Hybrid AD Cyber Resiliency Suite Foundation

Description

The Foundation Service Offering will assist the Customer with the installation, configuration, and testing of Recovery Manager for Active Directory Disaster Recovery Edition, On Demand Recovery, Change Auditor for Active Directory and Change Auditor for Logon Activity, along with On Demand Audit and GPO Admin Software (the “Activities” for the “Software”).

This service offering includes the following phases:

- Planning: verify prerequisites, establish base architecture for the Software
- Installation: deploy the Software based on agreed architecture
- Configuration: customize the Software and components to Customer environment
- Testing: verify functionality of the Software
- Knowledge Transfer: demonstrate how to leverage the Software to meet Customer business requirements and how to manage the Software as business needs evolve

Outcomes

The services offering will support the more rapid deployment of the Software to provide auditing capabilities, GPO management, and disaster recovery of your environments. Our team helps you quickly drive your new solutions into production – ensuring your IT team is ready to utilize all the features like:

- Change Auditor and On Demand Audit
  - Audit reporting
  - Alerting
  - Object protection
  - Integration with other tools
- GPO Admin
  - GPO importing/exporting
  - GPO versioning
  - Role-based access to GPOs
  - GPO approval workflows
- Recovery Manager for Active Directory Disaster Recovery Edition
  - Backup schedules and design
  - Forest and Bare Metal Recovery Plans and Best Practices
  - Backup storage readiness

Approach and activities

A Quest Professional Services consultant will work with the necessary Customer stakeholders and subject matter experts on the following activities. The activities performed may vary based on the complexity of the Customer’s environment and technical needs outlined during the Planning Session.

Planning

Quest will host a planning session up to 6 hours with Customer to verify environment readiness and establish the base deployment architecture, during which Quest and Customer may discuss:

- Finalize logistics including scheduling, remote access requirements and web conferencing needs
- Review Project Scope and Activities
- Overview of Customer Environment, Requirements, and Goals
- Best Practices for Change Auditor and On Demand Audit
- Verify environment preparedness and prerequisites
- Discuss GPO Admin configuration storage and GPO backup storage options
- Identify/Review the various role groups that will be using GPO Admin
- Decide if client requires or needs GPO Admin Dashboard installed
- Convey Quest Best Practices on GPO Admin deployment and configuration
- Identify/Review disaster contingencies such as “go/no-go”, communication, and SLA’s
- Review Secondary Storage options
- Convey Quest Best Practices on forest recovery
- Determine Base Deployment Architecture for RMAD/DRE
- Develop Custom Forest Recovery and Clean OS Recovery Plans
- Identify/Review the various role groups that will be using On Demand Recovery
- Convey Quest Best Practices for On Demand Recovery deployment and configuration
- Provide a list of pre-engagement prerequisites to be in place prior to installation

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 (Change Auditor and On Demand Audit)

Quest will assist Customer with installation of Change Auditor components and services on designated server(s) in accordance with the deployment architecture defined during the planning session.

- Review and verify installation pre-requisites & permissions
- Install Change Auditor and deploy agents (up to 5 Coordinators and 10 agents)
- Using the Change Auditor Client, verify successful communication with the AD Forest and servers with agents installed
- Register and configure On Demand Audit

The Installation phase will be completed when both (1) Change Auditor has been installed on the server(s) designated in the planning phase document with communication with the applicable AD Forest and server; and (2) On Demand Audit has been registered and integrated with Change Auditor.

Installation (GPO Admin)

Quest will assist Customer with the installation of GPO Admin Components and Services on Designated Server(s) in accordance with the deployment architecture defined during the planning session.

- Review and verify installation pre-requisites & permissions
- Install GPO Admin (up to 2 servers)
- Using the GPO Admin console, verify successful communication with the AD Forest
- Install and configure the GPO Admin Dashboard (optional)

The Installation phase will be completed when GPO Admin has been installed on the server(s) designated in the planning phase document and communication with the applicable AD Forest has been established.

Installation (RMAD/DRE)

Quest will assist Customer with the installation 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.

