Quest

Quest® Recovery Manager for Active Directory
Disaster Recovery Edition 10.0.1

Deployment Guide

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.

Legend

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

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

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Recovery Manager for Active Directory Disaster Recovery Edition Deployment Guide
Updated - June, 2019
Version - 10.0.1

Contents

Introduction **5**

Permissions required to use Recovery Manager for Active Directory **6**

Permissions required to use Forest Recovery Console **9**

Permissions required to use Recovery Manager Portal **11**

Permissions required to access the SQL reporting database **13**

Installing Recovery Manager for Active Directory Disaster Recovery Edition **14**

Using the Setup Wizard 15

Performing a silent installation 15

Installing Forest Recovery Agent 18

Planning for Active Directory forest recovery **19**

Developing a custom forest recovery plan 19

Pre-recovery steps 19

Best practices for using Forest Recovery Console **21**

Best practices for deploying Recovery Manager Console **23**

Best practices for using Computer Collections **25**

Best practices for granular AD data restores **27**

Difference between agent-based and agentless methods of restoration 27

Agentless method 27

Permissions required for agentless method 27

Agent-based method 28

Permissions required for agent-based method 28

Restoring passwords and SID history **29**

Preserving passwords and SID history in object tombstones 29

Step 1: Make sure prerequisites are met 29

Step 2: Modify the searchFlags attribute value 30

Best practices for creating backups **31**

Develop a backup and restore plan 31

Determine which domain controllers to back up and how often 31

Methods for deploying Backup Agent 31

Retain recent backups 32
Where to store backups 32
Storing backups for granular online or complete offline restores 33
Storing backups for forest recovery 34

Technical characteristics **35**
Typical sizes of databases 35
Configuration database files 35
Reports database files 35
Typical backup creation times 36
Recommendations 36
Typical times to unpack backups 36

Communication ports **38**

About us **40**
Technical support resources 40

Introduction

This document provides information about deploying Quest® Recovery Manager for Active Directory Disaster Recovery Edition. It also includes some best practice recommendations for using Recovery Manager for Active Directory to back up and restore Active Directory data.

Recovery Manager for Active Directory Disaster Recovery Edition is a comprehensive, next-generation solution that helps you back up and restore Active Directory data. Recovery Manager for Active Directory dramatically reduces the time required to restore Active Directory and Group Policy data to minutes on average. This improves the availability of corporate networks and reduces network downtime.

For information about how to install the application components, refer to the Quick Start Guide supplied with this release of Recovery Manager for Active Directory Disaster Recovery Edition.

Permissions required to use Recovery Manager for Active Directory

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

Table 1: Minimum permissions

Task	Minimum permissions
Install Recovery Manager for Active Directory	The account must be a member of the local Administrators group on the computer where you want to install Recovery Manager for Active Directory. If during the installation you specify an existing SQL Server instance, the account with which Recovery Manager for Active Directory connects to that instance must have the following permissions on the instance: • Create Database • Create Table • Create Procedure • Create Function
Open and use the Recovery Manager Console	The account must be a member of the local Administrators group on the computer where the Recovery Manager Console is installed. The account must also have the following permissions on the SQL Server instance used by Recovery Manager for Active Directory: • Insert • Delete • Update • Select • Execute
Preinstall Backup Agent manually	The account you use to access the target computer must be a member of the local Administrators group on that computer
Upgrade Backup Agent	
Discover preinstalled Backup Agent instances	The account used to access the target domain controllers must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Be a member of the Backup Operators group on each target domain controller.
Uninstall Backup Agent	

Task	Minimum permissions
Update information displayed about Backup Agent in the Recovery Manager Console	
Automatically install Backup Agent and back up Active Directory data	To automatically install Backup Agent, the account must have: • Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Local Administrator permissions on the target domain controller. To back up data, the account must be a member of the Backup Operators group on the target domain controller.
Back up Active Directory using preinstalled Backup Agent	The account used to access the target domain controllers must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Be a member of the Backup Operators group on each domain controller to be backed up.
Perform a complete offline restore of Active Directory by using the Repair Wizard	If you restore data to a domain controller where User Account Control (UAC) is not installed or disabled: • The account you use to access the domain controller must be a member of the Domain Admins group. If you restore data to a domain controller where User Account Control (UAC) is enabled: • The account you use to access the domain controller must be the built-in Administrator on that computer. In both these cases, the account you use to access the domain controller must have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer.
Perform a selective online restore of Active Directory objects	**Agentless restore** The account used to access the target domain controllers must have: • Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Reanimate Tombstones extended right in the domain where objects are to be restored. • Write permission on each object attribute to be updated during the restore.

Task	Minimum permissions
	• 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. For more details, see the *Agentless method* section in User Guide. **Agent-based restore** • The account used to access target domain controllers must have domain administrator rights. For more details, see the *Agent-based method* section in User Guide.
Restore a Group Policy object	The account used to access the target domain controller must: • Be a member of the Group Policy Creator Owners group. • Have Full Control privilege on the Group Policy object. • Be a member of the Backup Operators group. • Have sufficient permissions to read/write Active Directory objects linked to the Group Policy object.
Automatically install Backup Agent and back up an AD LDS (ADAM) instance	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory that is located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance
Back up an AD LDS (ADAM) instance using preinstalled Backup Agent	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance.
Restore an AD LDS (ADAM) instance	The account used to access the computer hosting the instance must: • Have the Write permission on the folder %AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory located on the Recovery Manager for Active Directory computer. • Be a member of the local Administrators group on the computer hosting the AD LDS (ADAM) instance.

Permissions required to use Forest Recovery Console

The table below lists the minimum user account permissions required to perform some common tasks with Forest Recovery Console.

Table 2: Minimum permissions

Task	Minimum permissions
Start and use the Forest Recovery Console	Have Read access to the Recovery Manager for Active Directory backup registration database.
Access domain controllers in the recovery project	Have either domain administrator rights or all of the following permissions: • Reanimate Tombstone control access right (or be a member of a group that has this access right). By default, the **Reanimate Tombstone control access** right is only granted to domain administrators. Domain administrators can delegate the permission necessary to restore deleted objects to other users and groups by granting the user or group the Reanimate Tombstone control access right. A security risk can be introduced by delegating this permission to a user, because it allows the user to restore an account that may have a level of access greater than that of the user. By restoring such an account, the user in effect gains control of that account. This is because the LDAP API does not provide the capability to restore the backed up password, and so the user can set the initial password on the account. • Write access to each mandatory attribute that needs to be updated. • Write access to the Relative Distinguished Name (RDN) and other attributes that need to be updated. • Child-creation rights on the destination container for the object class that is to be restored. • Write access to universal and domain local groups in all domains in the forest.
Install or uninstall Forest Recovery Agent	Be a member of the local Administrators group on the target domain controller.
Check forest health if the **User authentication; RID Master and GC operation** option is selected on the **Settings** tab in the Check Forest Health dialog.	Have either domain administrator rights or all of the following permissions on the container for the test user account: • **Create/Delete** user objects Applies to: This object and all descendant objects • **Full Control** Applies to: Descendant User objects

For information about using the Forest Recovery Console, see *Forest Recovery Console* section of User Guide.

