ManageEngine
RecoveryManager Plus

Architecture

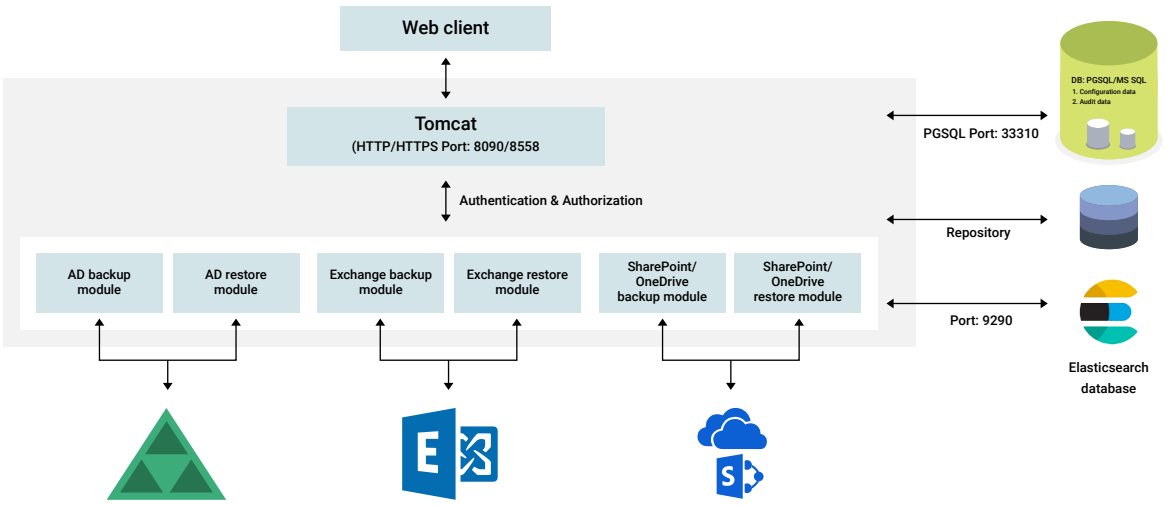
Table of Contents

1 Introduction

RecoveryManager Plus is a Windows Active Directory (AD), Office 365, and Exchange backup and restoration solution.

With RecoveryManager Plus, you can:

- Back up all AD objects such as users, groups, GPOs, OUs, computers, contacts, and dynamic distribution groups in your domain, and restore them to any previous version.
- Perform object-level and attribute-level restorations of AD objects.
- Back up all mailboxes in your Exchange (on-premises and Exchange Online) environment, and restore them when needed.
- Restore backups of on-premises Exchange mailboxes to a mailbox in an Exchange Online tenant and vice-versa.
- Back up all sites in your SharePoint Online and OneDrive for Business environment, and restore them when needed.
- Restore entire SharePoint Online and OneDrive for Business sites or just specific documents based on your need.



RecoveryManager Plus follows the client-server model and comes with a built-in PostgreSQL as its back-end database.

Client

The RecoveryManager Plus client can be accessed from a web browser by entering the IP address or computer name and port number of the RecoveryManager Plus server as the URL.

E.g., rmp-server:<portnumber> (or) 193.45.23.4:<portnumber>

Server

You can deploy RecoveryManager Plus in any Windows machine in your domain. Once the product is installed, it automatically discovers AD domains and Exchange servers. You can also manually add new domains and Exchange servers to the product.

You will need to manually add your Office 365 tenants.

Database

By default, RecoveryManager Plus comes bundled with a PostgreSQL database that stores all configuration information. However, you have the option to migrate to an external MS SQL database if you prefer. To ensure security, the database is password protected, and users' sensitive information is encrypted using the bcrypt algorithm. You can configure regular (daily, weekly, or monthly) back ups of your PostgreSL/MS SQL database to avoid data loss.

RecoveryManager Plus stores AD backup data in the Elasticsearch database that comes bundled with the product. The Elasticsearch database is secured with TLS encryption at REST and in the transport layer. You can also add additional Elasticsearch nodes to store your backup data at different locations.

RecoveryManager Plus stores the properties parsed from the backups of Exchange Online, SharePoint Online, OneDrive for Business, and on-premises Exchange in the Elasticsearch database that comes bundled with the product.

