). You must specify the path and name for the file to register.
- **Register Backups in Folder**. Registers all MTF-compliant backup files (.bkf) stored in the specified folder.

AD LDS (ADAM)

1. In the console tree, right-click the **Backups** node then right-click the **AD LDS (ADAM)** 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). You must specify the path and name for the file to register.
- **Register Backups in Folder**. Registers all MTF-compliant backup files (.bkf) stored in the specified 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.

Filtering backups

The properties of the **Backups | Active Directory**, **Bare Metal**, and **AD LDS (ADAM)** nodes allow you to have RMAD 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, Bare Metal node, or the AD LDS (ADAM) node

1. In the console tree, click **Backups**, and then select **Active Directory**, **Bare Metal**, or **AD LDS (ADAM)** in the details pane.
2. Right click and 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 RMAD 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 RMAD display only backups taken from the specified domain controller.
  - **Domain controller**. Provides a space for you to type the name of a domain controller. RMAD will display only backups taken from that domain controller.
  - **Domain**. Provides a space for you to type the name of a domain. RMAD 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. RMAD 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 Bare Metal backups

NOTE This option requires Recovery Manager for Active Directory Disaster Recovery Edition. Contact your account representative for more information.

The **General** tab enables you to filter the Bare Metal 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 RMAD 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 RMAD display only backups taken from the specified Bare Metal instance.
  - **Host**. Provides a space for you to type the name of a computer. RMAD will display only backups taken from Bare Metal instances hosted by that computer.
  - **Instance**. Provides a space for you to type the name of an Bare Metal instance. RMAD will display only backups taken from that Bare Metal instance.
  - **Site**. Provides a space for you to type the name of a site. RMAD will display only backups taken from Bare Metal 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**.

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 RMAD 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 RMAD display only backups taken from the specified AD LDS (ADAM) instance.
  - **Host**. Provides a space for you to type the name of a computer. RMAD 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. RMAD will display only backups taken from that AD LDS (ADAM) instance.
- **Site**. Provides a space for you to type the name of a site. RMAD 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**.

Integrity checks for Active Directory, Bare Metal, and AD LDS (ADAM) backups

To perform an integrity check

When a backup is created, a checksum is calculated for the backup file and saved in the backup file when the backup is registered. An integrity check recalculates the checksum and compares it to the checksum stored in the backup file.

NOTE: Regular BMR backups don't have checksum enabled by default. Only Secure Server BMR backups have checksum enabled by default.

The Checksum calculation is enabled by modifying the registry:
`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active Directory\Options\ChecksumCalculationMode`

The various keys for enable/disable Checksum Calculation are:

```
ChecksumAllDisabled = 0
ChecksumBkfRegularStorage = 1
ChecksumBkfSecureStorage = 2
ChecksumBkfAlways = ChecksumBkfRegularStorage | ChecksumBkfSecureStorage
ChecksumBkfOnTheFly = 4
ChecksumBmrRegularStorage = 8
ChecksumBmrSecureStorage = 16
ChecksumBmrAlways = ChecksumBmrRegularStorage | ChecksumBmrSecureStorage
ChecksumDefault = ChecksumBkfAlways | ChecksumBkfOnTheFly |
ChecksumBmrSecureStorage
```

1. In the Recovery Manager for Active Directory console, click the **Backups** node then click the **Active Directory**, **Bare Metal**, or **AD LDS (ADAM)** node.
2. Click a backup you want to check the integrity on.
3. An automatic integrity check will be performed on the import.
4. The following statuses can be displayed after the integrity check has finished:

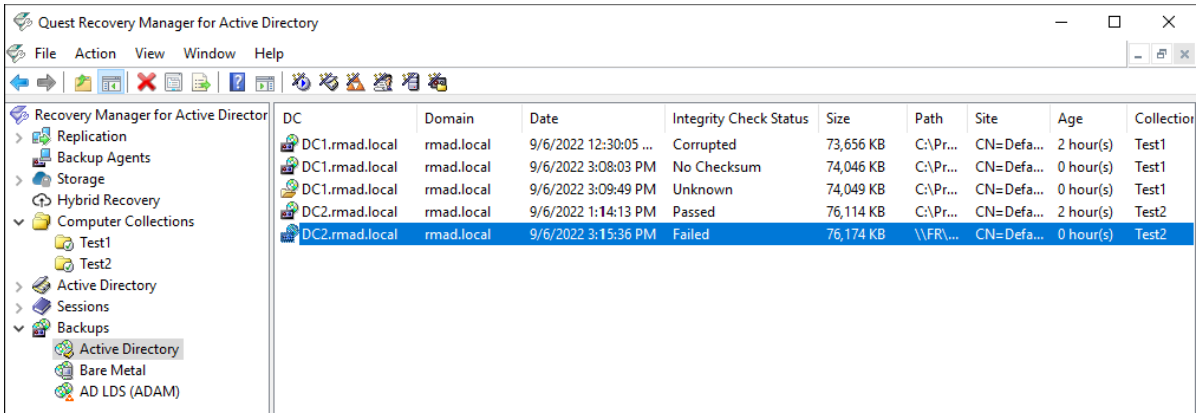
Status	Description
Passed	The newly calculated checksum value matches the previously calculated checksum stored in the backups file.
Unknown	The integrity check was not performed.
Running	The integrity check is in progress.
Failed	The backup is not accessible (wrong credentials) or may have been moved from the path.
No Checksum	The previously calculated checksum could not be read. This could be due to the backup being created by a previous version of the product. The backup also may have been damaged in such a way that the checksum was also affected.
Corrupted	The newly calculated checksum value does not match the previously calculated checksum stored in the backup file.

5. To manually perform an integrity check on any backup already in the Active Directory, Bare Metal, or AD LDS (ADAM) nodes:
6. Click a backup you want to perform the integrity check on.
7. Right click and select Check Integrity.
8. One of the statuses above will be displayed after running the manual integrity check.

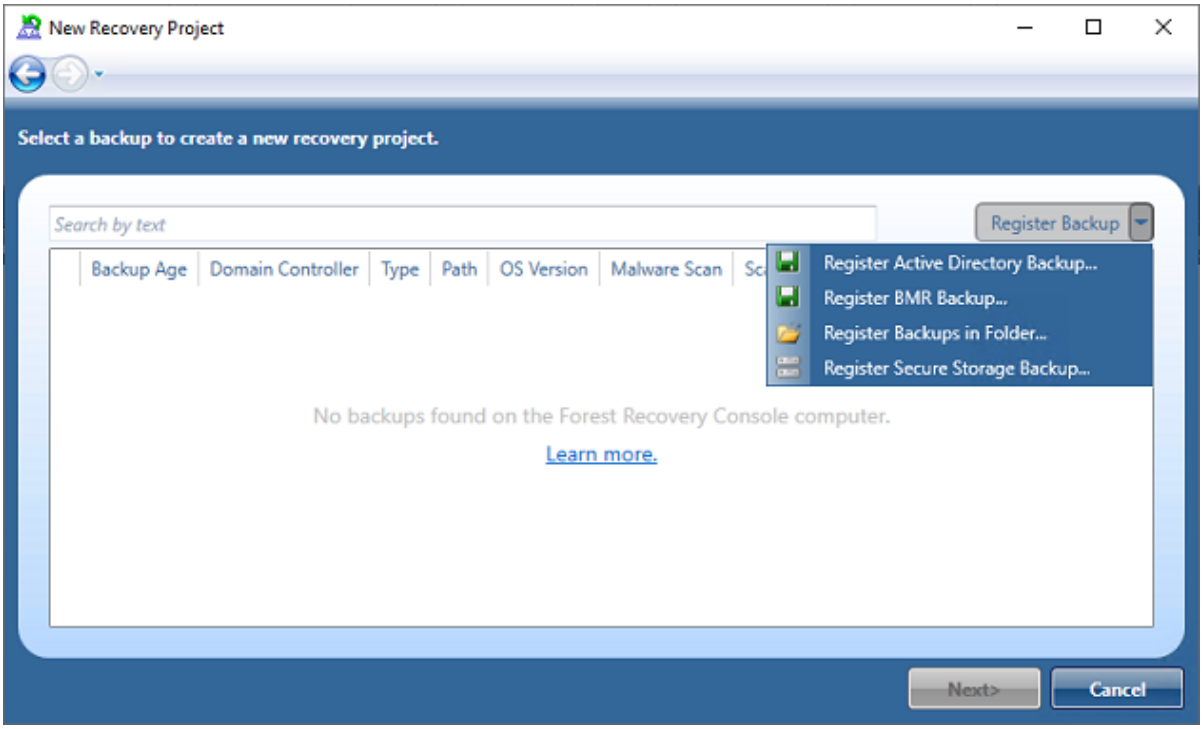
The following backup types are supported for integrity check after the backup registration:

Active Directory backups (.bkf)
AD LDS (ADAM) backups (.bkf)

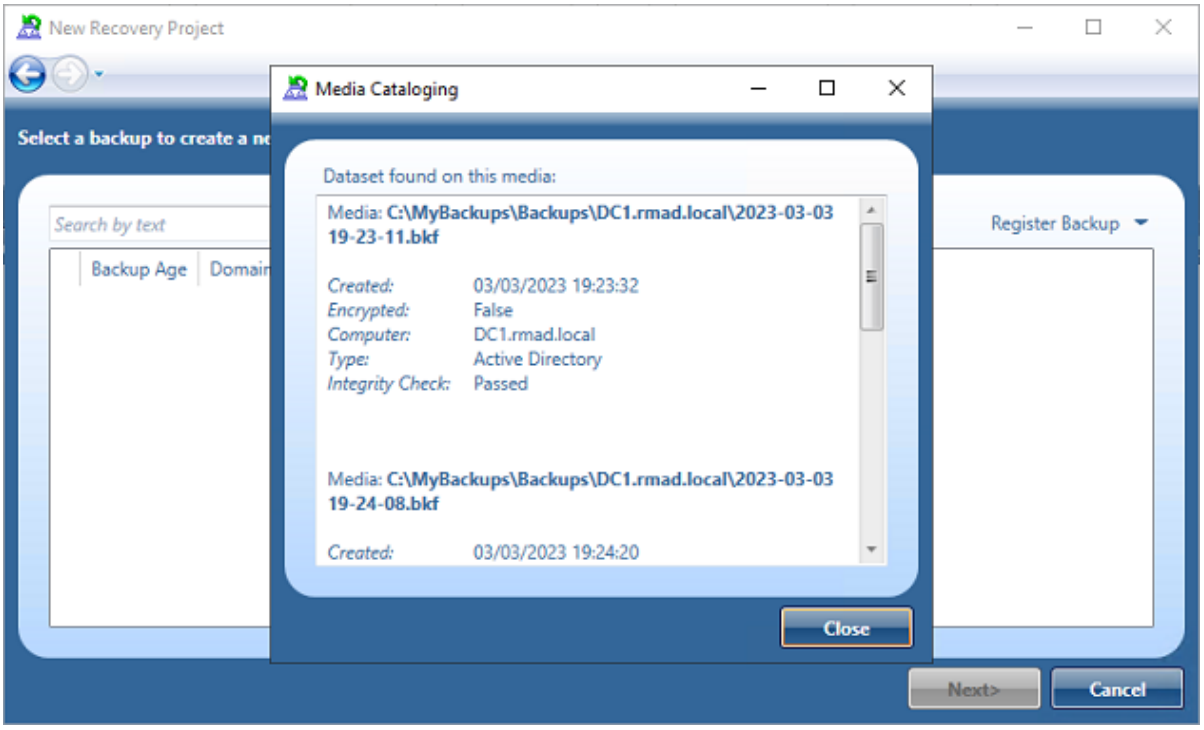
Offline Active Directory Database files (.dit) are ignored.



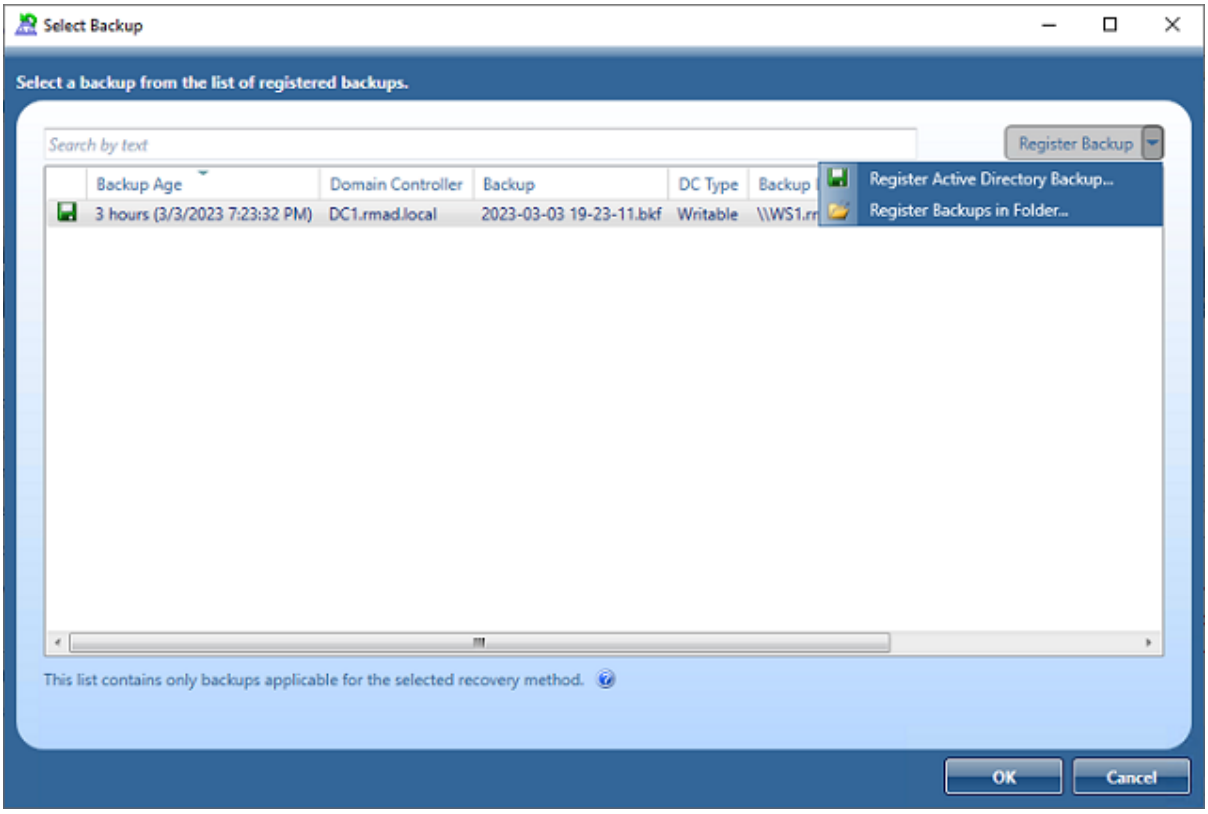
The registering of backups from New Recovery Project dialog in Forest Recovery Console, will automatically execute an integrity check when backups are registered using **Register Active Directory Backup…**, **Register BMR Backup…** and **Register Backups in Folder…** options.



