Disaster Recovery for Identity for Active Directory

User Guide

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

20 Enterprise, Suite 100

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.

Legend

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

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

Disaster Recovery for Identity for Active Directory User Guide
Updated - February 12, 2025

Contents

About Disaster Recovery for Identity for Active Directory

Disaster Recovery for Identity for Active Directory offers off-network abilities to manage on-premises domain controllers, including Active Directory® backups and restore operations, in the case of a disaster. It is essential for any modern business to have uninterrupted network and computer systems, which are essential for business continuity. Unforeseen outages, like directory service failures, can significantly disrupt operations. To mitigate such risks, critical infrastructure must be designed for swift recovery from failures.

The product leverages advanced technologies to minimize downtime resulting from Active Directory corruption or accidental modifications. This solution automates backups and enables rapid, remote recovery of data stores in Active Directory, and dramatically reduces the time required to restore Active Directory.

Disaster Recovery for Identity for Active Directory allows you to perform the following operations:

- Configure and manage backups using Backup Plans.
- Store Active Directory backups in Quest Azure tenant.
- Configure and manage recovery of an Active Directory Forest.
- Restore Active Directory using Restore to Clean OS method, allowing you to restore the entire forest or any of its parts on a freshly installed Windows machine.
- Set recovery method for individual domain controllers to Install Active Directory
- Schedule backup of domain controllers based on business needs.
- Verify recovery configurations to validate your disaster Recovery Plan.

The solution simplifies and automates the process of preparing for and responding to disasters, such as the corruption of directory object data. These disasters can stem from hardware or software failures, or accidental human errors. Some examples of forest-wide failures include:

- None of the domain controllers can replicate with its replication partner.
- Changes cannot be made to Active Directory at any domain controller.
- New domain controllers cannot be installed in any domain.

- All domain controllers have been logically corrupted or physically damaged to a point that business continuity is impossible (for instance, all business applications that depend on Active Directory are non-functional).
- A rogue administrator has compromised the Active Directory environment.
- An adversary intentionally or an administrator accidentally runs a script that spreads data corruption across the Active Directory Forest.
- An adversary intentionally or an administrator accidentally extends the Active Directory schema with malicious or conflicting changes.

Disaster Recovery for Identity for Active Directory can be started from Quest On Demand single SaaS command point. For more information about Quest On Demand, see the Quest On Demand product documentation.

To access On Demand, you need to provide On Demand credentials or use your existing Quest Software account. For more details, see Signing up for Quest On Demand in the *On Demand Global Settings User Guide*.

The following sections describe how to configure and work with Disaster Recovery for Identity for Active Directory:

- Disaster Recovery for Identity for Active Directory Module Overview
- Before You Start
- Sign up for On Demand
- Configuring Disaster Recovery for Identity for Active Directory
- Working with Disaster Recovery for Identity for Active Directory
- Environments
- Topology
- Backup Plans and Backups
- Recovery
- Events Management
- Task Management

2

Disaster Recovery for Identity for Active Directory Module Overview

The user interface of the administrative console consists of six main screens. The main screen, called **Environments**, is opened upon clicking **Recover** in the left hand navigation panel, and then **Active Directory:**

- **Environments**

The Environments screen is your starting screen. On this screen, you can view all environments available and a summary of each environment, and create new environments for your Active Directory forests.

- **Topology**

The Topology screen shows a list of domains and domain controllers linked to the Active Directory forest.You can also run forest discovery, manage Domain Controller Agents, and create Backup Plans from this screen.

- **Backup**

The Backup screen allows the user to create and run Backup Plans, and shows a list of Backup Plans created by the user. The Backups screen also displays a list of backups created from the Backup Plan(s).

- **Recovery**

The Recovery allows to create new Recovery Plans and view a summary of the Recovery Plans created by the user. The user can select a Recovery Plan to review details of the plan, update configurations, and perform Recovery Plan verification or environment recovery. When verification or recovery operations are running, the progress of the operation can be viewed by opening the Recovery Plan details from this screen.

- **Events**

The Events screen provides you with detailed information about errors and warnings that occur during discovery, backup, recovery and verification operations.

- **Tasks**

The Tasks screen allows you to view task statuses and manage them.

3

Before You Start

This section provides an overview of some of key information that should be considered when using Disaster Recovery for Identity for Active Directory. Understanding this information is essential for effectively using the product and troubleshooting any issues that may arise.

Backup Considerations and Best Practices

In this topic:

- How many domain controllers to backup?
- Backup frequency
- Active Directory backups vs Windows System State backups
- Backup storage and encryption

How many domain controllers to backup?

This depends on the recovery strategy you choose for your environment. Refer to the Forest recovery strategies section in the Recovery Considerations and Best Practices page.

It is recommended to back up at least two domain controllers from each domain in the forest that are DNS servers and FSMO role holders.

Backup frequency

When deciding on how often to create backups, it is important to note that in case of a disaster, you will need recent and reliable backups. These backups should be created around the same time (within 24 hours) to minimize potential discrepancies after the forest recovery process. The product allows you to restore a domain in the forest to its prior state at the time of the last trusted backup. Consequently, the restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted backup.
- All updates made to existing objects since the last trusted backup.

- All changes made to either the configuration partition or the schema partition in Active Directory since the last trusted backup (such as schema changes).

Quest recommends daily backups for each domain controller you want to be able to restore.

Active Directory backups vs Windows System State backups

The Active Directory and Windows System State backups are very similar. The key components that the product backs up as part of the Active Directory system state are the Registry, the NTDS.dit file, and SYSVOL.

What differences do they have?

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

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

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

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

Backup storage and encryption

Disaster Recovery for Identity for Active Directory encrypts backups with a password for added security. The passwords used for accessing backups are encrypted using organization specific keys stored in Microsoft Azure Key Vault and are protected using AES-256 algorithm. These passwords are unique, randomly generated and are each 16-characters long. The encrypted passwords are then stored as part of the backup metadata in the Azure SQL database. For details about encryption within Azure Key Vault, see the Privacy and Protection of Customer Data section in the *Quest On Demand Global Settings Security Guide*.

At rest, on-premises domain controller backups are stored in Azure Blob Storage and encrypted using AES-256 with the encryption key protected using PBKDF2 and SHA-2.

Recovery Considerations and Best Practices

In this topic:

- Recovery strategies overview
- Forest recovery strategies
- Recovery methods in Disaster Recovery for Identity for Active Directory

- About Domain Controller Agents and Hybrid Agents
- Server Access Credentials
- Handling DNS servers during recovery
- DNS configurations

Recovery strategies overview

Before you choose one of the recovery strategies described in this section, it is strongly recommended that you read Microsoft's Active Directory Forest Recovery Guide. When choosing a recovery strategy, note that every recovery is unique, and the strategy might need adjustments to suit your needs.

It is highly recommended to periodically test your chosen strategy to ensure that you are familiar with the process, and that the strategy can be run during a disaster. It is essential to have Recovery Plans created in Disaster Recovery for Identity for Active Directory before a disaster occurs. Refer to Creating and Editing a Recovery Plan for more details.

The product allows you to restore a domain in the forest to its prior state at the time of the last trusted backup. Consequently, the restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted backup.
- All updates made to existing objects since the last trusted backup.
- All changes made to either the configuration partition or the schema partition in Active Directory since the last trusted backup (such as schema changes).

Additionally, any software applications that were running on the domain controllers will need to be reinstalled on the domain controllers after recovery.

Forest recovery overview

At a high level, the forest recovery process using Disaster Recovery for Identity for Active Directory involves the following steps:

1. Restore domain controllers within each domain from backups using the Restore to Clean OS recovery method, utilizing the most reliable backups.

> **NOTE:** The greater the number of domain controllers restored from backups, the more rapid the recovery process will be. See Forest recovery strategies below on details how many domain controllers to restore.

2. Install Active Directory on the domain controllers that were not restored.

> **NOTE:** During Technical Preview, this will need to be completed manually. Click here for more information. After Technical Preview, the product will be able to install Active Directory to domain controllers automatically.

3. Wait for the domain controllers with reinstalled Active Directory to replicate Active Directory data from domain controllers restored from reliable backups.

Forest recovery strategies

Recovery strategy 1: Restore all critical domain controllers from backups

This strategy is recommended by Quest.

Advantages

- Rapid recovery of the most critical infrastructure allowing to get to business as usual faster.
- Enhanced stability of the recovery process compared to restoring only one domain controller per domain. The use of multiple backups ensures that the entire forest can be recovered, even if the restoration of some domain controllers is unsuccessful.
- The more domain controllers restored from backup, the closer recovered forest resembles its pre-failure state.

