Quest

Disaster Recovery for Identity for Active Directory

Security 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

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 Security Guide
Updated - January 10, 2025

Contents

1

Introduction

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity and availability.

This document describes the security features of Disaster Recovery for Identity for Active Directory. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

2

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.
- 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 is hosted in Microsoft Azure and delivers most of its functions via Microsoft Azure cloud services.

3

Architecture Overview

The following scheme shows the key components of the Disaster Recovery for Identity for Active Directory configuration.

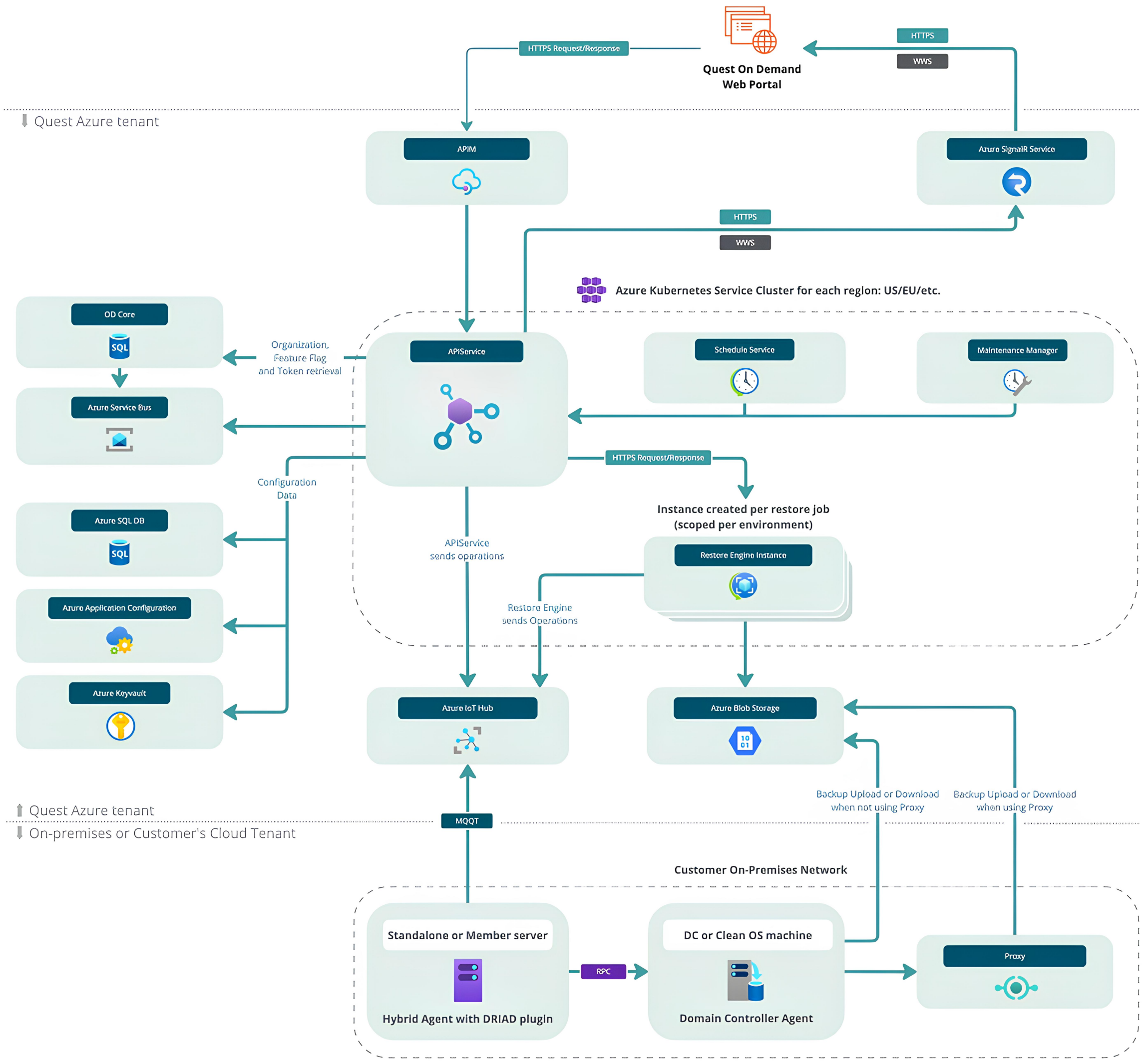

Figure 1: High-Level Architecture

If you are viewing on a browser, right click the image and click 'Open image/link in new tab/window' to view the diagram in more detail.