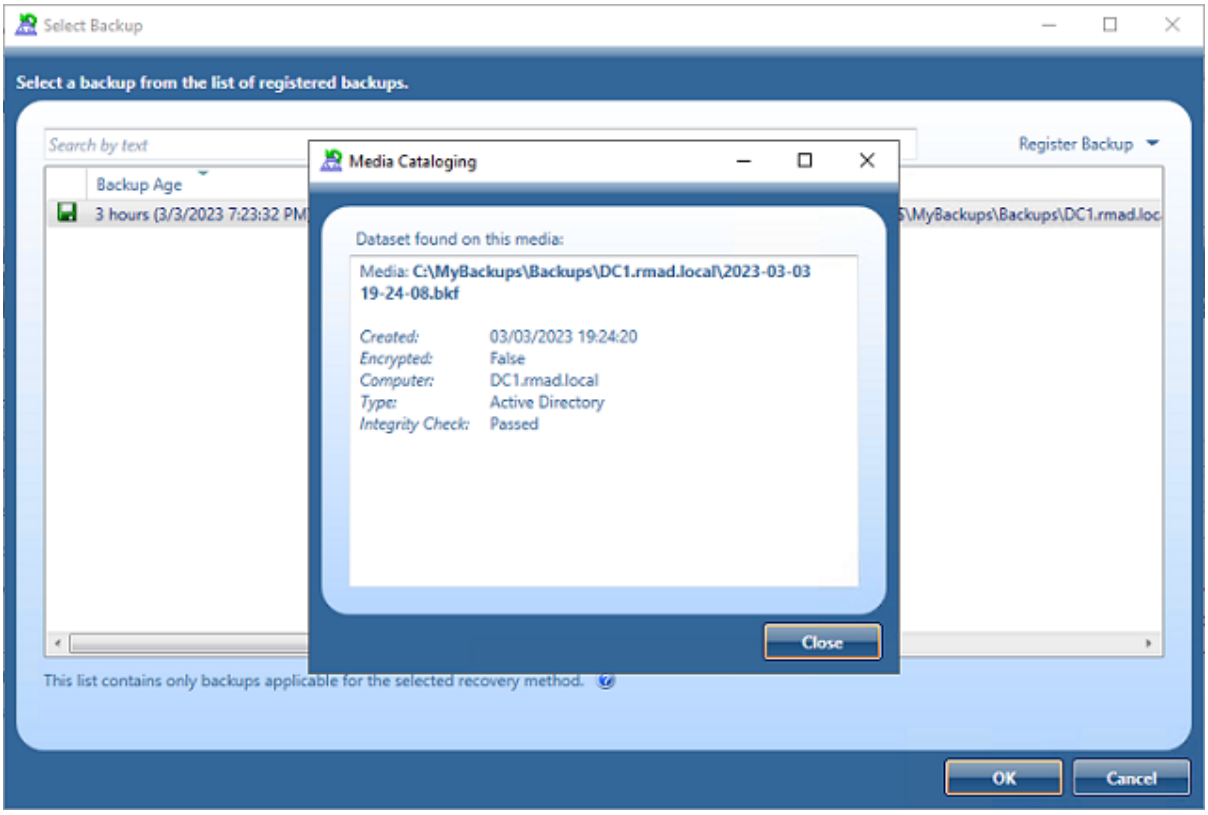
The result of the integrity check is available in the Media Cataloging dialog box.



Registering backups from Select Backup dialog in Forest Recovery Console automatically execute an integrity check for both Active Directory Backup and BMR Backup selection.



The result of the integrity check is available in the Media Cataloging dialog box.



Automatic execution of backup integrity checks from the RMAD Console and Forest Recovery Console can be configured in the registry:

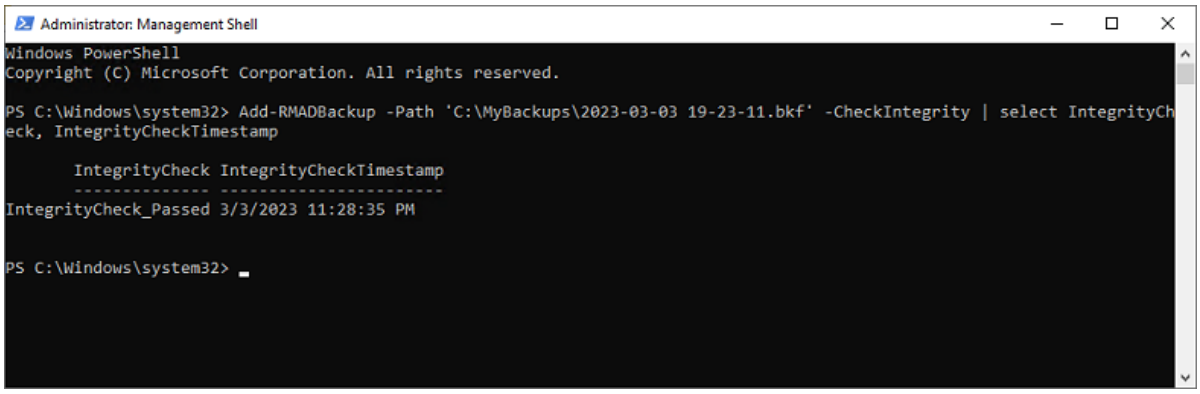
```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active
Directory\Options
IntegrityCheckOnBkfRegistration (REG_DWORD), can be 0 or 1 (default),
allows to run integrity check for AD and ADAM (AD LDS) backups at
registration.
IntegrityCheckOnBmrRegistration (REG_DWORD), can be 0 (default) or 1,
allows to run integrity check for BMR backups at registration.
```

The registering of backups can be done via PowerShell as a parameter has been added to the **Add-RMADBackup** cmdlet to allow an integrity check to be performed after the backup has been registered in the Active Directory database.

```
Add-RMADBackup -Path 'C:\MyBackups\2023-03-03 19-23-11.bkf' -CheckIntegrity
```

The result of the integrity check is available directly in the PowerShell Console or can be viewed in the RMAD Console:

NOTE: IntegrityCheckOnBkfRegistration and IntegrityCheckOnBmrRegistration registry settings do not affect the integrity check with Add-RMADBackup cmdlet.



Export List of Active Directory, Bare Metal, and AD LDS (ADAM) backups

To perform an Export

A list of the backups can be exported to a file for other processing or record keeping.

Exported lists can be saved in one of the following formats:

- Text (Tab delimited) (*.txt)
- Text (Comma delimited) (*.csv)
- Unicode Text (Tab delimited) (*.txt)
- Unicode Text (Comma delimited) (*.csv)

1. In the Recovery Manager for Active Directory console, click the **Backups** node then click the **Active Directory**, **Bare Metal**, or **AD LDS (ADAM)** node.
2. Right click and select Export List…
3. In the Export List dialog, select a location to save the file, enter a file name, and click Save .

Properties of registered Active Directory, Bare Metal, and AD LDS (ADAM) backups

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

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

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

General tab

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

On this tab, you can use the following elements:

- **Backup description:** The description of the backup including server name and date and time of when the backup was created.
- **Domain:** The domain of the server.
- **Created:** The date and time when the backup was created.
- **Backup location:** The location where the backup is stored on the RMAD server (scroll to right to read a long location).
- **Encryption:** The encryption status of the backup.
- **Original size:** The original size of the data before backup.
- **Backup size:** Size of the backup file.
- **Compression ratio:** The compression ration of the backup file compared to the original size.

Components tab

The **Components** tab displays information about the components included in the backup are such items as from Active Directory the SYSVOL size and path and from AD LDS (ADAM) the instances.

For Active Directory

The following items are components that are backed up for Active Directory:

- SYSVOL
- DIT Database
- SAM
- Security
- Software
- System
- Default
- NTUSER DAT
- Components

- SCHEMA.DAT

For AD LDS (ADAM)

The following items are backed up components for AD LDS (ADAM):

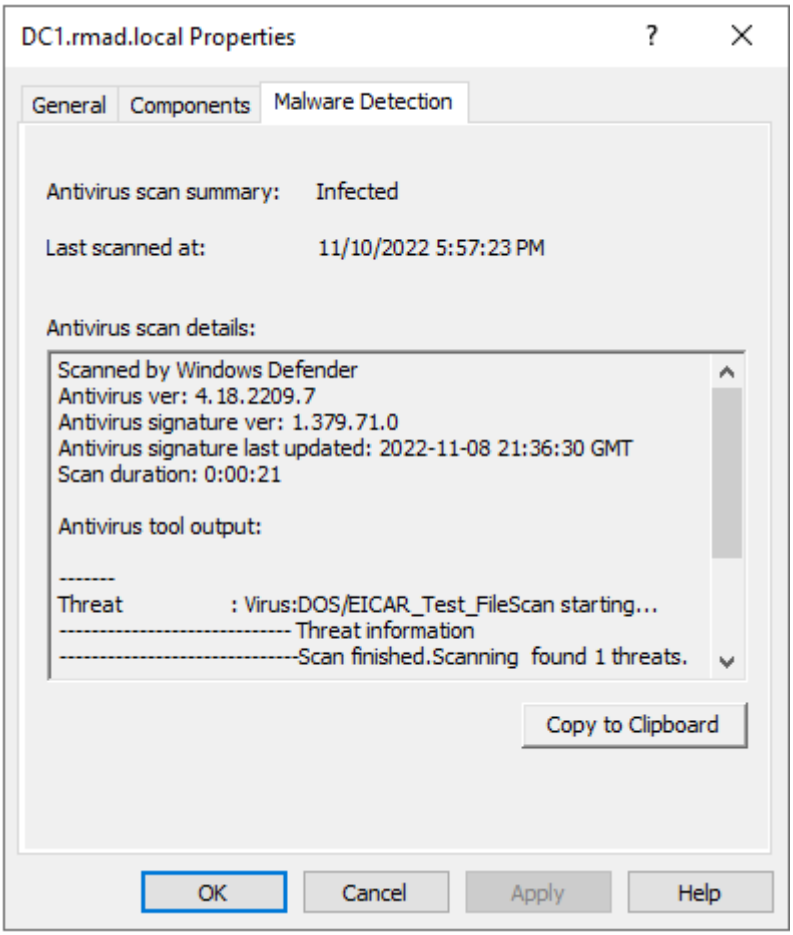
Instances on the AD LDS (ADAM) server.

Malware Detection tab

The **Malware Detection** tab displays information about the selected backup related to malware detection.

On this tab, you can see the following elements:

- **Antivirus scan summary:** A summary of the results of a malware scan.
- **Last scanned at:** The date and time of the last malware scan.
- **Antivirus scan details:** Details information on any malware issues discovered.
- **Copy to Clipboard:** Click to copy the **Antivirus scan details** to the clipboard.



Sample of malware detection

Restoring data

- Getting started with Active Directory recovery
- Managing deleted or recycled objects
- Restoring backed up Active Directory components
- Integration with Change Auditor for Active Directory
- 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 (RMAD). Please read it carefully before you start using the product to restore Active Directory® data.

This section covers:

- Active Directory recovery options
- Implications of the online restore
- Using agentless or agent-based method

Active Directory recovery options

Recovery Manager for Active Directory (RMAD) 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, database corruption, or complete Active Directory® 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.

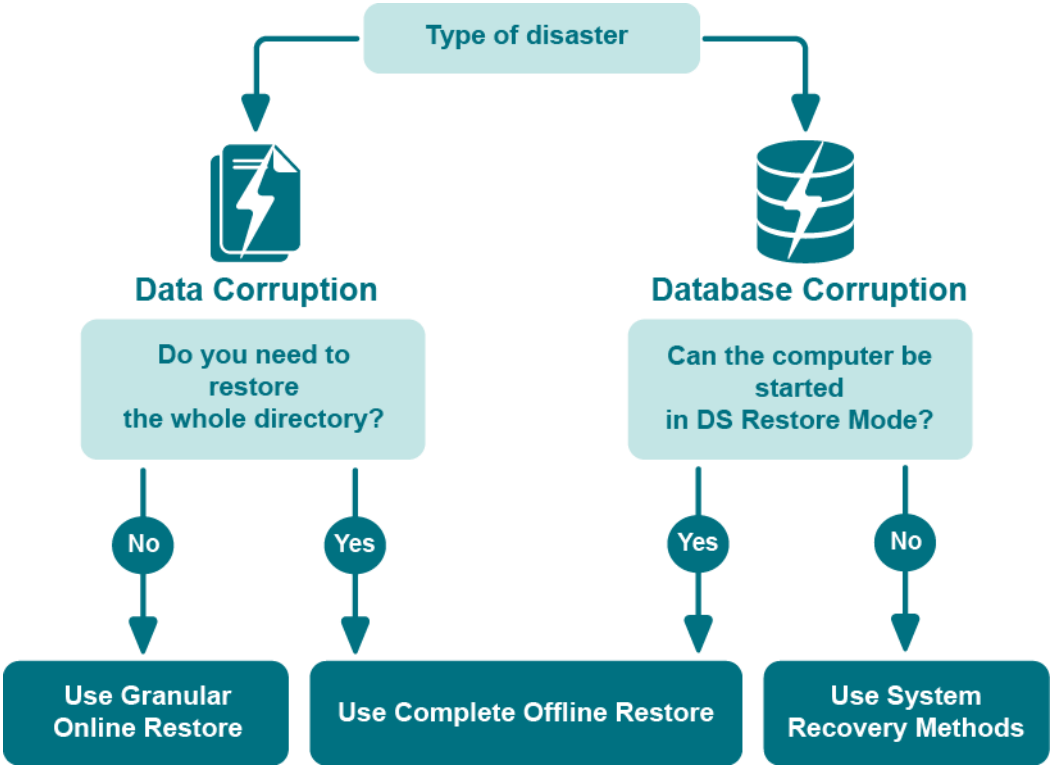


Figure: Active Directory® Recovery Options

RMAD offers the following recovery methods:

- Granular online restore
- Complete offline restore

Granular online restore allows you to restore individual directory objects from a backup, without restarting the target domain controller or affecting other directory objects. 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.

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, RMAD 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.

Granular online restore

To achieve near-zero downtime when recovering Active Directory®, RMAD 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.

For details, see Using granular online restore.

Undeleting (reanimating) objects

With RMAD, you can selectively recover deleted Active Directory® objects by undeleting (reanimating) them. To undelete (reanimate) an object, RMAD 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.

For more information, refer Managing deleted or recycled objects.

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.

For details, see Using complete offline restore.

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 "List of AD DS and AD LDS object attributes that Recovery Manager for Active Directory cannot restore" at Quest Support.

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

Configuration of the test lab:

- **Operating System:** Windows Server® 2008 R2
- **CPU:** 2 x Intel® Xeon® E5-2651 v2 1.8 GHz
- **RAM:** 7.5 GB

Performance test results:

Agent-based restore

Number of objects - Required time

- 1000 - 20 - 40 sec
- 10000 - 04 - 06 min
- 50000 - 23 - 34 min

Agentless restore

Number of objects - Required time

- 1000 - 40 - 70 sec
- 10000 - 06 - 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. 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 Restore Wizard, on the Domain Access Options page, make sure the **Use agentless method** radio button is selected. This ensures that only LDAP functions are used to access the domain controller.

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

1. Select the RMAD 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.

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 (RMAD).

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.
- There may be situations where a user with Admin/Standard privileges may run into issues with DCOM configuration. An error will be generated prompting the user that it is a DCOM issue. The DCOM service needs to be updated in this case for which detailed steps are listed in the following Knowledge Base article Quest Knowledge Base Article 332970 “Cannot create a remote object" - Access is denied at Quest Support.

To use the agent-based method

- In the Restore Wizard, on the Domain Access Options page, make sure the **Use agent-based method** radio button is selected, so that RMAD employs Online Restore Agent to perform the restore or compare operation.

NOTE User can select **Automatically configure firewall before the restore operation** check box, only if the **Use agent based method** radio button is selected.

Manual install of Online Restore agent

The Online Restore agent can be installed manually on a domain controller.

1. Locate **OnlineRestoreAgent.msi**, in the Recovery Manager for Active Directory installation folders and copy it to the domain controller.
2. Double click on the **OnlineRestoreAgent.msi** and follow the instructions to install.

A service called **Quest Online Restore Agent** will be installed.

The Online Restore Agent is installed as a **Manual start** service and in the **Stopped** state.

With the Online Restore Agent pre-installed, the RMAD Console will **Start** the service and then **Stop** it at the end of the operation. If the Online Restore Agent is not present, the agent will be installed and then uninstalled as normal.

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

1. Select the RMAD 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 (RMAD), 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 RMAD.
- To undelete (reanimate) an object, RMAD 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 RMAD.

In order you could selectively recover Active Directory® objects, the user account under which RMAD 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.

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 RMAD to undelete (reanimate) the object or restore it from a backup created with RMAD. 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 RMAD.

  If necessary, you can use RMAD 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 RMAD. 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 RMAD.

  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 RMAD 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:

   - **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.
   - **View objects in a hierarchy** - Select the **Deleted Objects** node in the console tree, then, from the main menu, select **Acton | 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 RMAD.

To recover all deleted objects in an organizational unit

1. On the RMAD 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 RMAD.

Recycling deleted objects

In the Active Directory® forest where Microsoft's Active Directory Recycle Bin is enabled, you can use RMAD 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 RMAD 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:

   - **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.
   - **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 **Acton | 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 RMAD Management Shell.

