ManageEngine
RecoveryManager Plus

RecoveryManager Plus

Architecture

www.recoverymanagerplus.com

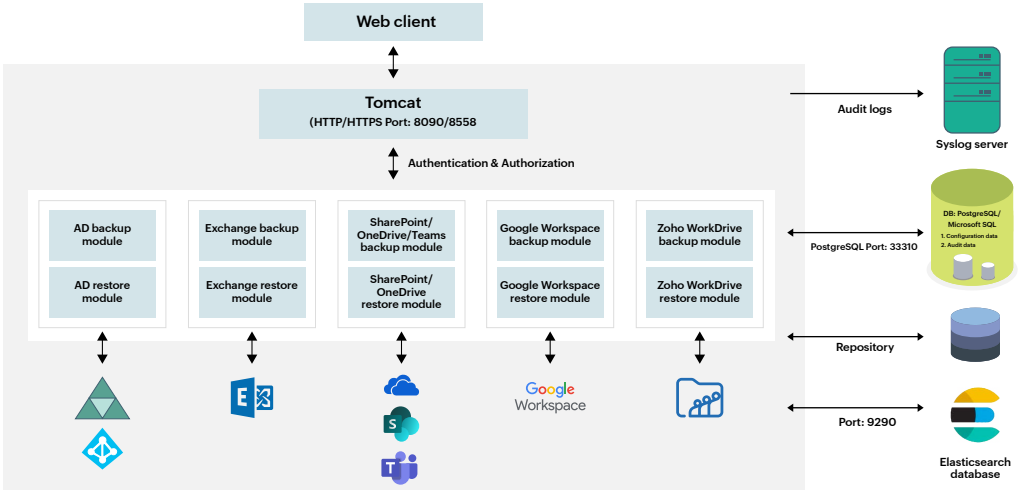
Table of Contents

1 Introduction

RecoveryManager Plus is an enterprise backup and recovery solution that supports applications like Active Directory (AD), Microsoft Entra ID (formerly Azure AD), Microsoft 365 (SharePoint Online, OneDrive for Business, and Microsoft Teams), Google Workspace, on-premises Exchange, and Zoho WorkDrive.

With RecoveryManager Plus, you can:

- Back up all domain controllers and restore them to any previous state.
- 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 and restore all SharePoint Online site collections, sites, lists, and document libraries.
- Back up and restore all files and folders in your OneDrive for Business environment.
- Back up and download all Microsoft Team sites, channels, and posts.
- Restore the entire SharePoint Online and OneDrive for Business sites or just specific documents based on your needs.
- Restore all list items in Microsoft Team sites to a backed-up state.
- Back up all mailboxes and user drives in your Google Workspace environment, and restore them when needed.
- Restore entire mailboxes and user drives or specific mails and documents based on your needs.
- Back up all the Team Folders data in your Zoho WorkDrive environment, including all folders, subfolders, and files.
- Restore an entire folder or even a single file from WorkDrive backups to any of its backed-up versions.



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

1.1 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>

1.2 Server

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

You will need to manually add your Microsoft 365 tenants, Google Workspace domains, and Zoho WorkDrive teams.

1.3 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 Microsoft 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) backups of your PostgreSQL/Microsoft SQL database to avoid data loss.
RecoveryManager Plus stores AD and Entra ID 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, Microsoft Teams, Google Workspace, on-premises Exchange, and Zoho WorkDrive in the Elasticsearch database that comes bundled with the product.

RecoveryManager Plus allows you to store your Active Directory, Microsoft Entra ID, Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups in local storage, NAS, and cloud repositories such as Azure Blob Storage, Azure Files, AWS, and Wasabi.
Additionally, you can store backups in an immutable format in Azure Blob Storage, AWS, and Wasabi to ensure against ransomware attacks and prevent unauthorized modifications or deletions.

RecoveryManager Plus stores all backup, recovery, and configuration audit logs in the database for auditing and compliance purposes. When integrated with a syslog server, the product ensures that each newly generated log is simultaneously stored in the database and forwarded to the syslog server. This enables centralized monitoring, simplifies log management, and enhances security visibility across your environment.

1.4 Client-server communication

RecoveryManager Plus authenticates the user who initiates the action; it then authorizes the action and makes the desired change in the AD domain controllers, Entra ID tenants, Exchange Online mailboxes, SharePoint Online, OneDrive for Business, Microsoft Teams sites, Google Workspace accounts, on-premises Exchange mailboxes, and Zoho WorkDrive teams. The backup data is then processed in the product and stored securely in the repository.

1.5 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 Java Database Connectivity (JDBC) to connect to PostgreSQL and Microsoft 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 database	Postgres database
TCP/IP 1433 and 1434 UDP	If you are running Recovery Manager Plus with Microsoft SQL database	Microsoft SQL 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

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 a technician, 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 orAD 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:

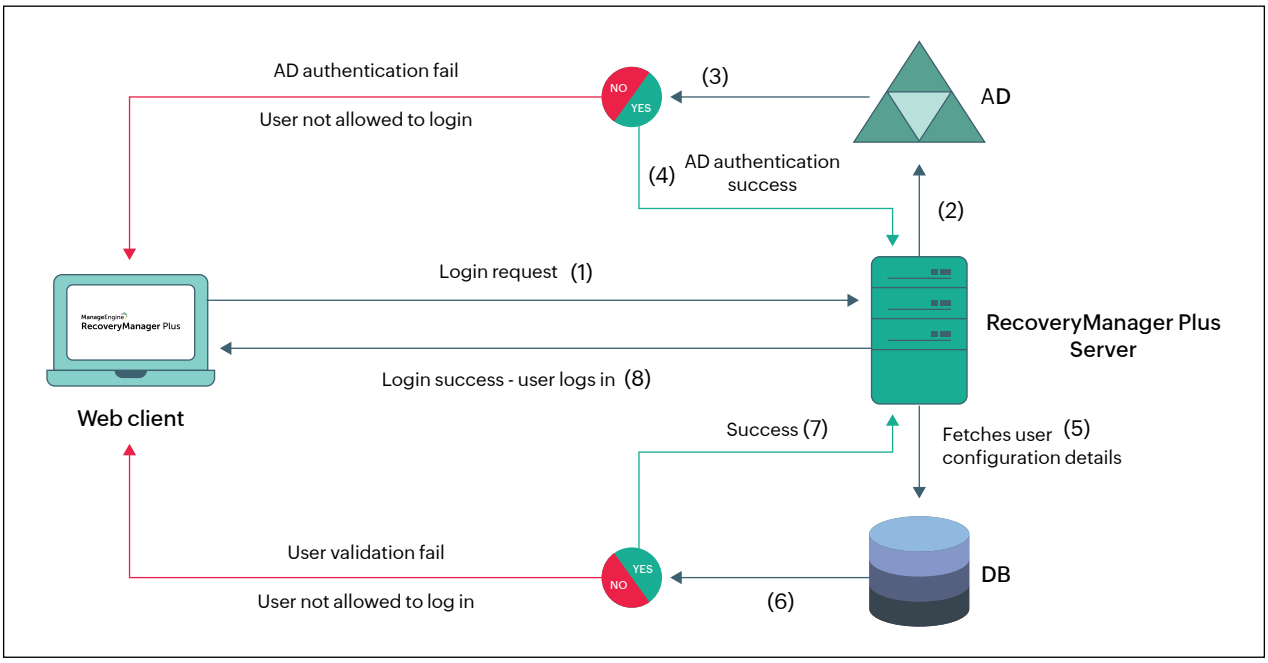
1. Performs Active Directory-based authentication.
2. Validates account details with the details in the RecoveryManager Plus' configuration database (PostgreSQL/Microsoft SQL).
3. Authorizes them.

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, Entra ID, Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Google Workspace, on-premises Exchange, and Zoho WorkDrive backups. 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.

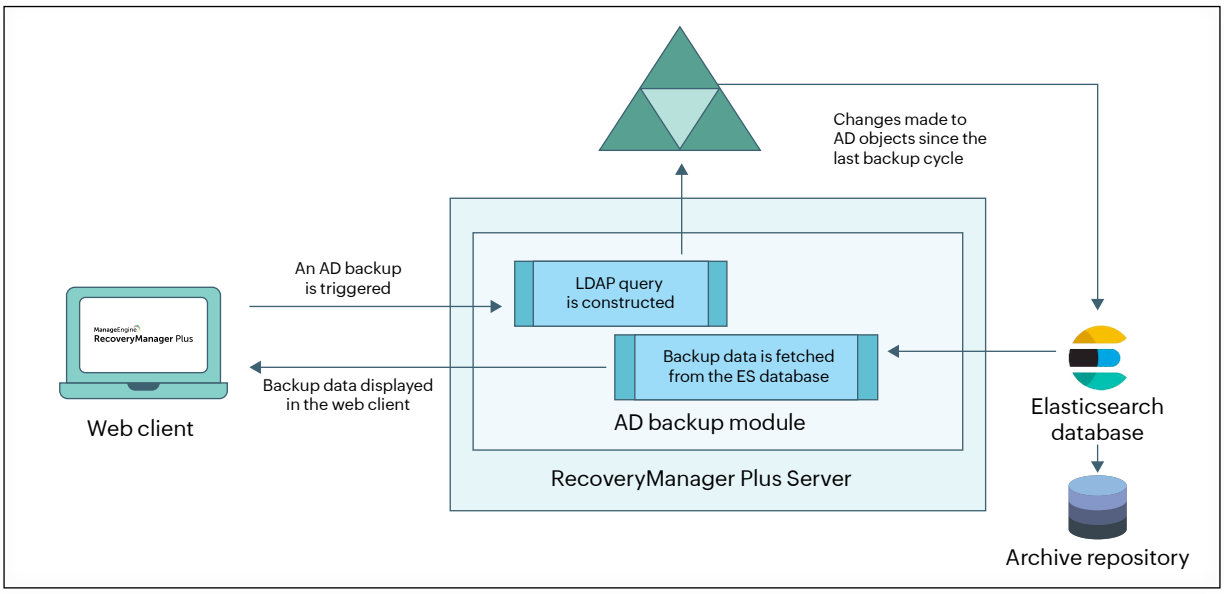
4 Modules

4.1. AD backup and recovery

RecoveryManager Plus backs up all AD objects in your domain, such as users, groups, GPOs, OUs, computers, contacts, and other critical information like Exchange attributes and users' group membership information. In addition, the product backs up domain controllers and lets you restore them to any previous state.

4.1.1. AD object backup

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 AD, and all the changes made to AD objects since the last backup cycle are identified. These values are indexed and stored in the product's built-in Elasticsearch repository. The tool then displays the list of all the backed-up objects in the UI.