Limitations

- The risk of reintroducing corrupted or unwanted data due to the use of multiple backups, there is no guarantee that corrupted or unwanted data from the backups will not be introduced into the recovered forest.

Recovery strategy 2: Restore one domain controller per domain from backups

Advantages

- Recommended by Microsoft - this recovery approach is aligned with Microsoft's best practices as outlined in the Planning for Active Directory Forest Recovery Guide.
- The limited number of backups allows for thorough inspection to ensure they are free of corruption or unwanted data.

Limitations

- Successful recovery of an entire domain relies on the successful restoration of a single domain controller. Active Directory can only be reinstalled on other domain controllers within the domain after the initial domain controller is successfully restored from backup.
- The full forest recovery process may be time-consuming.
- The original forest infrastructure is not preserved - as Active Directory is reinstalled on most domain controllers within the forest, the recovered forest will not be an exact replica of its pre-failure state.

Recovery strategy 3: Restore at least 2 domain controllers per domain from backups

Advantages

- Enhanced stability of the recovery process compared to restoring only one domain controller per domain. The use of multiple backups ensures that the entire forest can be recovered, even if the restoration of some domain controllers is unsuccessful.

Limitations

- The forest recovery process may be time-consuming.
- The original forest infrastructure is not preserved - as Active Directory is reinstalled on most domain controllers within the forest, the recovered forest will not be an exact replica of its pre-failure state.

Recovery methods in Disaster Recovery for Identity for Active Directory

The following recovery methods are available to perform recovery of the forest or specific domains in Disaster Recovery for Identity for Active Directory. Depending on your recovery strategy, a different combination of recovery methods may be needed to perform recovery.

Restore to Clean OS

The Restore to Clean OS method enables the restoration of the entire forest or specific domains onto freshly installed Windows machines. Domain controllers residing on virtual machines within Microsoft Azure or Amazon Web Services (AWS) can also be restored using the Restore to Clean OS method.

> **NOTE:** The initial step in the Restore to Clean OS recovery method involves promoting the selected Windows server to a domain controller. This operation is compatible with Windows Server 2016 or later machines utilizing File Replication Service (FRS) replication. Consequently, Restore to Clean OS is exclusively supported for Windows Server 2016 or later with DFS Replication.

The initial stage of the Restore to Clean OS recovery method involves installing the DNS server role on a domain controller. Therefore, it is recommended to use a backup created on an Active Directory-integrated DNS server for the Clean OS recovery process. While backups from non-Active Directory-integrated DNS servers can be used, the Automatic DNS Selection option should **not** be enabled for any domain controller for that domain. If your domain has Active Directory-integrated DNS servers restored from backup, you need to specify the DNS settings manually.

Following recovery, the domain controller restored using the Restore to Clean OS method synchronizes DNS partitions and continues to function as a DNS server.

If your domain utilizes external DNS, you must manually configure DNS settings for each domain controller within the domain. After recovery, the domain controller restored using the Restore to Clean OS recovery method will operate as a non-functional DNS server, allowing subsequent uninstallation.

If you are testing Forest Recovery in a lab environment and your production forest uses an external (non-AD integrated) DNS server:

1. To prepare the lab environment, you can install a new DNS server.
2. Create empty DNS zones on this server, mirroring your production DNS configuration.
3. Ensure that the Start of Authority (SOA) and Name Server (NS) records within each empty zone reference the FQDN DNS name of this server.
4. Ensure that the SOA and NS records within each empty zone reference the FQDN DNS name of this server.
5. Enable non-secure DNS dynamic updates.

For more on DNS settings, it is highly recommended that you visit the DNS configurations and the Handling DNS servers during recovery sections.

Recovery steps

1. Prepare a target machine using existing hardware or a virtual machine

A blank host should comply with the following requirements:

- The operating system version of the target machine must match the version of the failed domain controller.
- The target machine must have sufficient free disk space to accommodate Active Directory and SYSVOL data.
- The account specified to access the target machine must possess local Administrator privileges on that machine.

As previously mentioned, it is crucial that the Windows operating system version matches the deployed version. The Verify operation will issue a warning if a mismatch is detected between the target and backup Windows versions. The specific versions will be reported in the status information. If the Major and Minor versions do not match, indicating that at least one of the operating system versions is prior to 2016, an error message will be displayed.

2. Create Recovery Plan with Restore to Clean OS method

Create a Recovery Plan and use Restore to Clean OS method. Specify the IP of the prepared Target machine in the Domain Controller Configuration.

Install Active Directory

The Install Active Directory recovery method is used to install Active Directory on a clean machine. For Windows Server® 2012-based domain controllers, this option uses the Windows PowerShell® cmdlets InstallADDSDomainController.

The target server should be compliant with the following requirements:

- Operating system version should be equal to the original DC operating system.
- Operating system should follow organization security best practices (e.g. have latest updates,security software) since this operating system will be used to run the Active Directory Domain services after the restore.
- The physical disks should have enough free space to host the Active Directory® data after recovery.

Do Not Recover

The Do Not Recover method isolates the domain controller from other domain controllers and completely removes it from the domain; no actions are performed on the domain controller itself. This option should be used if the domain controller is inaccessible or you do not want to recover the domain controller due to any failures. Disaster Recovery for Identity for Active Directory removes all metadata of domain controllers that are set to Do Not Recover.

About Hybrid Agents and Domain Controller Agents

It is important to understand the distinction between Hybrid Agents and Domain Controller Agents:

Hybrid Agents

A Hybrid Agent is used to facilitate communication between On Demand and your on-premises environment. A Hybrid Agent must be manually installed on-premises. Refer to the *Creating and Installing a Hybrid Agent* section for more.

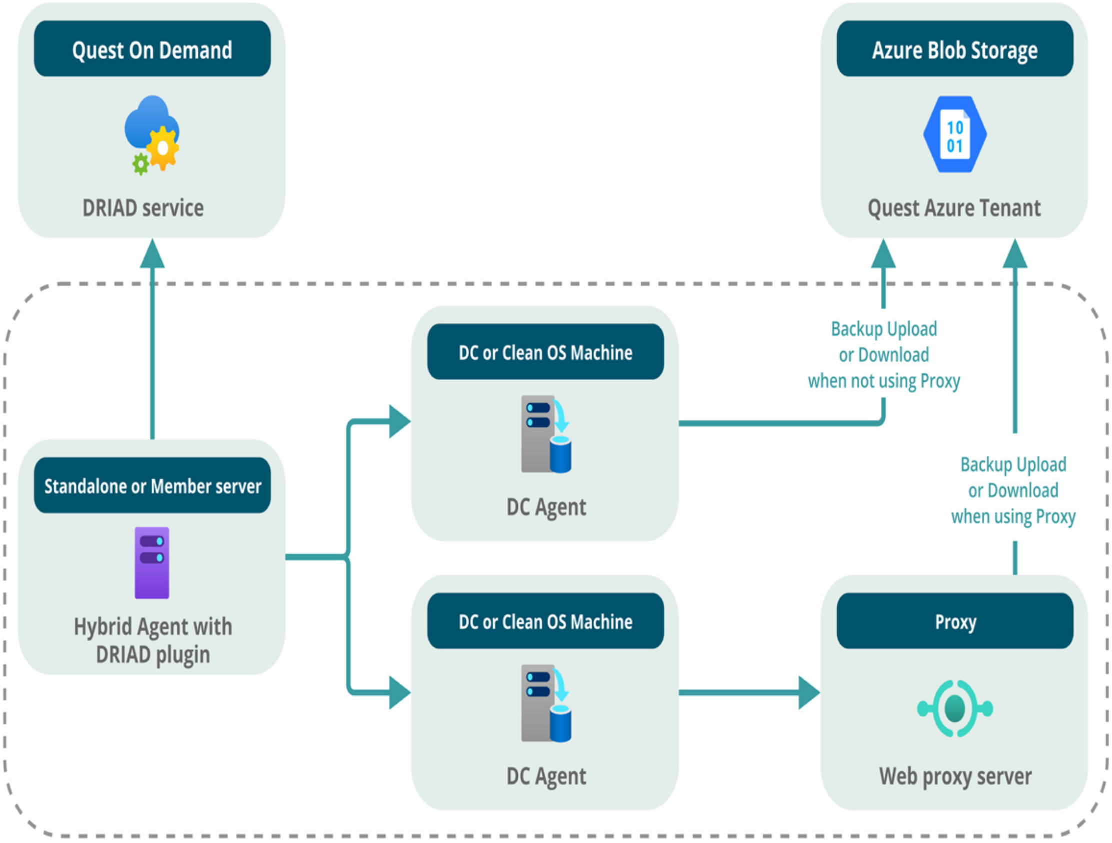
Ensure that the Hybrid Agent has a stable internet connection during the recovery operation and uses a DNS server that is not affected by the forest failure.