Recovering recycled objects

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

NOTE Recycled objects can be restored only using the agent-based restore method. This means that the backup that is used to restore recycled objects is created from the target domain controller. For more details, see Agent-based method.

To recover recycled objects

1. On the RMAD 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:

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 RMAD.

Restoring backed up Active Directory® components

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

- DIT Database
- SYSVOL
- Registry, including all registry hives and the file NTUSER.DAT

To restore backed up Active Directory® 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. Click **Next**.
3. Follow the wizard to walk through the restore process.

With the Repair Wizard, you can restore data from Active Directory® backups created by applications that store backups in Microsoft Tape Format (MTF), such as Windows Backup or Veritas™ Backup Exec™. 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.

Integration with Change Auditor for Active Directory

Recovery Manager for Active Directory (RMAD) can be integrated with Quest® Change Auditor for Active Directory to find out which user modified specific Active Directory® objects. Change Auditor is designed to collect information on all critical changes occurred in Active Directory® and track user and administrator activity. For more information about Change Auditor for Active Directory, visit Change Auditor.

The RMAD comparison reports on Active Directory objects can provide information on who (which user account) modified the objects being reported. This information is taken from the Change Auditor database.

From version 10.0.1, RMAD restores the deleted object(s) and continuously restores the last change (if any) that was made to the object attributes after creating the backup, using the data from the Change Auditor database.

In order to integrate, RMAD and Change Auditor must be installed in the same Active Directory® forest. For a list of the Change Auditor for Active Directory versions with which Recovery Manager for Active Directory can be integrated to provide information about the users that modified specific AD objects, see the Release Notes for this version of RMAD.

Required permissions

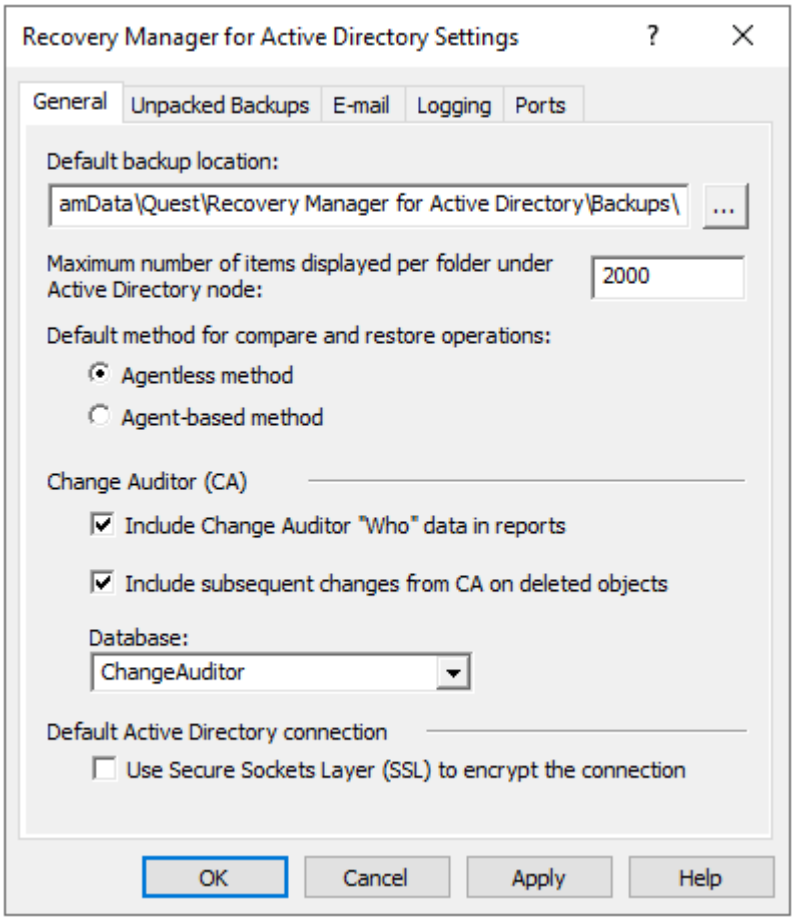
Read-only access for the Change Auditor database is required.

To enable Change Auditor integration

1. In the Recovery Manager Console, right-click the **Recovery Manager for Active Directory** console tree root and select **Settings**.
2. On the **General** tab the following options are available:
   - **Include Change Auditor "Who" data in reports**. When this checkbox is selected, the comparison report includes information on users who modified certain Active Directory® objects. To use this option, you must have Change Auditor for Active Directory installed in the home Active Directory® forest of RMAD.
   - **Include subsequent changes from CA on deleted objects**. When this option is selected, RMAD restores deleted object(s) and continuously restores the last change (if any) that was made to the object attributes after creating the backup.
   - **Database**. Allows you to specify the name of Change Auditor database.

     To specify the CA database server, instance, port, and name, use the following format: <Server Name>\<Instance Name>,<Port>\<Database Name>. **Example:** testserver.domain.com\testinstance,1432\ChangeAuditorDB

NOTE You can disable or enable Change Auditor integration later in the Online Restore Wizard for particular recovery sessions.



Details and limitations related to the continuous recovery ("Include subsequent changes from CA on deleted objects" option):

- The Continuous recovery feature lets you reapply all the object changes that were made between the backup creation and the object deletion.
  - Without the Change Auditor integration, the deleted object will be restored to the state in the backup.

- With the Change Auditor integration, the deleted object will be restored with both Change 1 and Change 2.
- RMAD cannot restore only Change 1 or Change 2.

- The Continuous recovery feature can be used only for deleted objects. It does not make sense to restore the object from backup and then apply Change 1 and Change 2, because it just gives the object's current state. Note that restore of Change 1 or Change 2 only is not supported by RMAD - but supported by Change Auditor. For details, see the Change Auditor for Active Directory documentation.

- Support for restore of non-string attributes, single string, and multiple string attributes.
- Support for the **member**/**memberOf** linked attributes. Other linked attributes cannot be restored. For instance, there is a backup that contains User 1. Then, the customer creates a new group and adds User 1 in this group. Then, User 1 is deleted. If the customer wants to combine data from backup and changes that were made between creating the backup and user deletion (data from the Change Auditor database) - User 1 will be restored as a member of this group.

To generate a report that shows who modified specific AD objects

1. To start Online Restore Wizard, open Recovery Manager Console. Then right-click the **Recovery Manager for Active Directory** console tree root and select **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 Change Auditor "Who" data in reports** check box, and then specify the Change Auditor database you want to use. Also, you can select the **Include subsequent changes from CA on deleted objects** option.
6. Step through the wizard until you reach the Operation Option page. Click **View Report**.

The Comparison report provides the following information:

- **Old value** column shows data from the backup or Change Auditor database.
- **New value** column shows changes that occurred in Active Directory® since the last backup.
- **Modified by** column provides information on who modified particular Active Directory® objects (only if you use integration with Change Auditor)

1 of 1 100% Find | N

Object DN	Object class	Type of change	Modified by
CN=TestUser,CN=Users,DC=rmad,DC=local	User	Deleted	RMAD\Administrator

Attribute name	Type of change	Old value	New value	Modified by
Is-Deleted	Added		TRUE	
Is-Recycled	Added		TRUE	
Account-Expires	Deleted	<never>		
Code-Page	Deleted	0		
Country-Code	Deleted	0		
SAM-Account-Type	Deleted	0x30000000 (USER_OBJECTNORMAL_USER_ACCOUNT)		
Last Name	Deleted	123456		RMAD \Administrator
Pwd-Last-Set	Deleted	5/20/2019 1:32:27 PM		
Primary-Group-ID	Deleted	513		
Object-Category	Deleted	CN=Person,CN=Schema,CN=Configuration,DC=rmad,DC=local		
Logon Name	Deleted	test@rmad.local		
Display Name	Deleted	TestUser		

The Restore report provides the following information:

- **Old value** column shows changes that occurred in Active Directory® since the last backup.
- **New value** column shows data that were restored from the backup or Change Auditor database
- **Modified by** column provides information on who modified particular Active Directory® objects (only if you use integration with Change Auditor)

Object DN	Object class	Type of change	Modified by
CN=SampleUserCa,CN=Users,DC=rmad,DC=local	User	Undeleted	RMAD\Administrator

Attribute name	Type of change	Old value	New value	Modified by
Phone Number (Others)	Added		Another Value	RMAD \Administrator
Phone Number (Others)	Added		First Number	RMAD \Administrator
Display Name	Added		SampleUserCa	RMAD \Administrator
Logon Name	Added		SampleUserCa@rmad.local	RMAD \Administrator
Phone Number (Others)	Added		Second Number	RMAD \Administrator
Phone Number (Others)	Added		Thirsd Number	RMAD \Administrator
Admin-Count	Deleted	0		RMAD \Administrator
Operator-Count	Deleted	0		RMAD \Administrator
Is-Deleted	Deleted	TRUE		RMAD \Administrator
Account-Expires	Modified	<never>	<never>	RMAD \Administrator
User-Account-Control	Modified	0x202 (ACCOUNTDISABLE | NORMAL_ACCOUNT)	0x200 (NORMAL_ACCOUNT)	RMAD \Administrator
Distinguished Name	Modified	CN=SampleUserCa \0ADEL:3c90f8e5-f5c9-4406-875f-a38b380677e8,CN=Deleted Objects,DC=rmad,DC=local	CN=SampleUserCa,CN=Users,DC=rmad,DC=local	RMAD \Administrator

Using granular online restore

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 RMAD 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.

To perform granular online restore, start the Online Restore Wizard and follow the instructions in the wizard.

NOTE RMAD 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 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 RMAD 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.

RMAD supports granular online restore from BMR backups.

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.

NOTE For Online Restore Wizard, Recovery Manager for Active Directory supports DC backups even if a DC, where the backups have been done, has been removed from the domain or renamed. The exception is the old computer object, or any other object directly or indirectly linked to the old computer object. For instance, if a user upgrades the operating system on a DC, renames it, and wants to use the old backup collected before changes in the environment were made - this scenario is not supported.

On the Domain Access Options page, you have the option to access the target domain controller using either LDAP functions only (agentless method) 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.

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, see the *Searching, browsing for, or importing objects* section below.
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.

Searching, browsing for, or importing objects

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.

Restoring AD LDS (ADAM)

With Recovery Manager for Active Directory (RMAD), 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 "List of AD DS and AD LDS object attributes that Recovery Manager for Active Directory cannot restore" at Quest Support.

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 RMAD.

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 RMAD.

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 RMAD. For more information on these attributes, see Quest Knowledge Base Article 59039 "List of AD DS and AD LDS object attributes that Recovery Manager for Active Directory cannot restore" at Quest Support.

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.

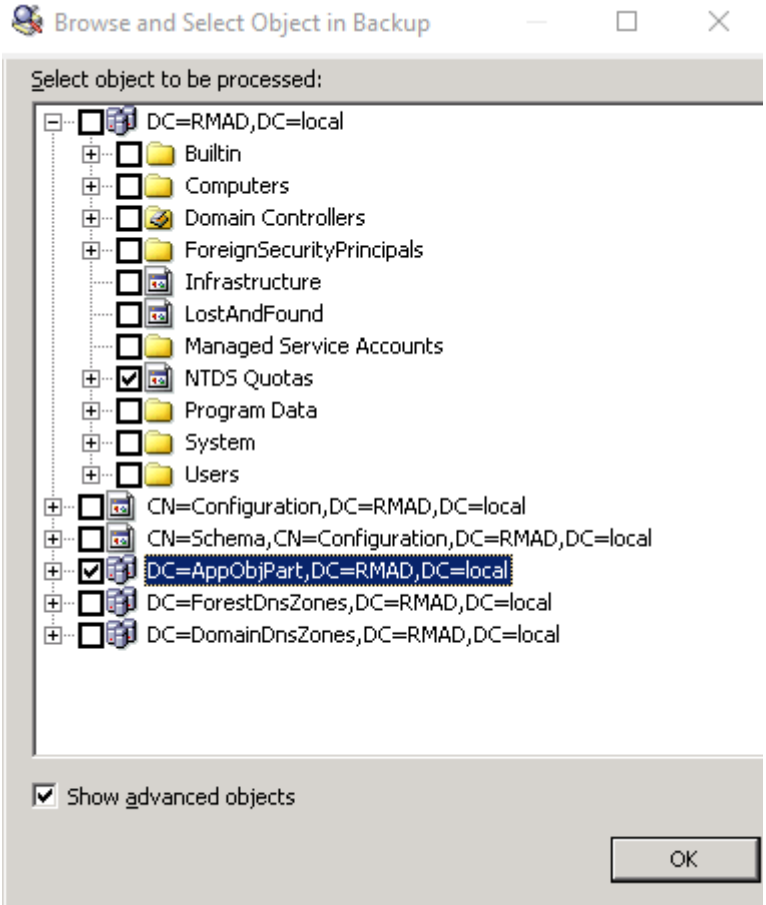
The entries in the upper part of the **Attributes** list allow you to select groups of attributes. For example, when you select **Account Information**, all account-related attributes are selected.

Restoring objects in an application directory partition

Application directory partitions are used to store application-specific data. When restoring Active Directory® from a backup, RMAD 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:
   - Select **Any type** from the **Find** list.
   - Click **Browse** and use the **Browse and Select Object in Backup** dialog box to select the application directory partition to search:



   - Ensure that the **Show advanced objects** check box is selected: otherwise, the dialog box displays only the domain directory partition.
   - 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

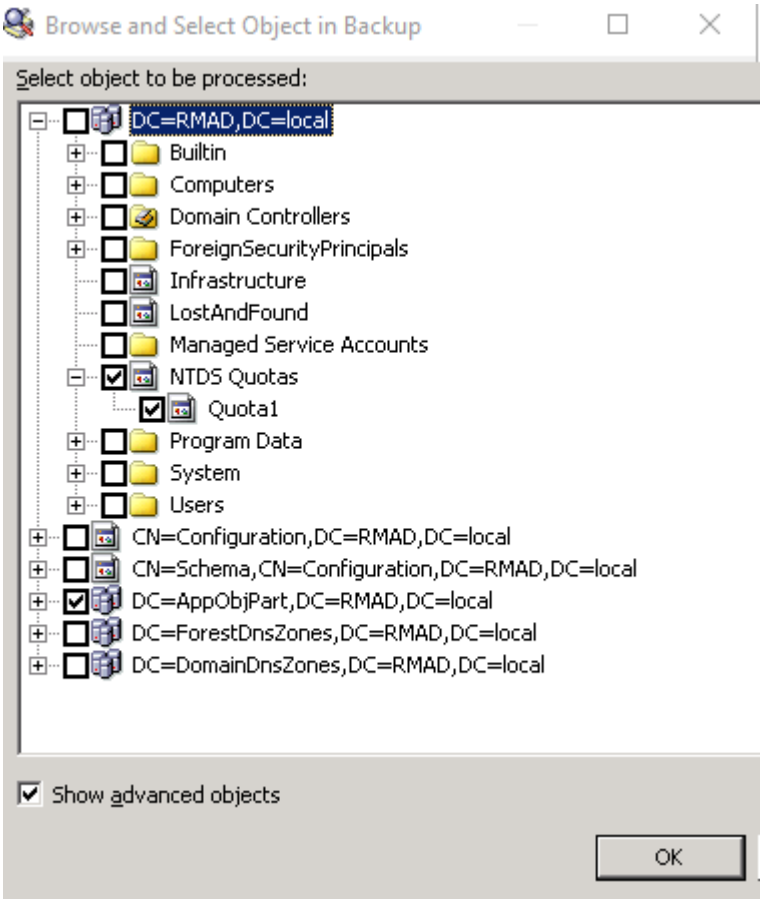
Object quotas are used to determine the number of objects that can be created in a given directory partition by a given administrator. Object quotas help prevent the denial of service situations that can occur if an administrator accidentally or intentionally creates so many objects that the domain controller 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 RMAD, 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® 2008 or later. To restore a deleted object, the user account under which RMAD 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® 2008 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.

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 (RMAD) 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 RMAD.