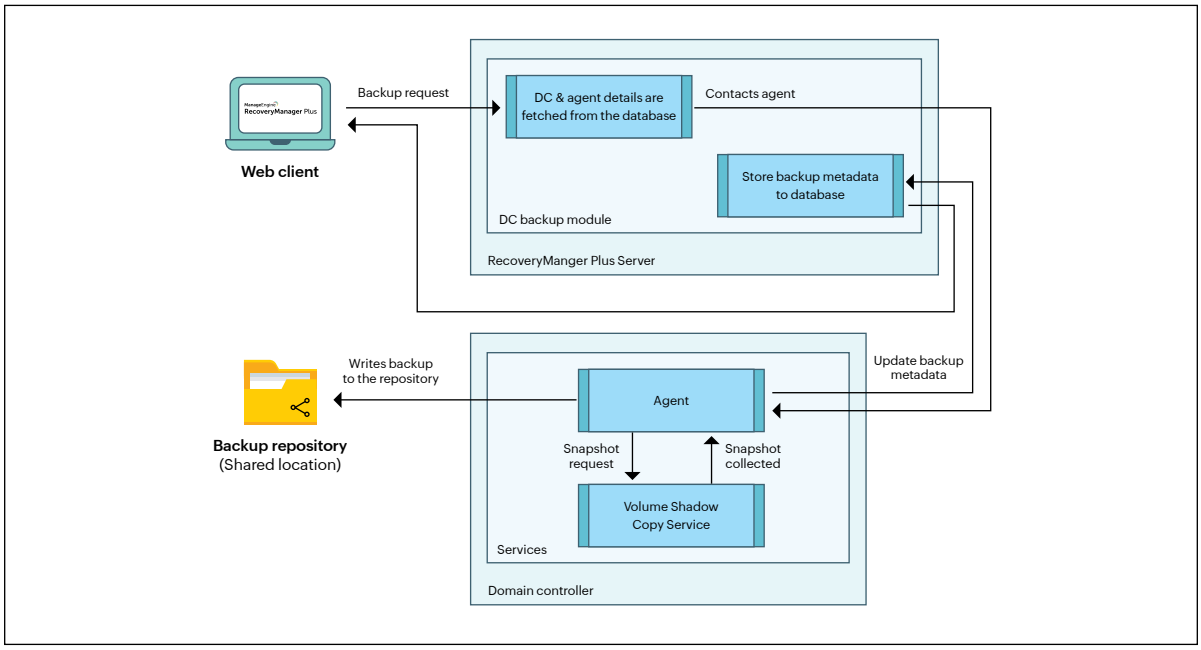


Storing all backed up data in Elasticsearch is not always ideal since it might cause performance issues. RecoveryManager Plus offers the flexibility to store older backed up data in an archive repository, and re-index it as needed for restoration. Archived backups can be stored in local, shared, NAS, or cloud repositories.

After a backup is completed, RecoveryManager Plus identifies backups that have exceeded the index period, de-indexes them, and moves them to the archive repository. The data remains in the archive repository until it surpasses the archive retention period, at which point it is permanently deleted.

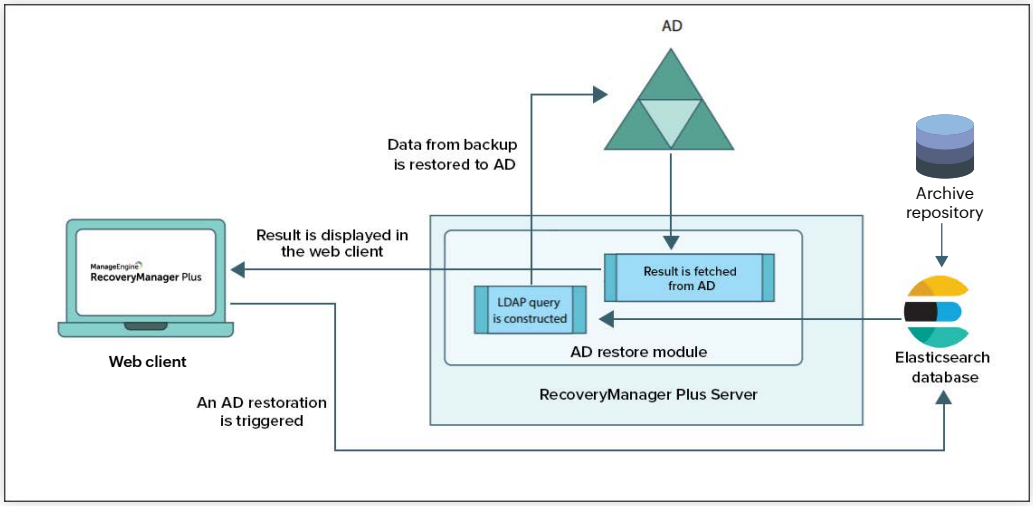
4.1.2. AD domain controller backup

When a domain controller backup is initiated, an agent is installed on the domain controller. The RecoveryManager Plus server sends the backup request to the agent on the domain controller. Using the native Windows Server OS service, Volume Shadow Copy Service, the agent takes complete snapshots of the domain controllers. It then writes them to the backup repository.