Client-server communication

RecoveryManager Plus authenticates the user who initiates the action; then it authorizes the action and makes the desired change in AD domain controllers, Office 365 tenants, and Exchange mailboxes. The backup data goes through the product's processing server after which it's securely stored in the repository.

Technology stack

- The client side of the application is developed using Javascript, jQuery plugin, and Ember framework.
- The server-side framework is developed using Java, Native C, and C#.
- RecoveryManager Plus uses JDBC (Java Database Connectivity) to connect to PgSQL and MS SQL databases.
- It also allows servers to communicate using the HTTP/HTTPS protocol.

Protocol and port	Usage	Type of traffic
TCP and UDP 389	Directory, replication, user and computer authentication, Group Policy, trusts	LDAP
TCP and UDP 88	User and computer authentication, forest-level trust	Kerberos
TCP and UDP 445	Replication, users and computer authentication, Group Policy, trusts	NTLM
TCP and UDP 464	Replication, user and computer authentication, trusts	Kerberos change/set password
UDP 137,138 and TCP 139	User and computer authentication	Netlogon, NetBios
TCP 33310	If you are running Recovery Manager Plus with Postgres DB	Postgres database
TCP/IP 1433 and 1434 UDP	If you are running Recovery Manager Plus with MSSQL DB	MSSQL database
TCP 135 and dynamic ports	Timezone offset of domain controller	WMI
TCP 5985 and TCP 5986	Group Policy	PowerShell remoting
HTTP port: 9290	Communication between the local Elasticsearch node and RecoveryManager Plus	Elasticsearch database
TCP port range: 9390	Communication between multiple Elasticsearch nodes	Elasticsearch database

2 Login process

The technician or administrator must log in to the application to perform management actions, generate reports, and delegate tasks.

The product has three built-in technician roles:

- Admin
- Operator
- Auditor

As technicians, you can configure any number of AD user accounts. Other than the default admin role, all roles can be modified or removed. You can delegate technician roles to AD users or to AD groups. Delegating a role to an AD group results in all group members receiving permissions to perform the tasks defined in that role. This delegation is non-intrusive; that is, this delegation empowers technicians to perform the necessary AD operations without actually elevating their rights in Active Directory.

When technicians log in, the tool:

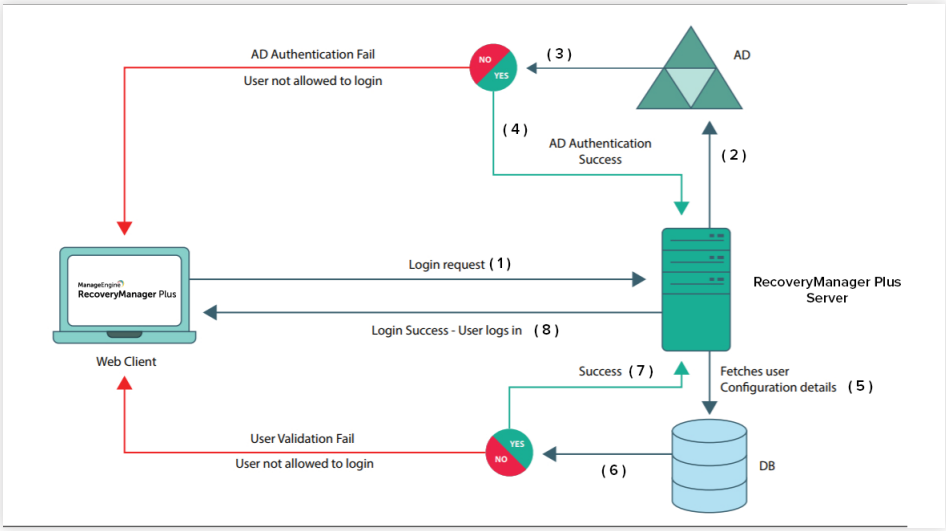
1. Performs Active Directory-based authentication.
2. Validates account details with the details in the RecoveryManager Plus's configuration database (PostgreSQL/MS SQL).
3. Authorizes them.

2.1. Authentication

Users can log in using their domain credentials. RecoveryManager Plus will perform LDAP* binding with the configured DC using ADsOpenObject API.