4

Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure and well protected datacenters in the world. They are subject to regular audits and certifications including Service Organization Controls (SOC) 1, SOC 2 and ISO/IEC 27001:2005.

Relevant references with additional information about the Windows Azure datacenter security can be found here:

- Microsoft Azure Trust Center: https://azure.microsoft.com/en-us/overview/trusted-cloud/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview?service=Azure#Icons
- Microsoft’s submission to the Cloud Security Alliance STAR registry: https://cloudsecurityalliance.org/star/registry/microsoft/
- Whitepaper: Standard Response to Request for Information – Security and Privacy: http://www.microsoft.com/en-us/download/details.aspx?id=26647
- Microsoft Global Datacenters: Security & Compliance: https://www.microsoft.com/en-us/cloud-platform/global-datacenters
- Azure data security and encryption best practices: https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

5

Overview of Data Handled by Disaster Recovery for Identity for Active Directory

Disaster Recovery for Identity for Active Directory manages the following type of customer data:

- On-premises environment information including Active Directory domain names and domain controller names. Environment information is stored and protected in the SQL database.
- Active Directory backup (.bkf) files stored in Geo-redundant Azure Blob Storage. Backups are replicated to secondary region.
- The application uses administrative account names and passwords to perform recovery operations. The data is stored encrypted with a unique organization encryption key that is stored separately in Azure Key Vault.
- Application logs.

6

Admin Consent and Service Principals

Disaster Recovery for Identity for Active Directory does not require access to the customer’s Entra ID and Microsoft 365 tenants. The product works primarily with Hybrid Agents to communicate to the customer’s on-premises Active Directory. No service principal is created in the customer’s Entra tenant.

7

Location of Customer Data

When a customer signs up for On Demand, they select the region in which to run their On Demand organization. All computation is performed and all data is stored in the selected region. The currently supported regions can be found here: https://regions.quest-on-demand.com/. All replication datacenters reside within the geographic boundaries of the selected region.

Windows Azure Storage (including Blobs, Tables, and Queues) is replicated three times in the same datacenter for resiliency against hardware failure. The data is replicated across different fault domains to increase availability. All replication datacenters reside within the geographic boundaries of the selected region. See this Microsoft reference for more details: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy.

Which types of data is stored in each service?

Azure Key Vault

- Per organization encryption key.

Azure Blob Storage

- On-premises domain controller backups uploaded from on-premises Domain Controller Agent (or user defined proxy).
- Cloud-generated recovery engine logs (domain names, domain controller names, account names)
- Per-environment communication certificate (also stored on-premises on ODJRS agent machine and domain controllers/cleanOS machines).

Azure SQL Database

- Environment configuration (username and encrypted password).
- On-premises Topology (forest name, domain names, domain controller names).
- Backup Plan configuration (on-premises domain controller names).
- Recovery Plan configuration (domain controllers, IP addresses, Site names, GC flags, FSMO roles, local/domain usernames and encrypted passwords).
- Tasks/events - can include details from errors.
- Backup metadata with domain, domain controller name, encrypted backup password and Blob name.

Azure Application Insights

- Logs from all microservices (except on-premises agents)

Azure Service Bus

- Operation logs (which can expose domain controller names).
- Operation results (include on-premises Topology - domain and domain controller names).
- ODJRS operation configuration.

SignalR

- Computer names for operations and tasks.

ODJRS Plugin/IOT hub (from API to on-premises plugin or agent)

- Topology Discovery (domain/forest name, username/password) sent to Hybrid Agent.
- Backup domain controller configuration (target domain controller name and IP addresses) sent to Hybrid Agent.
- Domain controller Restore configuration (target domain controller name and IP addresses) sent to Hybrid Agent.
- Domain Controller Agent installation configuration (target domain controller name, IP Addresses, local administrator account and password).
- Domain Controller Agent certificate for RPC communications.

Domain Controller Agent

- Temporary domain controller backup before upload to Blob storage.
- Domain Controller Agent communication key for RPC communications.

Datacenter locations

The following datacenters are used to store customer data:

For European organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica – North Europe (Ireland)
    - Secondary replica – West Europe (Netherlands)
- Logs are stored in Azure Data Explorer - North Europe (Ireland) – encrypted at rest

For US organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica - West US 2 (Washington)
    - Secondary replica - West Central US (Wyoming)
- Logs are stored in Azure Data Explorer - West US 2 (Washington) – encrypted at rest

For UK organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica – UK South
    - Secondary replica – UK West
- Logs are stored in Azure Data Explorer - UK South – encrypted at rest

8

Privacy and Protection of Customer Data

The most sensitive customer data processed by Disaster Recovery for Identity for Active Directory is the on-premises Microsoft Active Directory data, including users, groups and contacts and their associated properties. Disaster Recovery for Identity for Active Directory does not store or deal with end-user passwords of Active Directory objects (except passwords of the domain administrators when configuring domains or domain controllers).