- Review Installation pre-requisites & permissions
- Install RMAD/DRE (up to 2 servers)
- Discuss backup scope, frequency, storage, and retention
- Configure RMAD/DRE computer collections where appropriate (up to 2 collections)
- Register and integrate On Demand Recovery with Recovery Manager for Active Directory

The Installation phase will be completed when both (1) Recovery Manager for Active Directory Disaster Recovery Edition has been installed on the server(s) designated in the planning phase document with communication with the applicable AD Forest and server; and (2) On Demand Recovery has been registered and integrated with Recovery Manager for Active Directory.

Configuration (Change Auditor and On Demand Audit)

Quest will aid Customer with configuration of Change Auditor and On Demand Audit, according to the deployment architecture identified during the planning session.

- Configure coordinators (up to 5)
- Register and configure On Demand Audit with SpecterOps Bloodhound Enterprise
- Configure security groups (up to 10)
- Deploy auditing agents (up to 10)
- Define event auditing
- Create auditing templates and filters (up to 5 each)
- Create custom searches and reports (up to 5 each)
- Create AD Protection Templates (up to 10)
- Configure Azure tenants to audit (up to 5)
- Demonstrate enabling and disabling Change Auditor event forwarding to On Demand Audit

- Configure integrations with GPO Admin, Recovery Manager, Active Roles and IT Security Search (as applicable)

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

Configuration (GPO Admin server settings)

Quest will assist Customer with configuring GPO Admin in accordance with the deployment architecture identified during the planning session. Quest will aid Customer with:

- Initial configuration of all GPO Admin global settings
- Add required AD users and groups to access roles (Admin or User)
- Configure access role permissions for one role
- Configure SMTP and Exchange connectivity
- Discuss and configure the following remaining global server options per Customer needs:
  - GPO Backup storage will be local to GPO Admin server
  - GPO Admin configuration will be on local AD LDS or remote SQL (if SQL, Customer to verify access to the SQL prior to engagement)
  - All GPO Admin components and services are installed on a single server

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

Configuration (GPO Admin Workflows)

Quest will assist Customer with configuring up to five (5) Version Control container(s) in accordance with the workflow requirements identified during the planning session in order to familiarize Customer with the GPO Admin console.

- Create and configure up to five (5) Version Control container(s)
- Configure workflow permissions, notifications, and approvals for the VC containers (up to 2 hours)

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

Configuration (RMAD/DRE Domain Controller Backups)

Quest will aid Customer 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 computer groups
- Install agents on domain controllers (up to 10 agents)
- Configure Primary and Secondary backup locations
- Configure AD and BMR backups
- Create initial AD and BMR backups

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

Configuration (RMAD/DRE Forest Recovery)

Quest will aid Customer with configuring no more than two Forest Recovery Projects (including no more than 4 Domains and 10 Domain Controllers) in accordance with the deployment architecture identified during the planning session. The goal is to familiarize Customer with the Forest Recovery console.

- Review Forest Recovery System Architecture
- Review Forest Recovery Methods
  - Restore Active Directory on Clean OS
  - Restore Active Directory from backup
  - Reinstall Active Directory
- Create at least one Forest Recovery Project using any combination of Forest Recovery Methods
- Validate current forest health, including DC accessibility, replication, domain trusts, authentication, RID master, and GC operations
- Validate recovery project settings

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

Configuration (RMAD/DRE Bare Metal Recovery / Restore AD on clean OS)

Quest will assist Customer with configuring no more than two Bare Metal Recovery Projects (including no more than 4 Domains and 10 Domain Controllers) in accordance with the deployment architecture identified during the planning session. The goal is to familiarize the customer with the Bare Metal Recovery and the Restore AD on clean OS feature in the forest recovery console.

- Review phased recovery process
- Review Bare Metal Recovery System Architecture
- Review Bare Metal Recovery Methods
  - Restore Active Directory on Clean OS
  - Bare Metal recovery to auto created target virtual server (VMware or Hyper-V)
  - Bare Metal recovery to auto configured target physical server (iDRAC, HP ILO)
- Create at least one Bare Metal Recovery Project
- Review Restore AD on clean OS recovery method
- Validate recovery project settings

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

Configuration (On Demand Recovery)

Quest will assist Customer with configuring On Demand Recovery in accordance with the deployment architecture identified during the planning session. Quest will aid Customer with:

- Add up to two Azure AD tenants to On Demand Recovery
- Review backup strategies and options
- Create an initial Azure AD backup
- Configure backup schedule

- Integrate with RMAD/DRE
- Configure access control to On Demand Recovery console

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

Testing (Change Auditor and On Demand Audit)

Quest will participate in functional testing of Change Auditor based on configuration completed with Customer in the Configuration phase. The goal of this step is to give Customer personnel practical experience using Change Auditor.