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
- Data 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 RMAD performed on AD objects. Alternatively, you can generate and view a summary of all compare and restore operations performed with RMAD 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. To start Online Restore Wizard, open Recovery Manager Console. Then right-click the **Recovery Manager for Active Directory** console tree root and select **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 Additional 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 RMAD 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 RMAD. Alternatively, you can generate and view a summary of all compare and restore operations performed with RMAD 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. To start Online Restore Wizard for AD LDS (ADAM), open Recovery Manager Console. Then right-click the **Recovery Manager for Active Directory** console tree root and select **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 RMAD 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. To start Group Policy Restore Wizard, open Recovery Manager Console. Then right-click the **Recovery Manager for Active Directory** console tree root and select **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" at Quest Support.

Data about who modified Active Directory® objects

You can use the Recovery Manager for Active Directory (RMAD) reports to find out which user modified specific Active Directory® objects. To provide this functionality, RMAD requires another Quest product - Change Auditor for Active Directory. For details, see Integration with Change Auditor for Active Directory.

To generate a report that shows who modified specific AD objects

1. To start Online Restore Wizard, open Recovery Manager Console. Then right-click the **Recovery Manager for Active Directory** console tree root and select **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 Change Auditor "Who" data in reports** checkbox, and then specify the Change Auditor database you want to use. Also, you can select the **Include subsequent changes from CA on deleted objects** option. When this option is selected, RMAD restores deleted object(s) and continuously restores the last change (if any) that was made to the object properties after creating the backup, using data from the Change Auditor database.
6. Step through the wizard until you reach the Operation Option page. Click **View Report**.

Using complete offline restore

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. It is better to use Bare Metal Recovery in this case.

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.

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™. 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, RMAD 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 an Active Directory® backup. This restores the entire Active Directory® database along with the other Active Directory® 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.

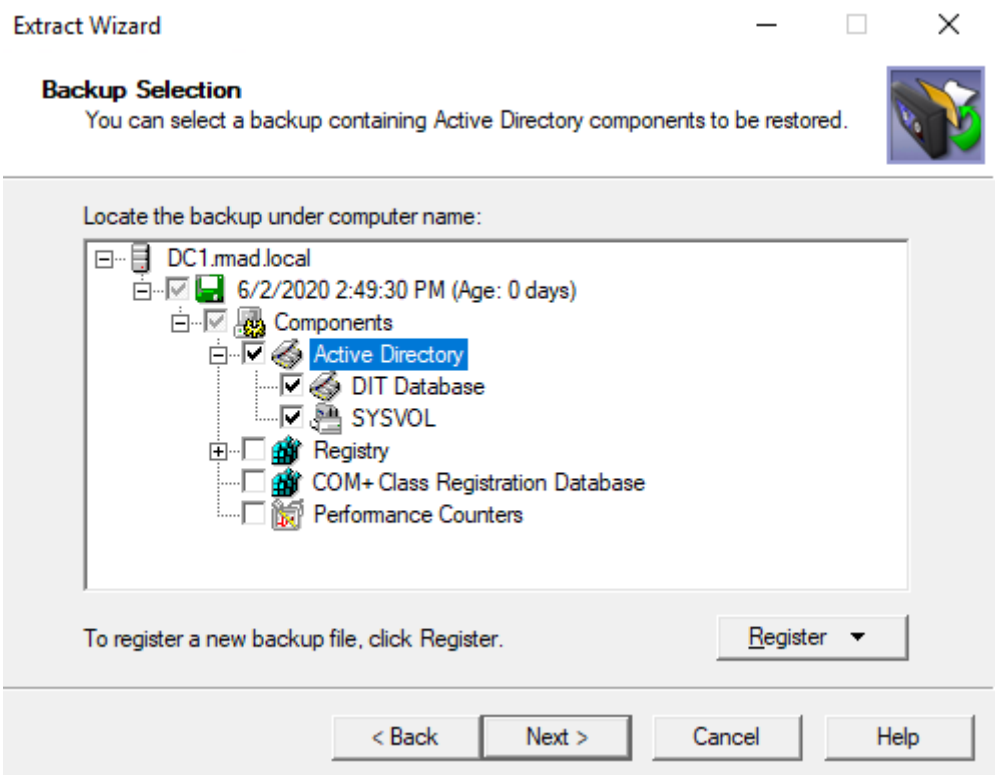
Since the Online Restore Wizard and Group Policy Restore Wizard allow you to authoritatively restore directory data with minimal effort and overhead, we recommend you to use those wizards rather than the Repair Wizard when you need to recover/undelete individual Active Directory® objects and Group Policy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

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 (RMAD) , you can selectively restore Group Policy information from normal Active Directory® 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 Active Directory®.

After RMAD 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 Active Directory® 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' Active Directory® can be created, for example, 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).
    - **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 Active Directory® 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 Active Directory® 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 2008-based domain controller from a backup
- Creating a Windows Server 2012-based domain controller or later from a backup

Creating a Windows Server® 2008 R2-based domain controller from a backup

This section describes how to create a Windows Server® 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 R2-based domain controller's Active Directory®.

   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 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 or higher from a backup

This section describes how to create a Windows Server® 2012 or higher 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 or higher computer
- Step 3: Use the Install-ADDSDomainController cmldet to install from media

Step 1: Create and extract a backup

1. Create a backup of a Windows Server® 2012-based or higher domain controller's Active Directory®.

   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 or higher computer

On the Windows Server® 2012-based or higher 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).

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)

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:

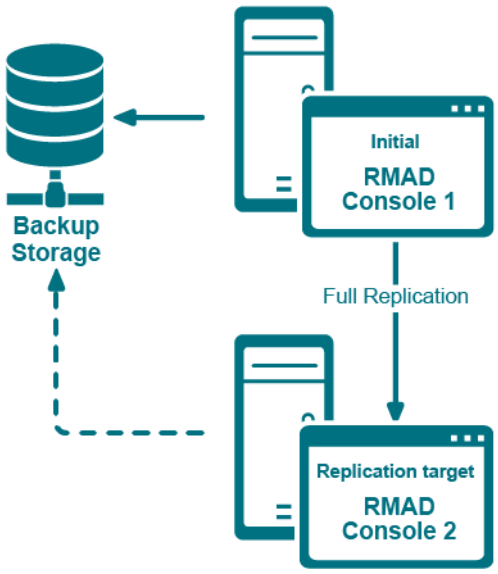
```
8 + current searchFlags attribute value = new searchFlags attribute value
```

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:
    - Start the ADSI Edit tool (Adsiedit.msc).
    - In the left pane of the console, right-click the **ADSI Edit** console tree root, and then on the shortcut menu click **Connect to**.
    - 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.
    - 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:
    - On the **Attribute Editor** tab, select searchFlags from the **Attributes** list, and then click the **Edit** button.
    - In the **Attribute Editor** box, enter the new value and click **OK**.

Full Replication

Recovery Manager for Active Directory (RMAD) provides an ability to switch from the initial Recovery Manager Console to the alternate instance of the console in case of any system failure, e.g. hardware failure. The Full replication feature lets you create a full copy of the initial console settings on the console that is used as a replication target, so that the target console can fully take over the initial console and perform exactly the same operations.



This functionality is based on the Recovery Manager Remote API Access service (installed by default) and PowerShell® commands. When the Full replication 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.

Which settings are replicated?

- Global settings
- Computer collection settings, including the retention policy setting
- Computer collections
- Secure Storage servers
- Backup schedule task
- 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").
  - Secure Storage backup information.

NOTE:

- The replication sessions will be retained for a default of 10 days. To set a different retention time, create a registry key, "**ReplicationSessionLimitDays**" in `HKLM\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active Directory` and set the key to the number of days required (decimal).
- You can specify a fallback account which will be used for replacing accounts in backup schedule tasks if these accounts cannot be replicated to the local console. It is recommended to specify a fallback account if backup schedule tasks use a regular Active Directory account, a local account or a gMSA account that cannot be resolved on the local console. Otherwise, the replication will fail.
- If the backup schedule account is a domain user or local user, it will be changed to "SYSTEM".
- If the user account is Managed Service Account (in Windows Server 2008 or higher) or Group Managed Service Account (in Windows Server 2012 or higher), make sure that the account works in the current console. Otherwise, it will be changed to "SYSTEM" too.
- All backups schedules are disabled after the replication.

For details on how to create a gMSA account, see Using Managed Service Accounts.

Configure the full replication in Recovery Manager Console

This section describes how to create a full copy of the initial console settings on the local instance of Recovery Manager Console and switch to the local console in case of the initial console failure.

NOTE Backups themselves are **not replicated** to the remote console and **only information** about the Backups of Active Directory which include the domain controller, domain, date of the backup and the size and location of the source backup.

IMPORTANT:

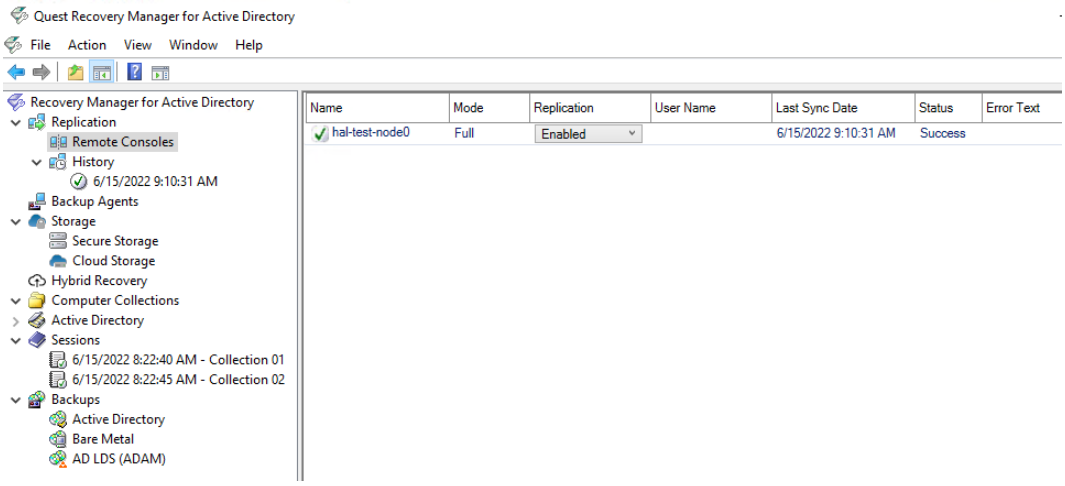
- It is recommended to use the full replication between consoles in the same datacenter to quickly switch to the target console in case of the initial console goes down.
- Single replication source mode: you can add several remote consoles to the replication list, but only one remote (initial) console can be used for replication.
- All discovered Backup Agent instances on the local console are deleted during the Full replication. The data from the initial console completely rewrite all other local data (collections, collection properties, etc).
- After the replication, data on the target console is read-only, but you can perform the compare and restore operations using this console.
- It is recommended that you schedule the backup tasks and the replication task so that they do not overlap.

To add a remote (initial) console to the local (replication target) console and force the replication

1. Open the local RMAD console.
2. Right-click **Remote Consoles** under 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. **Replication mode** provides the following options.
    - **Replicate backup information only (Backup mode)**
    - **Replicate backup information, collections, global settings and schedule (Full mode)**. Set Fallback account for performing schedule replication. The **Fallback Account** is a pre-configured account for replacing the account that is used by the backup creation task. Select **Do not specify credentials** which if choosen then only System or gMSA accounts that are availkable on both master and slave console machines will be kept after replicating backup tasks. Select **Use the following credentials** to add another account that has administrator privileges on the systems to be backup up.
    - Click the **Replicate forest recovery project files** check box to replicate the Forest Recovery Project files to the console. Click on the Configure button to specify the location of the Source project files (.frproj) and specify the Target folder location for the project files (.frproj).
5. Supply the credentials for the replication task. These credentials will be used to connect the source console that you have just added.
    - 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.

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 **Remote Consoles** and press **Replicate**.



9. To change the console properties, right-click the console instance from the list in the right pane and select **Properties**.
10. To remove the console instance from the replication console list, right-click the instance and click **Remove**.

IMPORTANT **To activate the target console in case of the initial console failure, go to the Remote Consoles node and set the replication status of the initial console to Disabled in the right pane.This action turns off the read-only mode on the target console and the console completely takes over the functions of the initial one.**

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 RMAD is not installed on the specified host.
  - If the Recovery Manager Remote API Access service has stopped
  - If you experience network connection problems
  - If the account that is used for the replication task is blocked, etc.

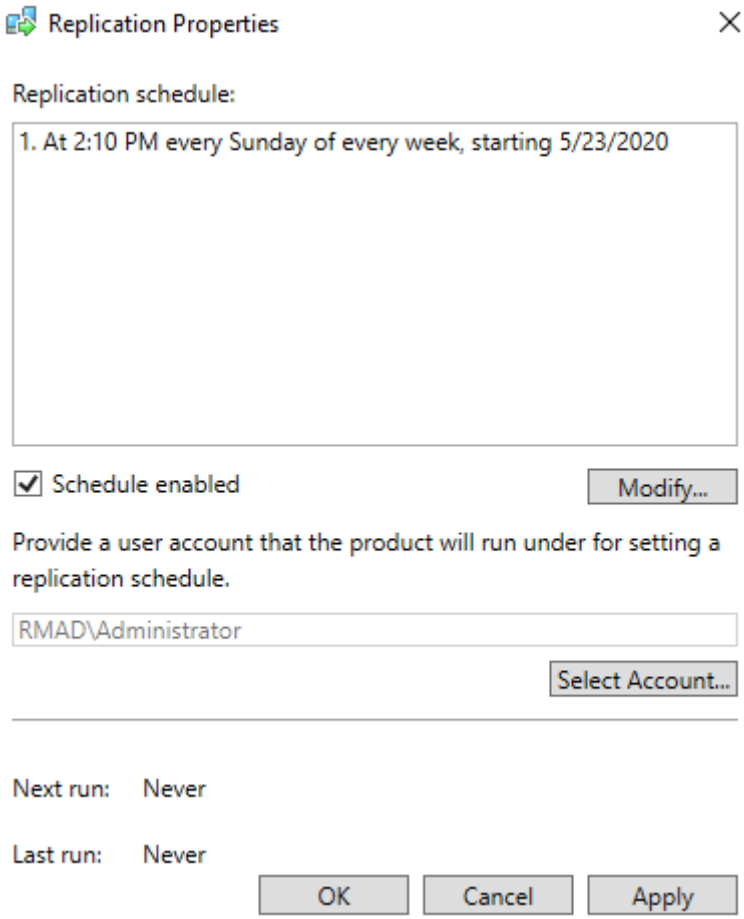
To view the replication history

NOTE Backups themselves are **not replicated** to the remote console and **only information** about the Backups of Active Directory which include the domain controller, domain, date of the backup and the size and location of the source backup.

1. Open the local Recovery Manager for Active Directory console.
2. Click **History** under the **Replication** node to view the list of replication sessions.
3. If you click a replication session, the right pane shows all remote consoles that are involved in the specified replication session.
4. To remove one or more replication sessions from the list, right-click the session node and select **Delete**. Multi-select is possible.

To create a replication schedule

1. In the RMAD console, right-click the **Remote Consoles** node under 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.