Each organization has its own blob storage container with an organization specific Encryption Scope.

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.

More information about Azure Queues, Tables, and Blobs can be found here:

- https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction
- https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

9

Separation of Customer Data

A common concern related to cloud based services is the prevention of commingling of data that belongs to different customers. Disaster Recovery for Identity for Active Directory has architected its solution to specifically prevent such data commingling by logically separating customer data stores.

Customer data are differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from the Quest On Demand Core that is created when the customer signs up with the application.

Row Level Security (RLS) is used to ensure data isolation between different organizations within a single Azure SQL Server database. Each database table includes an OrganizationID column. To enforce this isolation, RLS is enabled on all tables, restricting query results to only those rows where the OrganizationID matches the current user's organization, preventing unauthorized data access.

Recovery Manager for Active Directory (RMAD) pods are used only once and are not shared between different environments or organizations.

Each organization has its own Blob storage container with an organization specific Encryption Scope.

10

Network Communications

Internal network communication within Azure includes:

- Inter-service communication between Disaster Recovery for Identity for Active Directory components.
- Inter-service communication between Disaster Recovery for Identity for Active Directory and the On Demand platform.

The network communication is secured with HTTPS TLS 1.2 minimum and is not visible to the external public internet. Inter-service communication uses OAuth authentication using a Quest Entra ID service account with the rights to access the services. No backend services of Disaster Recovery for Identity for Active Directory can be used by end-users. The following scheme shows the communication configuration between key components of Disaster Recovery for Identity for Active Directory:

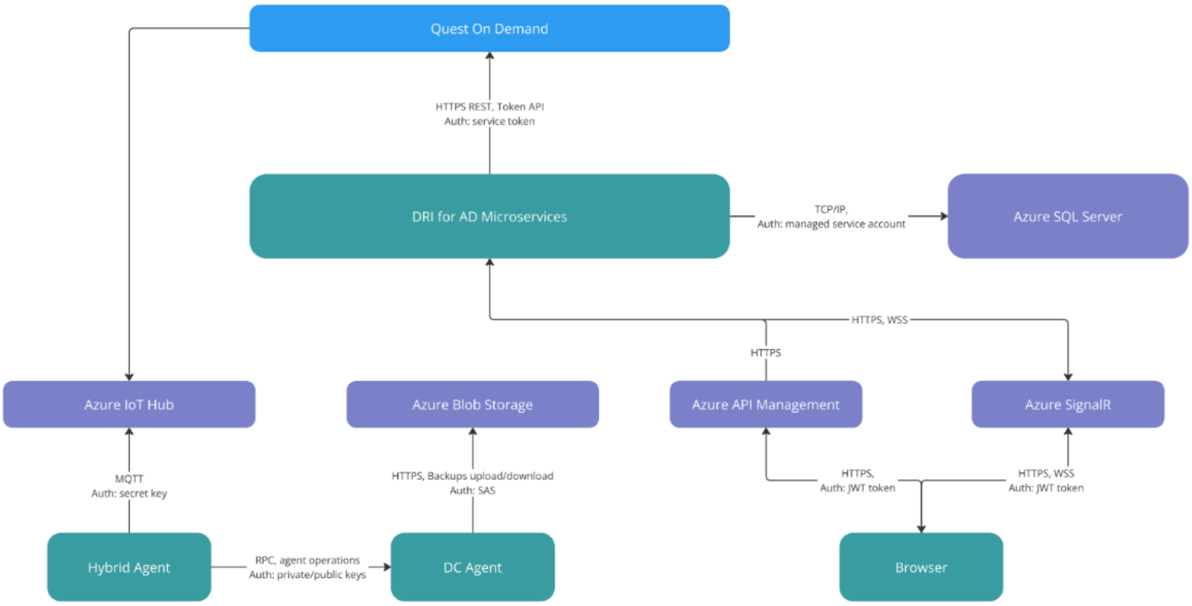

Figure 2: Component Communication Architecture

Disaster Recovery for Identity for Active Directory accepts the following network communication from outside Azure:

- Access to Disaster Recovery for Identity for Active Directory Web UI.
- Hybrid Agent deployed on customer on-premises server accessing Disaster Recovery for Identity for Active Directory backend via Azure IoT Hub.
- Domain Controller (DC) Agent deployed on customer domain controllers or target servers accessing Azure Blob Storage.

All external communication is secured with HTTPS TLS 1.2 minimum.