Permissions required to use Recovery Manager Portal

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

Table 3: Minimum permissions

Task	Minimum permissions
Install or uninstall Recovery Manager Portal	Be a local administrator on the target computer.
Access Recovery Manager Remote API Access service	To access a Recovery Manager for Active Directory instance, the Recovery Manager Portal requires the Recovery Manager Remote API Access service to be installed and running on the Recovery Manager for Active Directory computer. This service enables the following Recovery Manager for Active Directory features: integration with Recovery Manager Portal, RMAD console fault tolerance and support for hybrid environment. For information about minimum permission requirements for the service, refer *Step 1: Install Recovery Manager Remote API Access Service* in User Guide.
Start and use the Recovery Manager Portal	From version 8.7, Recovery Manager Portal can be run under Managed Service Account (in Windows Server 2008 or higher) or Group Managed Service Account (in Windows Server 2012 or higher). If you specify the MSA or gMSA account, add the '$' character at the end of the account name (e.g. domain\computername$) and leave the Password field blank (on the Specify Web Site Settings step of the wizard). • The Managed Service Account (in Windows Server 2008 or higher) or Group Managed Service Account (in Windows Server 2012 or higher) must be a member of the local Administrator group on the Recovery Manager for Active Directory machine. • In case of MSA or gMSA account, Recovery Manager Portal supports only Windows authentication to access the SQL Server databases.
To perform restore or undelete operation	User must be a member of the "Recovery Manager Portal - Recovery Operators" security group on the computer where the Recovery Manager Portal is installed. If you want to use the agentless recovery method, select the **Configure a list of delegates that can perform the restore and undelete operations** option on the **Portal Settings** tab. For more information about delegation, see the *Delegating restore or undelete permissions* section in User Guide.
To perform the undelete operation	User must be a member of the "Recovery Manager Portal - Undelete Operators" local security group on the computer where the Recovery Manager Portal is installed. If you want to use the agentless recovery method in Recovery Manager Portal,

Task	Minimum permissions
	select the **Configure a list of delegates that can perform the restore and undelete operations** option on the **Portal Settings** tab. For more information about delegation, see the *Delegating restore or undelete permissions* section in User Guide.
To modify the Recovery Manager Portal configuration and delegate restore permissions to other Recovery Manager Portal users	User must be a member of the "Recovery Manager Portal - Configuration Admins" local security group on the computer where the Recovery Manager Portal is installed.
To view the health summary and backup creation history for the Recovery Manager for Active Directory instances	User must be a member of the "Recovery Manager Portal - Monitoring Operators" local security group on the computer where the Recovery Manager Portal is installed.

Permissions required to access the SQL reporting database

The table below lists the minimum user account permissions required to access the SQL reporting database.

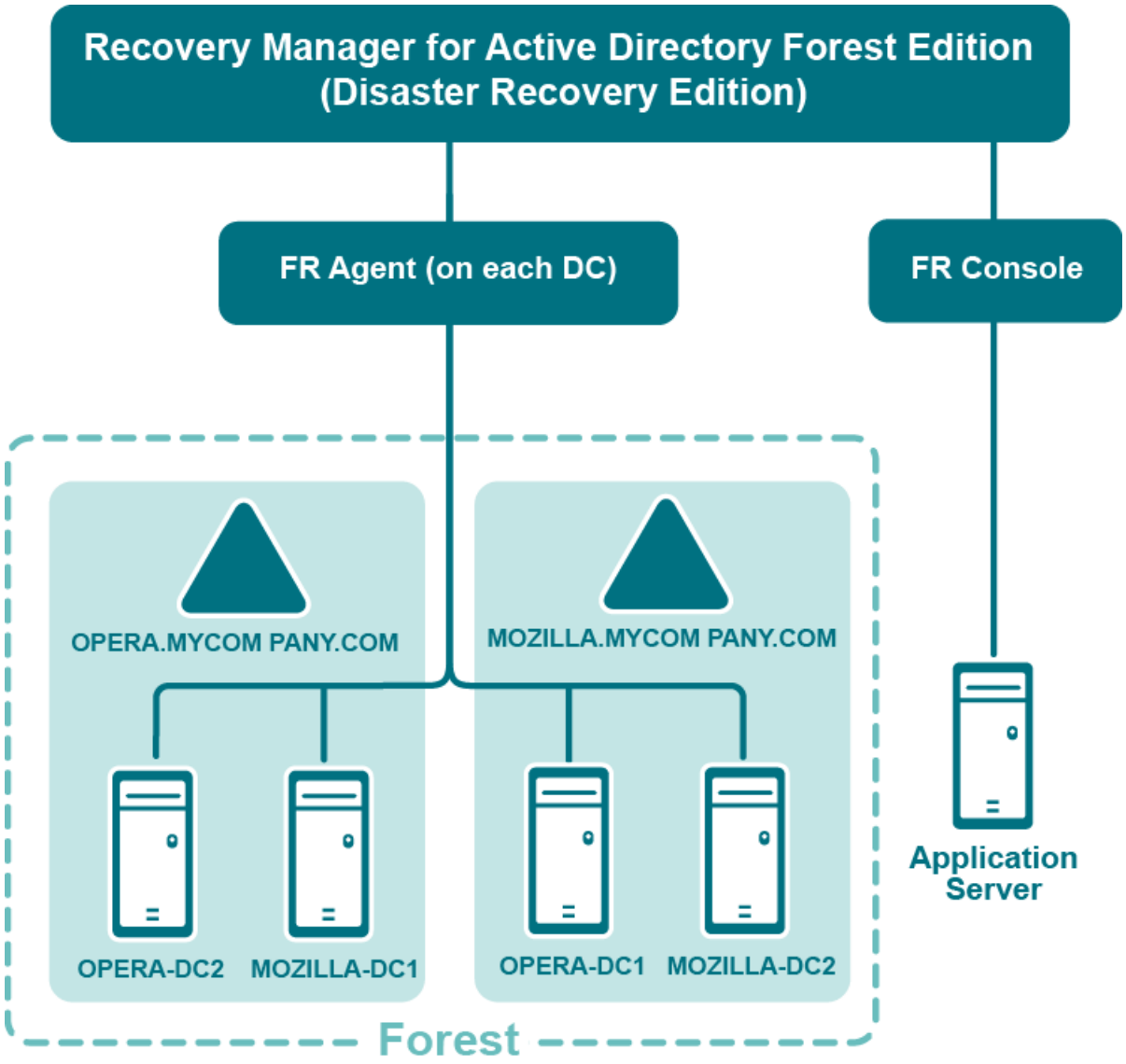
Table 4: Minimum permissions

Task	Minimum permissions
To 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 execute 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

