

Dell EMC PowerProtect Data Manager: Microsoft Exchange Backup and Recovery

Abstract

This white paper focuses on protecting a Microsoft® Exchange database using Dell EMC™ PowerProtect Data Manager, the next-generation data protection platform.

May 2021

Revisions

Date	Description
October 2020	Initial release
May 2021	Revised

Acknowledgments

Author: Sonali Dwivedi

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [5/6/2021] [Technical White Paper] [H18560]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	5
Audience	5
1 Overview.....	6
1.1.1 Protection storage	6
1.1.2 PowerProtect Data Manager	6
1.1.3 PowerProtect Data Manager agent service.....	6
1.1.4 Microsoft Exchange PowerShell interface for the application agent	7
1.1.5 SQLite database.....	7
1.1.6 Application Discovery Manager	7
1.1.7 Lockbox	7
1.1.8 Support for existing Microsoft application agent backups with Data Manager.....	8
2 Supported configurations	9
3 Installation and configuration of Microsoft application agent for Exchange Server	11
3.1 Prerequisites.....	11
3.2 Installation and configuration.....	12
3.3 User configuration: App Agent Exchange Admin Configuration tool.....	13
4 Microsoft application agent for Exchange database backup.....	15
4.1 Centralized backup.....	15
4.2 Federated backup of a DAG.....	16
4.3 Self-service backup	18
4.4 Parallelism for Microsoft application agent backup	19
4.5 Back up Exchange server with Microsoft application agent PowerShell backup cmdlet	19
4.5.1 Syntax to perform stand-alone server backups.....	20
4.5.2 Syntax to perform federated backup	20
4.5.3 Optional parameters for the Backup-Exchange cmdlet.....	21
5 Restoring Exchange Server databases.....	22
5.1 Prerequisite for Exchange Restore operation	22
5.2 Restore a backup to source database.....	22
5.3 Restore a backup to an alternate database	23
5.4 Granular level restores	23
5.4.1 Mount Backup.....	24

5.4.2	Managing mounted backups	25
5.4.3	Browse and recover granular-level data with ItemPoint for Microsoft Exchange Server	26
5.5	Granular level restores without Exchange Server	28
5.5.1	Prerequisites for granular level restores without Exchange Server	28
5.5.2	Command for granular level restores without Exchange Server	29
6	Replication and DD Cloud Tier	31
7	Disaster recovery of Exchange Server	34
7.1	Perform disaster recovery from the DD Cloud Tier	34
8	Conclusion	36
A	Technical support and resources	37
A.1	Related resources	37

Executive summary

Today's data protection is either too complex, requires multiple vendors, does not scale, or fails to meet the needs of fast-growing, modern, and agile organizations. As businesses continue to consume IT resources differently, there is a need for powerful, efficient, and trusted data protection. These solutions can enable organizations to transform and meet future demands when modernizing their IT environments.

Organizations strive to provide users with large mailboxes while reducing the requirements and complexity of their business-exchange backup data storage. With current trends, the user mailbox size is growing rapidly. This growth makes it more challenging, if not impossible, to back up all the business-exchange data within the nightly backup window.

Dell EMC™ PowerProtect software is the next-generation data management platform that transforms traditional data protection into comprehensive data management. PowerProtect software is defined with integrated deduplication for data protection, replication, and reuse.

This white paper outlines Microsoft® Exchange protection and recovery with PowerProtect software, which provides reliable and efficient data protection functionalities. The PowerProtect Microsoft application agent uses block-based backup technology to back up Exchange Server databases in stand-alone and database availability group (DAG) environments. This block-based technology tracks the changed blocks of the Exchange database and log files. A full backup backs up each selected Exchange database and its log files. An incremental backup backs up only the changed blocks.

Block-based backups are fast backups that have reduced backup times. This advantage is due to the way that the backup process respectively backs up only the occupied disk blocks and changed disk blocks of the Exchange database and log files. Block-based backups provide instant access to the backups.

Audience

This white paper is intended for customers, partners, and employees who want to better understand, evaluate, and explore Dell EMC PowerProtect Data Manager for Exchange server backup and recovery.

1 Overview

The Microsoft application agent enables an application administrator to protect and recover Exchange application data on the application host. Data Manager integrates with the Microsoft application agent to check and monitor backup compliance against protection policies. Data Manager also enables centralized scheduling for backups.

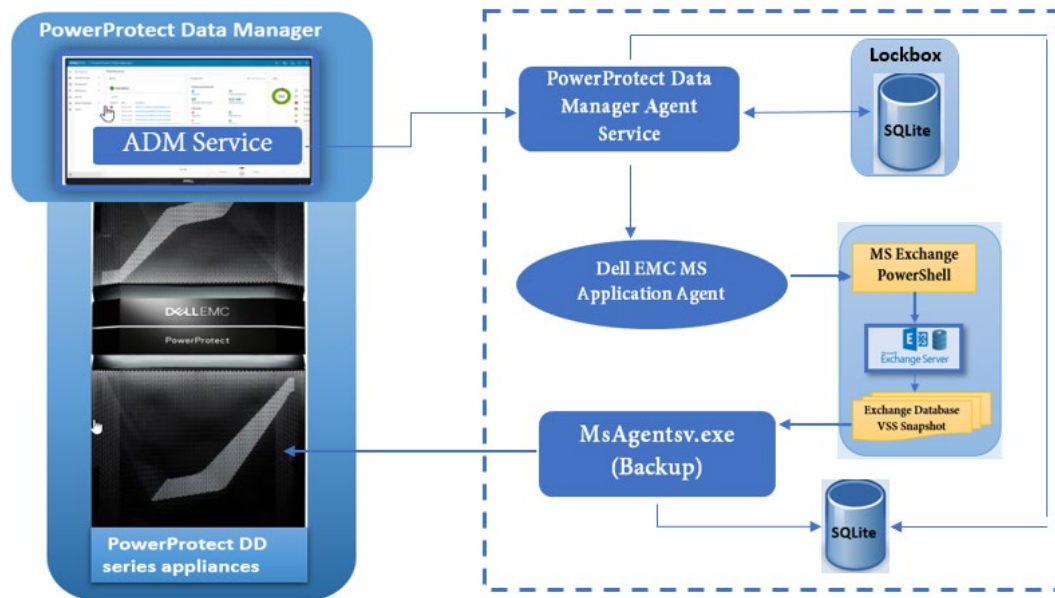


Figure 1 Microsoft application agent for Exchange Server

1.1.1 Protection storage

The first step in configuring Exchange Server integration with Data Manager is to ensure that you have a protection storage target that is configured to store the backup data. You can accomplish this task by adding one or multiple PowerProtect DD series appliances and add the protection storage using the Data Manager User Interface.

1.1.2 PowerProtect Data Manager

Use Data Manager with the application agent to perform the following operations:

- Automate the configuration of the application agent backup policy and protection storage settings
- Create a catalog of backups that are produced by the application agent, and monitor that catalog data to determine if retention policies are being adhered to
- Manage the life cycle of backups that are created by the application agent (ensure that the backups are marked for garbage collection based on the rules of the retention policy)

Data Manager does not change the way that the application agent works. Database administrators or backup administrators create the backups and perform the restores.

1.1.3 PowerProtect Data Manager agent service

The PowerProtect agent service is a REST API-based service, and the application agent installs this service on the application host. The agent service provides services and APIs for discovery, protection, restore, instant access, and other related operations. The Data Manager uses the agent service to provide integrated

data protection for the application assets. The PowerProtect agent service provides important functionality for the application agent operations with the Data Manager. The PowerProtect agent service performs the following operations:

- **Add-on detection:** An add-on integrates the application agent into the agent service. The agent service automatically detects the add-ons on the system for each application asset type and notifies the Data Manager. While multiple add-ons can operate with different asset types, only one agent service runs on the application host. Specific asset types can co-exist on the same application host.
- **Discovery:** The agent service discovers both stand-alone and clustered database servers (application systems), databases and file systems (assets), and their backup copies on the application agent host. After the initial discovery, when the agent service discovers any new application systems, assets, or copies, the agent service notifies the Data Manager.
- **Self-service configuration:** The agent service can configure the application agent for self-service operations by using information that is provided by the Data Manager. When you add an asset to a protection policy for self-service or centralized protection, the Data Manager automatically pushes the protection configuration to the agents. The Data Manager also performs this action if you modify the protection policy, including changing the DD Boost credentials.
- **Centralized backups:** The agent service performs the centralized backups as requested by the Data Manager.
- **Centralized restores:** The agent service performs the centralized restores as requested by the Data Manager.

1.1.4 Microsoft Exchange PowerShell interface for the application agent

The Exchange Management Shell is built on Microsoft Windows® PowerShell® technology and provides a powerful command-line interface that enables the automation of Exchange administration tasks. You can use the Exchange Management Shell to perform every task in the Exchange graphical management tools, plus tasks that you can perform elsewhere (for example, bulk operations). The application agent has PS/cmdlet interface that blends in with the Exchange shell, which gives Exchange administrators a seamless experience.