Where should the Hybrid Agent be installed?

The Hybrid Agent can be installed on a standalone or domain-joined server (although the use of a standalone server is highly recommended). It is important to ensure the Hybrid Agent is able to access Disaster Recovery for Identity for Active Directory even in the case of a disaster. For example, if the Hybrid Agent uses a domain controller as a DNS server and the domain controller goes down, this will prevent the Hybrid Agent from accessing the product and no backup or recovery will be possible. Therefore, it is important to ensure that an alternate DNS is specified and adjusted after the recovery to be able to continue using the product to perform backups in the restored environment.

Domain Controller Agents

A Domain Controller Agent is used to perform actions such as backup or restore against a single domain controller within your forest. A DC Agent should be installed on each domain controller you wish to perform certain operations like a restore from a backup during a recovery.


Quest On Demand
DRIAD service
Azure Blob Storage
Quest Azure Tenant
Backup Upload or Download when not using Proxy
Backup Upload or Download when using Proxy
DC or Clean OS Machine
DC Agent
Standalone or Member server
Hybrid Agent with DRIAD plugin
DC or Clean OS Machine
DC Agent
Proxy
Web proxy server

Permissions required for the Hybrid Agent and Domain Controller Agent can be found in the Required permissions section.

Server Access Credentials

The following are definitions for each credential when configuring domains or domain controllers:

Domain User

This account must be a domain administrator in the domain that is being restored. After the domain is restored, the password for this account is reset to the specified value, regardless of the value restored from the backup. Supported format is domain/username or username. If only the username is specified, then the local domain name is automatically added.

Local User

Specifies the account that will be used to access the target computer to install the agent before the target computer is promoted to a domain controller. This account must be a local administrator on the target computer. Supported format is machine/username or username. If only the username is specified, then the target machine name is automatically added.

DSRM Administrator

Specifies the account used to access the domain controller in Directory Services Restore Mode (DSRM) or the DSRM account used to promote the target computer to a domain controller in the Restore to Clean OS recovery method. After the forest is restored, the password for the DSRM Administrator account is reset to the specified value, regardless of the value restored from the backup.

Handling DNS servers during recovery

Active Directory is closely integrated with the DNS service. Each domain controller registers and maintains multiple Resource Records (RRs) within the DNS service. Different types of domain controllers register distinct sets of RRs. Disaster Recovery for Identity for Active Directory adjusts these records during the forest recovery process.

When configuring a Recovery Plan, consider the DNS infrastructure. For Active Directory-integrated DNS, ensure at least one DNS server per zone is restored from backup. Ideally, restore as many DNS servers as possible. Carefully consider the 'Use preferred DNS server(s)' option for each domain controller in the Recovery Plan, aligning with your DNS recovery strategy. The DNS client configuration of restored domain controllers will influence the DNS infrastructure detection during recovery. The solution will determine whether Active Directory-integrated DNS or external DNS is used, and identify the relevant DNS servers.

For Active Directory-integrated DNS scenarios with configured delegation and forwarding settings between parent and child domains, the Disaster Recovery for Identity for Active Directory ensures the restoration of DNS zone information, delegation and forwarding settings, Forest and Domain DNS zone replication settings, and, if applicable, Conditional Forwarders during the recovery process.

- If an external DNS is used, any inter-domain DNS relations are out of the Recovery Plan scope and are not affected by the recovery process.
- For DNS servers that have not been restored, its Resource Records associated with the DNS server are removed. This is performed during the *Configure DNS server* operation.
- If the Recovery Plan excludes certain domain controllers from the restoration process with the Do Not Recover method, their corresponding Resource Records are removed from DNS. This occurs during the *Clean up DNS records of removed domain controllers* operation. However, if excluded domain controllers remain operational and the DNS server allows non-secure dynamic updates, these domain controllers may still register their SRV records.

DNS configurations

When creating a Recovery Plan, you should specify a method for selecting a preferred DNS server for each domain controller in your Recovery Plan.

When creating or editing a Recovery Plan, you can choose one of the following DNS server selection methods:

- Select DNS server automatically - retrieves a list of all DNS servers that are in use in the forest and automatically assigns a DNS server that is operating correctly from the list to the current domain controller. This is selected by default.
- Use preferred DNS server(s) - input preferred DNS server(s), individually separated by a semicolon (;).

When you opt to automatically select a DNS server, Disaster Recovery for Identity for Active Directory retrieves a list of DNS servers utilized by domain controllers. Alternatively, use the *Preferred DNS servers* option and use external DNS servers that support dynamic updates and have DNS zones configured for each domain within the forest you intend to recover. For more on using DNS configurations with the Restore to Clean OS method, go to the Restore to Clean OS section in *Recovery methods in Disaster Recovery for Identity for Active Directory*.

The *Select DNS server automatically* option is recommended in the following cases:

- Your DNS is not Active Directory-integrated.
- Your DNS is Active Directory-integrated and you restore from backups the DNS servers (domain controllers) that act as the primary source for each DNS zone.

For non-Active Directory-integrated DNS (external DNS), the list of automatic DNS servers is prioritized. First, the IP addresses configured in the DNS client settings of the current domain controller are considered. Next, the preferred DNS addresses of other domain controllers within the same domain and their DNS client settings are included. This pattern continues for domain controllers in the parent domain hierarchy, sibling domains, and finally, direct child domains. During recovery, Disaster Recovery for Identity for Active Directory selects a functional DNS server from this prioritized list and assigns it to the domain controller.

For Active Directory-integrated DNS, the solution prioritizes DNS servers within the same domain. DNS servers are ordered based on the domain hierarchy, starting from the current domain and progressing up to the root. The primary DNS server is selected considering client settings and usage frequency within the DNS zone backup. The preferred DNS server's IP address from client settings is assigned to all restored domain controllers as the preferred address for the DNS zone they host. For alternate DNS servers, a list of other DNS servers hosting the DNS zone is obtained.

For forest-wide replicated DNS zones, the preferred DNS server is selected from the root domain. The DNS server designated as the primary for the root domain will also serve as the primary DNS server for any forest-wide replicated DNS zone.

If a domain controller is a DNS server itself, then a loopback address is included in the DNS server list (see the note below). By default, the number of DNS servers that can be selected automatically is limited to 3.

> **NOTE:** It is not recommended to uninstall or reinstall Active Directory on DNS servers that serve as the primary source for an Active Directory-integrated DNS zone. Additionally, removing such DNS servers from Active Directory during recovery is not recommended.

When you manually specify a DNS server or a list of DNS servers, Disaster Recovery for Identity for Active Directory initially attempts to assign the specified DNS server(s) to the domain controller. If the specified DNS server(s) are inaccessible or malfunctioning, the product automatically selects the DNS servers (primary and alternate) that were previously configured on the domain controller. Should this fail, the solution selects DNS servers from a list of all active DNS servers within the forest.

How does Disaster Recovery for Identity for Active Directory determine that the DNS server is available for use?

Disaster Recovery for Identity for Active Directory configures a DNS server on all network adapters of the domain controller and verifies its ability to register DC Locator resource records and A-type (host) records. If successful, this DNS server is designated as the preferred DNS server on all network adapters.

> **NOTE:** According to Microsoft's recommendations, DNS servers should include their own IP addresses in their DNS server lists. The loopback address (127.0.0.1) is best suited for secondary or tertiary DNS server roles on a domain controller. If the loopback address is specified in the incorrect order, the sequence will be automatically adjusted during DNS server configuration on the domain controller.

If you want to use the 'Use preferred DNS server(s)' method, ensure that you have at least one properly configured DNS server ready to work with the domain controllers being recovered. These DNS servers must support dynamic updates and have DNS zones configured for each domain within the forest you intend to recover. Assign one of these DNS servers to each domain controller in your Recovery Plan.

Security

In this topic:

- Required permissions
- Endpoint requirements
- Windows Firewall

Required permissions

This section describes specific permission requirements needed for agents and credentials in Disaster Recovery for Identity for Active Directory. For permissions needed to operate the product, go to the Roles and Permissions in On Demand page.

Method	Service	Permissions
Restore to Clean OS	Hybrid Agent	A service account used to run the Hybrid Agent service must be a local administrator account on the computer where the Hybrid Agent is installed. The domain FQDN\username should at least have forest-wide read permissions.
	Domain Controller Agent	A service account used to run the Domain Controller Agent is always a Local System account. An account used to install the Domain Controller Agent remotely a member of the Local Administrators group.
	Domain User	When configuring a domain or domain controller, this account must be a domain administrator in the domain that is being restored.
	Local User	When configuring a domain or domain controller, this account must be a local administrator on the target computer.