Installing Recovery Manager for Active Directory Disaster Recovery Edition

This section describes how to install and configure the application components (the Forest Recovery Console and Forest Recovery Agent).

The following diagram shows the Recovery Manager for Active Directory Disaster Recovery Edition deployment:



Recovery Manager for Active Directory Disaster Recovery Edition is designed to ensure intuitive operation and close integration with the Windows operating system.

Using the Setup Wizard

To install Recovery Manager for Active Directory Disaster Recovery Edition using the Setup Wizard

1. Run the file Autorun.exe, located in the root folder of the Recovery Manager for Active Directory installation CD.
2. In the Autorun window, click **Setup**, and then click **Recovery Manager for Active Directory Disaster Recovery Edition**.
3. Follow the instructions in the Setup Wizard.
4. On the **User Information** page, click **Licenses**. In the **License Status** dialog box, click **Browse License** to locate and open the license key file you want to use.
5. Follow the instructions in the wizard to complete the installation.

Performing a silent installation

A silent (or unattended) installation of Recovery Manager for Active Directory Disaster Recovery Edition does not require any user interaction. With this method, you specify the Recovery Manager for Active Directory Disaster Recovery Edition installation parameters at a command prompt before running the installation.

NOTE: You can only perform a silent installation ofRecovery Manager for Active Directory Disaster Recovery Edition when all of the following conditions are true:

- One of the Microsoft SQL Server versions listed in the System Requirements section in the Release Notes is accessible from the computer where you plan to install Recovery Manager for Active Directory Disaster Recovery Edition.
- One of the Microsoft SQL Server Reporting Services versions listed in the System Requirements section in the Release Notes is accessible from the computer where you plan to install Recovery Manager for Active Directory Disaster Recovery Edition or Quest Reports Viewer is installed on that computer.

To perform a silent installation of Recovery Manager for Active Directory Disaster Recovery Edition

- Enter the following syntax at a command prompt:

```
Msiexec /i "<Path to the Recovery Manager for Active Directory Disaster Recovery
Edition installation CD> \Setup\Rmadfe.msi" /qb
SQLSERVER="<SQLServerName>\<InstanceName>"
```

The table below describes the parameters you can use to perform a silent installation of Recovery Manager for Active Directory Disaster Recovery Edition.

IMPORTANT: When specifying the folder to be used as the default location for backup files (.bkf), make sure that the volume hosting the specified default backup storage folder has enough disk space. The backup files could reach several hundred megabytes in size.

Table 5: Silent installation parameters

Parameter	Description	Example
SQLSERVER	Specifies the name and instance of a local or remote SQL Server to store Recovery Manager for Active Directory Disaster Recovery Edition data. This is a required parameter.	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>"
SQLDBNAME_REPORTING	Specifies an existing or new database to store Recovery Manager for Active Directory Disaster Recovery Edition report data. This database resides in the SQL Server instance defined in the SQLSERVER parameter. If you specify a database that does not exist, it will be created. If the SQLDBNAME_REPORTING parameter is omitted, a new database with the following name is created and used: **RecoveryManager-Reporting- <name of the Recovery Manager for Active Directory Disaster Recovery Edition computer>**	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" SQLDBNAME_REPORTING= "<DatabaseName>"
INSTALLDIR	Specifies the Recovery Manager for Active Directory Disaster Recovery Edition installation folder. If this parameter is omitted, the following default folder is used: **%ProgramFiles%\Quest\Recovery Manager for Active Directory Disaster Recovery Edition**	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" INSTALLDIR="<PathToInstallationFolder>
BACKUP_PATH	Specifies the location where Recovery Manager for Active Directory Disaster Recovery Edition will store Active Directory backups. If this parameter is omitted, the backups are stored in **%AllUsersProfile%\Application Data\Quest\Recovery Manager for Active Directory\Backups**	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" BACKUP_PATH="<PathToStoreADBackups>"
SQLAUTHENTICATION	Specifies the SQL Server authentication method. You can use one of the following values:	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>"

Parameter	Description	Example
	• 0. Specifies to use Windows authentication credentials of the current user account. • 1. Specifies to use the authentication credentials set in the SQLUSERNAME and SQLUSERPASSWORD parameters. If this parameter is omitted, Windows authentication credentials of the current user account are used.	SQLAUTHENTICATION="0"
SQLUSERNAME	Specifies the user name for authentication on the SQL Server. This parameter is required if you set the SQLAUTHENTICATION parameter value to "1".	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" SQLAUTHENTICATION="1" SQLUSERNAME="<UserName>" SQLUSERPASSWORD="<Password>"
SQLUSERPASSWORD	Specifies the password for authentication on the SQL Server. This parameter is required if you set the SQLAUTHENTICATION parameter value to "1".	
VIEWER_ APPLICATION_TYPE	Specifies the application to be used for viewing Recovery Manager for Active Directory Disaster Recovery Edition reports. You can use one of the following values: • **local**. Specifies to use Quest Reports Viewer installed on the Recovery Manager for Active Directory Disaster Recovery Edition computer. • **remote**. Specifies to use Microsoft SQL Server Reporting Services installed on a remote computer.	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" VIEWER_ APPLICATION_TYPE="<Value>"
VIEWER_REPORTING_ SERVER	Specifies the HTTP address to access Microsoft SQL Server Reporting Services. This parameter is required if you set the VIEWER_ APPLICATION_TYPE parameter value to "remote".	Msiexec /i "E:\Setup\Rmadfe.msi" /qb SQLSERVER="<SQLServerName>\<InstanceName>" VIEWER_ APPLICATION_TYPE="remote" VIEWER_ REPORTING_SERVER= "http://<HTTPAddress>"

Installing Forest Recovery Agent

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

IMPORTANT: If Forest Recovery Agent was not installed on a target domain controller before a disaster occurred, the application may not be able to recover that domain controller.