During this authentication, the tool will validate the password with the domain controller, and check to see if the account is expired, locked out, or disabled in AD—or if its password has expired. If so, the binding will fail and the tool will not allow login.

*LDAP binding is only done for AD users. The built-in technicians will be authenticated using the information in the database.



2.2 Technician validation

When a user account is configured as a technician, information such as technician name, AD account status, role, and privileges are stored in the product's database. Once AD authentication is successful, user account information will be validated with this configuration. If there is no configuration* available, the user will not be allowed to log in.

*For group-based delegation, user configuration happens during the login process.

2.3. Authorization

In this step, the tool will fetch the delegated roles and domains from the configuration details stored in the database, assign them to technicians, and create sessions in browsers for technicians.

3 Delegation

3.1 Roles

RecoveryManager Plus offers predefined roles that can be assigned to users who do not need full administrative privileges. When users are set as technicians, they are provided the rights to configure specific areas of the application and perform certain basic tasks relating to your AD and Exchange backup. A user can be configured as a technician for a single domain or multiple domains.

You can create a single technician or multiple technicians in one-go. Each technician has a unique login ID. Every action that can be performed by a technician has an ActionID assigned to it. Every time a technician performs an action, the ActionID is mapped to the technician and recorded. You can view the list of all actions performed by any technician in the admin audit report.

3.2 Service account

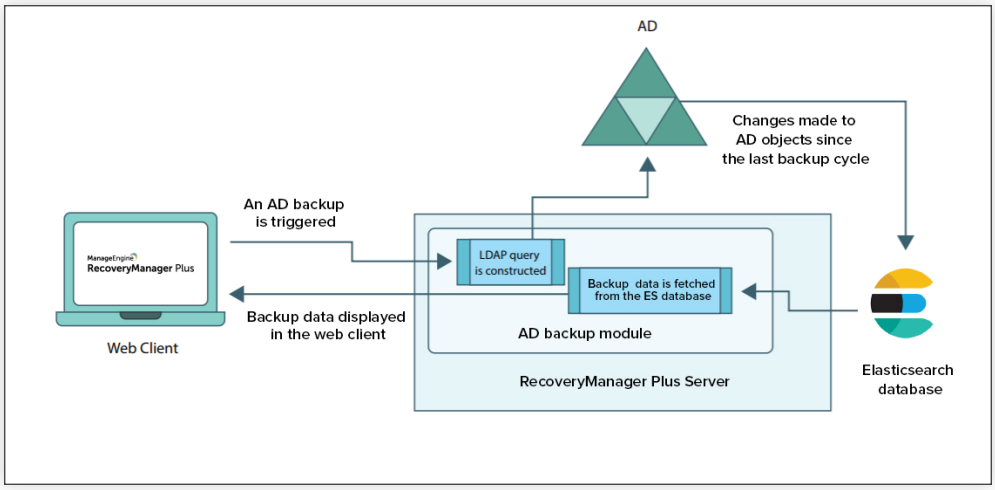
Once you log in to RecoveryManager Plus, you can add AD domains in the Domain Settings section. You can either use an account that belongs to the Domain Admins group (recommended) or a service account that has been assigned all the privileges required by the product. The credentials you provide while configuring the AD domain in the Domain Settings section are encrypted using the bcrypt algorithm and stored in the database.

