

Quest Recovery Manager for Active Directory
Disaster Recovery Edition 10.2.1

Release Notes



© 2021 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 – December 14, 2021

Quest® Recovery Manager for Active Directory Disaster Recovery Edition 10.2.1

Release Notes

These release notes provide information about the Quest® Recovery Manager for Active Directory Disaster Recovery Edition 10.2.1 release.

- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Security Fixes](#)
- [Known Issues](#)
- [System Requirements](#)
- [Product Licensing](#)
- [Getting Started with Recovery Manager for Active Directory](#)
- [Globalization](#)
- [Third-Party Contributions](#)

About Quest® Recovery Manager for Active Directory Disaster Recovery Edition 10.2.1

Recovery Manager for Active Directory enables fast, online recovery. Comparison reports highlight what objects and attributes have been changed and deleted in Active Directory enabling efficient, focused recovery at the object or attribute level. Accurate backups and a quicker recovery enable you to reduce the time and costs associated with AD outages and reduce the impact on users throughout your organization.

Recovery Manager for Active Directory is based on patented technology.

Recovery Manager for Active Directory 10.2.1 is a release with new features and functionality. See [New Features and Enhancements](#).

New Features and Enhancements

This section covers new features and enhancements in Quest® Recovery Manager for Active Directory 10.2.1.

Major Features

Recovery Manager for Active Directory 10.2.1

Cloud Storage

Recovery Manager for Active Directory Disaster Recovery Edition provides the ability to set up and use dedicated cloud storage locations for backups. Cloud Storage in combination with Tier 1 storage options ensure that your critical backups are always available in case of disaster.

By using Cloud Storage you can store your AD and BMR backups in the cloud ensuring that your backups are always accessible and protect your backup files with storage account properties such as immutability policies, and redundancy with different types of replication.

Secure Storage Server

Recovery Manager for Active Directory Disaster Recovery Edition 10.2.1 has enhanced the Secure Storage server feature.

New features available:

- New **Secondary Storage** tab on Computer Collection Properties to configure a Secure Storage server and provide required access credentials to read backups to be copied to secondary storage.
- New PowerShell cmdlets **Set-RMADStorageServerAllowedVolumes** and **Get-RMADStorageServerAllowedVolumes** available in the Management Shell to configure which volumes are allowed to store backups.
- The Secure Storage server properties dialog displays used and free space on each volume on the server including a warning indication when space is low.
- New validation performed during the installation of a Secure Storage agent to ensure the Secure Storage server is a standalone server and not domain joined.

IMPORTANT

An upgrade to the Secure Storage agent is required for new functionality. Refer to Upgrade and installation instructions below and the User Guide supplied with this release of the product.

Enhancements

General

Enhancement	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Usability improvements to the Computer Collections Properties dialog including removal of Logging tab and introduction of new tab for Secondary Storage	N/A	ADO-283362
Creation of Management Shell Guide which lists all available PowerShell cmdlets, with examples. Appendix removed from User Guide	N/A	ADO-275100

Enhancement	ID (old)	ID (new)
Support Microsoft Edge browser in the Web Portal	RMADFE-1372	ADO-220837
Add option to skip replication after recovery on RMAD portal UI	RMADFE-815	ADO-220726
New portal settings and improvements for Web Portal configuration	RMADFE-1182	ADO-220796
Recovery Manager for Active Directory 10.2		
Rename system state backups to Active Directory backups	RMADFE-3009	ADO-218405
Hide the "Components" tab in computer collection settings	RMADFE-3042	ADO-218415
SCOM 2019 support	N/A	ADO-219783
Pass through Synchronize across time zones from windows task scheduler to RMAD	RMADFE-952	ADO-220703
Create Logs Daily to be on by default	N/A	ADO-223980
Display operating system version for all backups	N/A	ADO-228741