For instructions on how to install Forest Recovery Agent on a target domain controller, see the User Guide supplied with this release of Recovery Manager for Active Directory Disaster Recovery Edition

Planning for Active Directory forest recovery

This section provides basic best practice information about planning the recovery of an Active Directory forest. For detailed instructions on how to restore the entire Active Directory forest or selected domains in the forest, please refer to the *Recovery Manager for Active Directory Disaster Recovery Edition User Guide* supplied with this release.

Developing a custom forest recovery plan

When planning for Active Directory forest recovery, you should first have a detailed topology map of your forests. The map should list all the information about the domain controllers, such as their names and backup status, and the trust relationships between them.

TIP: To perform a forest recovery, an Administrator account password is required for each domain in the forest. It is a good practice to archive the Administrator account password history and store the archive in a safe place.

Pre-recovery steps

Because of the complexity and critical nature of the forest recovery process, it is recommended that Active Directory administrator observe the following rules to prevent the forest failure:

- Use only reliable and tested hardware, such as hard disks, uninterruptible power supply, etc.
- Test any new configuration in a test lab before deploying it in your environment.
- Ensure that each domain in the forest has at least two domain controllers.
- Keep detailed logs about the health state of Active Directory on a daily basis, so that in case of a forest wide failure the approximate time of failure can be identified.
- Regularly back up all domain controllers in the forest with Recovery Manager for Active Directory.
- Install Forest Recovery Agent on all domain controllers in the forest.
- Using the Forest Recovery Console, create a recovery project for your forest. Verify the settings of your forest recovery project on a regular basis, especially when there are membership changes to the Enterprise Admins or Domain Admins group. This helps ensure that the IT staff fully understands the forest recovery plan.

  For more information on verifying the recovery project settings, see the *Recovery Manager for Active Directory Disaster Recovery Edition User Guide* supplied with this release.

TIP: It is a good practice to create a Computer Collection that includes all domain controllers in the forest and back up the Collection each time you make changes to the forest infrastructure. To ensure that the Forest Recovery Agent is automatically installed on all domain controllers, open the Recovery Manager console (MMC snap-in), and perform the following steps:

1. In the console tree, expand the **Computer Collections** node, and then select the Computer Collection that includes all domain controllers in the forest.
2. On the **Action** menu, click **Properties**, and then open the **Agent Settings** tab.
3. On the **Agent Settings** tab, select the **Ensure Forest Recovery agent is deployed** check box.
4. Click **OK**.

Best practices for using Forest Recovery Console

This section provides some best practice recommendations for installing and using the Forest Recovery Console and creating and storing Active Directory backups for forest recovery.

Table 6: Best practice recommendations

Recommendation	Justification
Install the Forest Recovery Console on a member server.	When installed on a domain controller, the Forest Recovery Console consumes its resources and may impair the domain controller's performance. In addition, domain controllers in your forest may require a restart during a forest recovery operation (for example, to boot in Directory Services Restore Mode). If you are using the Forest Recovery Console on a domain controller, Recovery Manager for Active Directory Disaster Recovery Edition cannot restart that domain controller during the forest recovery operation.
Use the Forest Recovery Console under a local administrator account.	Allows you to log on to the Forest Recovery Console computer and use the Console even if Windows authentication is not working properly in your Active Directory forest.
Run the verify settings operation on your recovery project at least once a month.	Enables Recovery Manager for Active Directory Disaster Recovery Edition to detect the changes occurred to your forest and update your recovery project accordingly. For more information about verifying recovery project settings, see the User Guide.
Store backups on domain controllers.	Store backups on the domain controllers for which they were created. This will substantially shorten the recovery time, as backups will not have to be transferred to the domain controllers during the recovery.
Create a recovery project while your Active Directory forest is healthy.	Do not postpone creating a recovery project until your forest becomes corrupt. The preferable method for creating a recovery project is to connect to a live domain controller and retrieve the forest infrastructure information from that domain controller.
Use separate Computer Collections for granular AD data recovery and forest recovery.	Granular Active Directory data recovery and full-scale forest recovery impose different requirements in terms of storing backups, backup creation frequency, and backup retention policies. To satisfy these requirements, you can create separate Computer Collections. • **Computer Collections for granular recovery**. Configure these Collections to back up Active Directory data at least once a day.

Recommendation	Justification
	• **Computer Collections for forest recovery**. Configure these Collections to back up data at least once in every five days. To avoid backup copying to domain controllers prior to the recovery, store each backup on the domain controller for which the backup was created. Configure a backup retention policy to keep the optimal number of backups. Backups should not consume too much disk space. At the same time, you should have a sufficient number of backups to choose from in case of an Active Directory disaster.
Configure the Forest Recovery Console to access the ForestRecovery-Persistence SQL Server database under the Microsoft SQL Server administrator account (sa).	Enables Recovery Manager for Active Directory Disaster Recovery Edition to access and use the ForestRecovery-Persistence database even if Windows authentication is not working properly in your Active Directory forest. For more information about the ForestRecovery-Persistence database and the Recovery Persistence feature, see the “Resuming an Interrupted Forest Recovery Operation” section in the User Guide.
Disable the automatic backup creation immediately after you discover any issues in your Active Directory forest.	If an Active Directory disaster occurs, automatic backup creation paired with a backup retention policy may delete all the good and trusted backups you have. When your Active Directory forest becomes corrupt, bad data starts sneaking into the backups that are created automatically. At the same time, your backup retention policy continues to delete old backups that contain good and trusted data. As a result, you may end up with a corrupt Active Directory forest and without any good and trusted backups to restore data from.
Configure a standalone mail server to use in case of an Active Directory failure.	Provides a fallback solution for a situation where all mail servers in your forest are rendered inoperable because of an Active Directory failure.
Restore as many domain controllers from backups as possible.	Allows you to restore many domain controllers simultaneously and at the same time minimize the amount of replication traffic for the domain controllers you recover by reinstalling Active Directory.
Ensure you allow traffic on the required communication ports.	For more information about the required ports, see Communication ports.

Best practices for deploying Recovery Manager Console

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

It is recommended to install the Recovery Manager Console on a member server and not on a domain controller. When installed on a domain controller, the Recovery Manager Console consumes its resources and may impair the domain controller's performance.