1.1.5 SQLite database

SQLite is a C library that provides a lightweight disk-based database that does not require a separate server process. This library allows you to access the database using a nonstandard variant of the SQL query language. Some applications can use SQLite for internal data storage. This library is used in this solution to store information about all types of backups like self-service, centralized, and automatic log backup for Data Manager.

1.1.6 Application Discovery Manager

The Data Manager Application Discovery Manager (ADM) provides continuous discovery and mapping of applications. It also maps their dependencies and configurations concerning their underlying infrastructure in data-center environments. ADM allows accurate, real-time visibility into the data center from an application standpoint. It is critical for planning data-center consolidations and migrations as well as managing change impact, virtualization initiatives, and disaster recovery.

1.1.7 Lockbox

The lockbox is an encrypted file that the Microsoft application agent uses to store confidential data, such as login credentials, and protect that data from unauthorized access. For each PowerProtect protection policy,

the Data Manager creates a storage unit and automatically configures the lockbox on the application host. A source lockbox and replication target lockbox are created and configured on the application host.

When you first use the Data Manager UI to add the Microsoft application agent and create the protection policy for Exchange data protection, Data Manager automatically configures the lockbox for the Exchange server. The lockbox for the Microsoft application agent is created in the default directory

C:\ProgramFiles\DPSAPPS\common\lockbox. Data Manager integration requires the lockbox to be in the default directory.

1.1.8 Support for existing Microsoft application agent backups with Data Manager

The Microsoft application agent provides the capability to onboard existing stand-alone deployments, including their existing backups, to Data Manager. Existing backups are Microsoft application agent backups that are performed before you integrate the Microsoft application agent with the Data Manager software. They are also performed before you add an asset to a Data Manager protection policy. Note the following regarding existing backups:

- Onboarding of Exchange backup copies to Data Manager is supported only from backups performed with Microsoft application agent version 4.7 and later.
- You can onboard up to three previous months' worth of existing backups.
- Retention lock is not supported for discovered existing backups in Data Manager.
- Onboarding of DD Boost-over-FC backups is not supported.

With the onboarding capability, Data Manager provides the following centralized features:

- Visibility of both existing backups and any new self-service or Data Manager policy-driven backups of onboarded assets.
- Automatic configuration of target protection storage based on the Data Manager protection policies that are used for your database.
- All other functionality that is provided for Data Manager protection policies.
- Ability to create a storage unit (when creating a protection policy) on the specified DD system backup host that is managed by Data Manager. All subsequent backups of assets in that protection policy go to this new storage unit. This implementation takes the storage-unit information that is provided before you onboard triggering backups through scripts and overrides it with the storage-unit information that is provided by Data Manager.

2 Supported configurations

The solution described in this document supports the configurations listed below and in Table 1.

- Data Manager supports the coexistence of the Microsoft application agent and the File System agent on Windows.
- The Microsoft application agent does not support the Meta-Cache Database (MCDB) feature in Exchange Server 2019. Do not enable MCDB in Exchange Server 2019.

Table 1 Supported configurations

Category	Features	PowerProtect Microsoft application agent support
Configurations	IP DAG	Yes
	IP-LESS DAG	Yes
	Parent Child Domain	No
	Disjoint namespace	No
	Standalone	Yes
	Dual NIC	Yes
Backup	Full and Incremental	Yes
	Retention Management	Yes
	IP-Less DAG backup	Yes
	IP DAG	Yes
	Log truncation	Yes
	Application Consistent	Yes
	Writer level backup and database level	Yes
	Roll over Parallelism	No
	Exclude components during backup	Yes
Restore	Point in Time Restore	Yes
	Flat file Restore	No
	Recover to alternate Database	Yes
	GLR To and from RDB	No
	GLR to Alternate mailbox	Yes
	GLR to PST files	Yes
	GLR to non-Exchange Server	No
	GLR to Messages and Text	Yes
	Proxy GLR	No
	Roll Forward Recovery	No

Category	Features	PowerProtect Microsoft application agent support
	Redirected Restore	Yes
Backup and restore technology		VSS for Snapshot Block Based Backup for CBT/Data Transfer
PowerProtect DD series appliance support	PowerProtect DD series appliance	Yes
	PowerProtect DD Virtual Edition	Yes
	PowerProtect DD Retention lock	Yes
	PowerProtect DD cloud tier for LTR	Yes
Cloud support	Microsoft Azure®	No
	Amazon Web Services (AWS)	No
	ECS	Yes
Exchange versions supported	Exchange Server 2010	Yes
	Exchange Server 2013	Yes
	Exchange Server 2016	Yes
	Exchange Server 2019	Yes
	Windows Server® 2012	Yes
	Windows Server 2012 R2	Yes
	Windows Server 2016	Yes
	Windows Server 2019	Yes
	Windows Server Core 2019	No
Cloning		Yes

Note: The most up-to-date software compatibility information for the Data Manager software and the application agents is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

3 Installation and configuration of Microsoft application agent for Exchange Server

The Microsoft application agent enables an application administrator to protect and recover the Exchange application data on the application host. Data Manager integrates with the Microsoft application agent to check and monitor backup compliance against protection policies. Data Manager also enables central scheduling for backups.

3.1 Prerequisites

Ensure that your environment meets the following requirements for a new deployment or upgrade of Data Manager:

- A list of hosts that write backups to DD systems is available.
- DD OS version 6.1 or later and the DD Management Console (DDMC). All models of DD series systems are supported.

Note: DDMC is required with a DD OS version earlier than 6.1.2. With DD OS version 6.1.2 or later, you can add and use a DD series system directly without DDMC.

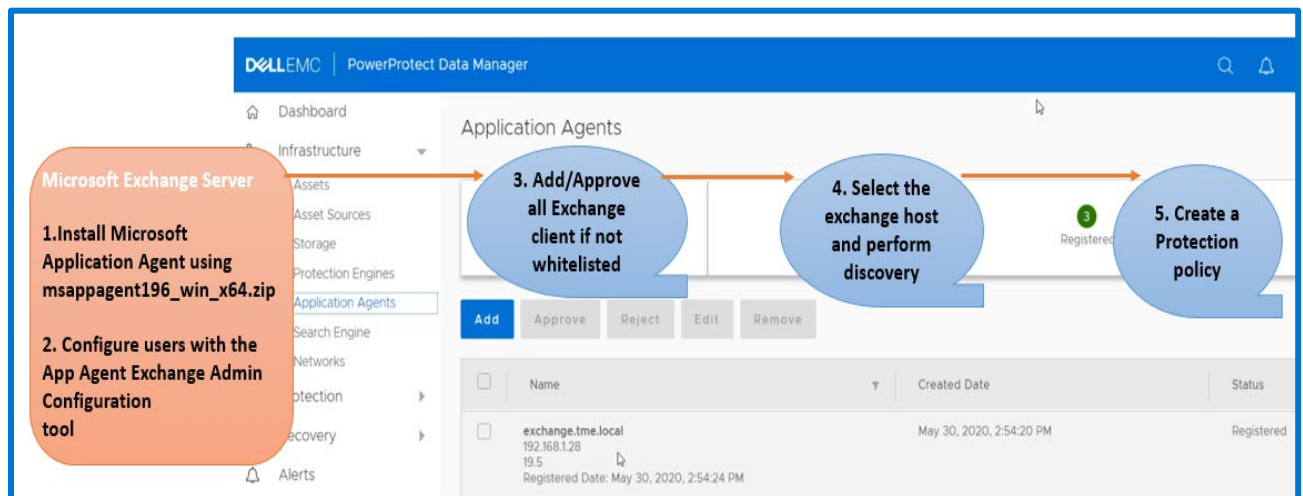
- Application agent version 19.5 or later is installed.
- License: A trial license is provided with the Data Manager software. For DPS applications, backup, and enterprise, you can contact Dell EMC Licensing Support for assistance with a permanent Data Manager license.
- Large environments require multiple Data Manager instances. Contact Champions.eCDM@emc.com for assistance with sizing requests.
- The Data Manager 19.6 download file requires the following:
 - VMware ESXi™ version 6.0, 6.5, 6.7, or 7.0
 - 8 vCPUs, 18 GB RAM, one 100 GB disk, and one 500 GB disk
 - The latest version of the Google Chrome browser to access the Data Manager UI
 - TCP port 7000 is open between Data Manager and the application agent hosts
- The Exchange Server environment meets the following prerequisites before you install the Microsoft application agent. Install the following applications on the Windows host:
 - Microsoft Exchange Server
 - .NET Framework 4.0 or later
- If installing ItemPoint for granular-level recovery, install .NET Framework 4.5.
- Ensure that all clocks on the Exchange Server host, domain controller, and Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
- Ensure that the Exchange Server and the Data Manager system network can see and resolve each other.
- Ensure that DNS is configured correctly on the application agent host for Exchange Server. Ensure that DNS is configured correctly on the Data Manager host and the name resolution matches.

3.2 Installation and configuration

Perform the following steps to install and configure the Microsoft application agent:

Prerequisite: Install PowerProtect DD Management Center (DDMC). Data Manager uses DDMC to connect to the DD systems. See the [PowerProtect DD Management Center Installation and Administration Guide](#) for instructions.