Endpoint requirements

Hybrid Agent requirements

TCP Port	Direction	Endpoints	Description
389	Outbound	Domain Controllers	LDAP port to domain controllers to discover environment.
445	Outbound	Domain Controllers	SMB port to domain controllers to install Domain Controller Agents.
443	Outbound	**EU** odjrs-euprod-eu-iothub.azure-devices.net https://odjrseuprodeugrssto.blob.core.windows.net https://odjrseuprodeusto.blob.core.windows.net **UK** odjrs-ukprod-uk-iothub.azure-devices.net https://odjrsukprodukgrssto.blob.core.windows.net https://odjrsukproduksto.blob.core.windows.net **US**	Agent connection to Disaster Recovery for Identity for Active Directory backend services (see On Demand Global Settings User Guide for more)

TCP Port	Direction	Endpoints	Description
		odjrs-usprod-us-iothub.azure-devices.net https://odjrsusprodusgrssto.blob.core.windows.net https://odjrsusprodussto.blob.core.windows.net	
80	Outbound	**EU** odjrseuprodeuiotinst--odjrseuprodeuiotacct.b.nlu.dl.adu.microsoft.com **UK** odjrsukprodukiotinst--odjrsukprodukiotacct.b.nlu.dl.adu.microsoft.com **US** odjrsusprodusiotinst--odjrsusprodusiotacct.b.nlu.dl.adu.microsoft.com	Agent connection to Disaster Recovery for Identity for Active Directory backend services (see On Demand Global Settings User Guide for more)

Domain Controller Agent requirements

TCP Port	Direction	Endpoints	Description
445	Inbound		SMB port to allow automatic agent installation.
135	Inbound		RPC Endpoint Mapper port used by the RPC runtime.
49152-65535	Inbound		RPC dynamic port range to accept RPC connection from Hybrid Agent.
443 or proxy server port	Outbound	**EU** https://odradprodeusa.blob.core.windows.net **UK** https://odradproduksa.blob.core.windows.net **US** https://odradprodussa.blob.core.windows.net	Download and upload backups from Azure Blob Storage accounts.

Windows Firewall

A firewall in your environment may block network traffic on ports used by Disaster Recovery for Identity for Active Directory, potentially hindering backup and restore operations. Before using the product, ensure your firewall does not restrict traffic on the necessary ports.

You can configure built-in Windows Firewall on domain controllers to be backed up either automatically or manually. For firewall rules for the Hybrid Agent, see the On-premises agent requirements section in the *On Demand Global Settings User Guide*.

Automatic

This is enabled by default and will not configure any outbound firewall rules. Depending on your environment, you may need to configure outbound rules manually (allow outbound 443 or proxy port).

Manual

This is used if the automatic method fails for any reason, or if the automatic method has been disabled. Depending on your environment, you may also need to configure outbound rules manually (allow outbound 443 or proxy port).

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

Rule 1

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

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

Rule 2

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

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

Rule 3

Rule Type: Custom

Program Path: C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRestoreService64.exe

Service settings: Apply to all programs and services

Protocol: TCP

Local ports: RPC dynamic port range

Remote ports: Any

Local IP addresses: Any

Remote IP addresses: Any

Action: Allow the connection

Rule profile: Domain, Private, and Public

Allowed users: Any

Allowed computers: Any

PowerShell for the Rule 3 mn nmsettings: *New-NetFirewallRule -DisplayName "Rule 7" -Group DRIAD -Enabled True Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRestoreService64.exe"*

Sign up for Quest On Demand

To access Disaster Recovery for Identity for Active Directory, you need to sign up for the Quest On Demand service and create an organization. For that, go to Quest On Demand and use one of the following options:

- Sign up using the existing Quest account.
- Create a new Quest account and sign up for Quest On Demand.
- Join an existing On Demand organization.

For details, see Signing up for Quest On Demand in the *On Demand Global Settings User Guide*.

5

Configuring Disaster Recovery for Identity for Active Directory

Organizations and Regions

When you sign up for the On Demand service for the first time, you create an organization and you are granted the On Demand Administrator role. You can add additional organizations and administrators.

When selecting a region for an organization, this indicates where all Disaster Recovery for Identity for Active Directory services are running as well as the region for backup storage.

For more information about managing your organization see Managing organizations and regions in the *On Demand Global Settings User Guide*.

Access Control

Quest On Demand uses the Role-based Access Control (RBAC) security policy that restricts information system access to authorized users. Your Quest On Demand organization comes configured with a number of default roles which cannot be changed, but subscribers can create custom roles with the permissions to perform needed operations on the assets of the organization.

If you are the On Demand administrator or the owner of the subscription, you can add users to an existing organization and assign the required roles. If you are not the subscription owner or administrator, contact your On Demand administrator for access.

For more information on assigning roles, see Adding users to an organization in the *On Demand Global Settings User Guide*.

Roles and Permissions in On Demand

This section lists the minimum user account permissions required to perform specific Disaster Recovery for Identity for Active Directory tasks. Listed below are the role definitions and their associated permissions for Disaster Recovery for Identity for Active Directory. For more on roles in On Demand, go to Access Control: Roles section in the *On Demand Global Settings User Guide*.

Role definitions and permissions for Disaster Recovery for Identity for Active Directory

- **Recovery for AD Viewer:** The Recovery for AD Viewer role allows read only access to all areas of Recovery for Active Directory.
    - Can View All
- **Recovery for AD Backup Operator:** The Recovery for AD Backup Operator role allows to set up and manage backups and backup-related operations.
    - Can View All
    - Can Manage Backups
- **Recovery for AD Restore Operator:** The Recovery for AD Restore Operator role allows to manage all backup and recovery operations.
    - Can View All
    - Can Manage Backups
    - Can Manage and Verify Recovery Plans
    - Can Run Recovery
- **Recovery for AD Administrator:** The Recovery for AD Administrator role allows full access to Recovery for Active Directory.
    - Can View All
    - Can Manage Backups
    - Can Manage and Verify Recovery Plans
    - Can Run Recovery
    - Can Run Forest Topology Discovery
    - Can Manage Domain Controller Agents
    - Can Manage Environments
    - Can Configure Agents
    - Can Export Data: Recovery
    - Can Read Access Control Roles
    - Can Read Activity Trail: Recovery

- **Recovery Administrator:** The Recovery Administrator role allows full access to both Recovery for Active Directory and Recovery for Entra ID.
    - Can View All
    - Can Manage Backups
    - Can Manage and Verify Recovery Plans
    - Can Run Recovery
    - Can Run Forest Topology Discovery
    - Can Manage Domain Controller Agents
    - Can Manage Environments
    - Can Configure Agents
    - Can Export Data: Recovery
    - Can Read Access Control Roles
    - Can Read Activity Trail: Recovery

Permission definitions

The following table describes each permission used in Disaster Recovery for Identity for Active Directory.

Permission	Description
Recovery for AD: Can View All	View all areas of Disaster Recovery for Identity for Active Directory.
Recovery for AD: Can Manage Backups	Manage Backup Plans and backups, including starting, pausing and canceling backup tasks.
Recovery for AD: Can Manage and Verify Recovery Plans	Run and manage Recovery Plans and recovery, including starting, pausing and canceling recovery and verification tasks.
Recovery for AD: Can Run Recovery	Ability to start, pause and cancel recovery tasks.
Recovery for AD: Can Run Forest Topology Discovery	Ability to run, pause and cancel topology discovery.
Recovery for AD: Can Manage Domain Controller Agents	Ability to download, install and upgrade Domain Controller (DC) agents, as well as starting, pausing and canceling agent tasks.
Recovery for AD: Can Manage Environments	Ability to add a new or modify an existing environment.

Working with Disaster Recovery for Identity for Active Directory

This section provides step-by-step instructions for how to start using Disaster Recovery for Identity for Active Directory.

1. Go to Quest On Demand and sign up for Quest On Demand. For more details, refer to Sign up for Quest On Demand.
2. To launch Disaster Recovery for Identity for Active Directory, click **Recover** on the left pane, then click **Active Directory**. The **Environments** screen opens.

Below is a general overview of the steps required to successfully utilize Disaster Recovery for Identity for Active Directory:

1. Deploy Hybrid Agents on the standalone or domain-joined server connected to the forest you wish to backup and restore.
2. Add the Active Directory forest into Disaster Recovery for Identity for Active Directory by creating an environment and selecting the Hybrid Agent.
3. Discover Forest Topology and install Domain Controller Agents on the domain controllers you wish to backup.
4. Create Backup Plans and schedule regular backups of the domain controllers.
5. Create a Recovery Plan that will be used in case of disaster.
6. Verify the Recovery Plan on regular basis to find any potential issues with the plan.