Forest Recovery Edition

Enhancement	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Automatically enable File and Printer Sharing on the clean OS machine when installing FR agent	RMADFE-2778	ADO-242106
RMAD Console and Forest Recovery Agent cannot read AD configuration with more than 1000 sites	N/A	ADO-274279
Recovery Manager for Active Directory 10.2		
Forest Recovery simulation mode available	RMADFE-920	ADO-218277
The 'View Recovery Report' action should be available as one of the post recovery dialog actions	RMADFE-3034	ADO-218413
Encrypt credentials in Forest Recovery project using AESCryptoServiceProvider instead of TripleDESCryptoServiceProvider	RMADFE-2199	ADO-220948
Allow RMAD backup to continue if forest recovery agent cannot be installed	N/A	ADO-221433

Enhancement	ID (old)	ID (new)
Set default global catalog handling option to "Keep GC Intact"	N/A	ADO-223871
Show 'object's tombstone is expired' detailed warning in the Online Restore Wizard	RMADFE-1613	ADO-223987
Default recovery method to the Repromotion phase should be "Install AD", not "ReinstallAD"	N/A	ADO-234195
Tool to update backup creation date in simulation projects	N/A	ADO-234197
Keep previous recovery methods when changing recovery mode like Forest Recovery --> Repromotion --> Forest Recovery	N/A	ADO-234201
Every DC in simulation project should have a backup created for this domain controller so all recovery methods are available	N/A	ADO-234203

Disaster Recovery Edition

Enhancement	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Support console local storage as a primary storage for copying to Secure Storage server	N/A	ADO-280129
Smart instance type selection for Azure virtual machine creation with Restore to Clean OS feature	N/A	ADO-281406
In the Secure Storage node provide ability to sort/filter/group backups in the RMAD console	N/A	ADO-278538
As a part of server hardening check server and do not allow a domain joined server. Secure Storage agent will not be installed	N/A	ADO-258979
Ability to configure volume for backups on Secure Storage server. Default to copy backups to non system drives.	N/A	ADO-276487
Option to specify static IPs for Azure virtual machine creation	N/A	ADO-315595
Improvement for template selection in Restore to Clean OS	N/A	ADO-297078
Support verify for 'Restore to Clean OS' on live DCs, show warning when live DC is contacted	RMADFE-2933	ADO-218376
Show free disk space and warning when space is low for volumes on Secure Storage server	N/A	ADO-227980
Recovery Manager for Active Directory 10.2		
The current image file is not recreated if the file is not older than X days and the version of the Forest Recovery agent and network settings are not changed	N/A	ADO-218323

Enhancement	ID (old)	ID (new)
Document how to pre-configure clean external DNS server which is used for BMR or Clean OS recovery	RMADFE-3110	ADO-218435
Show computer collection type (system state/BMR) in the RMAD console collections grid	RMADFE-3228	ADO-218917
In "Restore to Clean OS" we need to disable Windows Updates before promoting machine to DC	N/A	ADO-229862
Recreate ISO when third-party drivers added or removed	N/A	ADO-230402
Log the recovery event with source disk configuration information	N/A	ADO-230457
Validate source and target disks layout match	N/A	ADO-230963

Resolved Issues

General Resolved Issues

Resolved Issue	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Allow to unselect Console storage immediately as alternative has been configured	N/A	ADO-220573
Large number of scheduled tasks can cause Console, Replication and PowerShell cmdlets to be extremely slow	RMADFE-1837	ADO-242166
RMAD Portal does not show proper backups	N/A	ADO-256164
Remove a BOM prefix from the script file	N/A	ADO-257798
Error in the web portal logs 'Cannot init EP configuration section'	N/A	ADO-273469
Unpacking the backup and the retention policy may fail if the DC cannot be accessed via LDAP from the RMAD console machine	N/A	ADO-279431
RPC calls to Backup Agent are not retried on RPC_S_SERVER_TOO_BUSY error	N/A	ADO-314812
Misleading 'Unable to map the network share IPC\$ on the computer' error message on attempt to map UNC share	N/A	ADO-316902