- Creating, running, and viewing reports (up to 5 reports)
- Verify that Object protection templates are working as designed (up to 10 templates)
- View forwarded Change Auditor events in the On Demand Console
- Verify successful integration with other Quest platforms (GPO Admin, Recovery Manager, Active Roles and IT Security Search (as applicable)

The Testing phase will be completed when all the applicable activities from the Configuration phase are validated.

Testing (GPO Admin)

Quest will participate in testing of GPO Admin workflows to provide Customer personnel with practical experience using GPO Admin.

- Provide a test script for the test user
- Verify the notification and approval emails are being delivered correctly
- Verify GPO lifecycle behaves as expected using test GPOs and OUs
- Verify functionality of the GPO Admin Dashboard

The Testing phase will be completed when notifications, lifecycle actions, and Admin Dashboard are shown to be functioning as expected and as described in the plan agreed upon in the Planning phase.

Testing (RMAD/DRE)

Quest will participate in Customer's disaster recovery exercise in an isolated lab environment. The goal of this step is to give Customer's staff practical experience using the forest recovery console in a recovery and validate recovery plans.

- Review forest recovery testing scope and parameters
- Run Forest recovery test(s) in the isolated environment to validate recovery methodology (up to 2 tests)
- Restore an Azure AD user and group
- Restore a hybrid AD user (optional, only for customer configured integration with Recovery Manager for AD)

The Testing phase will be completed when all the applicable activities from the Configuration phase are validated.

Knowledge Transfer (Change Auditor and On Demand Audit)

Quest will provide guidance to Customer by performing a knowledge transfer and product overview of the Change Auditor components and services implemented into Customer's environment throughout the course of the engagement and one 4-hour knowledge transfer session (if necessary), which may include:

- Review the items configured during the engagement
- Verify Customer can run, create, and view Audit reports
- Description of integration with other Quest offerings
- Introduction of Support resources

The Knowledge Transfer phase will be completed when the knowledge transfer session has occurred.

Knowledge Transfer (GPO Admin)

Quest will provide guidance to Customer by performing a knowledge transfer and product review of the GPO Admin components and services implemented into Customer's environment throughout the course of the engagement and one 2-hour knowledge transfer session (if necessary), which may include:

- Review the items configured during the engagement
- Review copying, exporting, and importing of GPOs and Synchronization Targets.
- Verify Customer can run and view GPO version difference reports
- Verify Customer can configure and use search folder
- How to change basic configurations, add High Availability and recovering a failed GPO Admin server
- Introduction of Support resources

The Knowledge Transfer phase will be completed when the knowledge transfer session has occurred.

Knowledge Transfer (RMAD/DRE)

Quest will provide guidance to the customer by performing a knowledge transfer and product review of the Recovery Manager for Active Directory Components and Services implemented into the Customer's Environment throughout the course of the engagement and one 2-hour knowledge transfer session (if necessary), which may include:

- Assistance with verifying the Recovery Manager for Active Directory implementation
- Verify Customer can backup and restore Active Directory
- Introduction of Support resources

The Knowledge Transfer phase will be completed when the knowledge transfer session has occurred.

Prerequisites and assumptions

Customer agrees to cooperate with Quest in its delivery of the Services. Customer agrees that the following responsibilities are solely Customer responsibilities that are required prior to and throughout the engagement or necessary and required assumptions about the engagement, as applicable:

- Customer's AD environment has adequate bandwidth and is not hindered by firewalls between Change Auditor servers and domain controllers.
- Commit a technical resource on a full-time basis to provide Quest with the assistance required.
- Provide project team members with suitable business expertise, technical expertise, and decision-making authority to ensure efficient project progress.
- Customer will secure and prepare the necessary hardware and pre-requisites, as listed in the System Requirements (Product Installation/QuickStart Guide) prior to the Installation phase.
- All activities will be performed remotely utilizing Quest provided web and voice conferencing

For more information, please contact your Account Manager.

SKU

PSR-DMX-FF	Active Directory Risk Protection Suite Foundation