

Quest Guardian - Managed Recovery Service

Overview

Quest Guardian - Managed Recovery Service is an annual subscription offered to new and existing Quest Recovery Manager Disaster Recovery Edition customers. Quest will help you develop a Forest Recovery Plan to be used in the event of an Active Directory (AD) or EntraID Critical Incident, ensuring that your organization recovers the directory in a timely manner.

During the subscription period, Quest will provide expertise to deploy a new RMAD DRE production platform and Quest Identity Recovery implementation or to modernize the configuration of an existing deployment.

This subscription provides you with monthly analysis and optimization reviews of the production platform to maintain the integrity of Active Directory Forest recoverability. In addition, Quest will guide you through two recovery simulations in your lab environment and lead a Recovery Tabletop exercise. Quest will also assist and guide you through critical incident response recovery events as commercially reasonable.

Outcomes

The Service offered will help you keep the Active Directory recovery platform healthy and optimized to satisfy business continuity objectives. Quest will provide critical incident response service to assist with the recovery of Active Directory functionality, as described herein.

- Analysis of current recovery objectives and recover platform implementation
- High-level review of your existing Active Directory recovery plans, crisis scenario requirements will be taken into account when architecting the recovery platform solution
- Validation of existing Quest Recovery Manager implementation to ensure platform functionality and integrity (and perform periodic product upgrades if deemed necessary)
- Deployment and configuration of Quest Identity Recovery (or review of existing deployment) at the beginning of the subscription period
- Verification that Directory backup and recovery approach aligns with industry and Quest best practices
- Expert operation of the Recovery platforms in the event of a critical incident requiring restoration of the AD Forest

Approach and Activities

A Quest Professional Services Consultant will work with your stakeholders and subject matter experts on the following activities. The actual activities performed will vary based on the complexity of your environment and technical needs outlined during the Baseline Planning Sessions.

Baseline Deployment of Recovery Solution

For a new Quest Guardian customer, Quest will assist with the planning, design, implementation and configuration validation of the Quest Recovery platforms. During this baseline deployment event, Quest will thoroughly document the configuration for future reference and maintenance.

Planning

Quest will host a planning session of up to four (4) hours with you to verify environment readiness and establish the base deployment architecture, during which Quest and you may discuss:

- Review Project Scope and Activities
- Overview of your Environment, Requirements, and Goals
- Review existing installation (when applicable)
- Review Installation pre-requisites, permissions & Quest best practices
- Identify Domain Controllers (at least two (2) per domain) that will be backed up
- Review backup schedule & retention best practices
- Review secondary storage options
- Estimate space needed for Primary (Tier 1) and Secondary (Tier 2) storage.
- Identify/Review disaster contingencies such as “go/no-go”, communication, and SLAs
- Convey Quest Best Practices on Directory recovery
- Determine Base Deployment Architecture or upgrade path (if needed)
- Develop Custom Forest Recovery and Clean OS Recovery Plans
- Identify/Review the various role groups that will be using Quest Identity Recovery
- Convey Quest Best Practices for Quest Identity Recovery deployment and configuration

The Planning phase will be completed with the delivery of the planning session document, including the items discussed during the planning session. This planning session document will be the phase's Project Deliverable.

Installation (RMAD DRE)

Quest will install or upgrade of Recovery Manager for Active Directory Components and Services on Designated Server(s) in accordance with the deployment architecture defined during the planning session.

- Validate installation pre-requisites & permissions per planning session
- Prepare the environment for RMAD DRE install or upgrade
- Install RMAD DRE
- Discuss backup scope, frequency, storage, and retention

The Installation phase will be completed when Recovery Manager for Active Directory Disaster Recovery Edition has been installed on the server(s) designated in the planning phase document, is communicating with the applicable AD Forest and server; and when Quest Identity Recovery has been registered and integrated with Recovery Manager for Active Directory (if within scope).