7

Environments

Upon the creation of your environment, information about your Active Directory environments can be found on the Environments screen. Each tile on the Environments screen displays the following information:

- **Status**

The Status section displays information on the status of a current or latest discovery, backup, verification and recovery of the environment. For more information on the individual statuses, go to the Recovery Plan Cards page.

- **Forest Summary**

The Forest Summary section shows the number of domains and domain controllers (DCs) in the environment. Click **View Topology** to see more details.

- **Hybrid Agent**

The Hybrid Agent section presents the FQDN of the Hybrid Agent, as well as if the Hybrid Agent is both connected and online. For more on Hybrid Agents, including how to add a Hybrid Agent, refer to the Managing your Microsoft Entra tenants and on-premises domains section in the *On Demand Global Settings User Guide*. You can configure the agent by selecting **Manage Agent**.

- **DC Agents**

The DC Agents section presents if the Domain Controller Agent(s) associated with the environment is online. You can download the agent package by clicking **Download Agent**. For more on Domain Controller Agents, either click About Agents or go to the About Domain Controller Agents and Hybrid Agents section in the *Before You Start* page.

On the Environments screen, you can perform the following actions:

- Add Environment - create an environment for the tenant. For more information, click go to the Creating and Configuring an Environment section.
- About Agents - this will show more information on Hybrid Agents and Domain Controller Agents. Click **Hybrid Agents** to manage your Hybrid Agent.

On each environment card, you can perform the following actions:

- Edit - edit the environment to change its environment name, associated Hybrid Agent, credentials used to perform topology discovery and agent proxy settings.
- Remove - remove the environment from Disaster Recovery for Identity for Active Directory.

Creating and Configuring an Environment

To use Disaster Recovery for Identity for Active Directory, you will need to add an environment, which will include your Active Directory forest.

An environment needs to be created in Disaster Recovery for Identity for Active Directory for every Active Directory forest you plan to be able to backup and restore. Environments are isolated from each other; each environment will have its own topology, agent management, Backup Plans, and Recovery Plans. If you have multiple production forests you want to backup and recover, each of them need to be added individually into the product.

Each environment also needs to have its own Hybrid Agent to facilitate communication between the product and on-premises Domain Controller Agents. It is highly recommended to regularly perform test recoveries in your test environment using the product to ensure it will work for you as expected in a production environment in case of a disaster. To perform recovery in your test environment, backups from the test environment need to be performed (you cannot use production backups in your test environment).

In this section:

- Creating and Installing a Hybrid Agent
- Creating a Disaster Recovery for Identity for Active Directory Environment

Creating and Installing a Hybrid Agent

Before you create an environment in Disaster Recovery for Identity for Active Directory, a Hybrid Agent will need to be installed on-premises. A Hybrid Agent is used to securely communicate with any installed on-premises Domain Controller (DC) agents. To facilitate communication with your environment, a Hybrid Agent must be manually installed on-premises. To do this:

1. Log in to On Demand using the credentials you used to sign up for On Demand.
2. In the navigation panel on the left, click **Tenants**.
3. Click **Hybrid Agents**.
4. Click **Add agent**.

When you click Add Agent, the How to Add an Agent screen is displayed. You must create a passphrase that will be used when you install the agent.

5. To create a passphrase, use one of the following options:
   - Click **Generate New** to get a new passphrase.
   - Enter a passphrase manually. The passphrase can be from 4 to 100 words (32 to 1024 characters long).
   - Edit a displayed passphrase to make it more complex (such as adding numbers or characters).
   - Enter a passphrase word count (from 4 to 100 words) and click **Generate New** to get a passphrase of the specified word count. **NOTE:** The passphrase must be from 32 to 1024 characters long.
6. When you decide to use the displayed passphrase, click **Copy and Continue**.
7. Once the installation package is ready, click **Download**. The agent package with a unique key is downloaded to your computer.
8. Copy the agent package to the server and double-click the AgentSetup.exe file. Go to the Adding an on-premises agent section in the *On Demand Global Settings User Guide* for more information.

> **NOTE:** The maximum number of Hybrid Agents is limited to 10 per On Demand organization. If you need a higher number of Hybrid Agents, contact Quest Support.

8. Install the agent by following the prompts in the command line. The copied passphrase will need to be provided.

> **NOTE:** The Recovery for Active Directory action is added automatically once the Hybrid Agent is selected for the Disaster Recovery for Identity for Active Directory environment. The action remains on the Hybrid Agent even if the Disaster Recovery for Identity for Active Directory environment have been deleted or has stopped using the Hybrid Agent.

For more on Hybrid Agent installation, refer to the Managing your Microsoft Entra tenants and on-premises domains section in the *On Demand Global Settings User Guide*.

Creating a Disaster Recovery for Identity for Active Directory Environment

You can then create an environment within Disaster Recovery for Identity for Active Directory. To do this:

1. On the Disaster Recovery for Identity for Active Directory **Environments** screen, click **Add Environment**.
2. Enter the environment name. This is a unique name to identify the environment.
3. Select the Hybrid Agent you created from the drop down menu.

> **NOTES:**
>
> - Agents that have already been assigned to other environments will not be populated in this drop down menu.
> - Only a single Hybrid Agent per environment is currently supported.

4. Enter the Active Directory domain username and password which will be used to discover Active Directory domains and domain controllers.

> **NOTES:**
>
> - The entered domain\username should at least have forest-wide read permissions.
> - When using a standalone agent, provide the domain FQDN\username.

5. Specify proxy configuration used by all Domain Controller Agents within the environment to upload and download the backups. You can use one of the following options:
    a. Use system proxy configuration. This is selected by default and will use proxy settings configured on the machine to get Internet access.
    b. Use a manually configured proxy. Specify the server address and port in the relevant boxes.
6. Click **Save**. Once a new environment is created, open the Topology screen to run a discovery of your Active Directory forest.

8

Topology

The Topology screen is where you can view a summary of your Active Directory forest.

Under the Forest Summary, you'll find the number of domains and domain controllers. It also displays the status and elapsed time of the latest run discovery.

On the Topology screen list, you can view:

- Domain Controller - the FQDN of the domain controller within the Active Directory forest.
- Domain - the FQDN of the domain within the Active Directory forest.
- Site - the name of the site in which the domain controller is located.
- DC Agent Status - the status of the Domain Controller Agent. The current Domain Controller Agent version and the available Domain Controller Agent version (if applicable) can be seen by hovering over each agent status. The agent statuses are:
    - Online - the Domain Controller Agent is online and the latest version is installed.
    - Outdated - the Domain Controller Agent is online and an older supported version is installed. Backup and recovery tasks will run, but an agent update to the latest version is strongly recommended.
    - Not Supported - the Domain Controller Agent is installed and online but the version is not supported and requires an update. Backup, verification and recovery operations cannot be performed.
    - Offline - the Domain Controller Agent is offline. The agent cannot be reached or is not installed.
    - Installing - the Domain Controller Agent is being installed.
    - Refreshing - the status of the Domain Controller Agent is being updated.
    - Unknown - the status of the Domain Controller Agent has not been checked yet. Click the **Refresh Agent Status** button to view the latest Domain Controller Agent status.

On the Topology screen, you can take the following actions:

- Run Discovery - run a discovery for domains and domain controllers for the linked Active Directory forest.
- Refresh Agent Status - refresh the Domain Controller Agent status.

NOTES:

- You can select a single or multiple domain controllers to refresh their status only.
- The agent status is automatically refreshed each time a backup is performed.

- Install Agent - deploy or upgrade a Domain Controller Agent on one or multiple domain controllers. See Installing a Domain Controller Agent for more.
- Download Agent - download the Domain Controller Agent package. For more on Domain Controller Agents, either click About Agents or go to the About Domain Controller Agents and Hybrid Agents section in the *Before You Start* page.
- Create Backup Plan - create a Backup Plan for the selected domain controllers on the Topology screen. For more on this, go to Backup Plans and Backups.

Topology Discovery

Upon the creation of your environment, click **Run Discovery** to run a discovery for domains and domain controllers for the selected environment. To run a discovery, the user will need the *Recovery for AD: Can Run Forest Topology* permission. Go to the Roles and Permissions in On Demand page for more information. The status of the last run discovery is displayed at the top of the page. You can also view the list of domains and domain controllers associated with the environment, and can change the environment by using the drop down menu, and selecting the desired environment.

NOTE: Topology will need to be manually re-discovered when a domain controller or domain configuration is changed on-premises.

CAUTION: Recovery Plans should be pre-created based on the latest topology to ensure full preparedness in case of a disaster.