- Install the Microsoft application agent on the Exchange Server host.
 - a. In the **Data Manager** UI, click **System Settings > Agent Downloads**, select the Microsoft application agent download package **msappagent196_win_x64.zip**, and download the package to the Windows Exchange Server host.
 - b. Log in to the Exchange Server host as an Administrator to install the Microsoft application agent.
- Configure the required user privileges on the Exchange Server host using **App Agent Exchange Admin Configuration** tool.
- Add or approve the Microsoft application agent in Data Manager.
- Discover the Exchange application host.
- Create a protection policy to protect the Exchange host.
 - On each node in the DAG, repeat the steps to install the Microsoft application agent, and add and discover the application host in Data Manager.
 - Protection of the nodes in a DAG requires that all the nodes be registered to the Data Manager server.
 - You cannot perform a backup to a secondary PowerProtect DD series appliance. You can only restore from a secondary PowerProtect DD series appliance.



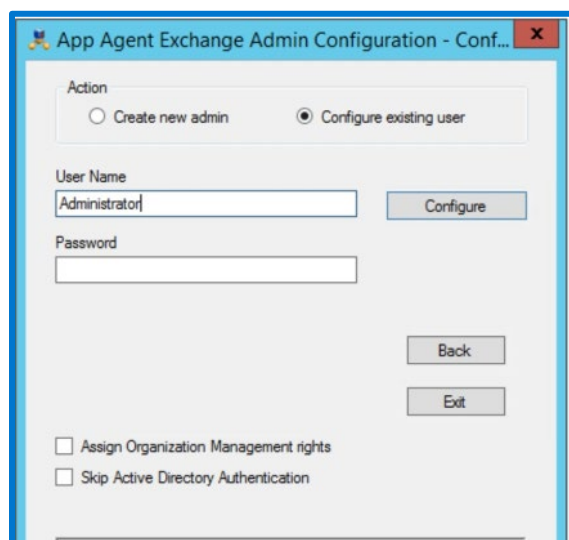
3.3 User configuration: App Agent Exchange Admin Configuration tool

Note the following points when using the App Agent Exchange Admin Configuration tool:

- To protect a stand-alone Exchange Server or Exchange DAG with the Microsoft application agent, you must configure an account with the required privileges. The App Agent Exchange Admin Configuration tool simplifies configuring security group memberships by ensuring that users have all the required Active Directory security group memberships and PowerShell management roles.
- To use the App Agent Exchange Admin Configuration tool, you must be logged in with domain administrator permissions. You can use an existing non-administrative user to run the App Agent Exchange Admin Configuration tool. However, this action is only possible if you select **Skip Active Directory Authentication** and configure the user on each Exchange Server node. This option skips the Active Directory authentication and authorization operations for the user. It only sets the user as the Microsoft application agent Exchange user account in the registry for backup and recovery operations.
- The Microsoft application agent uses the user account that is set in the registry by the App Agent Exchange Admin Configuration tool to perform backups and database or granular level recovery.
- To create a Microsoft application agent Exchange administrator account, the App Agent Exchange Admin Configuration tool performs the following steps:
 1. Creates an Active Directory user account
 2. Creates the custom Exchange security group **Dell EMC App Agent Exchange Admin Roles**
 3. (Optional) allows selecting **Assign Organization Management** rights

Members of the Organization Management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization.

Note: If you select **Assign Organization Management** rights, the Microsoft application agent adds the user to the Organization Management group. The tool does not create the Dell EMC App Agent Exchange Admin Roles security group. If you do not select this option and do not select the **Skip Active Directory Authentication** option, the Microsoft Application Agent creates an Active Directory security group **Dell EMC App Agent Exchange Admin Roles** and adds the user to that group.



- Permissions that the Exchange Admin Configuration tool configures:
 - Security group memberships on the Microsoft application agent client host:
 - > Local Administrator
 - Security group memberships on Domain Controller:
 - > Remote Desktop Users
 - Exchange Security Group memberships:
 - > Exchange Servers
 - > Dell EMC App Agent Exchange Admin Roles, which include:
 - Exchange Roles
 - Database Copies
 - Databases
 - Disaster Recovery
 - Mailbox Import Export
 - Mail Recipient Creation
 - Mail Recipients
 - View-Only Configuration
- You can perform the following actions after clicking **Configure Admin User**:
 - Create a Microsoft application agent Exchange Admin user, configure the permissions that are required for Exchange backup and recovery (both database and GLR), and set the user account in the registry.
 - Update an existing Exchange Admin user's permission to those that are required for Exchange backup and recovery (both database and GLR) and set the App Agent Exchange administrator account in the registry.
 - Set an existing user as an App Agent Exchange Admin account in the registry.

Note : For detailed steps for replication and cloud tier see [PowerProtect Data Manager Administration and User Guide](#).

4 Microsoft application agent for Exchange database backup

The Microsoft application agent uses block-based backup technology to back up Exchange Server databases in stand-alone and DAG environments. Block-based backup (BBB) technology tracks changed blocks of the Exchange database and log files as follows:

- A full backup backs up each selected Exchange database and log files.
- An incremental backup backs up only the changed blocks.

Block-based backups have reduced backup times because the backup process respectively backs up only the occupied disk blocks and changed disk blocks of the Exchange database and log files. During the backup, the application agent scans a volume or a disk where Exchange databases reside and backs up only changed blocks that are related to Exchange database.

Block-based backups provide instant access to the backups. These backups enable you to access databases using ItemPoint and perform granular restores.

Block-based backups use the following technologies:

- The Volume Shadow Copy Service (VSS) snapshot capability on Windows creates consistent copies of the source volume for backups.
- The Virtual Hard Disk (VHD), which is sparse, backs up data to the target device.

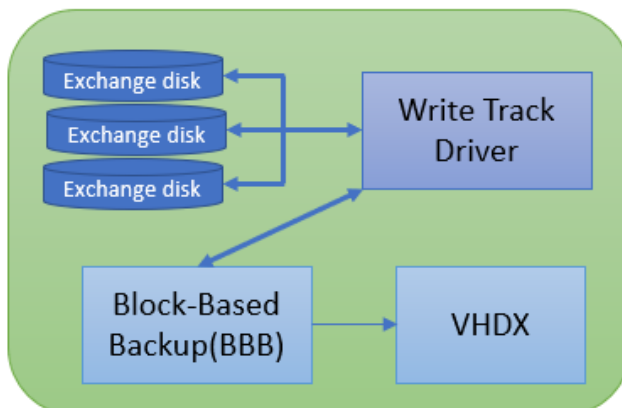


Figure 2 Block-based backups

4.1 Centralized backup

With centralized backups, the agent service coordinates the centralized backups as requested by the Data Manager. The backup is triggered according to the schedule, and Data Manager manages the complete protection life cycle.

The data protection attributes are specified when you create the centralized protection policy. These attributes include Type, Purpose, Assets, Schedule, Retention, and SLA. After you create the protection policy, the lockbox is automatically created, and the configuration information is saved in SQLite database called `configinfo.db`.

The following steps and Figure 3 describe the centralized backup workflow:

- The backup schedule starts, and the ADM service triggers the protection policy which sends a REST API request to Data Manager agent service.
- The Data Manager agent service receives the requests and sends the backup request to the Microsoft application agent.
- The Microsoft application agent requests Exchange VSS to generate snapshots for each database.
- `MsAgentsv.exe` transfers the Exchange backup data blocks in VHDX format.
- The data blocks are transferred from the snapshot to the PowerProtect DD series appliances. The first backup with the centralized policy is always full, and all incremental backups are virtual synthetic full.
- Once the backup is completed, backup metadata information is stored in SQLite database.
- The PowerProtect agent service sends the backup-complete information to the ADM service, and the Data Manager UI reflects the backup completion status.

During the next discovery process, the stored metadata is sent to the ADM service, and the same metadata is updated in Data Manager UI as copies.