Backup Configuration

Quest will aid you with configuration of Active Directory and Bare Metal backups in accordance with the deployment architecture identified during the planning session.

- Review backup strategies and scheduling
- Review backup methods
- Create and populate at least two (2) computer collections
- Deploy agents on domain controllers
- Configure Primary and Secondary backup storage locations
- Configure AD and/or Bare Metal backups
- Create initial AD and/or Bare Metal backups

The Backup Configuration phase will be completed when all the applicable activities are completed.

Forest Recovery Configuration

Quest will aid you with configuring no more than three (3) Forest Recovery Projects (including up to ten (10) Domains and twenty (20) Domain Controllers) in accordance with the deployment architecture identified during the planning session. The goal is to familiarize you with the forest recovery console.

- Review Recovery Project Settings
- Review Recovery Modes and Recovery in Phases
- Review Recovery Methods
- Create at least one (1) Project using Forest Recovery Mode and any combination of Forest Recovery Methods
- Review tools available in the Forest Recovery Console
- Validate current forest health, including DC accessibility, replication, domain trusts, authentication, RID master and GC operations
- Deploy Forest Recovery Agents

- Validate recovery project settings
- Save the forest recovery project(s)
- Schedule console configuration backups to secondary storage

The Forest Recovery Configuration phase will be completed when all the applicable activities are completed.

Quest Identity Recovery Configuration

Quest will assist you with configuring Quest Identity Recovery in accordance with the deployment architecture identified during the planning session. Quest will aid you with:

- Add up to three (3) Azure AD tenants to Quest Identity Recovery
- Review backup strategies and options
- Create an initial Azure AD backup
- Configure backup schedule
- Integrate with RMAD/DRE
- Configure Quest Identity Recovery hybrid integration with the RMAD server
- Configure access control to Quest Identity Recovery portal

The Quest Identity Recovery Configuration phase will be completed when all of the applicable activities are completed.

Baseline Review of Existing Production Deployment

For our existing recovery customers, Quest will perform a thorough analysis of your RMAD DRE and Identity Recovery deployment to ensure all components meet best practices and effectively satisfies your business continuity needs. During this review event, Quest will document the configuration of the recovery platform configuration for future reference and maintenance. Updates to the existing deployment will follow the steps above.

Testing Walkthrough

Quest will participate in your disaster recovery exercise in an isolated lab environment. The goal of this exercise is to give your staff practical experience using the forest recovery console in a recovery and validate recovery plans. You will be responsible for creating an isolated environment to conduct the walkthrough. Quest and you will perform the following activities, as indicated below:

- Review AD Forest recovery testing scope and parameters
- You prepare test environment
- Install RMAD DRE and copy backup file from production
- You isolate test environment

- Run Forest recovery test(s) in an isolated environment to validate recovery methodology
- Restore an Azure AD object(s) using the Quest Identity Recovery Portal
- Restore hybrid AD objects using the Quest Identity Recovery Portal (optional, only for customer configured integration with Recovery Manager for AD)

Two (2) test events are scheduled during the subscription year, typically after the initial installation and halfway through the year. The Testing phase will be completed when all the applicable activities from the Testing Walkthrough phase are validated.

Knowledge Transfer

Quest will provide guidance to you by performing a knowledge transfer and product review of the Recovery Manager for Active Directory Components and Services implemented into your Environment throughout the course of the engagement. If requested, Quest may conduct an additional knowledge transfer session (up to two (2) hours), which may include:

- Assistance with verifying the Recovery Manager for Active Directory implementation
- Verify you are able to backup and restore Active Directory
- Introduce Support resources

The Knowledge Transfer phase will be completed when the Testing Walkthrough phase is completed, or when the knowledge transfer session has occurred.