Resolved Issue	ID (old)	ID (new)
Installation fails with an invalid error message when using a local windows credential to connect to the remote SQL server	N/A	ADO-317818
'Insufficient rights' error in the web portal fixed. Addition of a domain is now changed to allow all domain admins by default	RMADFE-2437	ADO-319010
Online Restore Wizard cannot undelete an object using a non-administrative account. Restoring an object in Online Restore Wizard using a non-administrative account may result in the following error for NT-Security-Descriptor attribute: "Cannot retrieve attribute value(s) from Active Directory. Possible reason: Insufficient access rights." To ignore this error, the NT-Security-Descriptor attribute can be excluded from the list of restored attributes.	N/A	ADO-293311
Recovery Manager for Active Directory 10.2 Hotfix 1		
Installation of Quest personal certificates to the local certificate store failed. Receive error message to install Quest certificates later. This should not be required.	N/A	ADO-274643
Computer Collection scheduled tasks removed after upgrade to 10.2 if gMSA used as the scheduled task account	N/A	ADO-280854
rmad.db3 file gets overwritten during an uninstall -> install of version 10.2	N/A	ADO-283069
Cannot retain the uncheck "Global Catalog Servers" option in the Advanced tab of the Computer Collection properties window	N/A	ADO-230397
It will display 'Network access is denied' error in Win2016/2019 if specify account to restore GPO with "domain\username" format	N/A/	ADO-233623
Cannot see some advanced objects in the object picker in Online Restore Wizard	N/A	ADO-275027
Recovery Manager for Active Directory 10.2		
Security Vulnerability - Sensitive comments embedded within client-side code sent to an end user machine	RMADFE-3244	ADO-218142
Security Vulnerability - Runtime hardening (SEP, ASLR and other)	RMADFE-3248	ADO-218146
Full replication fails when a DC is selected for the option 'Unpack each backup upon its creation' in the master console	RMADFE-1858	ADO-218500
Storage agent settings are not applied on install	N/A	ADO-219910
No progress/wait indication after clicking 'OK' on the 'Add Console...' dialog	N/A	ADO-224321
Backup fails if the Domain Controllers OU has a AzureADKerberos computer object in it as part of Azure AD FIDO deployment	N/A	ADO-227903
Improve documentation with information on number of scheduled computer collections for optimal performance	N/A	ADO-232614

Resolved Issue	ID (old)	ID (new)
Access Violation in the ProcessRequest function and crashes service	N/A	ADO-232682
Remove mutual exclusion mechanism between replication process and restore process	RMADFE-1575	ADO-237972
Display correct backup info and support restore for Collections with containers (not DCs)	N/A	ADO-240580
Retriable VSS error causes undefined behavior in Backup Agent on retry	N/A	ADO-241825
Modify the configuration to remove collision problems with SHA1, moved to SHA256	N/A	ADO-253913
Retention policy ignores collection and consider backups of all collections	N/A	ADO-259645
Recovery Manager for Active Directory 10.1.1 HF1		
RMAD console crashes while building comparison report.	N/A	ADO-240300
Recovery Manager for Active Directory 10.1.1		
Agent-based online restore can result in Isass process crash.	RMADFE-3233	ADO-218222
Unable to restore AD object when user provides smart card PIN and username hint.	RMADFE-3132	ADO-218574
Configuring a backup schedule is disabled when creating a backup from Recover Manager for Active Directory > Create Backup .	RMADFE-3260	ADO-219136
SCOM pack Get Collections call results in Access denied errors.	RMADFE-3025	ADO-220574
Increasing number of scheduled tasks makes Console, Replication, and Cmdlets extremely slow.	RMADFE-1837	ADO-223040
RMAD console crashed due to missing DLL Microsoft.Xaml.Behaviors.dll.	N/A	ADO-226682
After restore a User Object Member Of is different than in Active Directory	N/A	ADO-230090