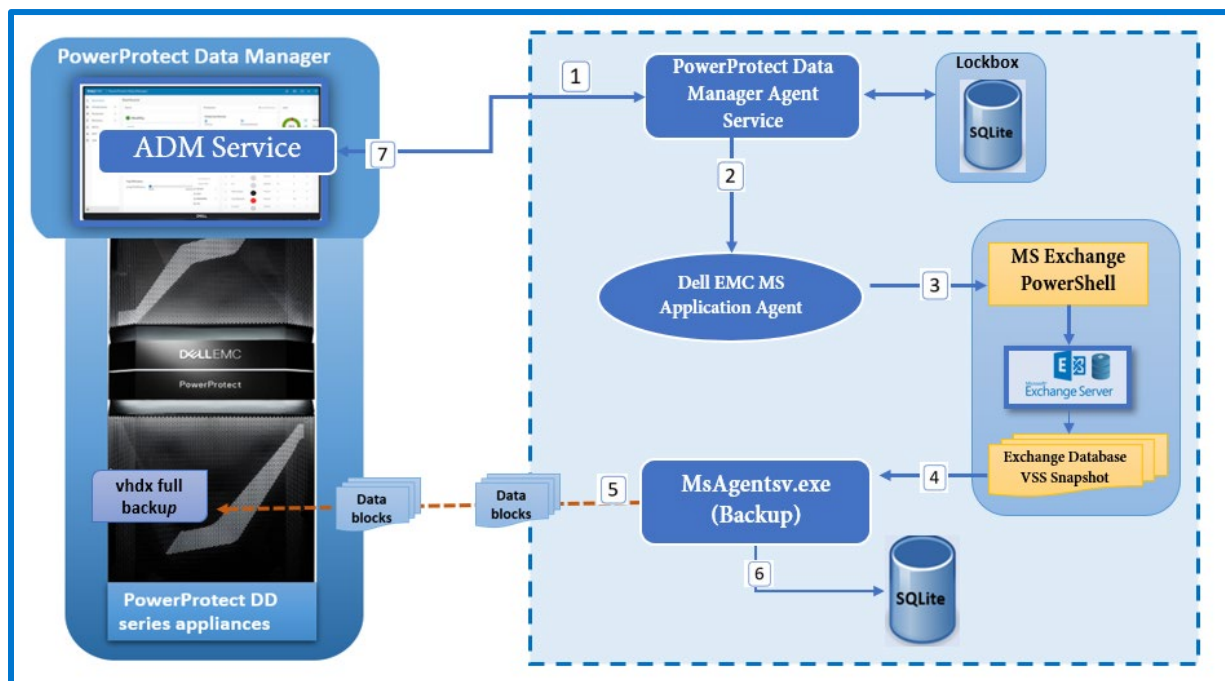


Figure 3 Centralized backup workflow

4.2 Federated backup of a DAG

A database availability group (DAG) environment can contain multiple passive copies of databases that are distributed across multiple Exchange servers. When you back up either active or passive database copies in the DAG environment, all DAGs use the federated backup method to best handle fail-over scenarios.

The federated backup method provides the following benefits:

- Allows backups of passive database copies to continue even when the passive database copies move among Exchange servers.
- Enables you to back up all DAG members, including stand-alone and public-folder-mailbox databases, by using a single save set. You are not required to perform a separate backup of each node.

Figure 4 shows three servers in a DAG (MBX1, MBX2, and MBX3) and four databases (DB1, DB2, DB3, and DB4). According to the preferred server order list (PSOL), MBX3 first backs up all passive copies available (DB3 and DB4), MBX2 backs up DB2, and then MBX1 backs up only DB1.

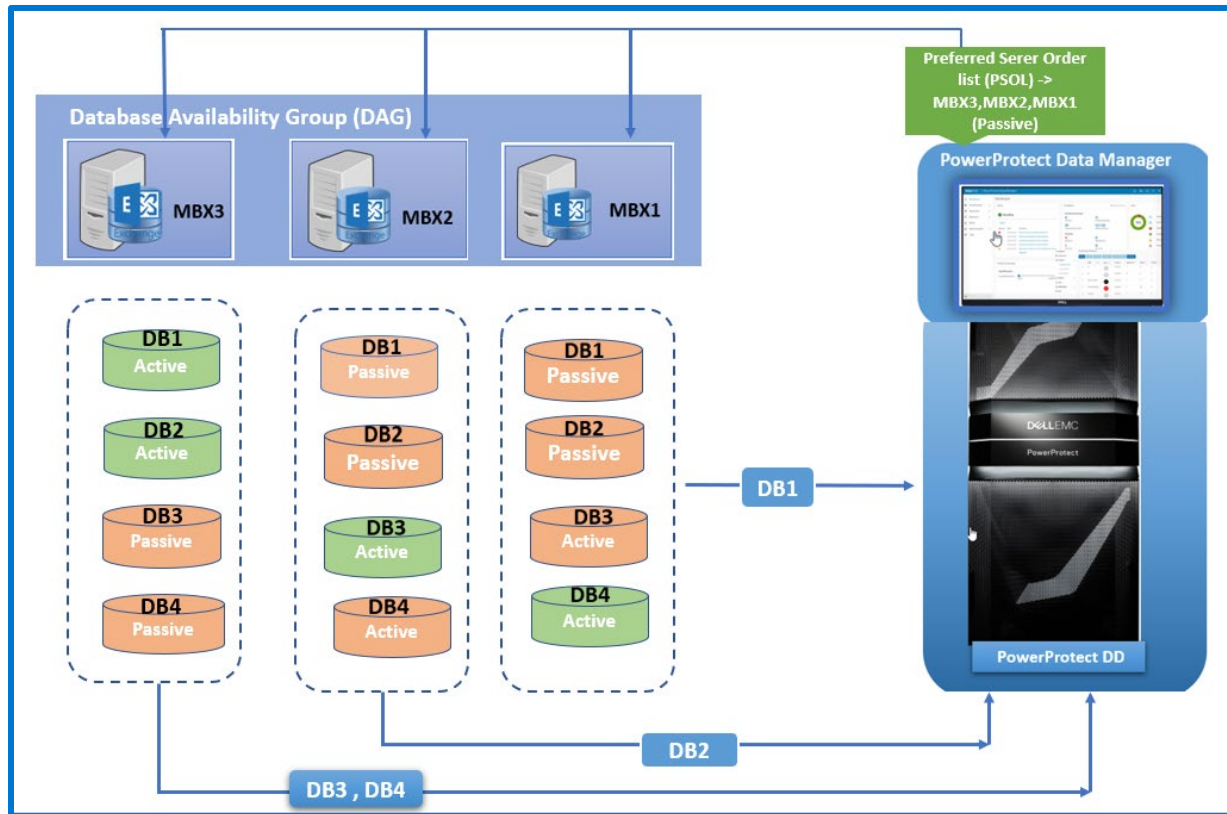


Figure 4 Federated backup of a DAG

The following steps describe the sequence of operation:

- When the backup starts, the PowerProtect ADM service initiates the `getPreferredNode()` PSOL.
- The Exchange add-on fetches the preferred server order list of assets through PowerShell.
- The Data Manager backup agent service triggers the preferred node list for the set of databases to be backed up.
- The `MsAgentstv.exe` processes the backup request and indexes the backup metadata in SQLite.

4.3 Self-service backup

To enable self-service protection, when you create the Exchange protection policy, select **Self-Service Protection**. When performing a self-service stand-alone backup of a DAG asset, the backups appear under the DAG asset.

The Microsoft application agent supports full and incremental block-based backups.

Note: For self-service backups, do not select assets from multiple protection policies in the same backup request. This is a limitation of the Microsoft application agent.

The following steps and Figure 5 describe the workflow of a self-service backup:

- To import the backup parameters to the object, the Exchange administrator or backup admins use Microsoft Exchange PowerShell to run the `Import-ExchangeBackupConfigFile` cmdlet with the `-Backup` parameter.
- The credentials required for connecting to the PowerProtect DD series appliance are extracted from the lockbox.
- A backup command is initiated from Exchange PowerShell, which launches the Microsoft application agent.
- The agent requests Exchange VSS to create a snapshot for each database.
- `MsAgentsv.exe` transfers the Exchange backup data blocks in VHDX format. The data blocks are transferred from the snapshot to the PowerProtect DD series appliances.
- Once the backup is completed, it is updated in the SQLite database with the backup metadata.
- When the ADM service runs a discovery process, it checks with the Data Manager agent service if any backups have occurred since the last discovery.
- The service checks the metadata database, updates the PowerProtect ADM service with the backup details, and updates the Exchange server. The backup copies are now visible in the Data Manager UI.

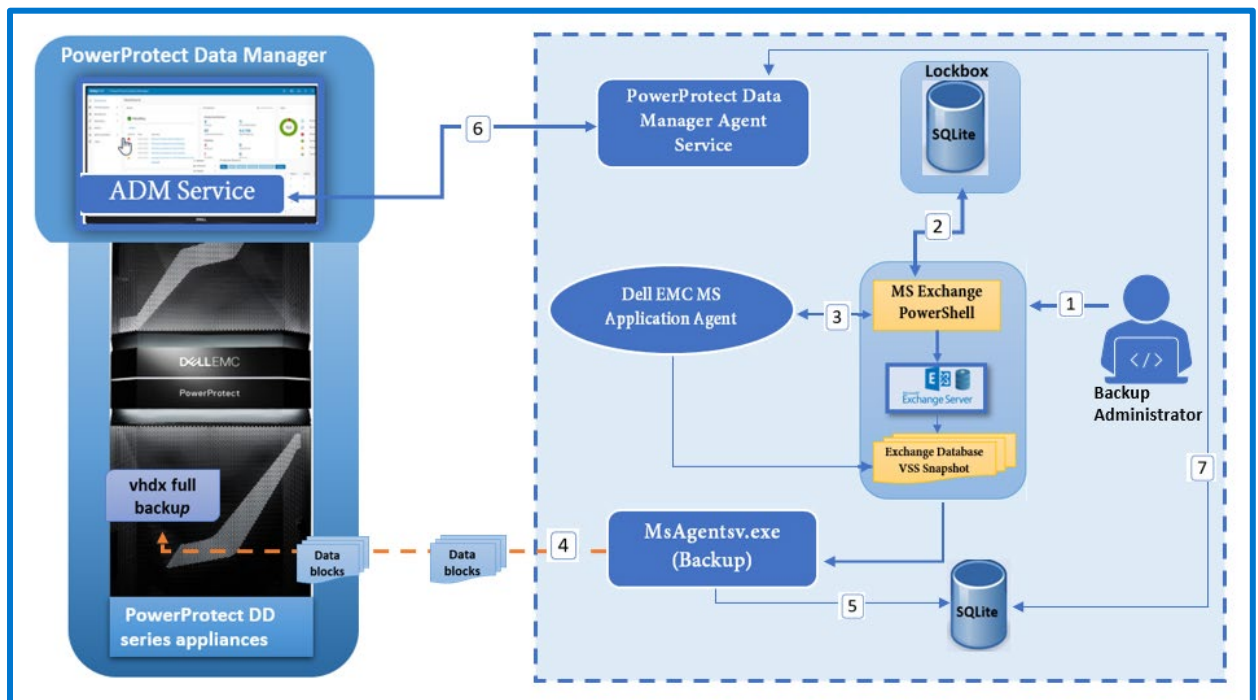


Figure 5 Self-service backup workflow

4.4 Parallelism for Microsoft application agent backup

To configure the parallelism setting for a centralized backup of Exchange databases, set the **clientParallelism** parameter value in the **userlockbox.cfg** file on the Exchange server host.