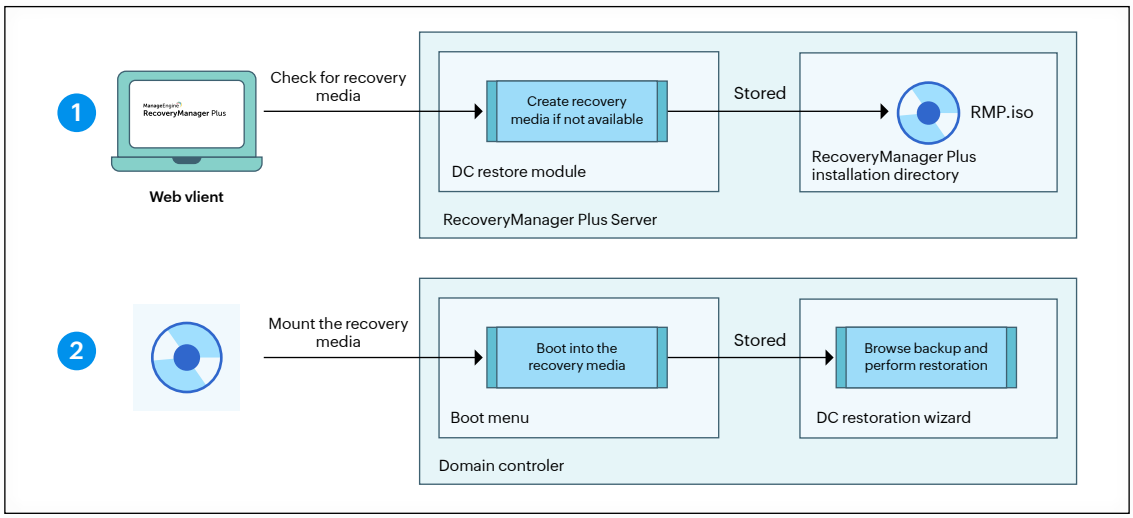
4.1.3. AD object recovery

When a recovery action is initiated, the administrator first begins by searching the Elasticsearch database for the data to be restored. If the data is not found, it must be retrieved from the archive repository and re-indexed to the Elasticsearch database for restoration. When the data is found in the Elasticsearch database, an LDAP query is generated, allowing RecoveryManager Plus to fetch the data. This value is then restored to AD, and the result is displayed in the UI.



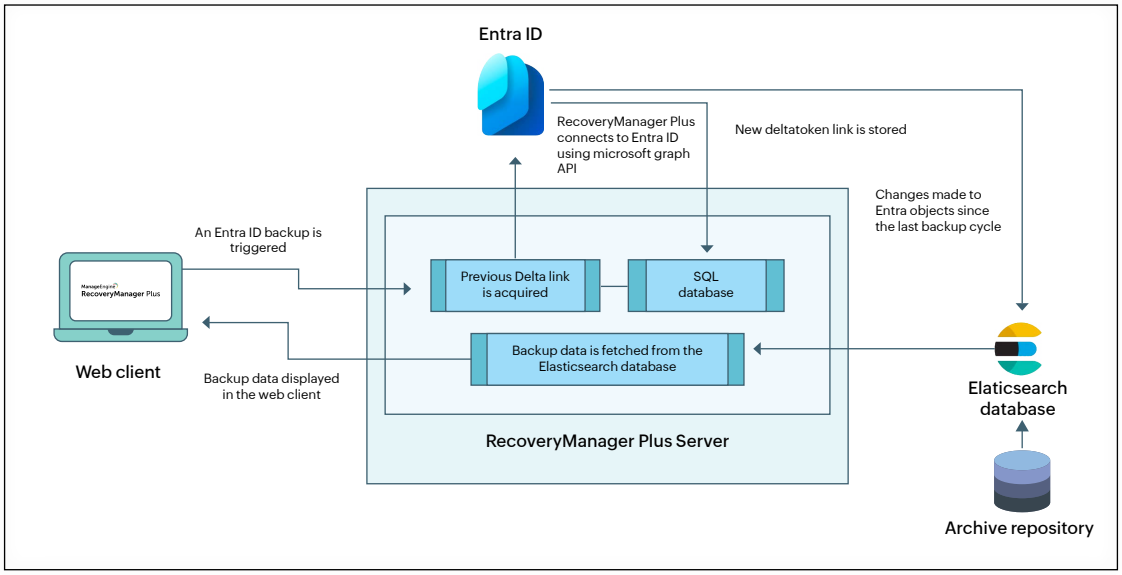
4.1.4. AD domain controller recovery

When you wish to restore a domain controller, RecoveryManager Plus creates recovery media during the initial backup, which can be used for subsequent backups. If the recovery media is available, the domain controller has to be booted using the recovery media created. The Domain Controller Restoration Wizard then starts. Enter the backup location and the credentials for accessing the network location in the wizard. Confirm the provided details within the wizard to proceed with the restoration process.



4.2. Microsoft Entra ID backup

RecoveryManager Plus backs up all Entra ID objects in your tenant, including users, groups, devices, applications, service principals, directory roles, subscribed SKUs, and domains. When an Entra ID backup is triggered, the web client sends the input to the server via HTTP/HTTPS. The deltatoken from the previous backup is fetched from the SQL database. RecoveryManager Plus then connects to Entra ID through the Microsoft Graph API and fetches the data modified since the last backup cycle. All changes made to Entra ID objects since the last deltatoken are indexed and stored in the product's built-in Elasticsearch repository. A new deltatoken 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.