4 Modules

4.1 Active Directory backup

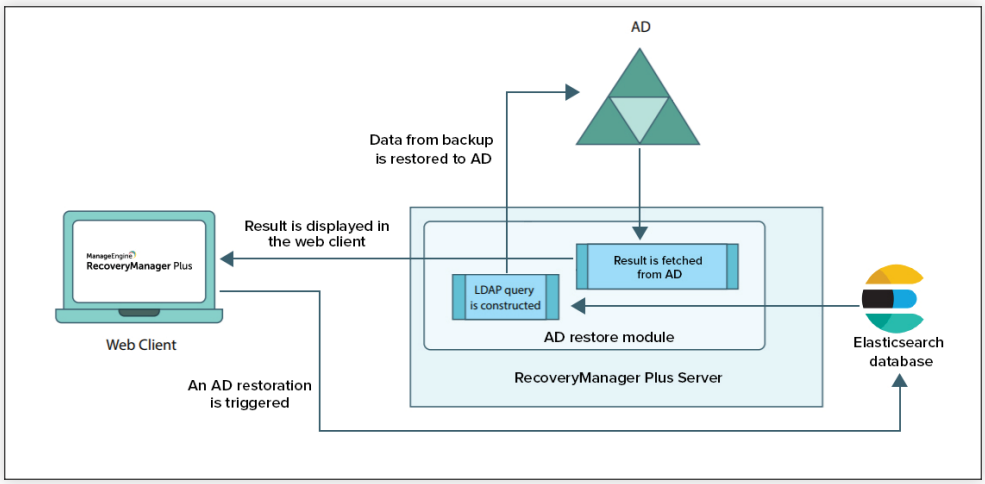
RecoveryManager Plus backs up all AD objects in your domain, such as users, groups, GPOs, OUs, computers, and contacts. Besides these, the product also backs up other critical information like Exchange attributes and group membership information of users.

When an AD backup is triggered, the web client sends the input to the server via HTTP/HTTPS. Based on this input, an LDAP query will be constructed. The LDAP query is executed in Active Directory, and all the changes made to AD objects since the last backup cycle are identified. These values are then stored in the Elasticsearch database. The tool will then display the list of all backed up objects in the UI.



4.2 Active Directory recovery

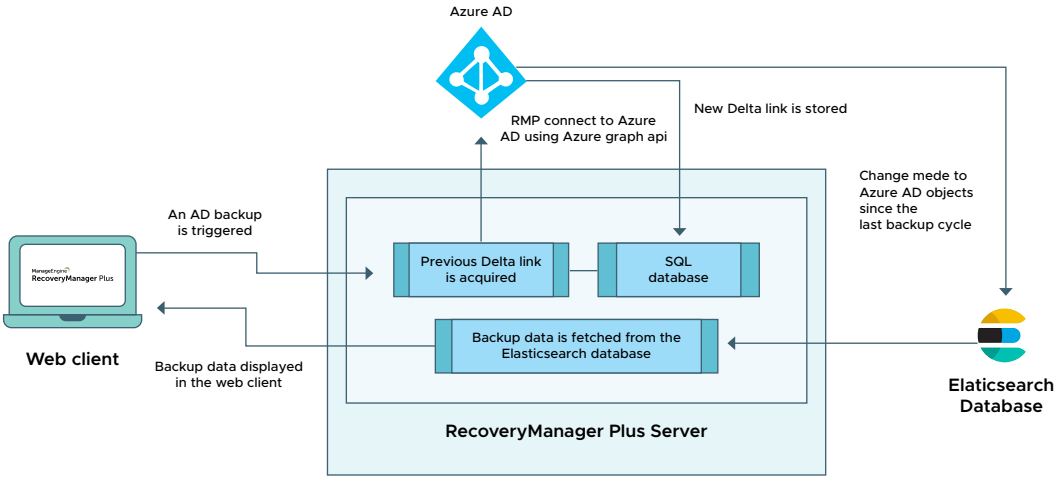
When any recovery action is triggered by the administrator, an LDAP query is generated and the RecoveryManager Plus server fetches the data to be restored from the Elasticsearch database. This value is then restored to AD, and the result is displayed in the UI.



4.3 Azure Active Directory Backup

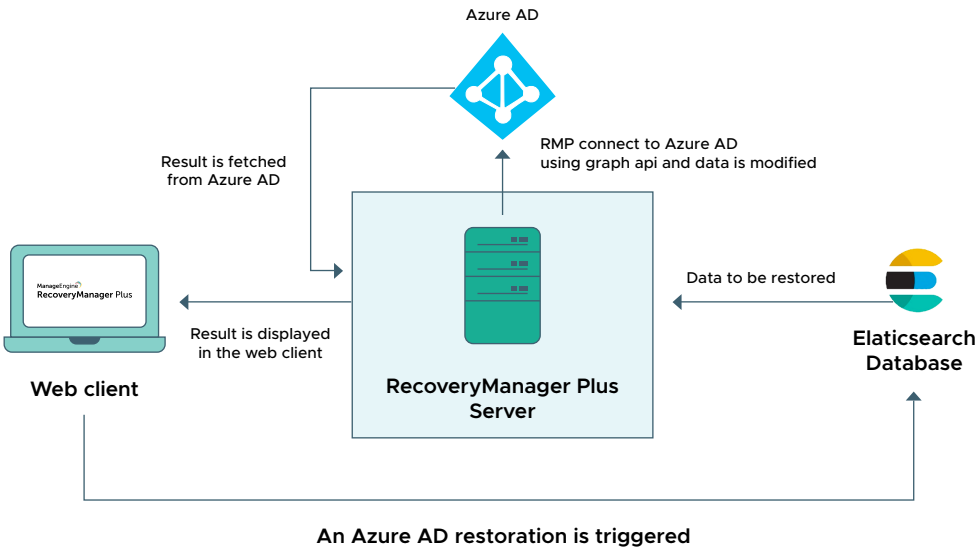
RecoveryManager Plus backs up all Azure AD objects in your tenant, including users, groups, devices, applications, service principles, directory roles, subscribed SKUs, and domains.