The Hybrid Agent communicates with the On Demand cloud through Azure’s IoT Hub service. The agent itself behaves as an IoT device. All communications with Azure are conducted over the MQTT protocol using the Microsoft Azure Device Client library.

Communication keys are required to facilitate communication between the Hybrid Agent and Domain Controller Agent.

The Disaster Recovery for Identity for Active Directory user interface uses OAuth authentication with a JWT token issued to a logged in user.

11

Authentication of Users

The customer logs in to the application by providing On Demand user account credentials.

For more information about user authentication, please refer to the Quest On Demand Global Settings Security Guide.

12

Role Based Access Control

Disaster Recovery for Identity for Active Directory provides the common authentication via Microsoft Entra ID. Quest On Demand is configured with default roles that cannot be edited or deleted and also allows you to add custom roles to make permissions more granular. Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform. For more information on role-based access control, please refer the Quest On Demand product documentation.

13

FIPS 140-2 Compliance

Disaster Recovery for Identity for Active Directory cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions.

More information:

- Security recommendations for Blob storage: https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations
- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips
- Microsoft FIPS backgrounder: https://learn.microsoft.com/en-us/compliance/regulatory/offering-fips-140-2
- Encryption in the Microsoft Cloud: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-the-microsoft-cloud-overview
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

14

SDLC and SDL

The On Demand team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest’s corporate network have access to these systems. Therefore, should an On Demand developer leave the company, this individual will no longer be able to access On Demand systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

In addition, the On Demand Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling.
- OWASP guidelines.
- Regularly scheduled static code analysis is performed on regular basis.
- Regularly scheduled vulnerability scanning is performed on regular basis.
- Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments.

On Demand developers go through the same set of hiring processes and background checks as other Quest employees.

15

Third Party Assessments and Certifications

Penetration Testing

On Demand has undergone a third-party security assessment and penetration testing yearly since 2017. The assessment includes but is not limited to:

- Manual penetration testing.
- Static code analysis with Third Party tools to identify security flaws.

A summary of the results is available upon request. No OWASP Top 10 critical or high-risk issues have been identified.

Certification

On Demand is included in the scope of the Platform Management ISO/IEC 27001, 27017 and 27018 certifications:

- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements: **Certificate Number: 1156977-3**, valid until **2025-07-28.**
- ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **Certificate Number: 1156977-3**, valid until **2025-07-28**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **Certificate Number: 1156977-3**, valid until **2025-07-28**.

16

Operational Security

Source control and build systems can only be accessed by Quest employees on Quest’s corporate network (domain security). If a developer (or any other employee with access to Disaster Recovery for Identity for Active Directory) leaves the company, the individual immediately loses access to the systems.

All code is versioned in source control.

Access to Data

Access to Disaster Recovery for Identity for Active Directory data is restricted to:

- Quest Operations team members.
- Particular Quest Support team members working closely with Disaster Recovery for Identity for Active Directory product issues.
- The product development team to provide support for the product.

Access to Disaster Recovery for Identity for Active Directory data is restricted through the dedicated Quest Azure Active Directory security groups. For different types of data (e.g., product logs, customer data, and sensitive data) different access levels and lists of allowed people are assigned. Quest employees do not have access to backups.

Permissions Required to Configure and Operate Disaster Recovery for Identity for Active Directory

Quest Operations team members have access to the Quest’s production Azure Subscription and monitor this as part of normal day to day operations. Disaster Recovery for Identity for Active Directory developers have no access to Quest’s production Azure Subscription.

To access Disaster Recovery for Identity for Active Directory, a customer representative opens the On Demand website and signs up for an On Demand account. The account is verified via email; thus, a valid email address must be provided during registration.

An organization is automatically created once the new account is created.

Permissions for 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.

Permissions for 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 should be a member of the Domain Administrators group on the target domain controller, or a member of the Local Administrators group if the target computer is a Clean OS computer.

Operational Monitoring

Disaster Recovery for Identity for Active Directory internal logging is available to Quest Operations and Disaster Recovery for Identity for Active Directory development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data (e.g. error messages reporting usernames or email addresses, etc.) can become a part of internal logging for troubleshooting purposes.

Production Incident Response Management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. Disaster Recovery for Identity for Active Directory relies on Azure infrastructure and as such, is subject to the possible disruption of these services.

- Quest On Demand services status page is available at https://status.quest-on-demand.com/
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/

17

Customer Measures

Disaster Recovery for Identity for Active Directory security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with data recovery. Particular care needs to be given to protecting the credentials of the Microsoft Entra tenant Global Administrator accounts and Microsoft 365 tenants Global Administrator accounts.

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