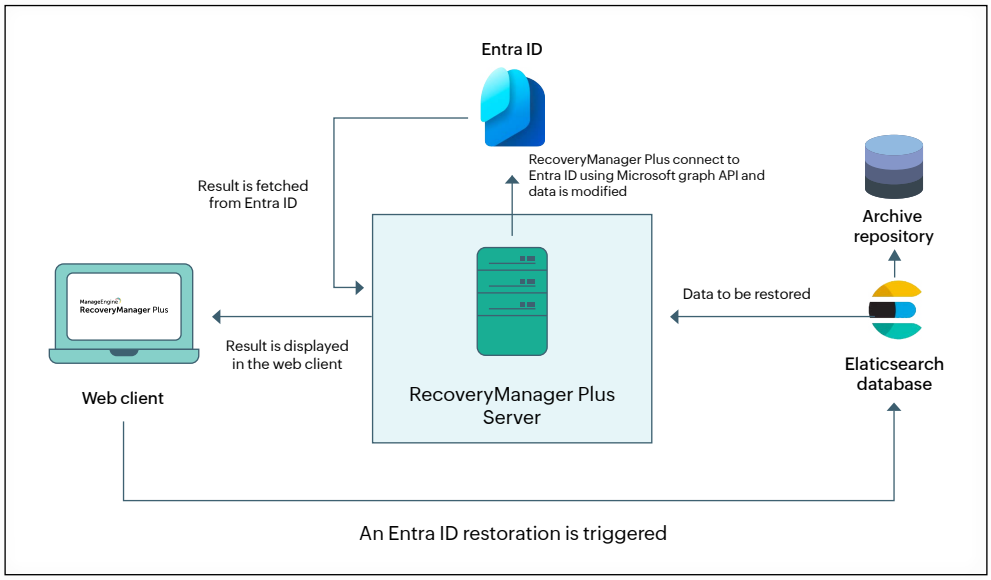


Storing all backed up data in Elasticsearch is not always ideal since it might cause performance issues. RecoveryManager Plus offers the flexibility to store older backed up data in an archive repository and re-index it as needed for restoration. Archived backups can be stored in local, shared, NAS, or cloud repositories.

After a backup is completed, RecoveryManager Plus identifies backups that have exceeded the index period, de-indexes them, and moves them to the archive repository. The data remains in the archive repository until it surpasses the archive retention period, at which point it is permanently deleted.

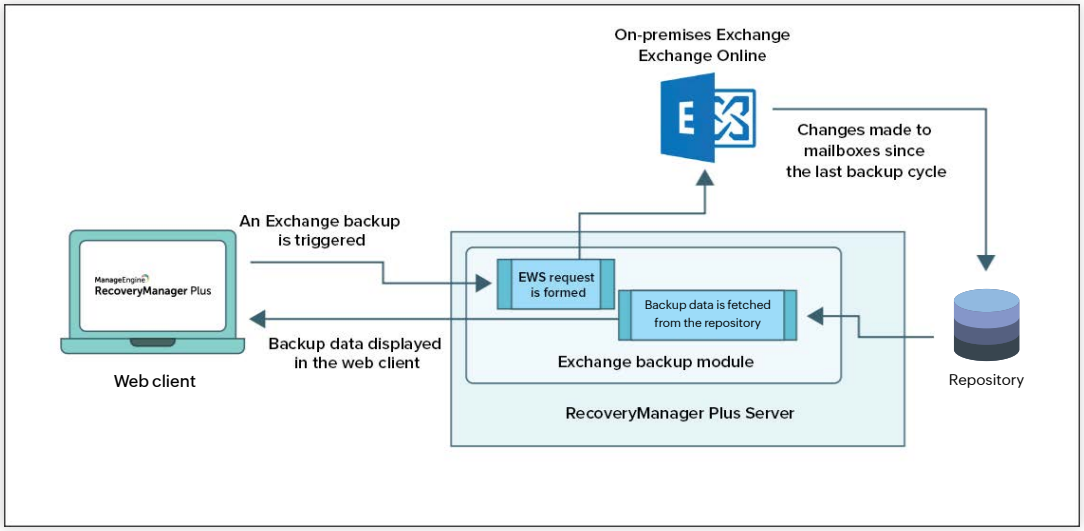
4.3. Microsoft Entra ID recovery

When a recovery action is initiated, the administrator first begins by searching the Elasticsearch database for the data to be restored. If the data is not found, it must be retrieved from the archive repository and re-indexed to the Elasticsearch database for restoration. When the data is found in the Elasticsearch database, RecoveryManager Plus then connects to Entra ID through the Microsoft Graph API, and the values are restored to Entra ID. The result is then displayed in the UI.



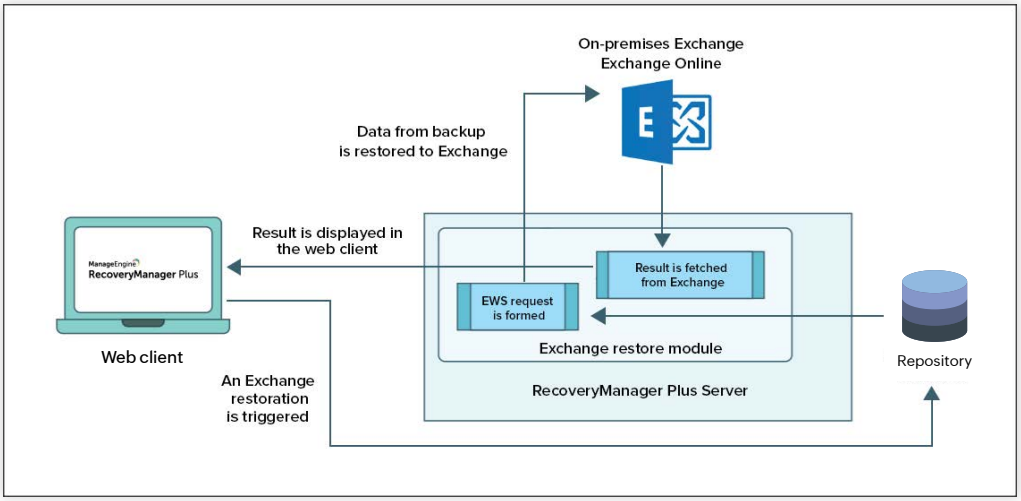
4.4. Exchange backup

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.