Forest Recovery Resolved Issues

Resolved Issue	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		

Resolved Issue	ID (old)	ID (new)
Check Forest Health can get stuck on the second step	RMADFE-3041	ADO-218559
New recovery project, selecting a Backup display the adding time in the Backup Age colum instead of backup age	N/A	ADO-237971
'There is no PREFERRED_DNS value' error occurs, if no DNS server is found on installing Active Directory	RMADFE-2437	ADO-242191
Feature loss in Forest Edition: Cannot skip a backup for non-authoritative DCs in Sysvol recovery mode	N/A	ADO-245551
'There is no PREFERRED_DNS value' error when a 'Select preferred DNS' agent operation did not return a result it causes product to hald and cannot be skipped or aborted	N/A	ADO-253457
Resume Forest Recovery show 'Password is incorrect'	N/A	ADO-254788
Installing Forest Recovery agent hangs if SMB shares are disabled	N/A	ADO-285225
Recovery Manager for Active Directory 10.2 Hotfix 1		
During upgrade a DBImport error occurs when antimalware status data exists. Caused by debug logging on by default.	N/A	ADO-274622
GPO Comparison Report is not working	N/A	ADO-278211
Recovery Manager for Active Directory 10.2		
Email notification template contains invalid text and status message	N/A	ADO-252659
Verification email contains incorrect backup data	N/A	ADO-252866
Creating ADVL fails when unable to access VConverter error	N/A	ADO-253382
Wrong replication partner is selected in IFM recovery on second phase. IFM failed	N/A	ADO-253681
IFM script does not automatically reboot DC after installed AD DS tools. IFM failed	N/A	ADO-253778
Install AD moethd on second pahse may fail with "Unable to connect to the replication source"	N/A	ADO-225791
IPSec isolation policy was not removed successfully when previous forst recovery is aborted and left dirt data	N/A	ADO-237004
IPSec isolation policy was not removed successfully during restore	N/A	ADO-237049

Resolved Issue	ID (old)	ID (new)
The "Reset computer account" operation fails when some other recovery operation failed and retried earlier	RMADFE-2659	ADO-242197
After upgrade from 10.1 to 10.1.1, the Verify Settings in Forest Recovery console send emails with some kind of strange status messages	N/A	ADO-242679
Recovery Manager for Active Directory 10.1.1 HF1		
Forest Recovery fails if the only drive encrypted with BitLocker is removed.	N/A	ADO-222308
Recovery Manager for Active Directory 10.1.1		
IPv6 based UNC Path support.	RMADFE-3232	ADO-218913
Scanning of all backups does not stop when one of the processes ends urgently.	N/A	ADO-219145
Errors when trying to restore SYSVOL: Need to improve the RPC stability.	N/A	ADO-228250
ADVL converter returns 500 error.	N/A	ADO-230091
Error when booting VM: "Invalid location type. Location accepts only VIDatastore objects."	N/A	ADO-233811

Disaster Recovery Resolved Issues

Resolved Issue	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Cache and reuse the extracted WinRE images	RMADFE-3206	ADO-218577
Health Check wizard should work after Restore to Clean OS	N/A	ADO-226971
Bare Metal Recovery backup does not work with SAN policy set to OfflineAll	RMADFE-1955	ADO-242174
Restore Clean OS failed if original DC has encrypted volumes	RMADFE-2857	ADO-242202
Recreate ISO when third-party drivers added or removed	RMADFE-2928	ADO-242204
Installing Active Directory may fail with access denied due to lack of permissions to write the objects into Computers OU. To workaround, user must set the <i>JoinDomainBeforeInstallAD</i> option to True in FRConsoleSettings.xml file. This will	RMADFE-3101	ADO-242598

Resolved Issue	ID (old)	ID (new)
skip joining OU Computers during the promotion of the DC and join it directly to OU Domain Controllers.		
Incorrect filtering of backups on the secure storage server	N/A	ADO-278874
Password showing in clear text for event id 403, showing PowerShell script name, the user name, and password	N/A	ADO-281399
Project verification with Zero touch configured reboots the working servers to WinRE mode	N/A	ADO-283230
Unable to verify settings if Azure virtual machine exists or is shut down	N/A	ADO-304177
Forest Recovery with VMWare machine creation fails if source has BIOS firmware and more than one critical disk	N/A	ADO-313724
Console crashes if storage server refresh fails when secure storage backups node is selected	N/A	ADO-315182
Failed to establish DNS configuration after recovery with Azure virtual machine	N/A	ADO-318396
Failed to prepare infrastructure on Azure VM with 'QuestSoftware.RecoveryManager.AD.ForestRecovery.LocalizableException: Cannot find path because it does not exist' message	N/A	ADO-318660
Change the warning which explains that the recovery ISO should be dismounted	N/A	ADO-318768
Error message prompting the user failed because the host program or the command type does not support user interaction, after failing to create VM in Azure and Retry All operations for a specific DC	N/A	ADO-319038
Cannot validate argument on parameter 'VM'. The argument is null or empty	N/A	ADO-319040
Unable to access the backup on Azure file share during Clean OS Restore to Azure VMs	N/A	ADO-304022
For Azure VM creation, a cloned Infrastructure platform template is not automatically selected on the infrastructure tab after Service Principle generation	N/A	ADO-259493
Azure VM creation does not work with Az Powershell module 7.0.0. API changes in Service principal management commandlets used by RMAD.	N/A	ADO-323193
Recovery Manager for Active Directory 10.2 Hotfix 1		
Zero touch against Dell server not working. Forward slash in the ISO access credentials is required.	N/A	ADO-274417
Integrity check may fail if the storage server is registered using an IP address	N/A	ADO-274471
Double backslash in the backup path on the storage server causes failure	N/A	ADO-274472