- The default parallelism setting for a centralized Exchange backup is **16**. You can override this default setting with the **clientParallelism** parameter setting in the configuration file.
- For a self-service Exchange backup, you can specify the parallelism with the **-Parallelism** parameter setting in the **Backup-Exchange** PowerShell cmdlet.

Based on the number of CPUs on the host and the parallelism setting, the application agent uses the following effective parallelism value for a centralized Exchange backup:

- **With 10 or more CPUs:** The effective parallelism equals the minimum number of CPUs and the parallelism setting, minus 4. For example, with 12 CPUs and a parallelism of 16, the effective parallelism value is 8 (12 minus 4).
- **With 4 to 9 CPUs:** The effective parallelism equals the minimum of the number of CPUs and the parallelism setting, minus 2. For example, with 8 CPUs and a parallelism of 10, the effective parallelism value is 6 (8 minus 2).
- **With fewer than 4 CPUs:** The effective parallelism equals the number of CPUs. For example, with 2 CPUs, the effective parallelism value is 2.

If the effective parallelism value is 8, then 8 threads are created for the Exchange backup, with each thread assigned to transfer either an EDB file or the related log files. An asset transfer is complete only when an EDB file and the related log files are both copied to the DD system. Using 8 threads, 4 assets are backed up in parallel from the host.

4.5 Back up Exchange server with Microsoft application agent PowerShell backup cmdlet

Use the **Backup-Exchange** PowerShell cmdlet to back up Exchange Server to a PowerProtect DD series appliance. All cmdlets support the standard common PowerShell parameters. The Microsoft article [Exchange Server PowerShell \(Exchange Management Shell\)](#) provides the list of common parameters and their description.

For self-service backups with protection policies created through Data Manager, run the **Import-ExchangeBackupConfigFile** cmdlet with the **-Backup** parameter to import the backup parameters to the object.

4.5.1 Syntax to perform stand-alone server backups

See the following syntax to perform stand-alone server backups:

```
[<configuration_object>] | Backup-Exchange -BackupViaBlockBasedBackup -
ClientName <FQDN_of_Exchange_Server> -DataDomainHost <Data_Domain_hostname> -
DataDomainHostPath /<Data_Domain_storage_path> -DataDomainUser
<Data_Domain_username> [<optional_parameters>]
```

- **<configuration_object>** (optional):
Specifies the configuration object that was imported using the Import-ExchangeBackupConfigFile cmdlet.
- **-ClientName <FQDN_of_Exchange_Server>**:
Specifies the FQDN of the Exchange Server to use for indexing the backup.
- **-BackupViaBlockBasedBackup**:
Specifies that the backup is a block-based backup. You can use the -BBB alias for the -BackupViaBlockBasedBackup parameter.
- **-DataDomainHost <Data_Domain_hostname>**:
Specifies the PowerProtect DD series appliance server hostname. You can use the -S, -SH, -DDHost, or -StorageHost alias for the -DataDomainHost parameter.
- **-DataDomainHostPath /<Data_Domain_storage_path>**:
Specifies the full path to the Data Domain storage unit for the backup. The PowerProtect DD series appliance user must have appropriate access rights to this path. You can use the -Path, -DevicePath, -StoragePath, -StorageHostPath, or -DataDomainPath alias for the -DataDomainHostPath parameter.
- **-DataDomainUser <Data_Domain_username>**:
Specifies the PowerProtect DD series appliance username. Full credentials are retrieved from the lockbox to authenticate with the host. -DDUser, -StorageUser You can use the -DDUser or -Storage User alias for the -DataDomainUser parameter.

See the following example backup command:

```
Backup-Exchange -ClientName myexchange.msapp.com -BackupViaBlockBasedBackup -
DataDomainHost myDD.lss.example.com -DataDomainPath /SU_DD163 -DataDomainUser
DD163_user
```

See the following example backup command with a configuration object:

```
$serverinfo | Backup-Exchange
```

4.5.2 Syntax to perform federated backup

See the following syntax to perform a federated backup:

```
[<configuration_object>] | Backup-Exchange -BackupViaBlockBasedBackup -
ClientName <FQDN_of_Exchange_Server_DAG> -DataDomainHost <Data_Domain_hostname>
-DataDomainHostPath /<Data_Domain_storage_path> -DataDomainUser
<Data_Domain_username> {[<-BackupActive>] | [<-BackupPassive>] | [<-BackupPreferred>]}
[<-IncludeStandaloneDatabases>] [<-
ServerOrderList<comma_separated_list_of_servers>] [<optional_parameters>]
```

- **-ClientName <FQDN_of_Exchange_Server_DAG>**:
Specifies the FQDN of the database availability group instance to use for indexing the backup.
- **{<-BackupActive> | <-BackupPassive> | <-BackupPreferred>}** (optional):

Specifies that the database backup preference is either active (-BackupActive), passive (-BackupPassive), or preferred (-BackupPreferred).

- **-IncludeStandaloneDatabases** (optional):
Specifies to include stand-alone databases and public folder databases in the backup.
- **-ServerOrderList <comma_separated_list_of_servers>** (optional):
Specifies the preferred Exchange Server order list if you must select multiple copies. Separate multiple servers with commas.

See the following example federated backup command:

```
Backup-Exchange -Identity TestDB, 'Mailbox Database 1250665181' -ClientName
DAG1.msapp.com -BackupViaBlockBasedBackup -DataDomainHost myDD.lss.example.com -
DataDomainPath /SU_DD163 -DataDomainUser DD163_user -Preferred -ServerOrderList
node1, node2 -IncludeStandaloneDatabases
```

See the following example federated backup command with a configuration object:

```
$serverinfo | Backup-Exchange -Identity TestDB, 'Mailbox Database 1250665181'
```

4.5.3 Optional parameters for the Backup-Exchange cmdlet

The following list describes the optional parameters for the Backup-Exchange cmdlet:

- **-Incremental:**
Specifies that the backup level is a block-based incremental backup. If you do not specify this parameter, the backup is taken at the full level.
- **-Retention +<number>{d | m | w | y}:**
Specifies the period in which to retain a backup. After the period passes, the backup expires. The default retention period is 30 days. The maximum retention date is 02-07-2106.
- **-Identity <database identity>:**
Specifies the identity of the database to back up. If you do not specify this parameter, the operation backs up all databases.
- **-LockBoxPath <full_path_to_lockbox>:**
Specifies the folder that contains the lockbox file, which contains encrypted information about the registered hosts and the corresponding usernames in pairs. Each pair is associated with a password that the backups use.
- **-ExeFileName <msagentsv.exe_path>:**
Specifies the full path to the application program executable msagentsv.exe. Use this option only for diagnosis. In normal operations, the cmdlet automatically locates the installed application.
- **-AsJob {\$true | \$false}:**
Runs the cmdlet as a background job. The command returns an object that represents the job and displays the command prompt. You can continue to work in the session during the job.
- **-Parallelism <parallelism_value>:**
Specifies the parallelism setting for the backup.

Note: To get complete list of available options, see the [PowerProtect Exchange Server Guide](#)

5 Restoring Exchange Server databases

You can perform database restores or granular level restores directly to the Exchange application host using the Microsoft application agent. The agent supports the following types of database restores:

- **Normal restore:** Restore of a database to the original source database.
- **Alternate database restores:** Restore of a database to another database that is different from the source database.

5.1 Prerequisite for Exchange Restore operation

You must run the **set-mailboxdatabase** cmdlet to allow an Exchange database to be restored from a backup.

```
set-mailboxdatabase <mailbox_database> -AllowFileRestore $true
```

- **<mailbox_database>:**
Specifies the name of the database that is the target for the restore operation.
- **-AllowFileRestore \$true:**
Specifies to allow restore operations for the database.

Note: Run this command for each target database for the restore operation.