When an Azure AD backup is triggered, the web client sends the input to the server via HTTP/HTTPS. The Delta Link from the previous backup is fetched from the SQL database. RecoveryManager Plus then connects to Azure AD through the Azure Graph API and fetches the data modified since the last backup cycle. All changes made to Azure AD objects since the last Delta link are backed up and stored in the backup repository. A new Delta link is generated and stored in the SQL database to be used for the next backup cycle. The backup stored in the repository is fetched and displayed in the web client.



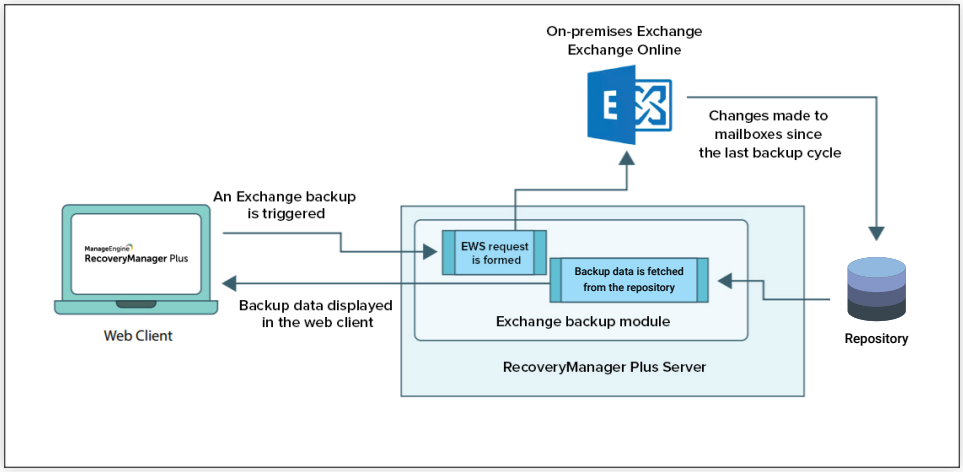
4.4 Azure Active Directory Recovery

When any recovery action is triggered by the administrator, RecoveryManager Plus fetches the data to be restored from the Elasticsearch database. RecoveryManager Plus connects to the Azure AD through the Azure Graph API and the values are restored to Azure AD. The result is then displayed in the UI.