Resolved Issue	ID (old)	ID (new)
Cannot perform BMR restore in 10.2 if the source machine is BIOS with a SCSI boot volume	N/A	ADO-277893
"System.ArgumentException: An item with the same key has already been added" error during BMR recovery when multiple DCs configured to boot using iLO	N/A	ADO-282728
Dell and HP ZeroTouch settings are converted to templates on upgrade	N/A	ADO-283208
Template selection and configuration usability improvements and clarification with better text	N/A	ADO-297078
Recovery Manager for Active Directory 10.2		
An error "Index(zero based) must be greather than" during BMR recovery on the Restore disks step	N/A	ADO-218575
When processing Bare Metal Active Directory recovery for Korean Windows, it created error message in 'Run pre-recovery checks' step	N/A	ADO-219702
During BMR recovery restart domain controller in normal mode hanging	N/A	ADO-227232
"Collection diagnostic data" tool fails to collect data from target machine in Clean OS and BMR modes	N/A	ADO-227427
Cannot bind parameter 'DomainMode' to the target error	N/A	ADO-232543
DC restored with 'Restore to Clean OS' method from backup without DNS partition should not be selected as Primary DNS server	RMADFE-3100	ADO-242133
Recovery Manager for Active Directory 10.1.1 HF1		
Restore to clean OS fails if original DC has encrypted volumes.	RMADFE-2857	ADO-232951
Recovery Manager for Active Directory 10.1.1		
Impossible to collect an encrypted BMR backup when Bitlocker was hardened by GPOs.	RMADFE-3212	ADO-218269
Cannot create BMR backup for the domain controller with Data Duplication enabled on a non-critical volume.	RMADFE-3211	ADO-218929
Impossible to collect an encrypted BMR backup when GPO "Choose drive encryption method and cipher strength (Windows 10 [Version1511] and later)" is set.	RMADFE-3213	ADO-219148
Error when processing Bare Metal Active Directory Recovery in Forest Recovery Console.	N/A	ADO-222538
"Invalid server certificate" error occurs when connecting to vCenter.	N/A	ADO-227404
Bare Metal Recovery fails with error "The process terminated unexpectedly" if the target disk is too small.	N/A	ADO-230712

Resolved Issue	ID (old)	ID (new)
Permissions applied based on current documentation and BMR restore does not work - no access to list data stores.	N/A	ADO-232623

Security Information

Recovery Manager for Active Directory fully supports Transport Layer Security (TLS) 1.2. It is recommended that you upgrade to TLS 1.2 for secure communications.

Security Resolved Issue	ID (old)	ID (new)
Recovery Manager for Active Directory 10.2.1		
Do not use SHA1 for key derivation function to generate hash for creation of AES-256 key for backup encryption	---	---

Known Issues

General Known Issues

Known Issue	ID (old)	ID (new)
Backups may contain invalid FQDNs that are registered automatically, so they cannot be selected in the Forest Recovery Console. Workaround: Use the Active Directory browse method to add the DCs to a collection when creating backups, or perform backup creation for the DCs (with correct FQDN) directly. To use the Active Directory browse method, click All Domain Controllers in the console tree, right-click a domain controller on the right pane and press Add to Collection .	RMADFE-2851	ADO-220570
Recovery Manager for Active Directory does not show changes to GPO administrative templates in the GPO comparison report.	RMADFE-805	ADO-220632
Group Policy restore might fail with the error "Network access is denied" if you run the RMAD console under a local account, and this account has the same username and password as the domain account you use to restore Group Policy in the domain.	RMADFE-2162	ADO-226664
Online Restore Wizard (agent-based restore) does not work on Windows Server 2016 and Windows Server 2019 with Local Security Authority (LSA) protection and Secure Boot enabled.	RMADFE-1996	ADO-226670