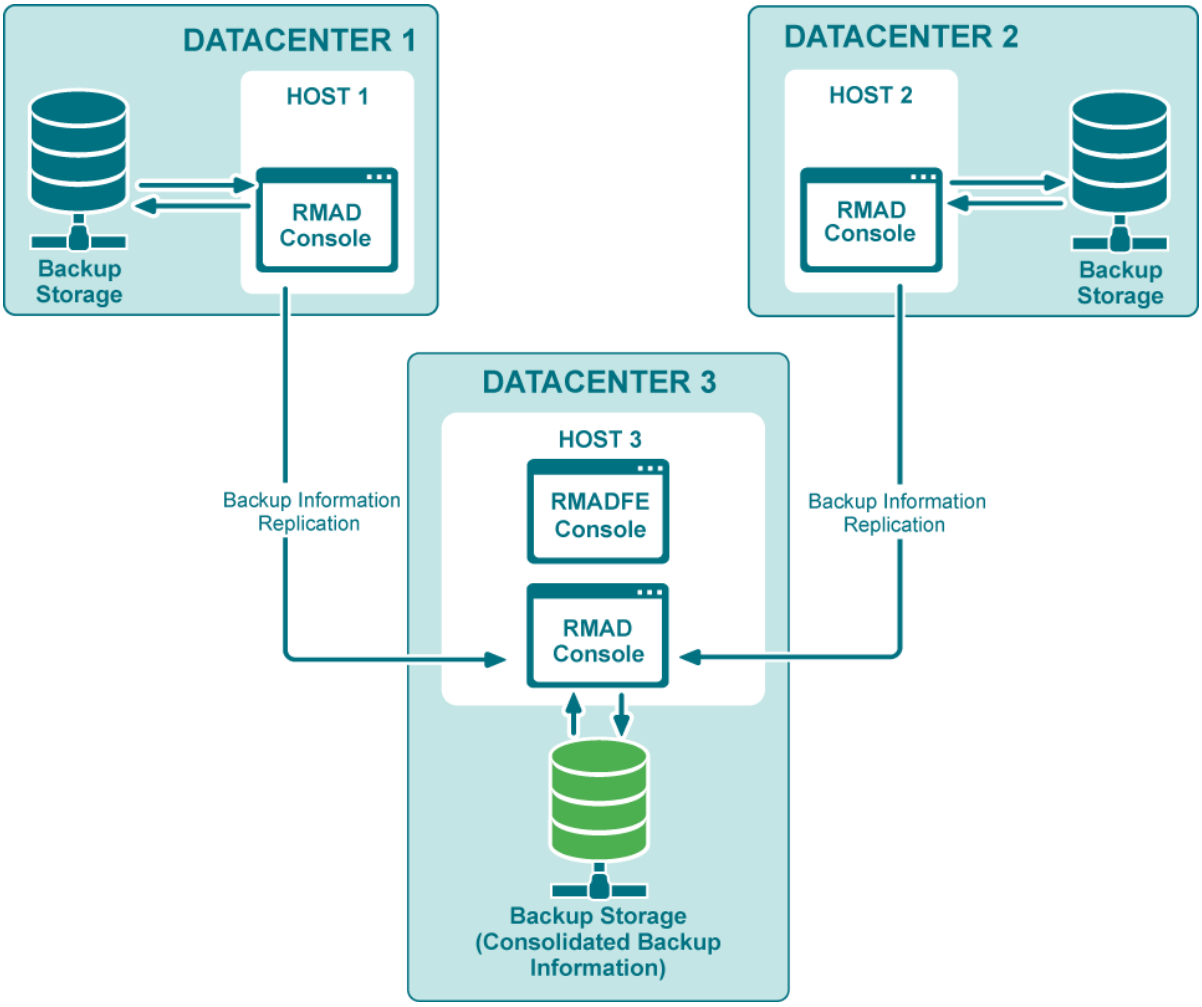


3. Make sure that the **Schedule enabled** option is selected in the **Replication Properties** dialog.
4. Provide a user account that will be used to start the replication schedule task using **Select Account…** in the **Replication Properties** dialog. Minimum requirements for the account are listed above depending on the replication mode.
5. Click **OK**.

NOTE You can specify Managed Service Account (in Windows Server® 2008 or higher) or Group Managed Service Account (in Windows Server® 2012 or higher) to run the replication schedule task. Note that you must add the dollar 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 RMAD machine.

Consolidating backup registration data

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. Recovery Manager for Active Directory (RMAD) allows you to consolidate backup information from multiple backup registration databases on a single RMAD computer. The main user scenario for using this functionality is to make this data available to Forest Recovery Console. So, Forest Recovery Console must be installed together with Recovery Manager Console on the computer that hosts consolidated backup database to access and use the backup files created by all other RMAD instances installed in your environment.



This functionality as well as the Full replication feature is based on the Recovery Manager Remote API Access service (installed by default) and PowerShell® commands. When the backup replication is enabled, the current console connects to the Recovery Manager Remote API Access service on the remote RMAD console, then imports the data.

NOTE The TCP port **52132** is required for Recovery Manager Remote API Access service.

Configure replication of backup information in Recovery Manager Console

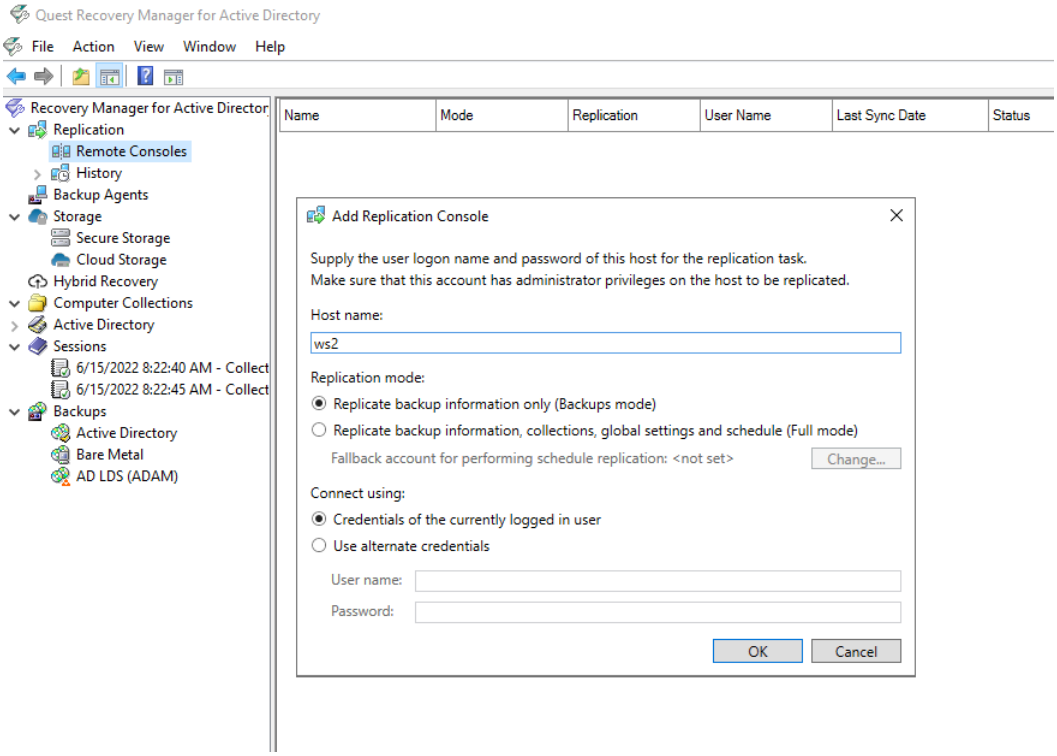
This section describes how to configure replication of backup information from remote consoles to the local backup storage.

IMPORTANT:

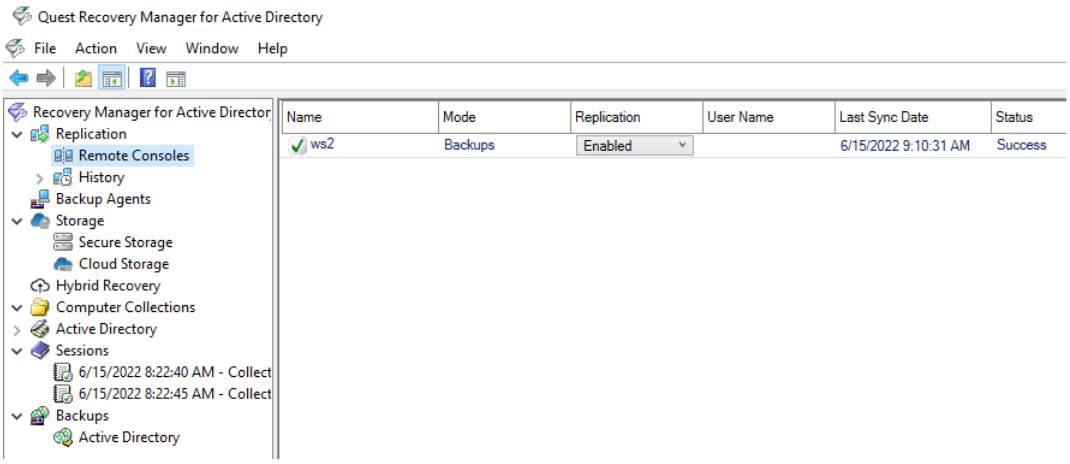
- It is recommended to use this option for consoles that reside in geographically remote datacenters.
- Consolidating backups does not affect the backup files.
- Replication of backup information is one way. If you need to configure two-way replication, you should configure it explicitly in both instances of Recovery Manager Console.
- 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 consolidated with the backups from remote consoles.
- It is recommended that you schedule the backup tasks and the replication task so that they do not overlap.

To add a remote console to the local console and force the replication of backup information

1. Open the local Recovery Manager for Active Directory console.
2. Right-click **Remote Consoles** under 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 **Replicate backup information only (Backups mode)**. This option lets you replicate backup information from the replication source.



5. Supply the credentials for the replication task. These credentials will be used to connect the source console that you have just added.
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 **Remote Consoles** and press **Replicate**. This option forces the replication for all consoles in the list, not only for the selected one .



9. To change the console properties, right-click the console instance from the list in the right pane and select **Properties**.
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 RMAD on the specified computer." in the following cases:
  - If the target computer does not exist or RMAD is not installed on the specified host.
  - If the Recovery Manager Remote API Access service has stopped
  - If you experience network connection problems
  - If the account that is used for the replication task is blocked, etc.

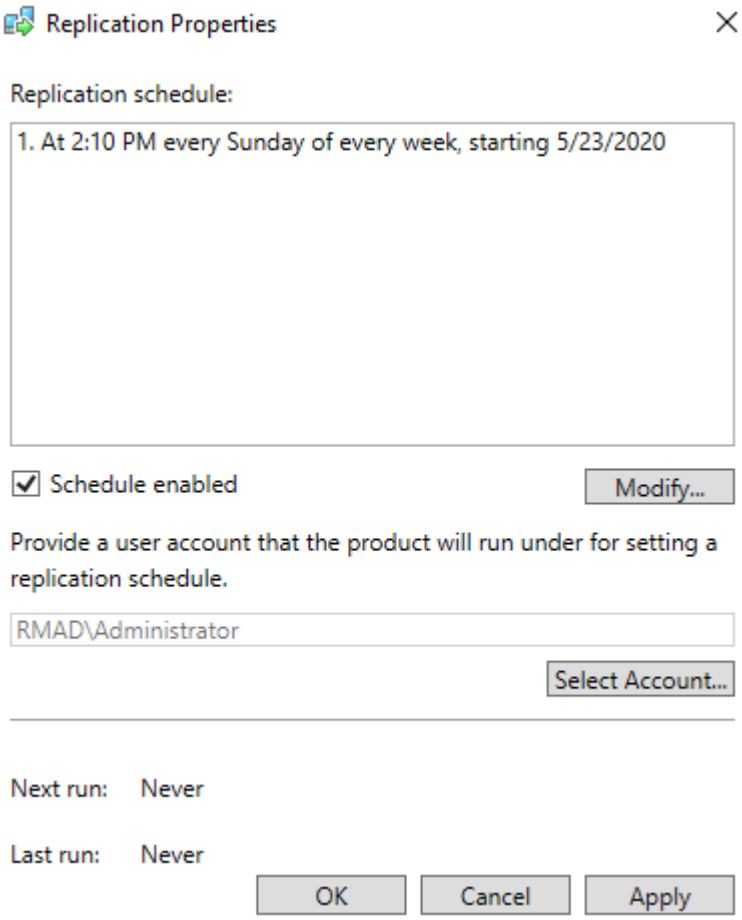
To view the replication history

1. Open the local RMAD console.
2. Click **History** under the **Replication** node to view the list of replication sessions.
   The list shows the replication sessions for the past 10 days by default. To change the default number of days, edit the value of the registry HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Quest\Recovery Manager for Active Directory\Synchronization\ReplicationSessionLimitedDays
3. If you click a replication session, the right pane shows all remote consoles that are involved in the specified replication session.
4. To remove one or more replication sessions from the list, right-click the session node and select **Delete**. Multi-select is possible.

To create a replication schedule

1. In the RMAD console, right-click **Remote Consoles** under 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**.

NOTE You can specify Managed Service Account (in Windows Server® 2008 or higher) or Group Managed Service Account (in Windows Server® 2012 or higher) to run the replication schedule task. Note that you must add the dollar 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 RMAD machine.

Monitoring Recovery Manager for Active Directory

Recovery Manager for Active Directory (RMAD) 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 RMAD. 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 2022, 2019, 2016, and 2012 R2

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.xml** or **Quest.Recovery.Manager.for.Active.Directory.Limited.xml** file supplied in the RMAD distribution package. When you are finished, click **Open**.
7. Click **Install** and follow the on-screen instructions to complete the Management Pack installation.

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.

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
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

Rule	Default setting
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

Health dashboards

In the SCOM Operations console, Recovery Manager for Active Directory (RMAD) 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.

RMAD object properties monitored by RMAD Management Pack

Recovery Manager Console

Regular Management Pack

- **TargetComputer** Display name of a RMAD console instance
- **Version** Version of a RMAD console instance

Limited Management Pack

- **TargetComputer** Display name of a RMAD console instance
- **Version** Version of a RMAD console instance

Computer Collection

Regular Management Pack

- **DisplayName** Display name of a computer collection
- **ID** Computer collection ID
- **AgentSideBackupPath** Remote storage
- **ConsoleSideBackupPath** Location of the backup storage on the RMAD Console side
- **CollectFEMetaData** Indicates what metadata is collected
- **HasCollectionItems** Indicates whether a computer collection has collection items

Limited Management Pack

- **DisplayName** Display name of a computer collection
- **ID** Computer collection ID
- **AgentSideBackupPath** Remote storage
- **ConsoleSideBackupPath** Location of the backup storage on the RMAD Console side

- **CollectFEMetaData** Indicates what metadata is collected
- **HasCollectionItems** Indicates whether a computer collection has collection items

Computer

Regular Management Pack

- **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

Limited Management Pack

- **TargetComputer** Name of a domain controller

Health checks performed by RMAD Management Pack

Recovery Manager Console

Regular Management Pack

- Checks whether there are computer collection in the RMAD console instance.

Limited Management Pack

- Does not perform any checks.

Computer Collection

Regular Management Pack

- Checks whether a computer collection has collection items.

Limited Management Pack

- 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

Regular Management Pack

- 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.

Limited Management Pack

- 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

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.

For a list of all available PowerShell® commands, see the Management Shell Guide supplied with this release of the product.

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 Recovery Manager Console. This tool is called Diagnostic Data Collector.

When gathering diagnostic data, the Diagnostic Data Collector collects the following:

- **From Recovery Manager Console machine**
  - Collects the Recovery Manager Console log
  - Collects the Recovery Manager for Active Directory event logs
  - .db3 database files
  - Recovery Manager for Active Directory configuration files
- **From Domain Controller**
  - Collects Backup and Restore agent logs
  - Collects system event logs
  - Windows debug logs
  - Runs Microsoft Netdiag, Dcdiag, Nltest, MsInfo32 and Repadmin tools (in diagnostic mode only), and then collects the output provided by these tools. The tools are started by **Collectdcdata.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 RMAD 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 Recovery Manager Console, right-click the computer collection or the domain controller from the right-pane and select **Collect diagnostic data…** from the shortcut menu.
2. If you need to collect diagnostic data for the Recovery Manager Console machine, right-click on the Console root and select **Collect diagnostic data…**.
3. 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 file, e.g. **CollectedLogs_10_20_2015 07_23_25.zip**
4. Specify credentials to access the domain controllers.
5. Select the **Delete collected logs from domain controllers** option to delete collected RMAD\RMADFE logs from domain controllers.
6. Click the **Collect** button and wait for the operation to complete.

If you successfully collected data, 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 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.

Appendices

- Frequently asked questions
- Best practices for using Computer Collections
- Best practices for creating backups
- Ports Used by Recovery Manager for Active Directory
- Backup Wizard
- Online Restore Wizard
- Online Restore Wizard for AD LDS (ADAM)
- Group Policy Restore Wizard
- Repair Wizard
- Extract Wizard
- Technical characteristics
- 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 RMAD. Alternatively, you can restore the entire Active Directory® database, and then select individual objects for authoritative restore.

While RMAD 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 RMAD 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, RMAD 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, RMAD 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 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 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® 2008 R2 or later.