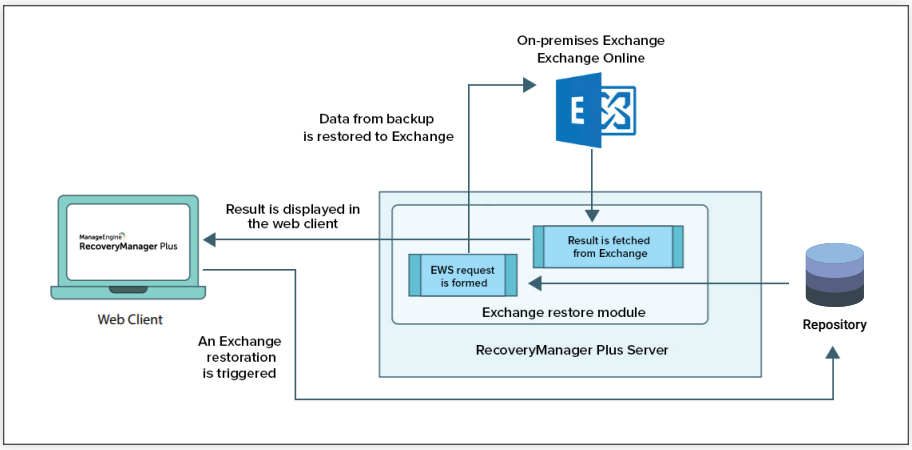
4.5 Exchange backup

When a backup is initiated for an on-premises Exchange Server mailbox or an Exchange Online mailbox, an EWS request is created with the mailbox's SMTP address, folder ID, and sync state information. This EWS request identifies the items in the mailbox that have been created, modified, and deleted since the last backup cycle. Then, the binary data and properties of those items are extracted and stored in the repository. Once the backup process is complete, the result of the backup operation is displayed on the product dashboard. The backed-up data can be viewed from the Exchange restore page.



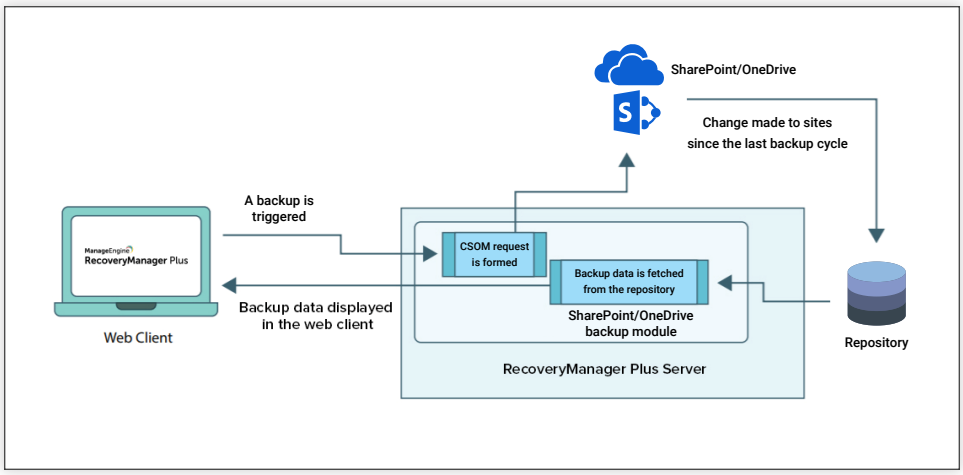
4.6 Exchange recovery

When restoration of a mailbox item is triggered, the binary value is obtained from the repository, and an EWS request is created with the mailbox's SMTP address and folder ID. The backup data is then restored to the mailbox and folder as specified in the EWS request, and the result is displayed on the product dashboard and the restore history page.



4.7 SharePoint Online/OneDrive for Business backup

When a backup is initiated for a SharePoint Online or OneDrive for Business site, a Client Side Object Model (CSOM) request is created with the site's URL and change token information. This CSOM request identifies items in the SharePoint Online or OneDrive for Business sites that have been created, modified, and deleted since the last backup cycle. Then, the binary data and properties of those items are extracted and stored in the repository. Once the backup process is complete, the backed-up data can be viewed from the SharePoint/OneDrive restore page.

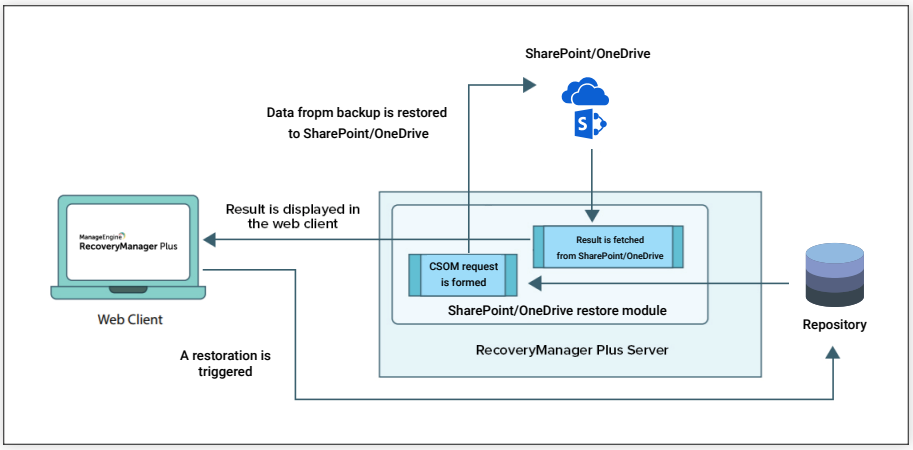


4.8 SharePoint Online/OneDrive for Business recovery

When restoration of a SharePoint Online or OneDrive for Business site item is triggered, the binary value is obtained from the repository. Once the binary value has been retrieved, the product will perform the following steps:

- If a new subsite has to be created, a CSOM request is created for that subsite. This is only applicable for SharePoint Online restoration and not for restoring OneDrive for Business sites.
- The metadata of the site and lists contained in the site will be restored.
- List items will be created or updated in the target lists based on the choice made during restoration.

Once the restoration is complete, the result is displayed on the product dashboard and the restore history page.



5 Security measures against vulnerabilities

5.1 SQL injection

A successful SQL injection exploit can read sensitive data from the product's database, modify data, execute administrative operations on the database (such as shutdown of the DBMS), and recover the content of a given file on the DBMS file system. In some cases, it can also issue commands to the operating system.

Sample SQL injection code:

```
username = request.getParameter("username"); password =
request.getParameter("userpass"); sql = "SELECT * FROM Users
WHERE Name ='" + username + "' AND Pass ='" + password + "'";
```

How RecoveryManager Plus handles SQL injections:

code (the intention of the operation) before passing each parameter to the query. This allows the database to distinguish between code and data, regardless of the user input. Prepared statements ensure that SQL commands inserted by an attacker do not change the intent of a query.

For example, if an attacker were to enter the password abc123 or '1'='1', the parameterized query wouldn't be vulnerable; it would instead look for a username which literally matched the entire string abc123 or '1'='1'.

Example code

Since SQL recognizes that it is a parameter, it'll escape any control characters that the attacker might try to inject.

```
username = getRequestString("username"); password =
getRequestString("password"); sql = "SELECT * FROM Users WHERE Name = ?
AND Pass = ? "; PreparedStatement pstmt = connection.prepareStatement( sql
); pstmt.setString( 1, username ); pstmt.setString( 2, password ); try { ResultSet
results = pstmt.execute( ); }
```

6 Confidentiality

RecoveryManager Plus employs the following measures to uphold the confidentiality of user data:

- By default, the backup database is password protected.
- Only authorized users can carry out operations in the product.
- No user details are exposed without authorization.

7 Integrity

The data displayed in the product's dashboard is fetched from the Elasticsearch database. The application interacts with your Active Directory and Exchange environments only when a backup or restoration is carried out. The dashboard is also updated only when a backup or a restoration operation has been carried out. The product application does not modify any data.

8 Accountability

Audit logs hold the details of all AD and Exchange backup and restoration activities performed by admins and technicians. Every action is recorded; this includes mailbox item restorations, AD attribute restorations, and even changes made to the backup settings. Audit reports provide details such as what action was performed on which object, the technician who performed that action, the time at which it was performed, and the status of the action.

The audit reports will display the following information for every operation:

- Name of the technician who performed the task
- Action name (example: adding a new tenant, exporting to PST)

STEP 3 Associate the certificate with RecoveryManager Plus

1. Copy the '.keystore' file from the <installation_directory>\ManageEngine\ RecoveryManager Plus\jre\bin location and paste it at the <installation_directory> \ManageEngine\RecoveryManager Plus\conf location.
2. At the <installation_directory>\ManageEngine\RecoveryManager Plus\conf location, locate the 'server.xml' file and take a backup of that file.
3. Open the server.xml file using an editor and navigate to the last connector tag.
4. Replace the value of the keystore file with the location of your keystore ('./conf/<keystore_name>.keystore).
5. Replace the value of the 'keystorePass' with the password given during keystore creation.
6. Save the server.xml file and start RecoveryManager Plus (Start → All Programs → RecoveryManager Plus → Start RecoveryManager Plus).
7. Once the RecoveryManager Plus service has started, launch the RecoveryManager Plus client.

Click here to download a guide on how to install an SSL certificate in RecoveryManager Plus.