Web Portal Known Issues

Known Issue	ID (old)	ID (new)
After upgrading the web portal, improvements on the Configuration tab are not immediately seen. It is required to clear the browser cache.	N/A	ADO-323365

Forest Recovery Known Issues

Known Issue	ID (old)	ID (new)
Recovery Manager for Active Directory Forest Edition (Disaster Recovery Edition) does not check version of Forest Recovery Agent inside the ISO image file.	N/A	ADO-226671
The start type of Windows Defender Firewall service cannot be restored in Windows Server 2019.	N/A	ADO-226672

System Requirements

Before installing Recovery Manager for Active Directory, ensure that your system meets the following minimum hardware and software requirements.

NOTE Recovery Manager for Active Directory supports only IPv4 or mixed IPv4/IPv6 networks.

- Recovery Manager for Active Directory Forest Edition can backup and restore domain controllers that are running on virtual machines in Amazon Web Services (AWS) or Microsoft Azure. Note that such domain controllers cannot be restored with the Bare Metal Active Directory Recovery method because there is no way to boot them from an ISO image.

Recovery Manager for Active Directory requirements

Processor

Minimum: 1.4 GHz

Recommended: 2.0 GHz or faster

Memory

Minimum: 2 GB

Recommended: 4 GB

These figures apply only if the Active Directory domains managed by Recovery Manager for Active Directory include 1 million objects or less. Increase RAM size by 512 MB for every additional 1 million objects.

Hard disk space

Full installation including the prerequisite software: 2.7 GB of free disk space

In case all the prerequisite software is already installed: 260 MB of free disk space

NOTE | Additional storage space is required for a backup repository, at least the size of the backed-up Active Directory database file (**Ntds.dit**) and the **SYSVOL** folder plus 40MB for the transaction log files.

Operating system

NOTE | Machine that hosts the Recovery Manager for Active Directory 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. 32-bit operating systems are not supported.

Installation

- Microsoft Windows Server 2019, 2016, 2012 R2, and 2012
- Microsoft Windows 10 x64, 8.1 x64

Targets for backup, restore, or compare operations

- Microsoft Windows Server 2019, 2016, 2012 R2 and 2012 (including Server Core installation)

The Windows Server Backup feature is supported for Windows Server 2012 R2 or higher. Make sure that the feature is installed on all domain controllers in your environment.

Microsoft .NET Framework

Microsoft .NET Framework version 4.5.2 or higher

Microsoft .NET Framework version 4.7.2 or higher is required for use of Microsoft Azure virtual machines with Restore Active Directory to Clean OS recovery method

Microsoft SQL Server and its components

Microsoft SQL Server versions

Microsoft SQL Server is required for the following Recovery Manager for Active Directory features: Comparison Reporting, Forest Recovery Persistence and Recovery Manager Portal.

Supported SQL Server versions:

- Microsoft SQL Server 2019, 2017, 2016, 2014 and 2012 (Enterprise, Business Intelligence, Standard, Express, Web, or Developer Edition)

Microsoft SQL Server components

Microsoft System CLR Types for SQL Server 2012

If this component is not installed, it will be installed automatically by the RMAD setup.

Microsoft SQL Server Reporting Services

To display reports, Recovery Manager for Active Directory can integrate with Microsoft SQL Server Reporting Services (SRSS) 2016, 2017 and 2019.

Microsoft Operations Manager

Supported Microsoft Operations Managers for the RMAD Management Pack for Microsoft Center Operations Manager (SCOM):

- Microsoft System Center Operations Manager 2019, 2016, 2012 R2, and 2012

Microsoft Windows PowerShell

Microsoft Windows PowerShell version 5.0 or later

Integration with Change Auditor for Active Directory

Supported versions of Change Auditor for Active Directory: from 6.x to 7.x.