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 RMAD. 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. RMAD 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, RMAD 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 How to force authoritative and non-authoritative synchronization for DFSR-replicated sysvol replication.

How do I change the Backup Agent port number?

RMAD 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 RMAD, 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.

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.

Best practices for using Computer Collections

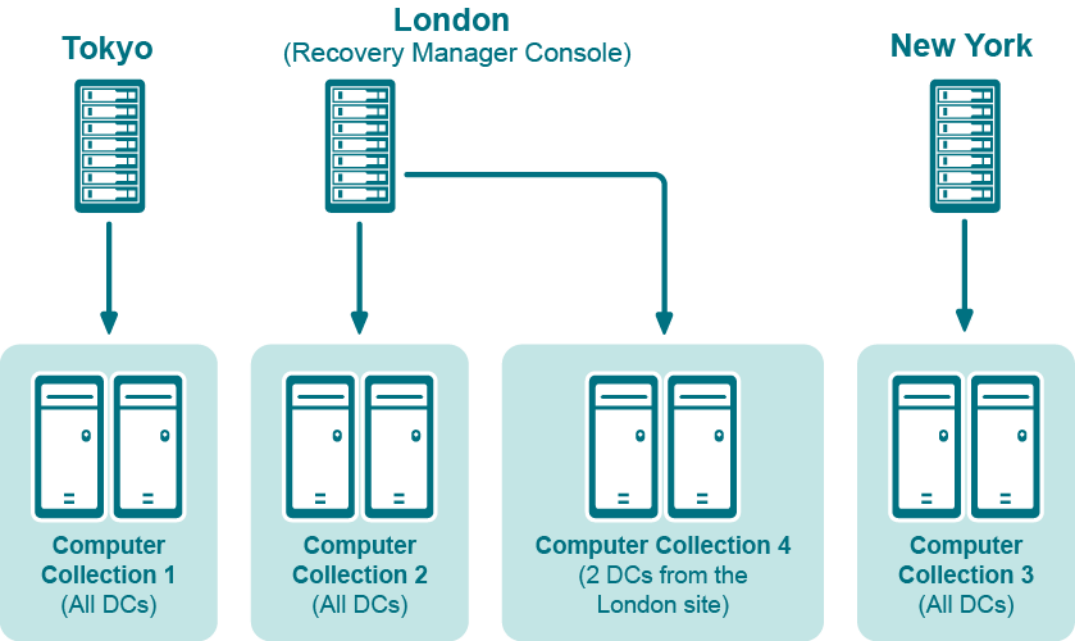
It is recommended to add computers to the same Computer Collection if you want to do any of the following:

- Back up the same System State components on all these computers.
- Apply the same backup storage policy to all these computers.

For instance, you may want to store domain controller backups in one central location accessible to the Recovery Manager Console over a fast link. This scenario eliminates the need to copy the backups across the network before running an online restore operation and allows you to centrally manage the restore.

- Set up the same backup creation schedule for all these computers.

The following diagram provides an example of using Computer Collections:



Example of Using Computer Collections

In this example, the Recovery Manager Console is installed in the London site. Computer Collections 1, 2, and 3 include all domain controllers from the Tokyo, London, and New York sites, respectively. Computer Collection 4 includes two domain controllers from the London site. Backups of these two domain controllers are accessible to

the Recovery Manager Console via a fast link and can be used to perform selective online restores of Active Directory® objects.

Technical characteristics

This section provides some technical characteristics of the product.

- Typical sizes of databases
- Typical backup creation times
- Typical times to unpack backups

Typical backup creation times

The backup creation time depends on the Active Directory database size (NTDS.dit file) and the compression method Backup Agent uses when processing NTDS.dit. You can specify the compression method on the **Performance** tab in the **Computer Collection Properties** dialog box. For more information, refer to the User Guide supplied with this release of RMAD.

The following table illustrates the typical backup creation times for different compression methods. This table has been obtained for the following configuration:

- The NTDS.dit file size: 3.14 GB
- The RMAD computer hardware: CPU 2x Intel® Xeon® 2.8 Hz; RAM 1 GB

Typical backup creation times

Compression method	Backup file size	Backup creation time (min:sec)
None	3.17 GB	09:07
Fast	1.27 GB	07:35
Normal	1.22 GB	08:27
Maximum	1.2 GB	17:54

Recommendations

The backup creation times for your Active Directory® database may vary based on size of the database and a number of other factors including the hardware on the domain controller and how densely the Active Directory® database is populated. You can use the examples above as a guide in determining how long it will take to backup your own Active Directory® database, but keep in mind that these times are not directly related to the size of the database (i.e. a 6 GB database may not take exactly twice as long to backup as a 3 GB database). The best way to determine what to expect for backup times in your own environment is to create a backup of a production domain controller.

Compression ratios can vary depending on how densely populated the Active Directory® database is, but typically using a higher compression method has diminishing returns in terms of the final compressed size of the backup. To ensure both a reasonable backup time and a reasonable compressed backup size it is recommended to use either Fast or Normal compression.

Typical times to unpack backups

Before using a packed backup file (e.g. in the Online Restore Wizard), RMAD must unpack it.

The following table illustrates the typical times required to unpack backups.

NOTE You can manage the creation of the unpacked backups using the **Unpacked Backups** tab in the **Recovery Manager for Active Directory Settings** dialog box. You can also have the Online Restore Wizard or Group Policy Restore Wizard keep unpacked backups for future use. For more information, refer to the User Guide supplied with this release.

Typical times to unpack backups

Compression method	Packed backup file size	Backup unpacking time (min:sec)
None	3.17 GB	01:57
Fast	1.27 GB	01:29
Normal	1.22 GB	01:25
Maximum	1.2 GB	01:22

Typical sizes of databases

Configuration database files

Recovery Manager for Active Directory employs the following database files (.mdb):

- **Rmad.db3**. RMAD configuration database. It contains information on the console configuration, such as the managed Computer Collections, backup creation sessions, etc.
- **Backups.mdb**. RMAD backup registration database. It contains information on the registered Active Directory and AD LDS (ADAM) backups.

As a rule, the file size for .mdb files does not exceed 10 MB.

NOTE The database files are stored in the folder **%AllUsersProfile%\Quest\Recovery Manager for Active Directory**.

Reports database files

The Online Restore Wizard provides comparison and restore reports based on per-attribute comparisons of directory objects selected from a backup, with their counterparts in Active Directory® or another backup.

RMAD incorporates Microsoft SQL® Reporting Services (SRS). Microsoft SRS is the new reporting standard, replacing the XML-based comparison and restore reports offered by previous versions. For more information, refer to the User Guide supplied with this release of RMAD.

The size of the reports database file depends on the following parameters:

- Number of the directory objects the Online Restore Wizard has processed.
- Number of the processed attributes.
- Type of the processed attributes.
- Number of the available Online Restore Wizard sessions. Note that the information on all sessions is stored in a single reports database file.

To estimate the reports database file size, use the following empiric formula:

6 x <Number of processed objects> / 1000 [MB]

For example, if the Online Restore Wizard has processed 3,000 objects, the reports database file size will be approximately 18 MB.

Best practices for creating backups

This section provides some best practices for backing up Active Directory® data using RMAD.

Develop a backup and restore plan

It is recommended to follow these rules to prevent Active Directory® 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 production environment.
- Ensure that each domain in your Active Directory® 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 you could identify the approximate failure time.

Determine which domain controllers to back up and how often

To perform an online restore of deleted or corrupted Active Directory® objects, it is recommended to back up at least two domain controllers in each domain for redundancy. If you intend to restore cross-domain group memberships, then it is also necessary to back up a global catalog server. The global catalog server 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** enabled on the **Advanced** tab of the Computer Collection Properties dialog box.

It is recommended that you back up your domain controllers on at least a daily basis. In any case, back up all domain controllers each time you make important changes to your environment.

Methods for deploying Backup Agent

Recovery Manager for Active Directory (RMAD) employs a Backup Agent to back up data on remote domain controllers.

The Backup Agent must be deployed on each remote domain controller where you want to back up Active Directory® data.

There are two methods to deploy the Backup Agent:

- Have RMAD automatically deploy the Backup Agent before starting a backup creation operation and automatically remove the Agent after the operation is complete.
- Manually preinstall the Backup Agent on all target domain controllers where you want to back up Active Directory® data.

The latter method allows you to:

- Perform a backup operation without having domain administrator privileges. It is sufficient if RMAD runs under a backup operator's credentials.
- Reduce network traffic when backing up a Computer Collection.

- Back up domain controllers in domains that have no trust relationships with the domain where RMAD is running, solving the so-called “no trust” problem.

NOTE To preinstall Backup Agent, you can either use the Backup Agent Setup Wizard or perform a silent installation. For more information, refer to the Quick Start Guide supplied with this release of RMAD.

Retain recent backups

If you create full backups on a daily basis as recommended earlier in this document, you should configure a backup retention policy to maintain the backups created in the last two weeks (14 last backups for each domain controller). This approach will provide you with a sufficient number of backups to recover from an Active Directory® failure that remained undetected for some time. For information on how to configure a backup retention policy, refer to the User Guide supplied with this release of Recovery Manager for Active Directory.

In addition to the retained backups, you can also archive at least one domain controller backup on a weekly basis. This will allow you to retrieve Active Directory® data (for instance, deleted objects) from a period past the recent backup history you retain. Make sure that these archived backups cover the entire tombstone lifetime period (180 days by default).

For security reasons, keep at least one copy of each backup off-site in a properly controlled environment in order to protect it from possible attacks by malicious individuals via the network.

Where to store backups

For each Computer Collection, you can specify where to store the Collection’s backup files. You can store backups on the computer running RMAD, the domain controller being backed up, or any available network share.

This section provides general recommendations where to store backups to be used in specific restore scenarios, such as granular online restore of directory objects, complete offline restore of Active Directory®, or Active Directory® forest recovery.

Storing backups for granular online or complete offline restores

The following diagram shows the recommended method for storing the backups you plan to use for granular online restores of directory data or complete offline restores of Active Directory®:

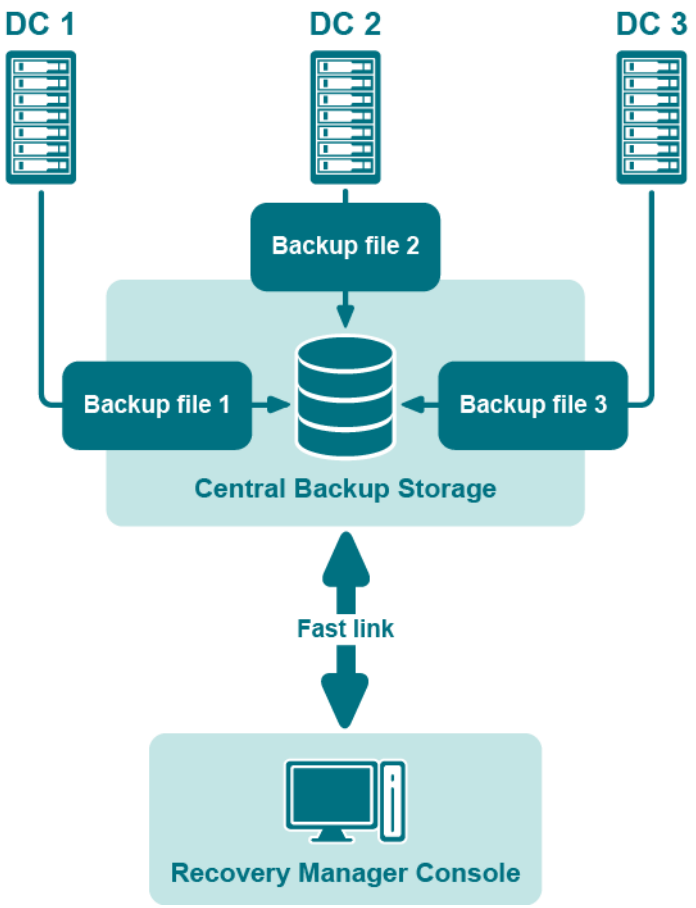


Figure: Backups for Granular Online or Complete Offline Restores

It is recommended that you store such backups in a central backup storage accessible to the Recovery Manager Console via a fast and reliable link. Such a link is required because during a restore operation backup, files may be copied or unpacked from the central backup storage to the computer where you are using the Recovery Manager Console.

Storing backups for forest recovery

The following diagram shows the recommended method for storing the backups you plan to use for forest recovery operations:

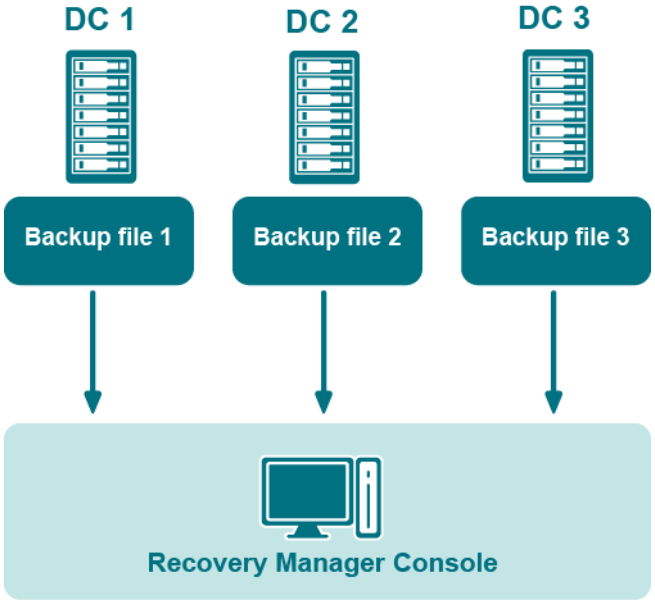
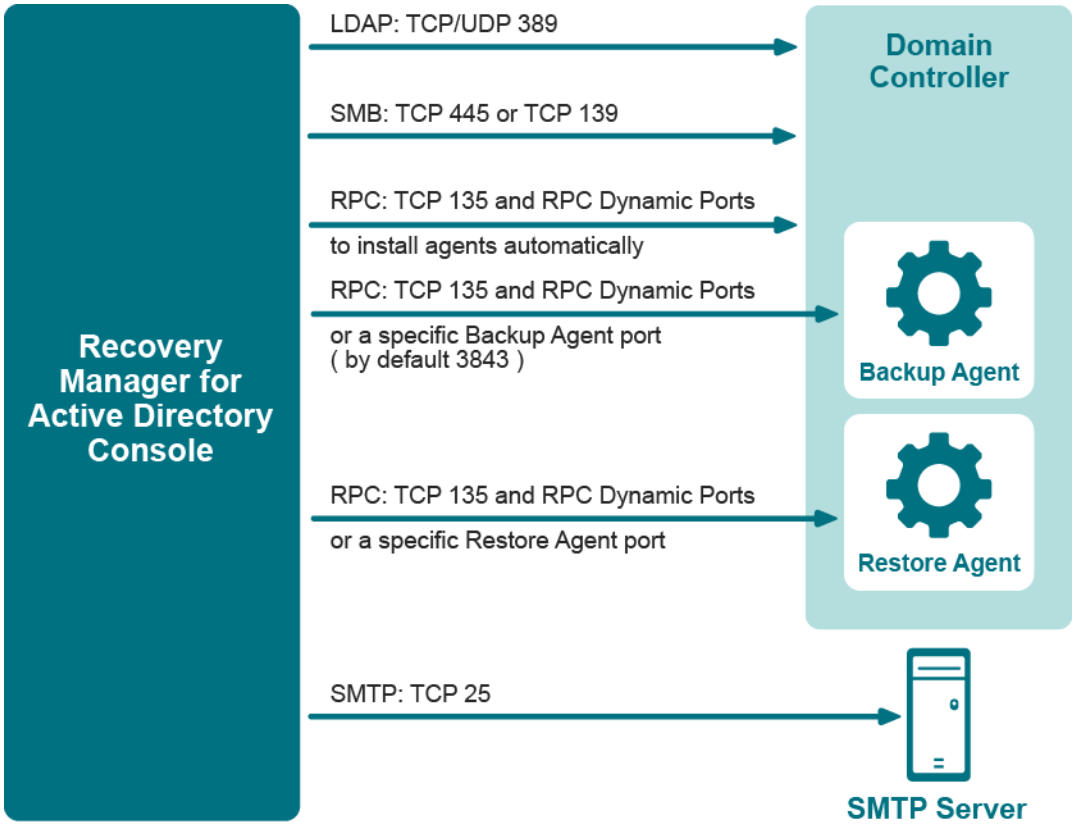


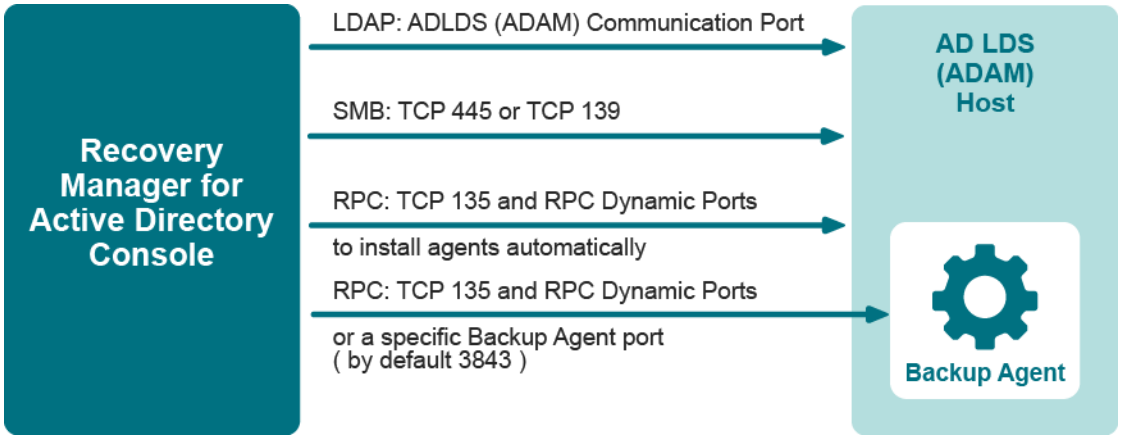
Figure: Backups for Forest Recovery

If you intend to use RMAD to recover the entire Active Directory® forest or specific domains in the forest, it is recommended that you store each backup file on the domain controller being backed up. This will considerably decrease the network utilization during backup operations and speed up the recovery process. On top of that, storing backup files on target domain controllers simplifies the permissions required to access those files.