To perform a selective online restore of Active Directory data, it is sufficient to deploy one instance of the Recovery Manager Console in the Active Directory forest.

In order you could perform a complete offline restore of the Active Directory database by using the Repair Wizard, it is recommended to deploy an instance of the Recovery Manager Console in each Active Directory site.

A Computer Collection allows you to group the computers (domain controllers or AD LDS (ADAM) hosts) to which you want to apply the same backup creation settings. For more information on how to create and manage Computer Collections, see the User Guide supplied with this release of Recovery Manager for Active Directory.

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:

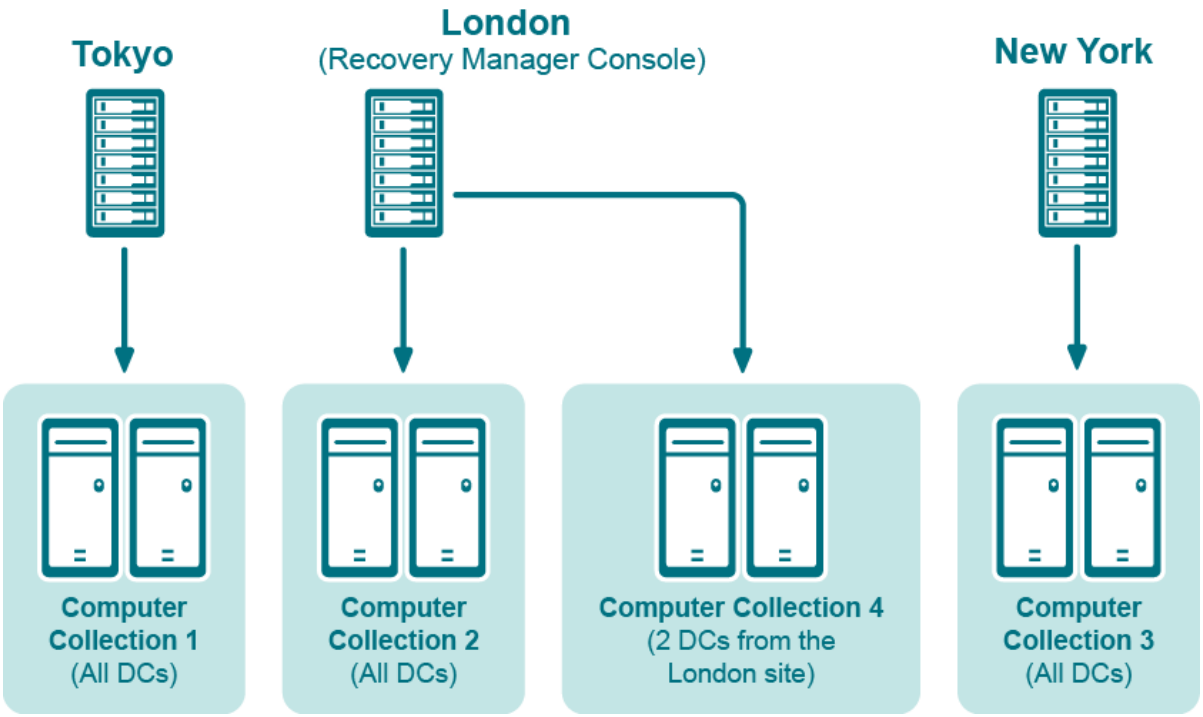


Figure 1: Example of Using Computer Collections

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.

Best practices for using Computer Collections

This section provides some recommendations for performing granular restore operations with Recovery Manager for Active Directory.

A Computer Collection allows you to group the computers (domain controllers or AD LDS (ADAM) hosts) to which you want to apply the same backup creation settings. For more information on how to create and manage Computer Collections, see the User Guide supplied with this release of Recovery Manager for Active Directory.

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:

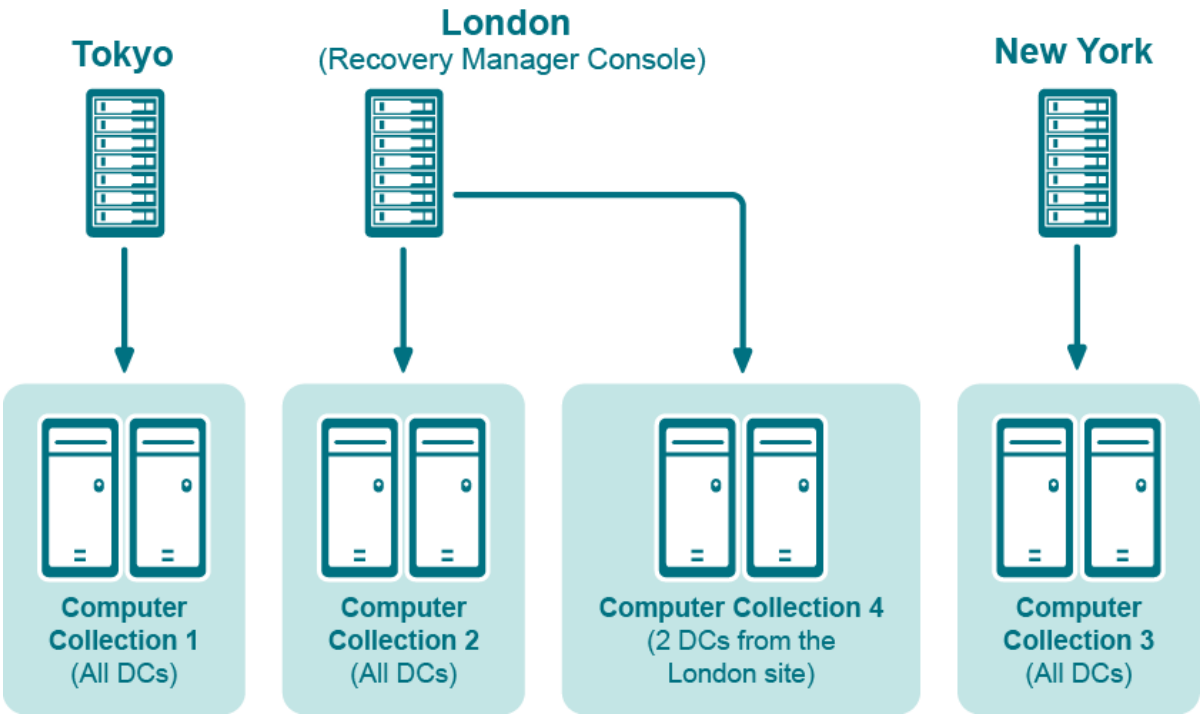


Figure 2: Example of Using Computer Collections

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.