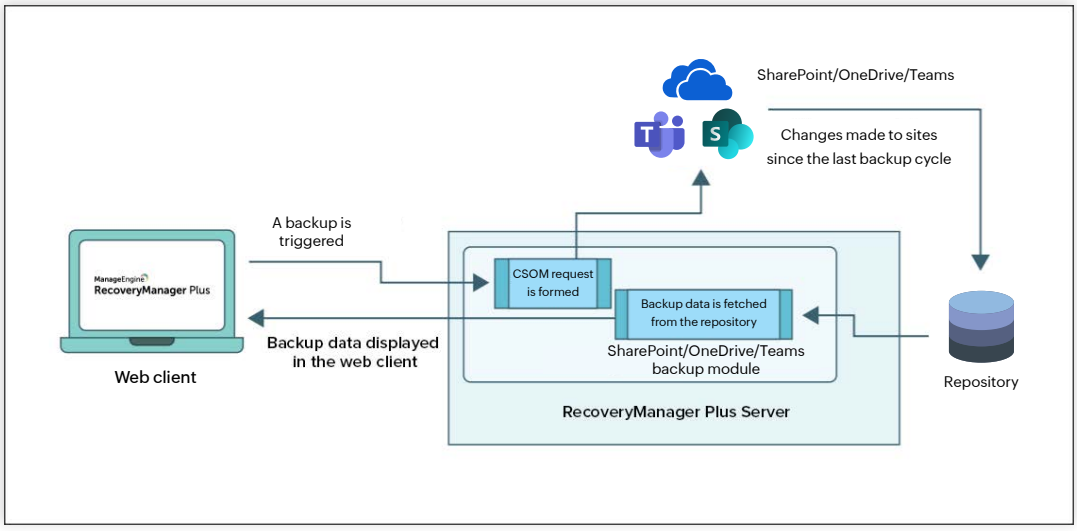
4.5. Exchange recovery

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.



4.6. SharePoint Online, OneDrive for Business, and Microsoft Teams backup

When a backup is initiated for a SharePoint Online, OneDrive for Business, or Microsoft Teams 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, OneDrive for Business, or Microsoft Teams 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.

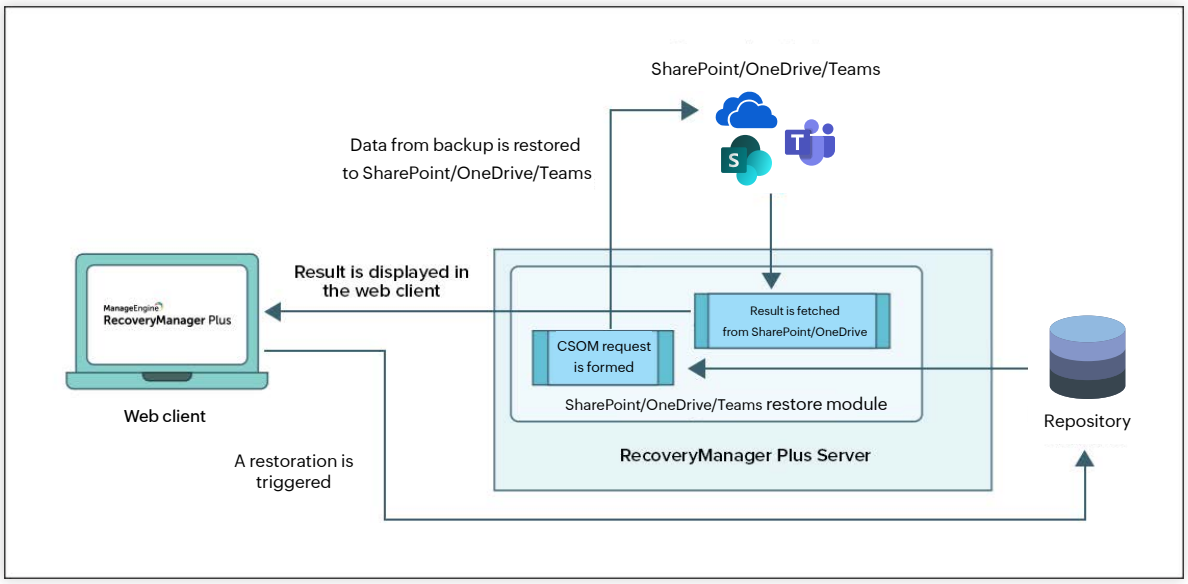


4.7. SharePoint Online, OneDrive for Business, and Microsoft Teams recovery

When restoration of a SharePoint Online, OneDrive for Business, or Microsoft Teams 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:

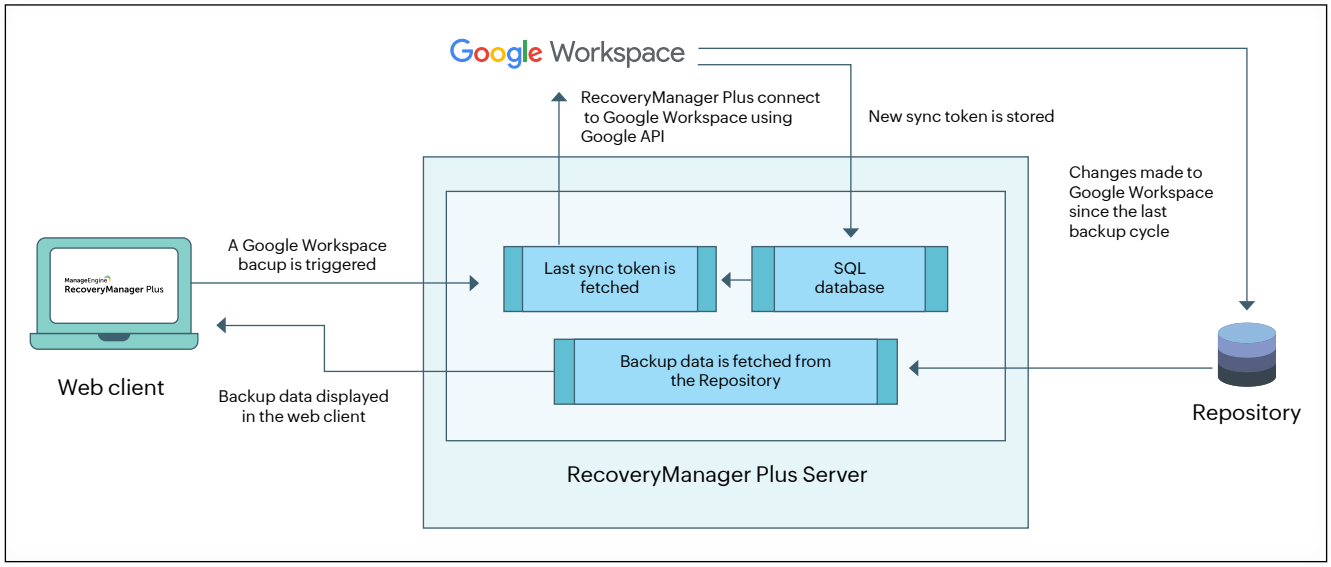
- If a new subsite has to be created, a CSOM request is created for that subsite. This is only applicable for SharePoint Online restoration and not for restoring OneDrive for Business sites.
- The metadata of the site and lists contained in the site will be restored.
- List items will be created or updated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



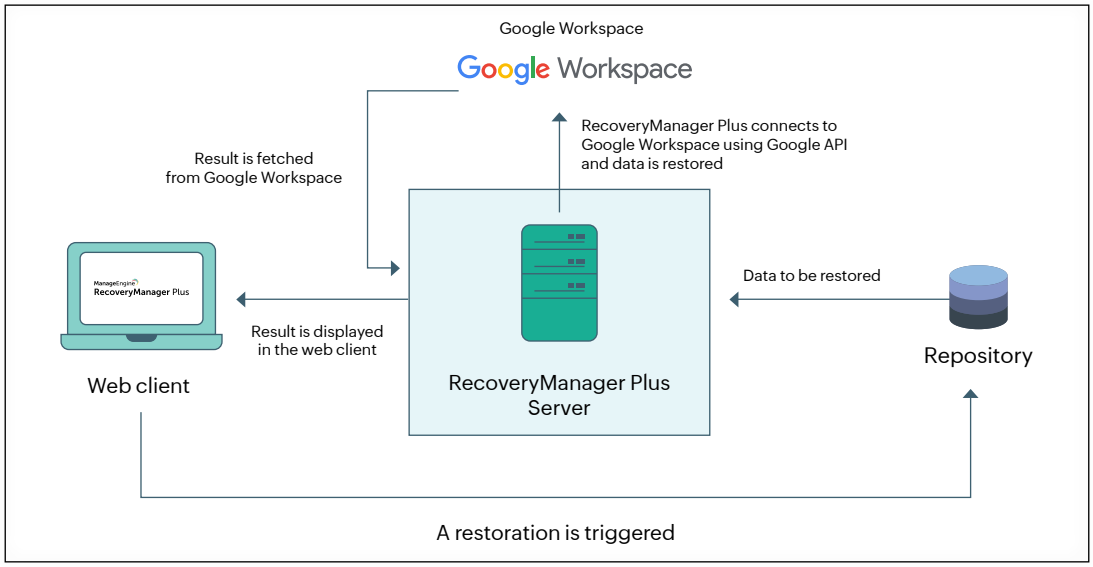
4.8. Google Workspace backup

When a backup is initiated for Google Workspace, the web client sends the input to the server via HTTPS, which is handled by the Google API services. RecoveryManager Plus fetches the sync token from the previous backup to identify the data modified since the last backup cycle. All changes made are backed up and stored in the backup repository. A new sync token 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.