Ports Used by Recovery Manager for Active Directory

This section provides information about the communication ports required to work with Recovery Manager for Active Directory.





Backup wizard

The Backup Wizard helps you create backups of domain controllers' Active Directory® components, including Active Directory® and Group Policy data. With this wizard you can select domain controllers whose Active Directory® is to be backed up, specify where to store backups, run backup immediately or schedule it for later, view and modify backup options.

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 Active Directory® components 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 Domain Controller by name

1. Click **Add** and then click **Domain Controller**.
2. In the **Select Computers** dialog box, supply the name of the Domain Controller 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 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 that contains any Domain Controllers to add.

If you select computers or containers before starting the Backup Wizard, the **Selected objects** list includes the objects you have selected.

To add AD LDS (ADAM) Host

1. Click **Add** and then click **AD LDS (ADAM) Host**.
2. In the **Select Computers** dialog box, supply the name or browse to the computer containing the AD LDS (ADAM) instance to add.

To add Domain Controllers using an import file

1. Create a text file that contains the Domain Controller 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.

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 RMAD, it points to the folder **%AllUsersProfile%\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**. 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 following table shows the steps and associated dialogs which will appear during the restore. On the left, are the steps and dialogs that will be taken/displayed for the **Compare, analyze, and optionally restore** selection, when made on the **Action Selection** dialog of the restore. Some of the dialogs will appear more than once, because you are given a chance to make changes based on the report that is generated. Also a restore report can be generated near the end of the restore.

On the right, are the steps and dialogs that are taken/displayed for the **Restore (skip compare analysis)** selection, when made on the **Action Selection** dialog of the restore. Since you are not going to generate a report and just want to restore there are a lot less steps/dialogs and only a restore report can be generated near the end of the restore.

Steps, if your choice is to compare and analyze an Active Directory item before doing a restore.	Steps, if your choice is to not compare and analyze an Active Directory item and go straight to doing a restore.
Wizard Operation Mode *Compare, restore, and report changes in Active Directory*	**Wizard Operation Mode** *Compare, restore, and report changes in Active Directory*
Domain Selection	**Domain Selection**
Backup Selection	**Backup Selection**
Backup Data Preparation	**Backup Data Preparation**
Domain Access Options	**Domain Access Options**
Objects to Be Processed	**Objects to Be Processed**
Action Selection *Compare, analyze, and optionally restore*	**Action Selection** *Restore (skip compare analysis)*
Processing Options	**Where to Restore Deleted Objects**

Steps, if your choice is to compare and analyze an Active Directory item before doing a restore.	Steps, if your choice is to not compare and analyze an Active Directory item and go straight to doing a restore.
Additional Options *Generate report*	**Processing Options**
Operation Start	**Additional Options** *Generate report*
Operation Progress	**Operation Start**
Operation Option *Proceed to restore*	**Operation Progress**
Objects to Be Restored	**Pop-Up** *Password Setting*
Where to Restore Deleted Objects	**Pop-Up** *Online Restore Wizard has undeleted some objects. Force replication?*
Processing Options	**Pop-Up** *Online Restore Wizard has changed some objects. Force incremental replication?*
Additional Options *Generate report*	**Operation Results**
Operation Start	**Completing the Online Restore Wizard**
Operation Progress	
Pop-Up *Password Setting*	
Pop-Up *Online Restore Wizard has undeleted some objects. Force replication?*	
Pop-Up *Online Restore Wizard has changed some objects. Force incremental replication?*	
Operation Results	
Completing the Online Restore Wizard	

The following table shows the steps and associated dialogs which will appear during the Database Compare. With this option, you can perform per-attribute comparison of objects between two Active Directory backups.

Steps, if your choice is to compare two backups and report the differences.
Wizard Operation Mode *Compare two backups and report the differences*
Domain Selection

Steps, if your choice is to compare two backups and report the differences.
Backup Selection
Backup for Comparison
Unpacked Backups Folder Selection
Backup Data Preparation
Objects to Be Processed
Action Selection (Compare two backups) *Compare two backups*
Processing Options
Additional Options *Generate report*
Operation Start
Operation Progress
Operation Option *To view comparison report, click View Report*
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.

Back to table

Domain Selection

Use this page to view a list of domains for which Active Directory® backups are available in RMAD 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 RMAD. 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).
- **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.

Back to table

Backup Selection

NOTE For Online Restore Wizard, RMAD supports DC backups even if a DC, where the backups have been done, has been removed from the domain or renamed. The exception is the old computer object, or any other object directly or indirectly linked to the old computer object. For instance, if a user upgrades the operating system on a DC, renames it, and wants to use the old backup collected before changes in the environment were made - this scenario is not supported.

Use this page to view a list of Active Directory® backups that are registered in the RMAD 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 180 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 RMAD backup registration database. RMAD 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).
  - **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.

NOTE Files are unpacked to a default folder. The setting for this folder can be found in the **Recovery Manager for Active Directory Settings** then the **Unpacked Backups** tab. The **Unpacked backups folder**, 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 specify another path, type the path to a new folder or click **Browse** to select it. When finished, click **Apply**.

Back to table

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).
    - **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.

Back to table

Unpacked Backups Folder Selection

This dialog is use with **Backup for Comparison** to optionally change the folder where RMAD will unpack the selected backups.

- **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 and only applies to the **Backup for Comparison**.

Back to table

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 Settings** 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.

Back to table

Domain Access Options

Use this page to specify a way the target domain to be accessed.

NOTE Agentless or agent-based method is set to **agentless method** by default. The setting for this can be found in the **Recovery Manager for Active Directory Settings** on the **General** tab. The **Unpacked backups folderDefault method for compare and restore operations**, displays the current selection.

- **Use agentless method to access domain controller**

  When selected, ensures that only LDAP functions are used to access the domain controller. This box will be selected if **Agentless method** is selected in the **Recovery Manager for Active Directory Settings** on the **General** tab. 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 another target domain controller, click **Browse**, and then select a domain controller from the **Select Domain Controller** dialog box.

- **Account used to access the target domain controller**

  Displays the user account with which RMAD will access the target domain controller. By default, the wizard accesses the domain controller with the account under which RMAD is running. To choose a different account, click **Change**, and then complete the **Select Account** dialog box.

- **Automatically configure firewall before the restore operation**

  When selected, the Windows Firewall settings will be configured automatically for the online restore operation. This check box is only made available if **Agent-based method** is selected in the **Recovery Manager for Active Directory Settings** on the **General** tab.

  Back to table

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:

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 through the backed up domain structure 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.

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®.

Back to table

Action 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.

Back to table

Action Selection (Compare two backups)

Use this page to specify what you want to do with the objects you selected.

- **Compare two backups**. This is the only option available which performs a per-attribute comparison of selected objects between two backups.
- **Restore (skip compare analysis)**. This option is not available on this dialog.

Back to table

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. From more information, see Select Attributes to Be Processed.

Back to table

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.

Additional 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 checkbox 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 checkbox 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 Change Auditor "Who" data in reports**. When this checkbox is selected, the comparison report includes the information on users who modified certain Active Directory® objects. To use this option, you must have Change Auditor for Active Directory installed in the home Active Directory® forest of Recovery Manager for Active Directory.
- **Include subsequent changes from CA on deleted objects**. When this option is selected, RMAD restores deleted object(s) and continuously restores the last change (if any) that was made to the object attributes after creating the backup, using data from the Change Auditor database.
- **Database**. Allows you to specify the name of Change Auditor database.

  To specify the CA database server, instance, port, and name, use the following format: <Server Name>\<Instance Name>,<Port>\<Database Name>. **Example:** testserver.domain.com\testinstance,1432\ChangeAuditorDB
- **Account used to access CA database**. Allows you to specify a user account to access the Change Auditor database.

  By default, the wizard accesses the Change Auditor database with the credentials of the current user that RMAD is running under. To choose a different account, click **Change**, and then select **SQL Server authentication using the below credentials**, enter the info and select **OK**.

For details about the Change Auditor-related options, see Integration with Change Auditor for Active Directory.

Back to table

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**.

Back to table

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.

- **Target**. The target domain the objects will be restored in.
- **Status**. The status of the comparison such as "Comparing objects…" and "The wizard has compared the objects".
- **Processing**. This field will display the FQDN of the objects being processed. When complete this field will be empty.
- **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.

During the final Operation Progress step of the restore operation, the following pop up dialogs will appear to allow the final actions for the restored account(s) or objects(s) to be performed.

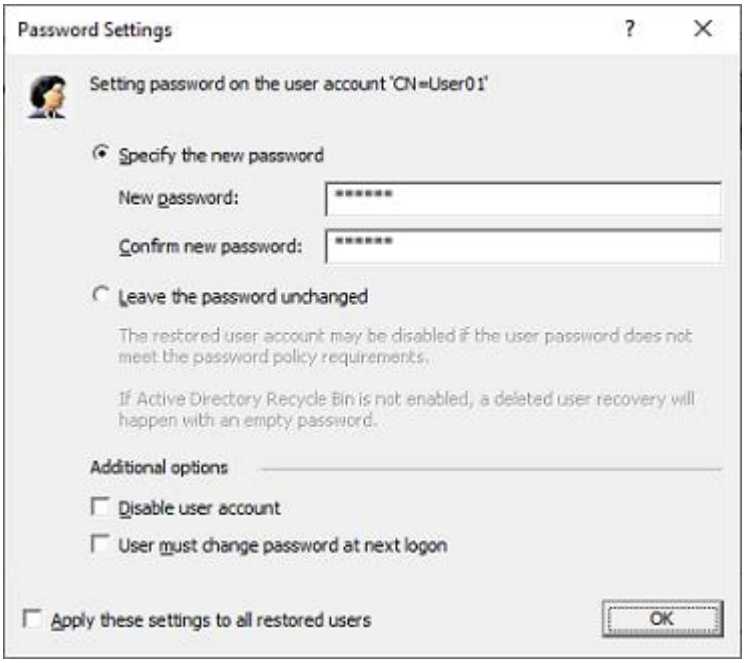
Back to table

Password Settings

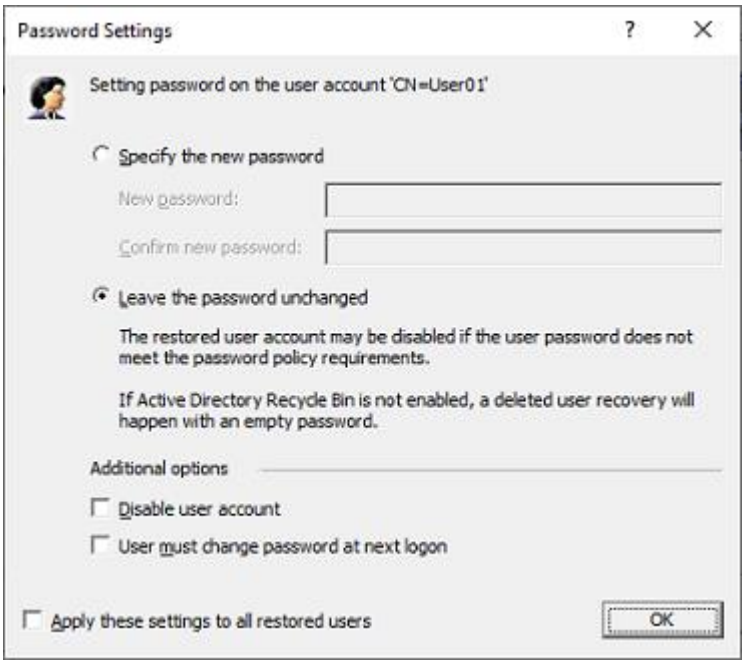
This dialog box enables you to specify the password and password settings for the user account you restore using the Online Restore Wizard.

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.
  If the Active Directory® Recycle Bin is not enabled, deleted user recovery will happen with an empty password.



- **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.

Back to table

Operation Progress Pop Ups

During the final Operation Progress step of the restore operation, there are a number of pop up dialogs that appear asking if certain Active Directory® incremental replications should be performed.

When Online Restore Wizard has undeleted some objects possessing linked attributes and to correctly restore linked attributes on all DCs, a replication must be carried out to all DCs before restoring linked attributes.

When Online Restore Wizard has changed some objects on the target DC, the changes should be propagated to the other DCs, an incremental replication can be done by the wizard.

Back to table

Operation Option (if the Compare, analyze, and optionally restore was selected in Action Selection dialog)

Use this page to analyze comparison reports and proceed to restore after the comparison was made.

- **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**.

  NOTE: The **Proceed to restore** option is not available if the **Compare two backups and report the differences** is selected on the **Wizard Operation Mode** dialog.