If any prerequisite software is not installed, the Setup program automatically installs it for you before installing Recovery Manager for Active Directory. If the prerequisite software to be installed is not included in this release package, it is automatically downloaded.

Continuous recovery: From version 10.0.1, Recovery Manager for Active Directory together with Change Auditor can restore 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.

Antivirus software that is supported for backup antimalware checks

The anti-virus checks are performed on the Forest Recovery Console machine running Windows Server 2016 or higher by means of antivirus software installed on the machine.

- Microsoft Defender
- Symantec Endpoint Protection 14.x
- Broadcom Endpoint Security (former name: Symantec Endpoint Protection 15)

Supported server management systems

- Integrated Dell Remote Access Controller (iDRAC) 8 and 9
- HP ProLiant iLO Management Engine (iLO) 3, 4 and 5
- VMware vCenter/ESX Server 6.0, 6.5, 6.7 and 7.0
- Microsoft Hyper-V Server 2012 or higher

Forest Recovery Agent requirements

Memory

1 GB (2 GB recommended)

Hard disk space

2 GB or more

Operating system

One of the following operating systems:

- Microsoft Windows Server 2019, 2016, 2012 R2, and 2012 (including Server Core installation)

Secondary Storage requirements

Secure Storage Server

- Operating system: Microsoft Windows 2016 or higher
- A stand-alone server to be used as your Secure Storage server. This server should be a workgroup server and not joined to an Active Directory domain.
- An account that will be used to deploy the Storage Agent on the Secure Storage server. This account must also be a local Administrator on the Secure Storage server.
- Physical access to the Secure Storage server. Once the server is hardened access with regular methods will be disabled.
- Sufficient storage space on the Secure Storage server for all backup files. For one backup file, the space required is at least the size of the backed-up Active Directory database file (Ntds.dit) and the SYSVOL folder plus 40MB for the transaction log files.

Cloud Storage

- Internet access available on the Recovery Manager for Active Directory console. A standard outbound HTTPS port 443 is used to upload data to Azure Blob.
- Azure subscription(s) to create and manage Azure Storage accounts and containers.
- A method of creating and managing Azure Storage accounts, containers, and policies for the storage account (lifecycle, immutability and replication policies).

Active Directory Virtual Lab requirements

Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2, 2016 or 2019

Software that must be installed on the Active Directory Virtual Lab computer:

- Microsoft SCVMM Console (supplied with the SCVMM version you plan to use)

Software that is installed on the source computer by Active Directory Virtual Lab console:

- Disk2vhd v2.01 utility

For more details, see the *Working with SCVMM 2012 R2 or higher* section in User Guide.

Supported operating systems for the Hyper-V host:

- Microsoft Windows Server 2012 R2 or higher.

VMware vCenter/ESX Server 6.0, 6.5, 6.7 and 7.0

- Active Directory Virtual Lab does not support conversion of Windows Server 2019 Domain Controllers using VMWare ESXi/vCenter server.
- Active Directory Virtual Lab does not support VMware ESXi 6.0.

- vCenter Converter 6.2 must be installed in your environment using the Client-Server installation setup option.
- vCenter Converter must be accessible to the Active Directory Virtual Lab.
- If the TLS 1.0 protocol is disabled on vCenter Converter and vCenter servers, then switch to TLS 1.2 on the ADVL server. For more details, see the following KB articles:
 - <https://kb.vmware.com/s/article/2145796>.
 - <https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/2960358>

Recovery Manager Portal requirements

Processor

1 GHz or faster

Memory

1 GB or more

Hard disk space

2 GB or more

Operating system

You can install the Recovery Manager Portal on a computer running one of the following x64 operating systems:

- Microsoft Windows Server 2019, 2016, 2012 R2, and 2012

Supported Web Browsers

- Microsoft Internet Explorer
- Google Chrome
- Microsoft Edge (Chromium-based versions only)

Microsoft .NET Framework

Microsoft .NET Framework version 4.5.2 or higher

Microsoft Internet Information Server (IIS)

Microsoft Internet Information Services (IIS) 8.5 or higher

Microsoft SQL Server and its components

Microsoft SQL Server versions

One of the following versions is required:

- Microsoft SQL Server 2019, 2017, 2016, 2014, and 2012 (Enterprise, Business Intelligence, Standard, Express, Web, or Developer Edition)

Required Microsoft SQL Server components

- Microsoft System CLR Types for SQL Server 2012

If this component is not installed, it will be installed automatically by the RMAD setup.