Best practices for granular AD data restores

This section provides some recommendations for performing granular restore operations with Recovery Manager for Active Directory.

Difference between agent-based and agentless methods of restoration

With Recovery Manager for Active Directory, you can access the target domain controller by using either LDAP functions (agentless method) or Restore Agent supplied with Recovery Manager for Active Directory (agentbased method). Each of these methods has its advantages, limitations, and requirements.

Agentless method

Table 7: Table 1:Advantages and limitations of the agentless method

Advantages	Limitations
• The use of LDAP functions makes the wizard operations less intrusive on the domain controller. • You do not need to have administrator rights to perform the restore and compare operations.	To restore some object attributes, such as User Password and SID History, you need to modify the Active Directory schema. For more information, see “Restoring Passwords and SID History” in the User Cuide.

Permissions required for agentless method

The account with which Recovery Manager for Active Directory accesses the target domain controller must have specific permissions to perform data restore task

Table 8: Table 2: Required permissions

Task	Required permissions
Restore object attributes	Write access to the attributes to be restored
Restore a deleted object	• Reanimate Tombstone control access right. • Write access to each attribute to be updated during the restore.

Task	Required permissions
	• Child-creation rights on the destination container for the class of the object to be restored.
Restore cross-domain group memberships	Write access to universal and domain local groups in other domains.

Agent-based method

Table 9: Advantages and limitations of the agent-based method

Advantages	Limitations
• Allows you to compare and restore any objects (including deleted ones) and any attributes (including User Password and SID History). • A restore operation can be performed on a domain controller running any version of the Windows operating system supported by Recovery Manager for Active Directory. • The agent-based method of restoration is generally faster than the agentless method.	• The target domain controller must be the same as the backup source. • The user account used to access the target domain controller must have domain administrator rights and be a member of the Backup Operators group in case the target domain controller is running Windows Server 2003. • Recovery Manager for Active Directory automatically installs Restore Agent (the file RstAgent.exe) before starting a restore and automatically removes it on completion. The size of the file RstAgent.exe is about 380,000 bytes

Permissions required for agent-based method

The account with which Recovery Manager for Active Directory accesses the target domain controller must:

- Have sufficient permissions to copy files to the target domain controller.
- Be Access Service Control Manager on the target domain controller.
- Have the Write access to universal and domain local groups in other domains (only for restoring crossdomain group memberships).

To meet the above requirements, the account must be a member of

- Administrators local group on each target domain controller
- Backup Operators or Domain Admins group on each target domain controller that runs Windows Server 2003 or a later version of Windows.

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

Best practices for creating backups

This section provides some best practices for backing up Active Directory data using Recovery Manager for Active Directory.

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 forestwide 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 **System State** tab of the Computer Collection Properties dialog box.

If you intend to use Recovery Manager for Active Directory to recover failed domain controllers (for example, using the Repair Wizard), it is recommended that you back up all domain controllers in all domains with the option **Collect Forest Recovery metadata** enabled on the **System State** tab of the **Computer Collection Properties** dialog box. This option creates backups that can be used by the Forest Recovery Console to recover a forest. For more information, refer to the User Guide supplied with this version of Recovery Manager for Active Directory Disaster Recovery Edition.

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

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 Disaster Recovery Edition.

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 (that is, 60 days or 180 days by default, depending on the Windows operating system version).

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 Recovery Manager for Active Directory, 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.

For more information on how to specify backup storage settings, see the User Guide supplied with this release of Recovery Manager for Active Directory Disaster Recovery Edition.

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:

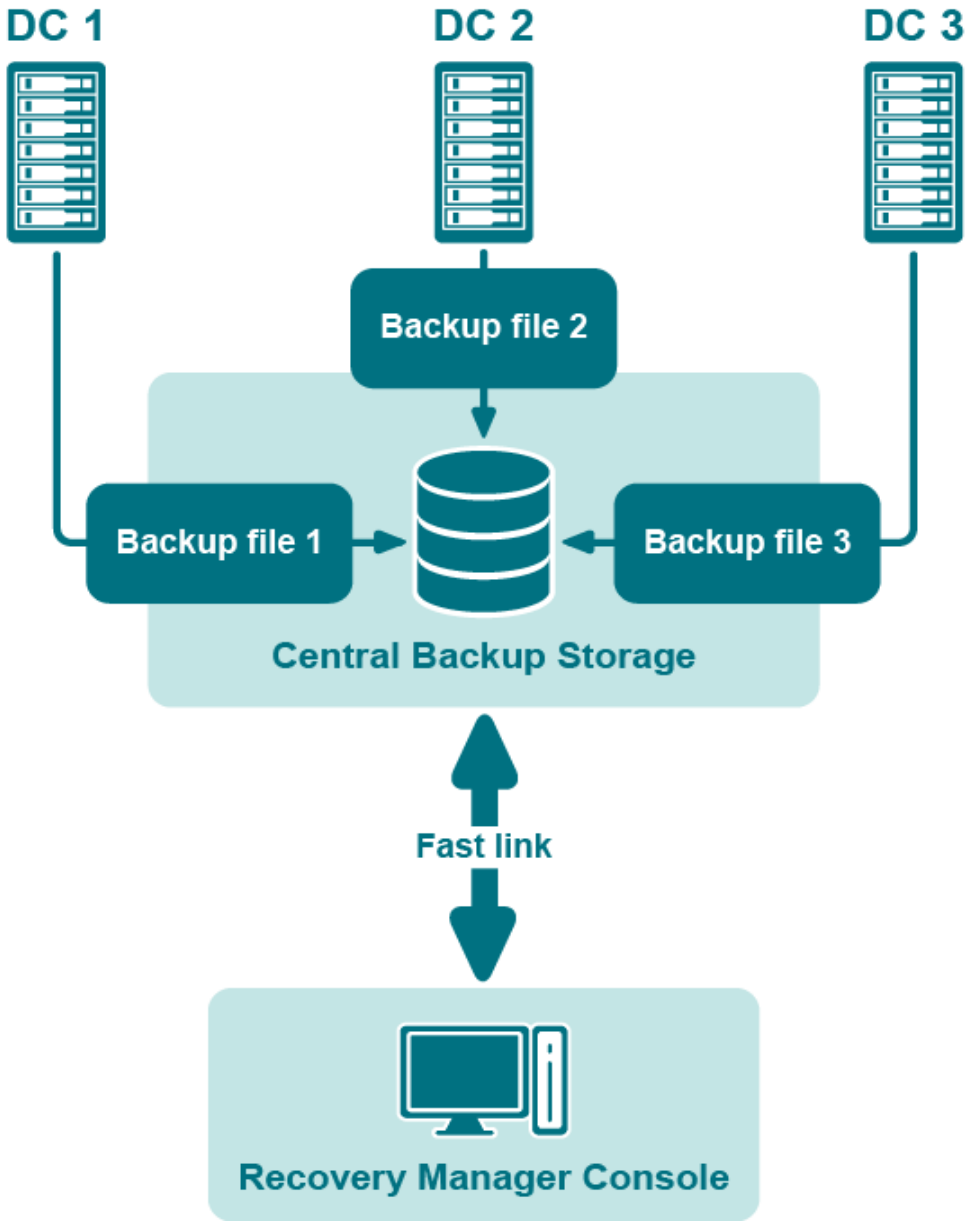


Figure 3: Backups for Granular Online or Complete Offline Restores

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:

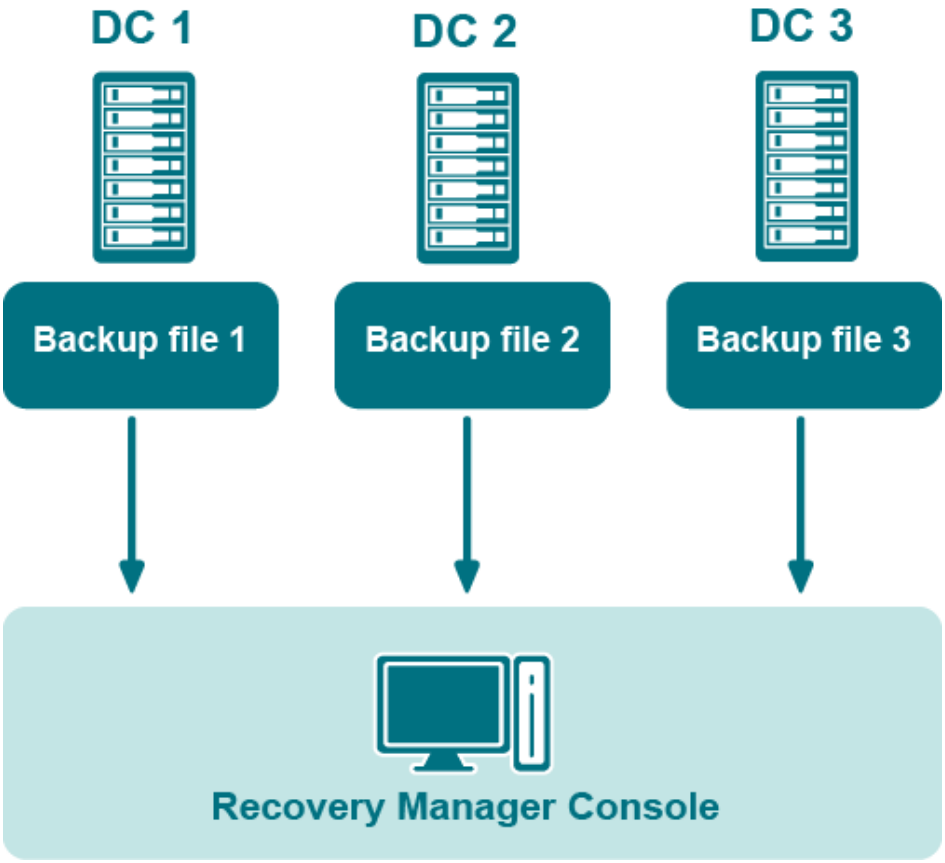


Figure 4: Backups for Forest Recovery

If you intend to use Recovery Manager for Active Directory 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.

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 sizes of databases

Configuration database files

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

- **ERDiskAD.mdb**. Recovery Manager for Active Directory configuration database. It contains information on the console configuration, such as the managed Computer Collections, backup creation sessions, etc.
- **Backups.mdb**. Recovery Manager for Active Directory 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%\Application Data\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.

Recovery Manager for Active Directory 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 Recovery Manager for Active Directory Disaster Recovery Edition.

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 3000 objects, the reports database file size will be approximately 18 MB.

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 Recovery Manager for Active Directory Disaster Recovery Edition.

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 Recovery Manager for Active Directory Disaster Recovery Edition computer hardware: CPU 2x Intel Xeon 2,8 Hz; RAM 1 GB

Table 10: 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.

If you are planning that backups created with Recovery Manager for Active Directory Disaster Recovery Edition be used by other MTFcompliant backup tools, set the data compression method to **None**.

Typical times to unpack backups

Before using a packed backup file (e.g. in the Online Restore Wizard), Recovery Manager for Active Directory must unpack it.