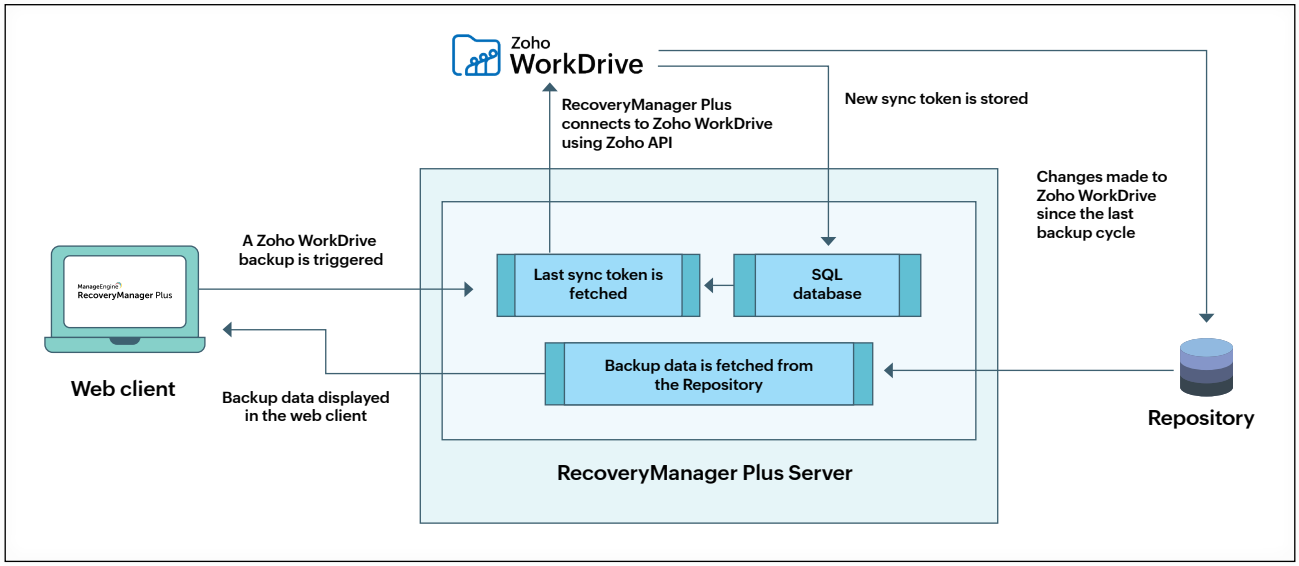
4.9. Google Workspace recovery

When any recovery action is triggered by the administrator, RecoveryManager Plus fetches the data to be restored (objectID, userID, and binary file information) from the Repository. RecoveryManager Plus uses the binary file information to restore the data. RecoveryManager Plus connects to Google Workspace through Google API services, and the objectID and userID information is used to perform the restoration. The result is displayed on the product dashboard and the Restore History tab.



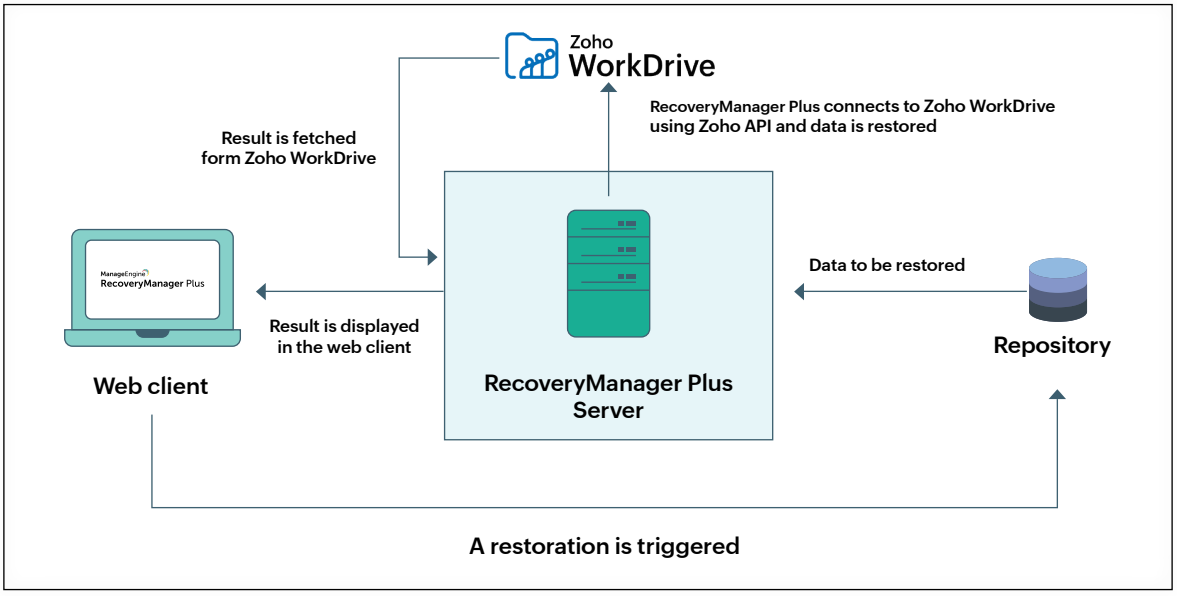
4.10. Zoho WorkDrive backup

When a backup is initiated for Zoho WorkDrive, the web client sends the input to the server via HTTPS, which is handled by the Zoho WorkDrive API services. RecoveryManager Plus fetches the sync token from the previous backup to identify the data modified since the last backup cycle. All the changes made are backed up and stored in the backup repository. A new sync token 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.



4.11. Zoho WorkDrive recovery

When any recovery action is triggered by the administrator, RecoveryManager Plus fetches the data to be restored (team, folder, permission, and binary file information) from the repository. RecoveryManager Plus uses the binary file information to restore the data. It connects to Zoho WorkDrive through Zoho WorkDrive API services, and the team, folder, and permission information is used to perform the restoration. The result is displayed on the product dashboard and the Operation History tab.



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'.

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

Example code

```
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 on the product's dashboard is fetched from the Elasticsearch database. The application interacts with your AD, Microsoft Entra ID, Exchange Online, Microsoft 365 (SharePoint Online, OneDrive for Business, and Microsoft Teams), Google Workspace, on-premises Exchange, and Zoho WorkDrive environments only when a backup or restoration is carried out. The dashboard is also updated only when a backup or restoration operation has been carried out. The product does not modify any data.

8 Accountability

Audit logs hold the details of all AD, Microsoft Entra ID, Exchange Online, Microsoft 365, Google Workspace, on-premises Exchange, and Zoho WorkDrive backup and restoration activities performed by admins and technicians. Every action is recorded; this includes AD and Entra ID attribute restorations, Exchange mailbox item restorations, SharePoint Online site restorations, OneDrive for Business and Microsoft Teams file restorations, Google Workspace file restorations, Zoho WorkDrive file 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, when it was performed, and its status.

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)
- Action category (example: backup, settings)
- Module in which the task was performed (example: Exchange)
- Action time
- Object name
- Status (the result of the task)

ManageEngine
RecoveryManager Plus

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

ADSelfService Plus | M365 Manager Plus

About RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive enterprise backup and recovery solution for Active Directory, Microsoft Entra ID, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams), Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies, backup immutability and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for minimizing downtime and ensuring seamless business continuity by backing up all application's data.

For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote Download