5.2 Restore a backup to source database

Use the **Restore-Exchange** cmdlet with the following syntax to restore a database to the source location (normal restore):

```
[<configuration_object>] | Restore-Exchange -NormalRestore {-BackupID  
<backup_ID> [-Identity <identity>] | -Backup <backup_object>} -ClientName  
<FQDN_of_Exchange_Server> -DataDomainHost <Data_Domain_hostname> -  
DataDomainHostPath /<Data_Domain_storage_path> -DataDomainUser  
<Data_Domain_username> <optional_parameters>
```

- **<configuration_object>** (optional):
Specifies the configuration object that was imported using the Import-ExchangeBackupConfigFile cmdlet.

Note: For Data Manager centralized and self-service workflows, run the **Import-ExchangeBackupConfigFile** cmdlet with the **-Restore** parameter to import the configuration parameters to the object.

- **-NormalRestore:**
Specifies that the database is being restored to the original source location. You can use the -Restore alias for the -NormalRestore parameter.
- **{-BackupID <backup_ID> [-Identity <identity>] | -Backup <backup_object>}:**
Specifies the backup to restore using either the backup identity or object. You must specify only one of the following options:
 - **-BackupID <backup_ID>:** Use a backup ID. Optionally, specify **-Identity <database_ID>** with **-BackupID** to specify the identity of one or more databases to restore.
 - **-Backup <backup_object>:** Use a backup object. You can retrieve the backup ID and object from the **Backup-Exchange** or **Get-ExchangeBackup** cmdlet output.

The following example restores the database TestDB by using a backup ID.

```
Restore-Exchange -NormalRestore -BackupID msapp_bbb: 1458138556 -Identity
TestDB -ClientName myDD.msapp.com -DataDomainHost ledmd035.lss.example.com -
DataDomainHostPath /SU_DD163 -DataDomainUser DD163_user
```

5.3 Restore a backup to an alternate database

Note: Before you perform a copy or alternate database restore, ensure that the target database exists. Use the **Restore-Exchange** cmdlet with the following syntax to restore a database to an alternate location (copy restore):

```
[<configuration_object>] | Restore-Exchange -CopyRestore -BackupID <backup_ID> -
Identity <identity> -RestoreDatabaseIdentity <target_identity> -ClientName
<FQDN_of_Exchange_Server> -DataDomainHost <Data_Domain_hostname> -
DataDomainHostPath /<Data_Domain_storage_path> -DataDomainUser
<Data_Domain_username> [<optional_parameters>]
```

- **-CopyRestore:**
Specifies that the database is being restored to an alternate location. You can use the **-Alternate** alias for the **-CopyRestore** parameter.
- **-BackupID <backup_ID>:**
Specifies the backup ID to restore. You can retrieve the backup ID from the **Backup-Exchange** or **Get-ExchangeBackup** cmdlet output.
- **-Identity <database_ID>:**
Specifies the identity of one or more databases to restore.
- **-RestoreDatabaseIdentity <target_identity>:**
Specifies the target identity of the alternate database to restore to. You can use the **-RestoreDB**, **-Target**, **-RDB**, or **-RestoreDatabaseID** alias for the **-CopyRestore** parameter.

The following shows an example of restoring the database TestDB to an alternate database (AlternateDB) using a backup ID:

```
Restore-Exchange -CopyRestore -BackupID msapp_bbb: 1458138556 -Identity TestDB -
RestoreDatabaseIdentity AlternateDB -ClientName ledmf175.msapp.com -
DataDomainHost myDD.lss.example.com -DataDomainHostPath /SU_DD163 -
DataDomainUser DD163_user
```

5.4 Granular level restores

To recover granular-level Exchange Server data, you must first mount the backup using the **Mount-ExchangeBackup** PowerShell cmdlet. When the backup is mounted, you can browse and recover granular items, such as mailboxes or folders, with **ItemPoint** for Microsoft Exchange Server.

Granular level restore can be performed on an Exchange server or proxy server where Exchange Server is not installed.

5.4.1 Mount Backup

To perform granular level restores, first mount the backups. Use the `Mount-ExchangeBackup` cmdlet with the following syntax to mount the backups:

```
[<mount_object> = <configuration_object>] Mount-ExchangeBackup {-BackupID
<backup_ID> [-Identity <identity>] | -Backup <backup_object>} -ClientName
<FQDN_of_Exchange_Server> -DataDomainHost <Data_Domain_hostname> -
DataDomainHostPath /<Data_Domain_storage_path> -DataDomainUser
<Data_Domain_username> [<optional_parameters>]
```

Result: The backup is mounted in a path like the following:

```
C:\Program
Files\DPSAPPS\MSAPPAGENT\tmp\BBBMountPoint\131248297060279537_{4A60AF18-86ED-
4BBDA1C9-2618F1AC1041}_5832\Program Files\Microsoft\Exchange
Server\V15\Mailbox\DB2\
```

Name	Date modified	Type	Size
132621977983768816_{E8EFB1E9-682B-4DB1-938A-8F9E5CB889AB}_6456	4/6/2021 9:19 PM	File folder	156,925,948 KB
132621978212581948_{CF2178D0-394E-480B-8467-96368F16BB8CD}_8772	4/6/2021 9:20 PM	File folder	156,925,948 KB
132621978441625109_{BAA76AEF-65B9-483E-B0AC-133224CF7E8C}_5972	4/6/2021 9:20 PM	File folder	156,925,948 KB
132621978670378214_{6FA1DFA0-1D4D-4EE2-A691-14F98BF32F1C}_2640	4/6/2021 9:21 PM	File folder	156,925,948 KB
132621978898971371_{FE3454CA-0CFB-4CEC-AA34-118CC3753293}_8856	4/6/2021 9:21 PM	File folder	156,925,948 KB
132621979127644438_{75F00DC9-CD81-40CE-885F-7559AE09D168}_7536	4/6/2021 9:21 PM	File folder	156,925,948 KB
132621979359367775_{A5016D33-E5B6-4703-BC4B-1D6C21376A05}_8776	4/6/2021 9:22 PM	File folder	156,925,948 KB
132621979588710913_{AEFF772B-2159-40F6-869B-0561D701C43C}_6404	4/6/2021 9:22 PM	File folder	156,925,948 KB
132621980160883742_{8BCD9D51-BF6D-44B9-87F9-F59519C8DA90}_8132	4/6/2021 9:23 PM	File folder	156,925,948 KB
132621980390126887_{F5ED187B-B3A7-4435-B7CA-0CABD9B2D32A}_9148	4/6/2021 9:23 PM	File folder	156,925,948 KB

Figure 6 Mounted backup

The mounted items are unmounted after you restart the host.

The following are examples of the `Mount-ExchangeBackup` cmdlet:

Mount all databases of a backup using a backup object:

```
Mount-ExchangeBackup -Backup $backups [0] -ClientName ledmf175.msapp.com -
DataDomainHost myDD.lss.example.com -DataDomainHostPath /SU_DD163 -
DataDomainUser DD163_user
```

Note: Mount point are created for each database as separate drives which is virtual, no data is restored until recovery commands are run from exchange powershell.

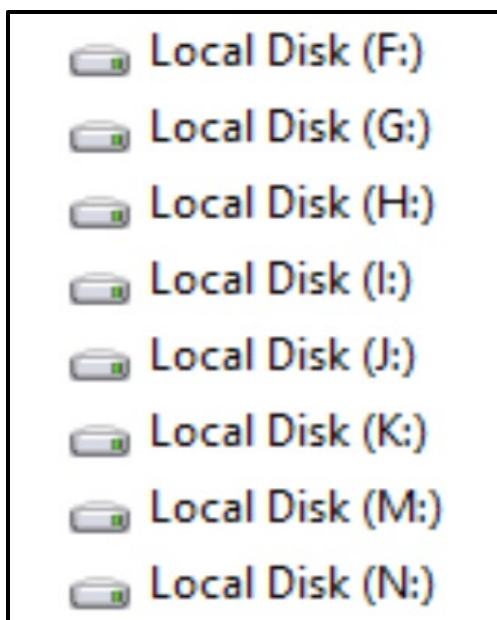


Figure 7 Virtual disk representing each database

Mount a single mailbox database database3 using a backup object and identity:

```
$mount = $serverinfo | Mount-ExchangeBackup -Backup $backup[0] -Identity
database3
```

5.4.2 Managing mounted backups

After a mount operation succeeds, the Mount Service system tray icon appears as shown in the following figure.

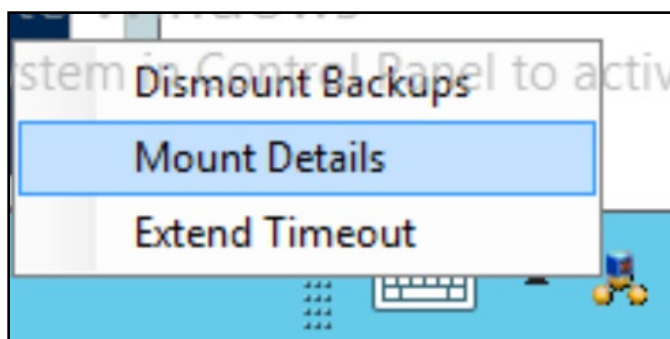


Figure 8 Mount service system tray icon

Right-click the Mount Service icon, and select any of the following options to perform corresponding tasks according to your requirement:

- **Dismount Backups:** Dismounts the mounted backups.
- **Mount Details:** Lists the mounted backups with mount details.