Installing a Domain Controller Agent

You can deploy a Domain Controller (DC) Agent on one or more domain controllers within the environment from the Disaster Recovery for Identity for Active Directory console. For more information on Domain Controller Agents, go to the About Domain Controller Agents and Hybrid Agents section in the *Before You Start* page.

To do this:

1. On the Topology screen, select one or more domain controllers, and click **Install Agent**.
2. Specify the credentials to install the Domain Controller Agent. You can use the credentials saved for the environment to install the DC Agents. These credentials must have Domain Administrator permissions to install the agent on the domain controller. This is enabled by default. For more on permissions, go to the Required permissions section in the *Before You Start* page. If you wish to use this option, click **Install Agent**. The Install Agent task will run and the Agent Status will change to *Installing*.
3. If you wish to use different credentials to install the Domain Controller Agent, deselect the **Use credentials saved for the environment** checkbox, and input the required credentials. Then click **Install Agent**. The Install Agent task will run and the Agent Status will change to *Installing*.

NOTES: If the installation fails, the agent status will be set to *Offline*. Go to the Tasks screen to view the reason for failure.

Manual installation

You also have the option to install the agent manually. To do this:

1. Download the Domain Controller Agent from the Environment card you are planning to install the Domain Controller Agent on.

   > **NOTE:** Domain Controller Agent bundles are unique per On Demand for Active Directory environment.

2. Copy the package to the machine and run the RecoveryAgent64.exe to install the Domain Controller Agent.

After the Domain Controller Agent installation has successfully been completed, the domain controller will have "Quest Forest Recovery Service" installed which is running as a Local System.

Once the agents have been installed on all desired domain controllers, you can now create a Backup Plan for your environment.

9

Backup Plans and Backups

Disaster Recovery for Identity for Active Directory is designed to scale efficiently in large, multi-domain environments. This solution provides excellent performance, creates backups for multiple computers in parallel, and is easily scalable to service additional domain controllers. Administrators can logically group domain controllers based on roles, location, or other criteria for easier management by creating different Backup Plans.

This product also utilizes Domain Controller Agents to streamline backup creation and application processes. This agent-based approach enhances scalability and reduces network overhead by compressing data before transmission and performing parallel backups for multiple domain controllers.

The Backup screen is where you can create and view Backup Plans and backups from each environment.

> **NOTE:** It is highly recommended that you visit the Backup Considerations and Best Practices section in the *Before You Start* page before you begin to create Backup Plans.

In this topic:

- Backup Plans
- Backups

Backup Plans

Disaster Recovery for Identity for Active Directory enables you to create backups of Active Directory components, including the database, on domain controllers. You can back up any domain controller on your network, and the backup process can be scheduled to run regularly without disrupting normal operations.

On the Backup Plans screen, you can create and configure a Backup Plan to backup one or more domain controllers within the Active Directory forest.

In this section:

- Creating and Editing a Backup Plan

On the Backup Plans screen, you can see a list of all Backup Plans within an environment. For each Backup Plan in the list, you can view:

- Name - the unique name for each Backup Plan.
- Schedule - if a schedule for the Backup Plan has been enabled or disabled.

- Next Schedule - the date and time of the next scheduled backup of the Backup Plan (if enabled).
- Last Run - the date and time of when the backup was last run.
- Status - last status of a backup session run for a Backup Plan.

On the Backup Plans screen, you can take the following actions:

- Create - create a Backup Plan for the environment.
- Edit - revise a Backup Plan.
- Refresh - refresh the list.
- Backup Now - run a backup immediately for the selected Backup Plan.
- Remove - remove the Backup Plan.

Creating and Editing a Backup Plan

Disaster Recovery for Identity for Active Directory allows users to automate backup creation, reducing network load and saving time. Once Backup Plans are created and scheduled, Disaster Recovery for Identity for Active Directory automates the backup process, requiring no further manual intervention.

To create a Backup Plan, click **Create** and select the following options:

1. On the Create Backup Plan dialog, under Backup plan name, enter a unique name to identify the Backup Plan, or use the preset name.
2. Optionally, you can schedule to run backups at regular intervals. To do this, click the **Enable Schedule** toggle, and input the recurring days and times at either a daily, weekly or monthly schedule. The toggle is disabled by default.
   a. For daily scheduling, select **Day** from the **Every** dropdown menu. Input the time using the dropdown menus with the 12-hour format. Then click **Continue**.
   b. For weekly scheduling, select **Week** from the **Every** dropdown menu. Select one or more days of the week for scheduling from the **On Days** dropdown menu, then input the time using the dropdown menus with the 12-hour format. Then click **Continue**.
   c. For monthly scheduling, select **Month** from the **Every** dropdown menu. Select one or more days of the month for scheduling from the **On Days** dropdown menu, then input the time using the dropdown menus with the 12-hour format. Then click **Continue**.
3. Select the domain controller(s) you wish to backup.

> **NOTES:**
>
> - The Domain Controller Agent must be installed on the domain controller in order to run backups. If you wish to backup a domain controller that has an Offline or Outdated status, install or upgrade the agent on that machine before running a backup.
> - Consider recovery strategies before selecting which domain controllers to backup.

4. To run the Backup Plan immediately, click the **Run Backup Now** box.
5. Click **Save**. The Backup Plan will appear in the list. You can edit the Backup Plan by clicking on the required Backup Plan and clicking **Edit**.

You can run the Backup Plan immediately by selecting the desired Backup Plan, and click **Backup Now**.

Each Backup Plan will have one of the following statuses:

- **Completed** - all domain controllers within the Backup Plan have been successfully backed up.
- **In Progress** - the backup is currently running.
- **Failed** - one or multiple domain controllers have failed to backup. Go to the Tasks screen for more details.
- An empty status will indicate that a backup has never been run.

Backups

The Backups screen allows you to view the backups generated from your Backup Plans.

> **NOTE:** Backups are stored for 180 days. After this period, the backups are automatically deleted.

On the Backups screen, you can see a list of all Backups within an environment. For each backup in the list, you can view:

- Backup Plan Name - the plan from which the backups were created.

> **NOTE:** If the Backup Plan has been deleted, its backups will remain and you will see *Backup plan has been deleted* as the Backup Plan name.

- Domain - the domain from which the backup was created.
- Domain Controller - the domain controller from which the backup was created.
- Created Time - the time and date from when the backup was created.
- Schedule Type - if the Backup Plan was either:
    a. ran via clicking Backup Now on the Backup Plans list (Manual).
    b. ran via a configured schedule (Scheduled).
- Size - the size of the backup.

On the Backups screen, you can take the following actions:

- Refresh - refresh the list of backups.

Once backups have been created, you can then create a Recovery Plan for your environment.

10

Recovery

The Recovery screen allows the user to create, manage and run a Recovery Plan for the restore of an Active Directory forest on-premises, including all domains and domain controllers. Disaster Recovery for Identity for Active Directory provides centralized remote management for domain controller recovery within your Active Directory forest. This product also allows you to centrally restore multiple domain controllers within a forest simultaneously, streamlining the recovery process and saving time compared to manual restoration of individual domain controllers. It is recommended to create and verify Recovery Plans prior to a disaster to ensure it is configured correctly. You can create multiple Recovery Plans to support multiple configurations. Consider reviewing the Recovery strategies overview section on the *Before You Start* page.

In this topic:

- Creating and Editing a Recovery Plan
- Recovery Plan Details
- Editing Domain Configurations
- Editing Domain Controller Configurations
- Verifying a Recovery Plan
- Recovering an Environment with a Recovery Plan
- Domain Controller Operations
- Recovery Plan Cards

A Recovery Plan allows you to manage the process for recovering either the entire Active Directory forest or specific domains. Each Recovery Plan includes a list of domain controllers to be restored, along with their associated configurations. By creating and reviewing the plan, you can gain a comprehensive understanding of the recovery configurations for each domain controller, enabling you to fine-tune the process as needed.

Disaster Recovery for Identity for Active Directory allows you to restore a domain in the forest to its state at the time of the last trusted backup. Consequently, the restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted backup.
- All updates made to existing objects since the last trusted backup.

- All changes made to either the configuration partition or the schema partition in Active Directory (such as schema changes).
- Additionally, any software applications that were running on the domain controllers will need to be reinstalled on the domain controllers after recovery.

> **NOTE:** It is highly recommended you make sure that the dangerous or unwanted data is not replicated to other domains in the forest.