- **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 RMAD.
    - The **Comparison** report provides the following information:

1 of 1 100% Find | N

Object DN	Object class	Type of change	Modified by
CN=TestUser,CN=Users,DC=rmad,DC=local	User	Deleted	RMAD\Administrator

Attribute name	Type of change	Old value	New value	Modified by
Is-Deleted	Added		TRUE	
Is-Recycled	Added		TRUE	
Account-Expires	Deleted	<never>		
Code-Page	Deleted	0		
Country-Code	Deleted	0		
SAM-Account-Type	Deleted	0x30000000 (USER_OBJECTNORMAL_USER_ACCOUNT)		
Last Name	Deleted	123456		RMAD \Administrator
Pwd-Last-Set	Deleted	5/20/2019 1:32:27 PM		
Primary-Group-ID	Deleted	513		
Object-Category	Deleted	CN=Person,CN=Schema,CN=Configuration,DC=rmad,DC=local		
Logon Name	Deleted	test@rmad.local		
Display Name	Deleted	TestUser		

        - **Old value** column shows data from the backup or Change Auditor database.
        - **New value** column shows changes that occurred in Active Directory® since the last backup.
        - **Modified by** column provides information on who modified particular Active Directory objects (only if you use integration with Change Auditor)
    - The **Restore** report provides the following information:

Object DN	Object class	Type of change	Modified by
CN=SampleUserCa,CN=Users,DC=rmad,DC=local	User	Undeleted	RMAD\Administrator

Attribute name	Type of change	Old value	New value	Modified by
Phone Number (Others)	Added		Another Value	RMAD \Administrator
Phone Number (Others)	Added		First Number	RMAD \Administrator
Display Name	Added		SampleUserCa	RMAD \Administrator
Logon Name	Added		SampleUserCa@rmad.local	RMAD \Administrator
Phone Number (Others)	Added		Second Number	RMAD \Administrator
Phone Number (Others)	Added		Thirsd Number	RMAD \Administrator
Admin-Count	Deleted	0		RMAD \Administrator
Operator-Count	Deleted	0		RMAD \Administrator
Is-Deleted	Deleted	TRUE		RMAD \Administrator
Account-Expires	Modified	<never>	<never>	RMAD \Administrator
User-Account-Control	Modified	0x202 (ACCOUNTDISABLE | NORMAL_ACCOUNT)	0x200 (NORMAL_ACCOUNT)	RMAD \Administrator
Distinguished Name	Modified	CN=SampleUserCa \0ADEL:3c90f8e5-f5c9-4406-875f-a38b380677e8,CN=Deleted Objects,DC=rmad,DC=local	CN=SampleUserCa,CN=Users,DC=rmad,DC=local	RMAD \Administrator

- **Old value** column shows changes that occurred in Active Directory® since the last backup.
- **New value** column shows data that were restored from the backup or Change Auditor database
- **Modified by** column provides information on who modified particular Active Directory® objects (only if you use integration with Change Auditor)

Back to table

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 value**s. 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®.

Back to table

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.

Back to table

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 RMAD.

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.

Back to table

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 AD LDS (ADAM) instance backup, compare a backup with an AD LDS (ADAM) instance, and compare two backups taken from the same AD LDS (ADAM) instance. The wizard has the following steps:

The following table shows the steps and associated dialogs which will appear during the restore. On the left, are the steps and dialogs that will be taken/displayed for the **Compare, analyze, and optionally restore** selection, when made on the **Action Selection** dialog of the restore. Some of the dialogs will appear more than once, because you are given a chance to make changes based on the report that is generated. Also a restore report can be generated near the end of the restore.

On the right, are the steps and dialogs that are taken/displayed for the **Restore (skip compare analysis)** selection, when made on the **Action Selection** dialog of the restore. Since you are not going to generate a report and just want to restore there are a lot less steps/dialogs and only a restore report can be generated near the end of the restore.

Steps, if your choice is to compare and analyze an AD LDS (ADAM) item before doing a restore.	Steps, if your choice is to not compare and analyze an AD LDS (ADAM) item and go straight to doing a restore.
Wizard Operation Mode *Compare, restore, and report changes in AD LDS (ADAM)*	**Wizard Operation Mode** *Compare, restore, and report changes in AD LDS (ADAM)*
AD LDS (ADAM) Instance Selection	**AD LDS (ADAM) Instance Selection**
Backup Selection	**Backup Selection**
Unpacked Backups Folder Selection	**Unpacked Backups Folder Selection**
Backup Data Preparation	**Backup Data Preparation**
AD LDS (ADAM) Access Options	**AD LDS (ADAM) Access Options**
Objects to Be Processed	**Objects to Be Processed**
Action Selection *Compare, analyze, and optionally restore*	**Action Selection** *Restore (skip compare analysis)*
Processing Options	**Where to Restore Deleted Objects**
Additional Options *Generate report*	**Processing Options**
Operation Start	**Additional Options** *Generate report*
Operation Progress	**Operation Start**
Operation Option *Proceed to restore*	**Operation Progress**
Objects to Be Restored	**Operation Results** *View Report*

Steps, if your choice is to compare and analyze an AD LDS (ADAM) item before doing a restore.	Steps, if your choice is to not compare and analyze an AD LDS (ADAM) item and go straight to doing a restore.
Where to Restore Deleted Objects	**Completing the Online Restore Wizard for AD LDS (ADAM)**
Processing Options	
Additional Options *Generate report*	
Operation Start	
Operation Progress	
Operation Results	
Completing the Online Restore Wizard for AD LDS (ADAM)	

The following table shows the steps and associated dialogs which will appear during the Database Compare. With this option, you can perform per-attribute comparison of objects between two AD LDS (ADAM) instance backups.

Steps, if your choice is to compare two backups and report the differences.
Wizard Operation Mode *Compare two backups and report the differences*
AD LDS (ADAM) Instance Selection
Backup Selection
Backup for Comparison
Unpacked Backups Folder Selection
Backup Data Preparation
Objects to Be Processed
Action Selection (Compare two backups) *Compare two backups*
Processing Options
Additional Options *Generate report*
Operation Start
Operation Progress
Operation Option *View Report*

Steps, if your choice is to compare two backups and report the differences.

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.

Back to table

AD LDS (ADAM) Instance Selection

Use this page to view a list of AD LDS (ADAM) instances for which backups are available in RMAD 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 RMAD. 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 RMAD 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.

Back to table

Backup Selection

Use this page to view a list of backups that are registered in the RMAD 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 RMAD 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.

Back to table

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.

Back to table

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.

NOTE: If the selected backup has previously been unpacked, then this page will not be display during the restore steps.

Back to table

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.

Back to table

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.

Back to table

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 to search for objects in the backup. Under Search results, select objects by selecting check boxes next to object names. If no object are returned, click on the **Find** drop down and select **Any type** and click on the **Find Now** button.
    - On the shortcut menu, click **Browse** and use the **Browse and Select Object in Backup** dialog to browse the directory tree and select an object. If nothing is displayed in the dialog box, click the **Show advanced objects** check box, then browse through the objects listed.
    - On the shortcut menu, click **Import** and use the **Open** dialog 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.
  - **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).

Back to table

Action 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 AD LDS (ADAM) instance, 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.

Back to table

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.

- **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.

Back to table

Additional 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.
- **Include Change Auditor "Who" data in reports**. When this checkbox is selected, the comparison report includes the information on users who modified certain Active Directory® objects. To use this option, you must have Change Auditor for Active Directory installed in the home Active Directory® forest of Recovery Manager for Active Directory.
- **Include subsequent changes from CA on deleted objects**. When this option is selected, RMAD restores deleted object(s) and continuously restores the last change (if any) that was made to the object attributes after creating the backup, using data from the Change Auditor database.
- **Database**. Allows you to specify the name of Change Auditor database.

  To specify the CA database server, instance, port, and name, use the following format: <Server Name>\<Instance Name>,<Port>\<Database Name>. **Example:** testserver.domain.com\testinstance,1432\ChangeAuditorDB
- **Account used to access CA database**. Allows you to specify a user account to access the Change Auditor database.

  By default, the wizard accesses the Change Auditor database with the credentials of the current user that RMAD is running under. To choose a different account, click **Change**, and then select **SQL Server authentication using the below credentials**, enter the info and select **OK**.

For details about the Change Auditor-related options, see Integration with Change Auditor for Active Directory.

Back to table

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**.

Back to table

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.

Back to table

Operation Option

Use this page to analyze comparison reports and proceed to restore after the comparison was made.

- **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**. If there are no objects to be restored, the "Proceed to restore** check box will not be available and a message **Restore is not available: the selected objects did not change since the time of backup.**
- **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.

Back to table

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. There is a drop down which allows for the section of **Show deleted and changed objects** (default), **Show deleted objects only** and **Show changed objects only**.
- **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.
- **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.
- **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®.

Back to table

Where to Restore Deleted Objects

Use this page to specify a container where to restore the AD LDS (ADAM) 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.

Back to table

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.

Back to table

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.

Back to table

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:

- Domain Selection
- Backup Selection
- Backup Data Preparation
- Select Domain Controller
- Group Policy Object Selection
- GPO Restore Options
- Link Restore Options
- Restore Process Start
- Completing the Group Policy Restore Wizard

Domain Selection

Use this page to view a list of domains for which Active Directory® backups are available in RMAD 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 RMAD. 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 180 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™.

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 Settings** 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.

Select Domain Controller

Use this page to specify a domain controller to restore Group Policy. The domain controller must be running and accessible from the network.

- **Domain controller**. Specifies the domain controller.
- **Change**. Click **Change** to specify your domain controller by NetBIOS name or DNS name in the dialog box that opens.
- **Select an account to restore Group Policy Objects**. Specifies the account to access your domain controller.
- **Change**. Click **Change** to specify an account in the dialog box that opens. This account must have permission to modify Group Policy Objects.
- Click **Next** to connect to the domain controller and prepare for the restore process (No backup data will be transferred until the restore starts).

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 Active Directory® components on a domain controller, including the Active Directory® database, SYSVOL and registry. With this wizard you can select a Active Directory® backup, select Active Directory® objects for authoritative restore, and perform a primary restore of SYSVOL including registry hives.

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 Active Directory components needed for the restore, browse the **Active Directory** branch in the Computer and Backup Selection window. For the selected computer, the window lists all backups that are available in RMAD. 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 RMAD 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

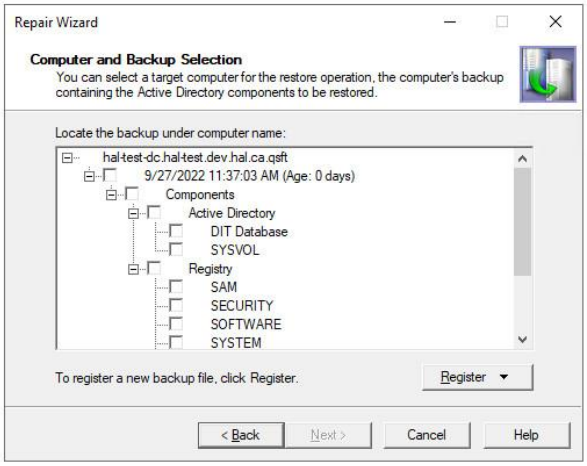
Click the computer whose backup you want to use, and then click the backup you want to use. Select the check box next to the backup and then click **Next**.

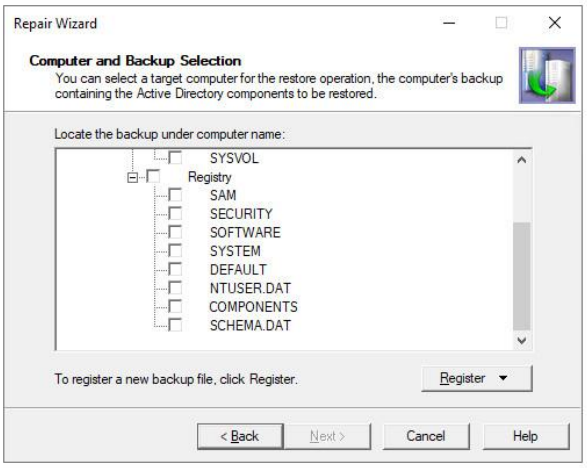
To select Active Directory components in a backup

Click the computer whose backup you want to use, and then expand the backup. Expand the Components then expand Active Directory for components such as DIT Database and SYSVOL.

To select Registry components in a backup

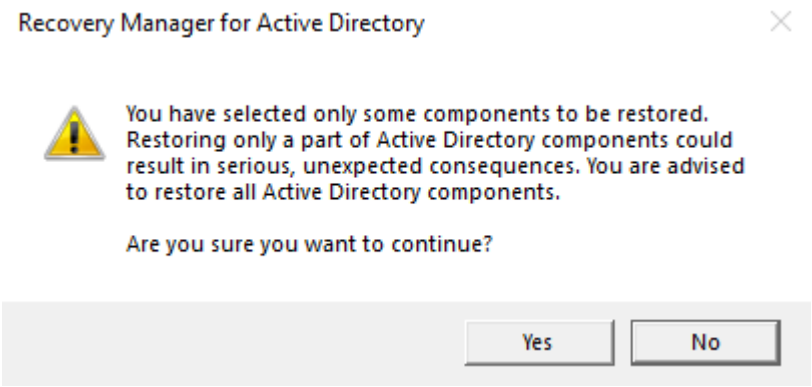
Click the computer whose backup you want to use, and then expand the backup. Expand the Components then expand Registry for components including all registry hives and the NTUSER.DAT file





Once your selection has been made, click **Next**.

If you have only selected some components from the backup, you will get a waring message stating that your selection could result in serious unexpected consequences. If you are sure you want to continue then select Yes otherwise select No.



Target Computer

Use this page to view where the Active Directory® data will be restored.

- **Restore Active Directory data on the computer**. Displays the computer name where the Active Directory® 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.
- **Account used to access the target computer**. Specifies the account to access your target computer.
- **Change**. Click **Change** to specify an account in the dialog box that opens. This account must have administrative rights to the target computer. If the target computer is in Directory Services Restore Mode, you must supply the user logon name and password of the Directory Services Restore Mode Administrator.

  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 (DSRM).

- **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 cancel 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 cancel the computer shutdown

- Click **Abort Shutdown**.

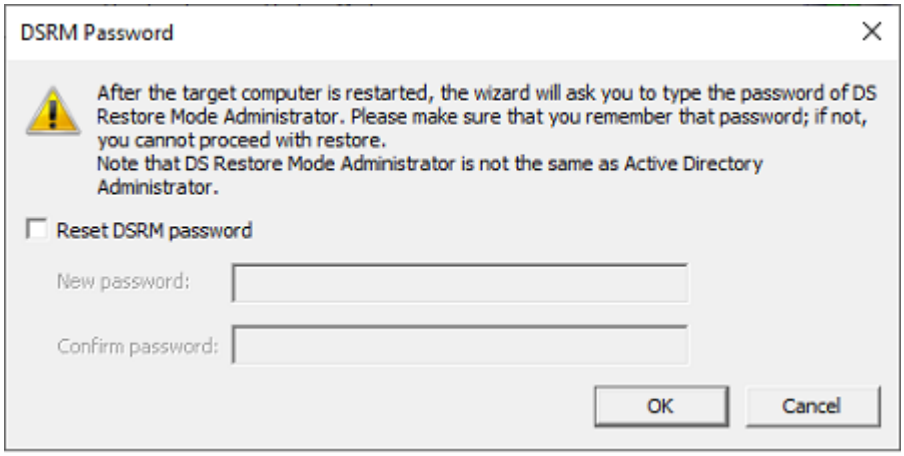
The Abort Shutdown button is available only during a 40-second grace period. The process of restarting the domain controller in Directory Services Restore Mode can take several minutes. The **Current Status** box allows you to examine the progress of the restart.

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.

DSRM Password

When you click **Next** a pop-up dialog will appear to allow you to reset the Directory Services Restore Mode (DSRM) password.



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 primary 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, RMAD 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%\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 Active Directory® 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 Active Directory® 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 RMAD. 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 Active Directory®. The list only includes the backups that are registered in the RMAD 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 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 Active Directory® 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 RMAD to the RMAD log. Events can be logged both on the target domain controller and on the RMAD computer.

- Common Events

- Recovery Manager Console events
- Backup Agent events
- Management Agent events
- Restore Agent events

Common Events

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.

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

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

Event ID	Event type	Description
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
2115	Information	A custom script was successfully run on the console machine. Collection: %35%r
2116	Information	A custom script was successfully run on the domain controller. Target DC: %6%r Collection: %35%r
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; Backup date: %13; Backup file: %12; Backup type: %41 GPOs list: "GPOs list"
2171	Information	The GPO restore operation was completed. Target DC: %6

Event ID	Event type	Description
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. Aarget 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
10003	Information	Console connected to '%89' on '%91' using authentication service '%90'.

Backup Agent events

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; Stop using Microsoft Volume Shadow Copy Service (VSS).
4712	Error	The backup process failed. Error text: %23
4713	Information	Preparing components for backup. Creating the Volume Shadow Copy Service (VSS) snapshot.
4714	Information	The preparation of components for backup was finished. Time spent: %26; The Volume Shadow Copy Service (VSS) snapshot has been created.
4717	Information, Warning (depends on a component)	The component '%25' will not be backed up.Reason: %35

Event ID	Event type	Description
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.

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

Restore Agent events

Event ID	Event type	Description
7001	Information	Online restore process was started. Source computer: %59; User: %1

Event ID	Event type	Description
7002	Information	The following objects were restored: %45
7003	Information	The online restore process was completed. Total number of the restored objects: %7
10002	Information	%89 started using authentication service %90.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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.