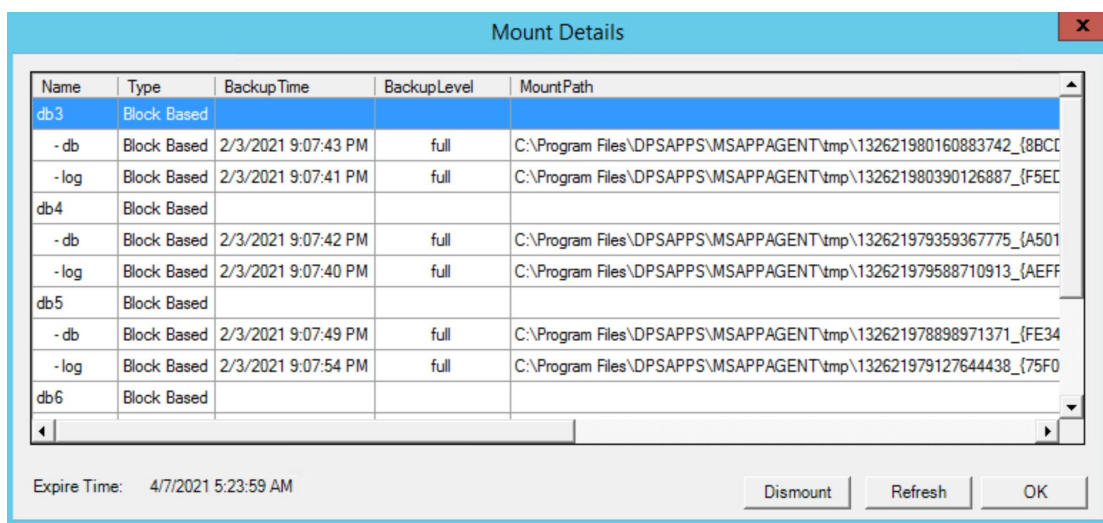


Figure 9 Mount Details

- **Extend Timeout:** Extends the timeout of the mount. The default value is 8 hours.

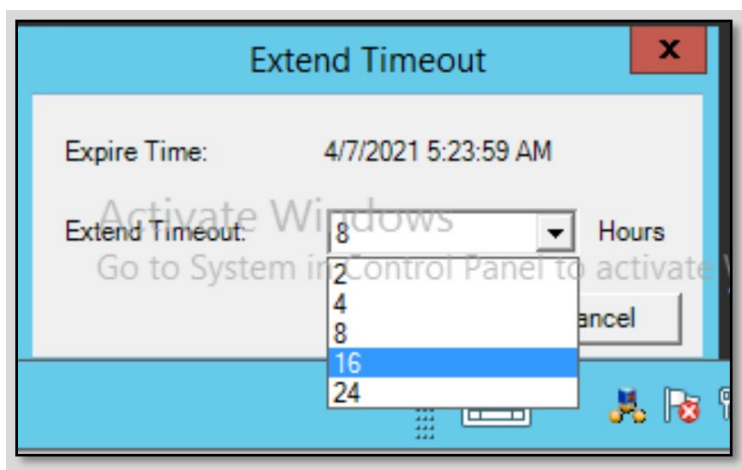


Figure 10 Extend Timeout

5.4.3 Browse and recover granular-level data with ItemPoint for Microsoft Exchange Server

The ItemPoint for Exchange Server User Guide provides more information about performing granular-level recovery of Exchange data. Perform the following steps:

- Launch ItemPoint.
- In ItemPoint, launch the **Restore wizard**.
- On the **Source Selection** page, select the source and specify the EDB and log file path from the mounted volume that contains the Exchange backup data (see the following screen). Click **Next**.

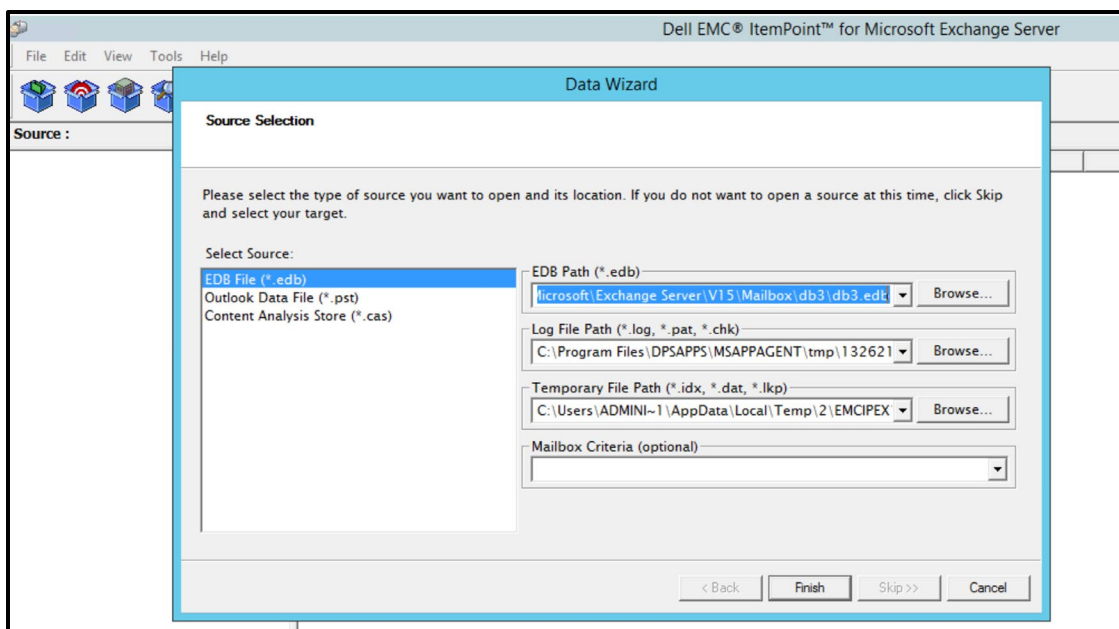


Figure 11 Source selection page of Dell EMC Itempoint

- On the **Target Selection** page, click **Skip**.

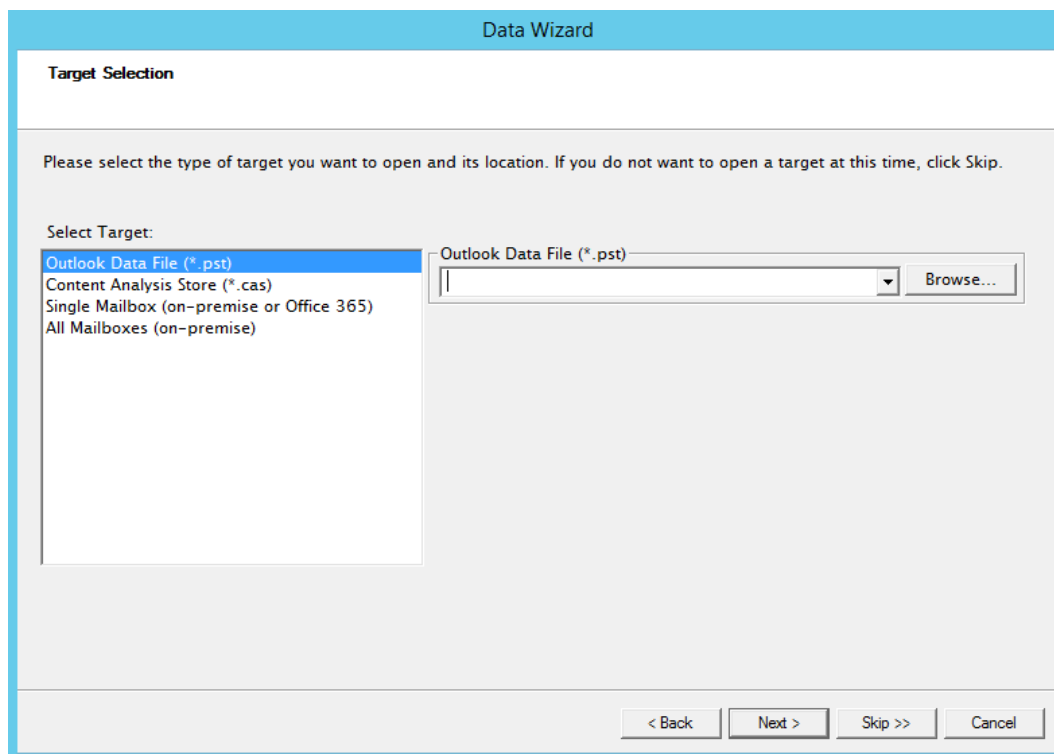


Figure 12 Target Selection page of Dell EMC Itempoint

- Follow the **Data Wizard** prompts to complete the granular-level recovery.