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

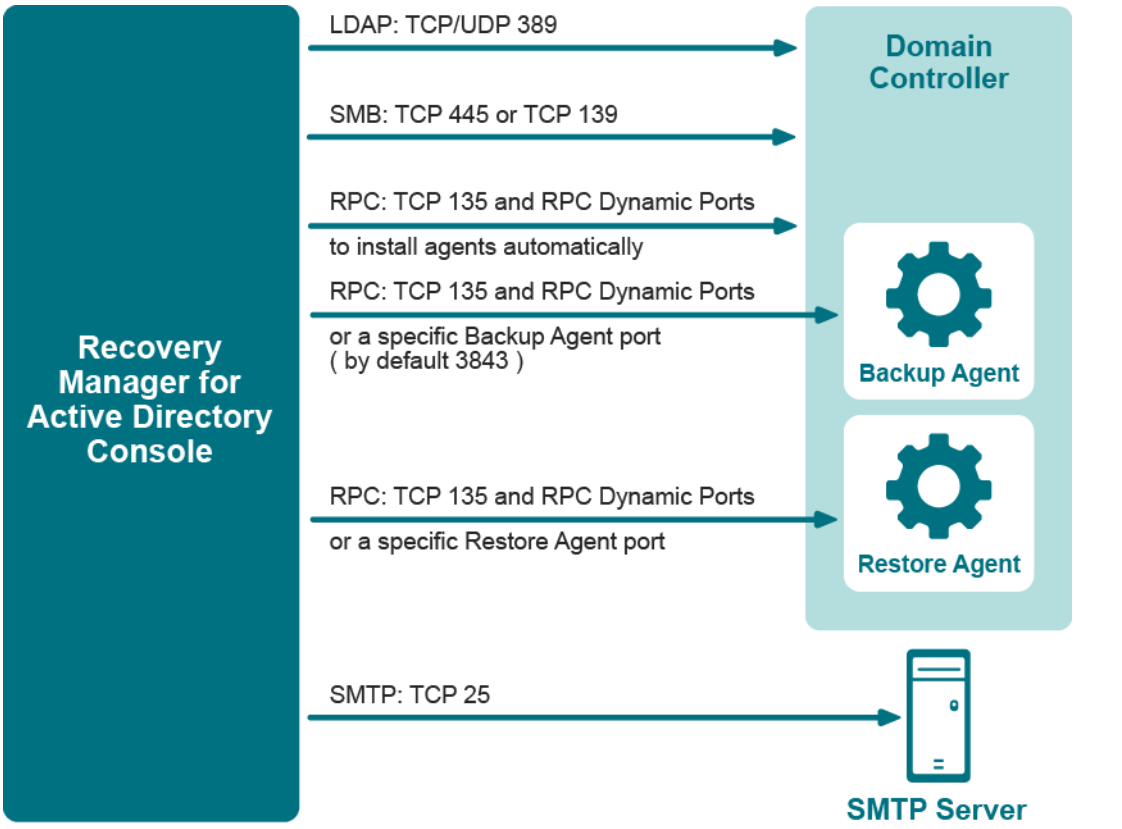
NOTE: You can manage the creation of the unpacked backups using the **Unpacked Backups** tab in the **Recovery Manager for Active Directory Settings** dialog box. You can also have the Online Restore Wizard or Group Policy Restore Wizard keep unpacked backups for future use. For more information, refer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

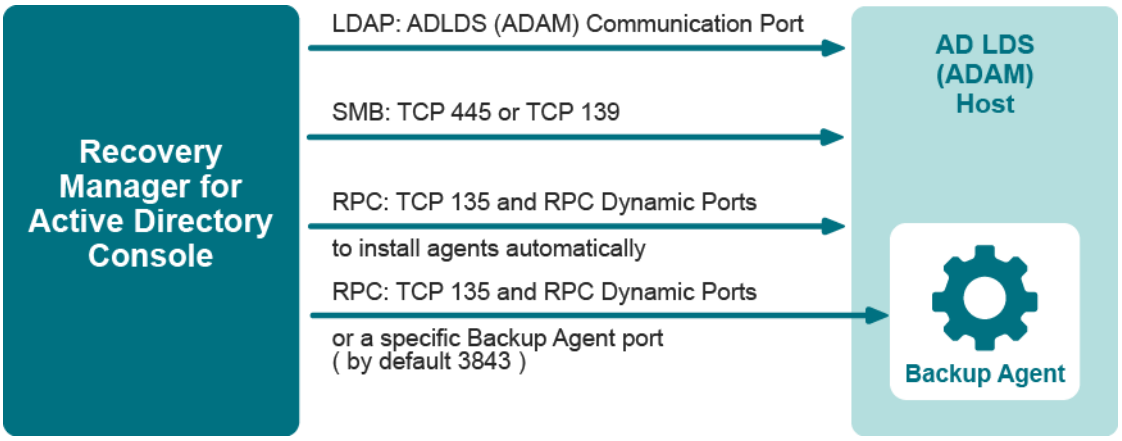
Table 11: Typical times to unpack backups

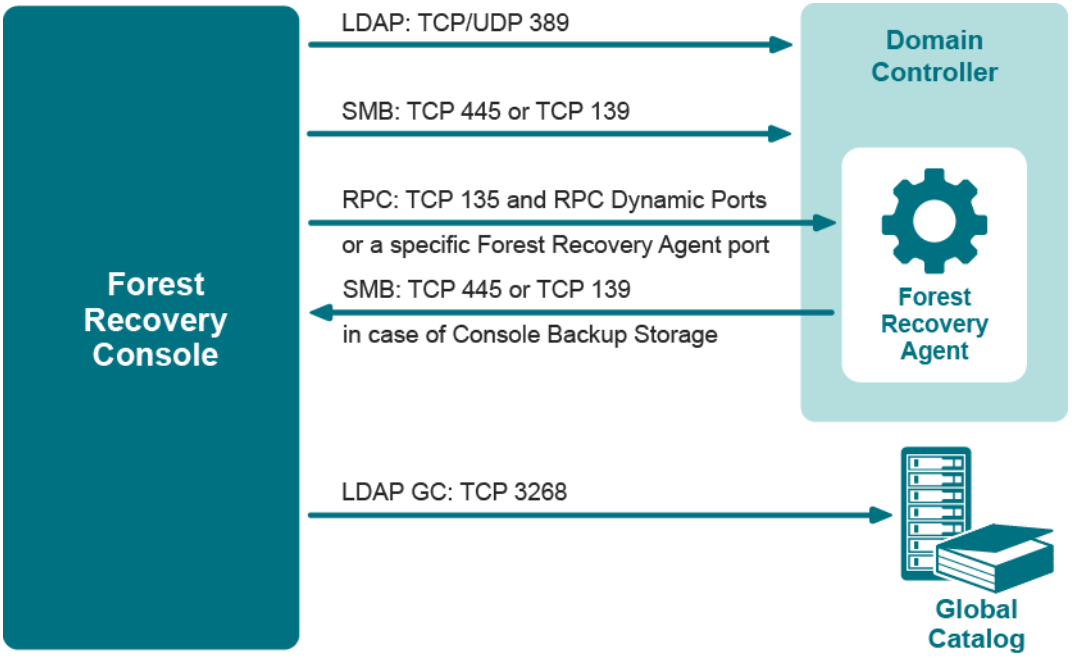
Compression method	Packed backup file size	Backup unpacking time (min:sec)
None	3.17 GB	01:57
Fast	1.27 GB	01:29
Normal	1.22 GB	01:25
Maximum	1.2 GB	01:22

Communication ports

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






Forest Recovery Console
LDAP: TCP/UDP 389
SMB: TCP 445 or TCP 139
RPC: TCP 135 and RPC Dynamic Ports
or a specific Forest Recovery Agent port
SMB: TCP 445 or TCP 139
in case of Console Backup Storage
Domain Controller
Forest Recovery Agent
LDAP GC: TCP 3268
Global Catalog

About us

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, nd 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