Creating and Editing a Recovery Plan

To create a Recovery Plan:

1. From the Recovery screen, click **Add Recovery Plan**.
2. Enter a unique name for the Recovery Plan, or use the preset name.
3. Select the primary recovery method for the Recovery Plan. This assigns the default recovery method to all domain controllers in the Recovery Plan. The recovery method can be changed at domain controller level. See Editing Domain Controller Configurations for more.
   a. Restore to Clean OS: restores the entire forest or any of its parts on freshly installed Windows machines. It is highly recommended that you visit the Restore to Clean OS section in the *Before You Start* page before you use this method.

> **NOTE:** For Technical Preview, the Restore to Clean OS method is the only available recovery method for a Recovery Plan. The dropdown menu is disabled by default.

4. From the drop-down list, select the maximum age of backups allowed in the Recovery Plan. This automatically selects the most recent backup for each domain controller that is not older than the specified number of days. If there is no domain controller backup that meets the criteria, a backup must be manually selected for that domain controller or the restore will fail. The default value is 14 days.
5. The table in the **Domains** section displays the domains within the environment. Select one or more domains to recover and specify configuration for the domain by clicking on the domain name. Refer to the Editing Domain Configurations section for more details. At least one domain controller from each selected domain must be recovered. Domains that are not selected are assumed to be operating correctly and no action will be performed for these domains.
6. Click **Save**. You will be taken to the Recovery Plan details screen.

You can edit a Recovery Plan by clicking **Configure**, then **Recovery Plan**. The Configure Recovery Plan screen will appear. You can then edit the same Recovery Plan configurations as seen in the steps above.

> **IMPORTANT:** If the Active Directory forest topology is changed on-premises (new domain controllers have been added or removed, domain controller roles are updated, etc), the environment will need to be manually re-discovered in the product and a new Recovery Plan needs to be created based on the updated topology.

Recovery Plan Details

Upon the creation of a Recovery Plan, you will be taken to the Recovery Plan details screen. Here you can view details of the domain controllers within the domains selected in the Recovery Plan.

> **NOTE:** The list of domain controllers is taken from the topology discovered by Disaster Recovery for Identity for Active Directory. If you see missing or additional domain controllers, or an incorrect domain controller type, run a discovery on the Topology screen and re-create a Recovery Plan.

On the Recovery Plan details screen, you can view the following information:

- Domain Controller - the FQDN of the domain controller.
- Domain - the FQDN of the domain selected for recovery.
- Status - the status of the domain controller.
- Current Operation - the operation currently running.
- Recovery Method - the recovery method selected for the domain controller. This can be changed to Do Not Recover in Domain Controller Configuration.
- Selected Backup - the completion date and time of the selected backup.

> **NOTE:** No Backup Available is displayed if there is no backup that meets the backup criteria.

- Type - the domain controller can be of the following types:
    - GC - Global Catalog

Above the action bar, you will see a the overall Recovery Plan summary of the verification/recovery task that is currently being performed in the Recovery Plan, including:

- the FQDN of the forest the environment is linked to and overall latest status of the Recovery Plan. See the Status section below for more.
- the overall time for the completed action.
- the number of domain controllers that have the following statuses:
    - Completed
    - Completed with Warnings
    - Canceled
    - Pending
        - Not Started
        - In Progress
        - Paused
        - Canceling
        - In Progress with Warnings
    - Failed
- the recovery mode with the number of domains selected.

On the Recovery Plan details screen, you can perform the following actions:

- Configure - edit the Recovery Plan's configurations, including modifying the Recovery Plan, the domain controller or the domain. See Creating and Editing a Recovery Plan, Editing Domain Configurations and Editing Domain Controller Configurations for more.
- Verify Plan - ensure that the configurations for the domain controller(s) within the Backup Plan are valid and can be used for forest recovery. Information on the verification will be displayed on the Domain Controller Operations screen.
- Start Recovery - begin running the Recovery Plan. Information on the recovery will be displayed on the Domain Controller Operations screen. Go to the Recovering an Environment with a Recovery Plan for more.
- Cancel - stops running the verification or recovery task.

NOTE: Individual domain controllers cannot be canceled from this screen.

CAUTION: Canceling a verification or recovery operation may result in a corrupt forest. Proceed with caution.

- View - view either events or tasks from the drop-down list for the Recovery Plan.

Status

The Status is displayed underneath the forest FQDN in the overall Recovery Plan summary as well as in the Status column for every domain controller. The Status column displays one of the following:

- Configuration errors if they exist in the Recovery Plan.
- Status of the ongoing or completed operation.

If a configuration error is present, open Domain Controller Configuration to view the full message.

By clicking on the status of the ongoing or completed operation, you can view the Domain Controller Operations for that domain controller. The status can include the following:

- Verify
  - Verification Starting - the verification operation is in the process of starting.
  - Verification in Progress - the verification operation is in progress.
  - Verification Completed - the verification operation has been completed.
  - Verification Completed with Warnings - the verification operation has been completed, but one or more operations have warnings. See Domain Controller Operations for more.
  - Verification Failed - the verification operation has failed.
  - Verification Canceling - the verification operation is in the process of being canceled.
  - Verification Canceled - the verification process has been canceled.
  - Verification Paused - the verification operation has been paused.

- Recovery
    - Recovery Starting - the recovery operation is in the process of starting.
    - Recovery in Progress - the recovery operation is in progress.
    - Recovery Completed - the recovery operation has been completed.
    - Recovery Completed with Warnings - the recovery operation has been completed, but one or more operations have warnings. See Domain Controller Operations for more.
    - Recovery Failed - the recovery operation has failed.
    - Recovery Canceling - the recovery operation is in the process of being canceled.
    - Recovery Canceled - the recovery process has been canceled.
    - Recovery Paused - the recovery operation has been paused.
    - Waiting For Other DCs - this operation is currently waiting for other domain controllers to finish their operations.

Editing Domain Configurations

You can edit domain configurations for the Recovery Plan by either:

a. Clicking on the domain FQDN in the Domain column on the Recovery Plan details screen,

b. Clicking on the domain FQDN in the Domains table on the Create/Edit Recovery Plan page, or

c. Clicking the checkbox for domain controller in the desired domain, then clicking **Configure**, then **Domain**. The Domain Configuration screen will appear.

> **NOTE:** Domain configurations are required when creating a Recovery Plan with the Restore to Clean OS method.

You can edit the following domain configurations:

1. Change Server Access Credentials. Definitions of each credential can be found in the Server Access Credentials section in the *Before You Start* page:

    a. Domain Username - an Active Directory Domain Admin account that existed when the backup was created.

    b. Domain User Password - the password for the above domain.

    c. Local Username - the username for the local account that has Local Administrator rights on the target.

    d. Local User Password - the password for the above local account.

    e. DSRM Administrator - the username for the DSRM administrator.

    f. DSRM Administrator Password - the password that the DSRM password will be set to when target machine is promoted to the domain controller.

    g. Confirm DSRM Administrator Password - confirm the above DSRM administrator password.

2. DNS Configuration. It is highly recommended that you visit the DNS configurations and Handling DNS servers during recovery sections in the *Before You Start* page:

    a. Select DNS server automatically - retrieves a list of all DNS servers that are in use in the forest and automatically assigns a DNS server that is operating correctly from the list to the current domain controller.

    b. Use preferred DNS server(s) - input preferred DNS server(s), individually separated by a semicolon (;). The use of the preferred DNS server can be seen in the Events screen.

Editing Domain Controller Configurations

You can edit domain controller configurations for the selected Recovery Plan by either:

a. Clicking on the domain controller FQDN in the Domain Controller column on the Recovery Plan details screen, or

b. Clicking the checkbox for the desired domain controller, then clicking **Configure**, then **Domain Controller**. The Domain Controller Configuration screen will appear.

You can edit the following domain controller configurations:

1. You can change the Recovery Method to the following states: Restore to Clean OS, Install Active Directory or Do Not Recover.

> **NOTES:**
>
> - It is highly recommended that you visit the Recovery methods in Disaster Recovery for Identity for Active Directory section in the *Before You Start* page before you use any of these methods.
> - If a domain controller is marked as Do Not Recover and then later changed to Restore to Clean OS (after successfully recovering domain credentials for a Restore to Clean OS recovery), the recovery status for all domain controllers will be reset. Therefore, if you run a recovery operation, it will start from the beginning for every domain controller, even if some were previously recovered.

2. (Install Active Directory method only) Under **Domain Controller Options**, configure the checkboxes as desired for the **Configure as a global catalog server** and **Install DNS server on the domain controller**.

    a. Configure as a global catalog server - Use this option if you need to reconfigure the global catalog on the domain controller during Active Directory® reinstallation. This option will be selected by default if the original domain controller was a global catalog. Microsoft recommends that all domain controllers provide DNS and global catalog services for high availability in distributed environments. For more information, click here.

    b. Install DNS server on the domain controller - During Recovery, the DNS server is installed during the **Install Windows features** step. This option is enabled by default.