Password and SIDHistory Recoverability Tool

You can only use the Password and SIDHistory Recoverability Tool if Microsoft's Active Directory Recycle Bin is not enabled in your environment.

Product Licensing

The Recovery Manager for Active Directory(RMAD) license 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 console tree root, and then click **About**.

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 key file, 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 returns a warning message each time you back up data. In this case, you can revoke licenses from the domains whose backups you no longer need. The revoked licenses are returned to the pool of available licenses and you can allocate them to a different domain.

CAUTION When you revoke licenses from a domain, all backups created by Recovery Manager for Active Directory 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**.

Getting Started

Upgrade and installation instructions

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(RMAD) supports a direct upgrade from version 10.0 and higher. If you have an earlier version of RMAD, the best practice is to upgrade the product to any of the supported versions, and then upgrade it to the latest version.

Alternatively, you can install the latest version of RMAD on a new clean machine and perform a full replication. The Full replication feature allows you to create a full copy of the primary Recovery Manager console settings on the new console instance. This option is supported starting from Recovery Manager for Active Directory version 9.0.1. For details, see the *Full Replication* section in User Guide.

For Recovery Manager for Active Directory Disaster Recovery Edition, after upgrade of Recovery Manager for Active Directory it is recommended to upgrade the Secure Storage agent on the Secure Storage server to the same version. With a hardened Secure Storage server, Recovery Manager for Active Directory does not automatically upgrade the agent and this must be completed with console (physical) access to the server.

NOTE | The Secure Storage server agent will continue to function when its version does not match the version of the RMAD console but new functionality may be lost.

Additional resources

Additional information is available from the following:

- Online product documentation [Support Portal](#)
- Recovery Manager Community <https://www.quest.com/community/products/recovery-manager/f/forum>

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

Third-Party Contributions

This product contains the third-party components listed below. For third-party license information, go to <https://www.quest.com/legal/third-party-licenses.aspx>. Source code for components marked with an asterisk (*) is available at <http://opensource.quest.com>.

List of third-party contributions

Component	License or acknowledgment
7-ZIP 19.0	Copyright 1999-2019 Igor Pavlov Copyright 2015-2016 Apple Inc. All rights reserved.
AeroWizard 2.2.3	MIT 1.0
AutoFixture 4.12.0	MIT 1.0
AutoMapper 4.1.1	MIT 1.0
Azure.Storage.Common 11.2.3	MIT Template 2020
Boost 1.72.0	Boost 1.0
EntityFramework 6.4.4	Apache 2.0
Fody 4.2.1	MIT
FontAwesome.WPF 4.7.0.9	MIT
Microsoft.Azure.Storage.Blob 11.2.3	MIT Template 2020
Group Controls 1.8	Apache 2.0 Copyright Notice - Group Controls 1.5.3
Microsoft.Dism 2.0.20	MIT
Microsoft.PowerShell.3.ReferenceAssemblies 1.0.0	MIT
Microsoft.Xaml.Behaviors.Wpf 1.1.19	MIT
MinHook 1.3.2.1	MinHook 1.0 Copyright 2009 Tsuda Kageyu All rights reserved.
MinHook 1.3.3	MinHook 1.0 Copyright 2009 Tsuda Kageyu All rights reserved.
Newtonsoft.Json.dll 6.0.6	MIT
PropertyChanged.Fody 2.6.1	MIT
RazorEngine 3.10.0	Apache 2.0
SSH.Net 2016.1.0.2016.1.0	MIT
System.Management.Automation 6.2.2	MIT Template 2020
System.ValueTuple 4.5.0	MIT 1.0
TaskScheduler 2.8.18	MIT

Component	License or acknowledgment
Task Scheduler Managed Wrapper 2.8.18	MIT
TimeSpan Helper Library 2.2	New BSD N/A
Windows Installer XML Toolset (aka WiX) 3.14	Microsoft Reciprocal License (MS-RL) N/A

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.