Recovery Tabletop Exercise

Quest will facilitate a tabletop exercise, in which you will walk through a simulated Directory failure or compromise scenario to validate your recovery processes. You will have the opportunity to validate your ability to recover services, make critical decisions, and coordinate stakeholders, without performing recovery actions in production. Topics covered may include:

- Incident Detection and Escalation
- Categorizing an Incident from a Critical Incident
- Recovery Decision Making
- Recovery Environment Preparation
- Domain Controller Recovery
- Identity and Credential Recovery
- Application Dependency Recovery
- Business Service Restoration
- Recovery Validation
- Communications

The Tabletop Exercise phase will be completed when the walkthrough has been completed and the evaluation document has been delivered.

Maintenance Review of Quest Identity Recovery Production Deployment

Scheduled monthly during the subscription year, Quest will perform a maintenance review of your Identity Recovery components and configuration. Any calls for assistance outside of this review will need to be performed on a time and materials contract basis.

- Verify the production recovery implementation is optimized and configured according to Quest best practices
- Review of existing backup and recovery documentation
- Review AD backup scope, frequency, storage, and retention
- Review Quest backup agent health installed on domain controllers
- Review AD / BMR backup creation health
- Confirm that AD backups are functional and protected
- Validate Forest Recovery console project settings
- Validate applied recovery methods
- Validate agent health installed on domain controllers
- Validate current forest health, including DC accessibility, replication, domain trusts, authentication, RID master, and GC operations
- Reconfigure the existing implementation in production based on identified gaps
- Run Forest Health Check of Active Directory production environment

Critical Incident Response

- In the event of a qualified incident, Quest will assign services personnel to aid in the restoration of Active Directory as part of your business continuity operation.
- When notified, Quest will assign and deploy PSO engineer(s) within two (2) hours of your initial support call to Quest identifying a severity level 1 issue. After a briefing of the scenario, the Quest team will assist you to determine the best AD restoration strategy and workflow.
- Operate RMAD DRE to restore phase 1 Domain Controllers (Forest or Domain Recovery mode), as determined during planning.
- Quest will assist with at least 1 run of Phase 2 (repromotion mode).
- Analyze any errors with restoration and provide guidance to resolve environmental issues (DNS settings, data cleanup, etc.).
- Provide guidance, as necessary, to expedite the restoration of the AD environment supporting core business operations.
- Your team is responsible for restoring any additional infrastructure or applications to full operational capacity and scope.

Prerequisites and Assumptions

As part of the Active Directory Recovery as a Service offering, you agree to cooperate with Quest in its delivery of the Service and to the following responsibilities:

- Quest Guardian is currently under an active maintenance contract for the duration of this subscription.
- Scope of this offering is limited to protecting three (3) Active Directory Forests.
- Participation in additional Customer Disaster Recovery training or simulation events are not included with this offering.
- All activities will be performed remotely utilizing phone and web conferencing.
- You will commit a technical resource on a full-time basis to work with the Quest consultant and provide assistance as necessary.
- You will provide project team members with suitable business expertise, technical expertise, and decision-making authority to ensure efficient project progress. The activities described above are a general description of software consulting services that Quest may provide during the subscription year.
- You agree to make recommended changes (in a timely manner) to the Quest Guardian platform configuration by the Quest PSO team to maximize AD Forest recovery operability.
- Quest will provide critical incident response services as described above, up to seventy-two (72) hours during the subscription year. Upon your request, Quest will provide additional services based on Quest current services rates, billed according to the terms in the services agreement governing these Services.
- You may schedule additional business continuity consulting services, such as quarterly disaster recovery testing, utilizing the Quest current services rates, billed according to the terms in the services agreement governing these Services.
- Your AD environment has adequate bandwidth and is not hindered by firewalls for remote agent installation.
- You can allow specific ports and URL access from Recovery Manager for AD to connect to the Quest SaaS platform, in order to perform the integration (optional, only for existing Recovery Manager for AD customers).
- Ensure that the existing infrastructure and hardware configuration is sufficient to support the environment. You will secure and prepare the necessary hardware and prerequisites, as listed in the System Requirements and planning document.

SKU

BAA-ATA-FF

Quest Guardian - Managed Recovery Service