3. The Target Server box will be empty by default. If the Target Server IP is empty, verification will run its operations against the source domain controller and a warning will be recorded. To perform a recovery, the Target IP must be populated, otherwise the recovery will fail.

> **NOTE:** The target server should be compliant with the following requirements:
>
> - Operating system version should be equal to the original domain controller operating system.
> - Operating system should follow organization security best practices (e.g. have latest updates, security software) since this operating system will be used to run the Active Directory Domain services after the restore.
> - The physical disks should have enough free space to host the Active Directory data after recovery.

3. (Restore to Clean OS method only) Change whether to select backups automatically based on the backup selection criteria configured for the Recovery Plan or use a manually selected backup.
   a. By default, a backup is selected automatically according to the backup selection criteria. To select a backup for the domain controller, select **Manual**, then select the backup from the drop-down menu.
4. Change server access credentials. By default, domain-level credentials are used. To specify credentials for the selected domain controller, check the **Override domain-level credentials** box, and input the credentials mentioned in the *Editing Domain Configurations* section above.

Verifying a Recovery Plan

To minimize downtime during Active Directory forest recovery, it is recommended to regularly verify your Recovery Plan configurations. The following is performed during a Recovery Plan verification:

> **NOTE:** If the target machine is not provided, the below steps will be completed against the source domain controller.

- Check connectivity to the Hybrid Agent and Domain Controller Agents.
- Install or upgrade the Domain Controller Agent on a target machine when the Target Server IP has been provided.
- Ensure that the target server has correct OS, drive letters and enough disk space.
- Verify access to the backup from the Domain Controller Agents.

If Recovery Plan has not been verified, all the above steps will take place during the recovery (except that Target Server IP has to be provided for a successful recovery).

To verify a Recovery Plan:

1. From the Recovery screen, open the desired Recovery Plan.
2. Click **Verify Plan**. All domain controllers which are not set to *Do Not Recover* in the Recovery Plan will then be verified. The current status of the verification of each domain controller can be seen in the Status column and the Domain Controller Operations screen. See Domain Controller Operations for more.

Recovering an Environment with a Recovery Plan

Once Recovery Plan verification has been completed successfully, you can proceed with the recovery. See the Verifying a Recovery Plan section for more.

NOTES:

- It is highly recommended that you visit the Recovery Considerations and Best Practices section in the *Before You Start* page before you recover an environment.
- Ensure that the Recovery Plan you wish to use for recovery has been created based on the latest forest topology.

To begin recovery:

1. Click on the desired Recovery Plan you wish to use for recovery from the Recovery tab.
2. Click **Start Recovery**, and read the information that is displayed. Confirm that the hybrid machine is configured with a DNS server, and that you want to begin recovery immediately, by checking the corresponding checkboxes. Then click **Start Recovery**.

All domain controllers in the Recovery Plan that are not set to Do Not Recover will then be recovered. The current status of the recovery of each domain controller can be seen in the Status column and on the Domain Controller Operations screen. See Domain Controller Operations for more.

Domain Controller Operations

By clicking on the status of a domain controller, you can open the Domain Controller Operations screen. This can only be accessed during or after verification or recovery.

NOTE: If the Recovery Plan has been edited, the Recovery Plan summary and Domain Controller Operations will be cleared and a recovery will need to be performed again to access the status.

This screen details the operations performed on a domain controller when verifying a Recovery Plan or recovering an environment.

Above the toolbar, you can see the progress of both the domain controller and the Recovery Plan:

- On the left hand side, you can view the status of the domain controller, including the progress of the verification/recovery, how many operations on the domain controller have been completed, are pending, have warnings or have failed.
- On the right hand side, you can view the status of the Recovery Plan, including the overall summary of the Recovery Plan and the overall time taken for the verification/recovery.

You can view the following information for the domain controller on the Domain Controller Operations screen:

- Operations - click on each operation to reveal the domain controller operation details, including details on any actions with warnings or errors.
- Elapsed Time - the duration of time taken for the running of the operation.
- Completion Date - the date and time for when the operation finished running.

On the Domain Controller Operations screen, you can perform the following actions:

- Skip and Continue - Allows you to skip the current failed recovery step for the domain controller you selected and continue the domain controller’s recovery. This action is recommended only if you have manually completed the failed recovery step on the domain controller.
- Retry Last - Allows you to rerun the failed recovery step on the domain controller you selected. This action is recommended when you manually fixed the issue that had caused the recovery step to fail.
- Cancel - Cancels the recovery or verification operation for the selected domain controller.

> **CAUTION:** Canceling a verification or recovery operation may result in a corrupt forest. Proceed with caution.

- View Events - opens the list of events for the domain controller for the latest or currently running task of the Recovery Plan.

Recovery Plan Cards

You can view the Recovery Plans that have previously been created by either clicking **All Recovery Plans** in the top left hand corner of the Recovery Plan details screen, or by clicking the Recovery tab.

Each card contains the following information:

Status

The Status section shows how your Recovery Plan is processing. Clicking on the status opens up the Task screen filtered by the specific Task ID this status is displaying. The status can include the following:

- New - the Recovery Plan has just been created and has not been ran.
- Verify
  - Verify Recovery Plan in Progress - verification of the Recovery Plan is in progress.
  - Last Successful Verify Recovery Plan - the time of the last successful verification of the Recovery Plan.
  - Verify Recovery Plan Canceling - the verification of the Recovery Plan is in the process of being canceled.
  - Verify Recovery Plan Canceled - the verification of the Recovery Plan has been canceled.
  - Verify Recovery Plan Failed - the time of the last failed verification of the Recovery Plan.
  - Verification Paused - the verification has been paused.
- Recovery
  - Recovery in Progress - the Recovery Plan is in the process of recovering the environment.
  - Last Successful Recovery - the time of the last successful recovery of the environment.
  - Recovery Canceling - the recovery of the Recovery Plan is in the process of being canceled.
  - Recovery Canceled - the recovery of the Recovery Plan has been successfully canceled.
  - Recovery Failed - the time of the last failed recovery of the Recovery Plan.
  - Recovery Paused - the recovery has been paused.

Summary

The Summary section shows an overview of the configuration of your Recovery Plan. This includes the following information:

- Recovery Method - the primary method of recovery used in the Recovery Plan.
- Selected Domains - the total number of domains in the forest and how many of those domains which were selected for the recovery.
- Number of DCs - the number of domain controllers in the domains selected for recovery in the Recovery Plan.

With the Recovery Plan cards, you can perform the following actions:

- Open - view Recovery Plan details.
- Remove - remove the Recovery Plan.

11

Events Management

The Events screen displays the events that have occurred while performing tasks such as backups, verification and recovery.

On the Events screen, you can take the following actions:

- Filter by the severity of the event you wish to view, and the date it was created, by clicking **Filter**.
  - Filter by the severity of the event; click the checkbox of one or more of the following severities: Information, Warning or Error
  - Filter by the date the event was created; choose the desired date and time from, and date and time to, then click **Apply**.
- Click **Refresh** to get the most up to date events for the environment.
- Use the **Export** option to export the selected log data into a .csv format. To do this:
  1. Select the event(s) you wish to export by clicking on the desired checkbox(es). To select all events (including events on other pages in the list, if applicable), select the top checkbox, in the table header.
  2. Click **Export**.
- Click **Edit Columns** to filter the list to include/exclude the following columns:
  - Date Created
  - Severity
  - Task Type
  - Object Name
  - Description
- Change the environment by using the drop down menu on the top right hand side of the screen.

12

Task Management

The Tasks screen allows you to view individual tasks, their statuses and when they were created.

On the Tasks screen, you can take the following actions:

- Filter by the severity of the event you wish to view, and the date it was created, by clicking **Filter**.
  - Filter by the status of the event: Queued, Running, Completed, Failed, Canceling or Canceled.
  - Filter by the date the event was created; choose the desired date and time from, and date and time to, then click **Apply**.
- Click **Refresh** to display the latest task information.
- Select a task, and click **Cancel** to stop the task in progress. To do this:
  1. Select the task(s) you wish to cancel by clicking on the desired checkbox(es).
  2. Click **Cancel**.

> **NOTE:** To cancel all tasks, you must select the top checkbox, in the table header, on each individual page of the list, if applicable.

> **CAUTION:** Canceling a verification or recovery operation may result in a corrupt forest. Proceed with caution.

- Click **Edit Columns** to filter the list to include/exclude the following columns:
  - Type
  - Status
  - Object Name
  - Created
  - Elapsed Time
  - Details
- Change the environment by using the drop down menu on the top right hand side of the screen.

About us

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

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product