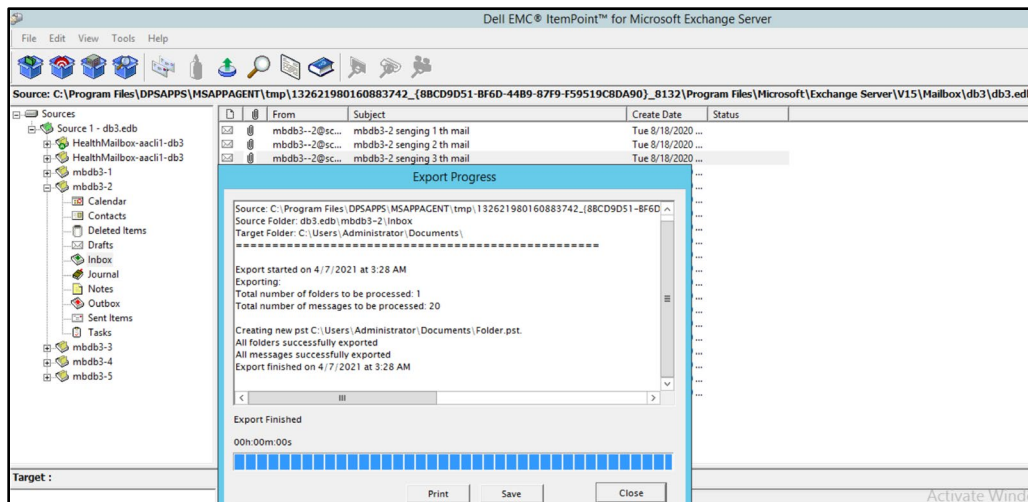


Figure 13 Export completion screen of Dell EMC Itempoint

- Once the granular-level recovery is complete, dismount the backup.

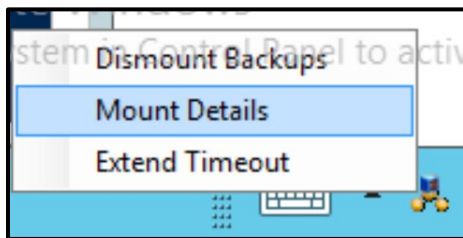


Figure 14 Dismount backup using system tray icon

5.5 Granular level restores without Exchange Server

Starting with version 19.8 of Data Manager and Microsoft application agent, you can perform the granular level restore of an Exchange Server data backup on a proxy server where the Exchange Server is not installed. After you meet the prerequisites, you must run the required commands and mount the backup using the `Mount-ExchangeBackup` PowerShell cmdlet. Once the backup is mounted, you can browse and recover the granular items, such as mailboxes or folders, with ItemPoint for Microsoft Exchange Server.

5.5.1 Prerequisites for granular level restores without Exchange Server

Before you perform the granular level restore of an Exchange backup on a proxy server without the Exchange Server, you must meet the following prerequisites:

- Login to proxy server as Administrator user.
- Install Microsoft application agent for Exchange plugin as explained in section [Installation and Configuration](#).

Note: It is not required to run App Agent Exchange Admin Configuration tool as no backups will be performed.

- Create a lockbox.txt file with details :the exchange client name, DD storage unit name, and DD storage unit user of the protection policy:
 - To obtain the storage unit name login to the Exchange node, run the following command:

```
$serverconfig=Import-ExchangeBackupConfigFile -backup
```

Note the details of the DD, storage unit, and client name from the command output.

- To obtain the DD Boost user of the storage unit login to the DD, run the following command:

```
ddboost storage-unit show
```

Note the name of the user. Ensure that you have the password for the DD user that originally performed the Exchange backup.

Sample contents of the *lockbox.txt* file are as follows:

```
CLIENT=aacli1.scan.com
DEVICE_PATH=/scan_centralized-ppdm-58-127-9426f/PLCTLTP-7d9bd6e5-295f-430c-
a8b9-d49af5d07f47
DEVICE_HOST=10.118.211.52
DDBOOST_USER=scan_centrali-ppdm-58-127-9426f
LOCKBOX_PATH="C:\Lockbox\lockbox.txt"
DEBUG_LEVEL=9
BACKUP_TYPE=blockbasedbackup
```

5.5.2 Command for granular level restores without Exchange Server

To perform the granular level restore of an Exchange backup on a proxy server without the Exchange Server, you must first create the lockbox from Exchange Server then run the following commands:

1. To connect to the DD series appliance where the backup is stored for which the granular level restore must be performed, run the following command:

```
msagentadmin administration -P -z C:\Lockbox\lockbox.txt
```

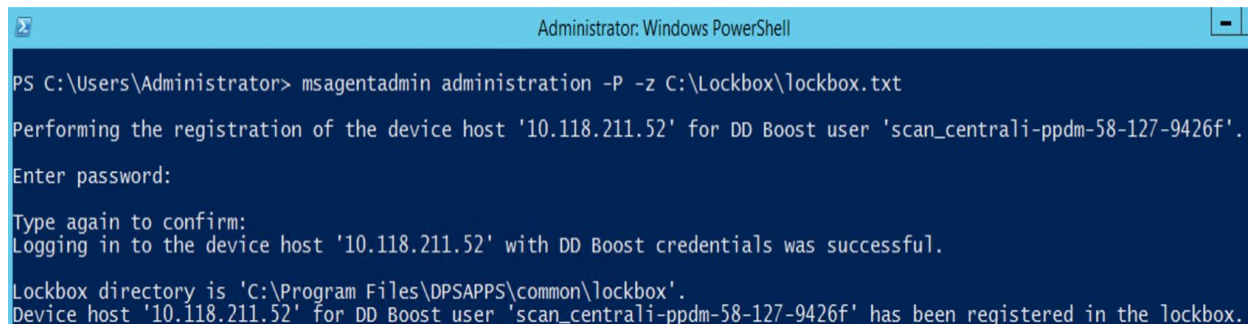


Figure 15 Command to connect to DD series appliance

2. To import the configuration parameters to the object, run the following command, where \$s contains all the configuration parameters to the object:

```
$s=Import-ExchangeBackupConfigFile -ConfigFile C:\Lockbox\lockbox.txt
```



```

Administrator: Windows PowerShell
PS C:\Users\Administrator> $s=Import-ExchangeBackupConfigFile -ConfigFile C:\Lockbox\lockbox.txt

Summary of imported attributes :

DataDomainUser = scan_centrali-ppdm-58-127-9426f
DataDomainHost = 10.118.211.52
DataDomainHostPath = /scan_centralized-ppdm-58-127-9426f/PLCTLTP-7d9bd6e5-295f-430c-a8b9-d49af5d07f47
ServerOrderList =
BackupViaBlockBasedBackup = True
ClientName = aac11
DebugLevel = 9
LockBoxPath =
DataDomainFibreChannelHost =
DeleteDebugLogsInDays = 32767
Retention =

```

Figure 16 Command to import configuration parameter

- To save the backup to the variable \$backups, which is used to mount the backup for the granular-level restore, run the following command:

```
$backups = $s | Get-ExchangeBackup
```

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> $s | Get-ExchangeBackup
WARNING: 02/10/21 04:54:46.475374 ACL ACE dump: mode_to_acl result
WARNING: 02/10/21 04:54:46.475374 ACE for [WIN-DIBKIP5JQS\Administrator]: 0xc0070180
WARNING: 02/10/21 04:54:46.476375 ACE for [WIN-DIBKIP5JQS\None]: 0xc0010000
WARNING: 02/10/21 04:54:46.476375 ACE for [\Everyone]: 0xc0010000

BackupDateTimeUTC      BackupExpiryDateTimeUTC BackupID      ClientName      Successful BackupDatabases
-----
2/3/2021 3:40:54 PM    6/23/2021 3:36:50 PM    msapp_bbb:1612366854 aac11.scan.com True            {db7, db6,...

PS C:\Users\Administrator> $backups = $s | Get-ExchangeBackup
WARNING: 02/10/21 04:57:20.786225 ACL ACE dump: mode_to_acl result
WARNING: 02/10/21 04:57:20.786225 ACE for [WIN-DIBKIP5JQS\Administrator]: 0xc0070180
WARNING: 02/10/21 04:57:20.786225 ACE for [WIN-DIBKIP5JQS\None]: 0xc0010000
WARNING: 02/10/21 04:57:20.786225 ACE for [\Everyone]: 0xc0010000

```

Figure 17 Command to save the backup to variable

- To mount the Exchange database backup including the databases and log files from a DD, run the following command:

```
$s | Mount-ExchangeBackup -Backup $backups[0] -Verbose
```

Mount backup[0] which is essentially latest backup to the Non-Exchange windows server. Backup copies are mounted in VHD format.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> $s | Mount-ExchangeBackup -Backup $backups[0] -Verbose
VERBOSE: Mounting the backup.
Exchange Server is not installed on this machine, So only Item point restore is supported.

MountPath                                                    BackupID
-----
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738690833810... {msapp_bbb:1612366762}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738693123341... {msapp_bbb:1612366763}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738695430874... {msapp_bbb:1612366693}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738697719605... {msapp_bbb:1612366726}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738700010436... {msapp_bbb:1612366669}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738702298768... {msapp_bbb:1612366674}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738704587399... {msapp_bbb:1612366662}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738706879031... {msapp_bbb:1612366660}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738709173063... {msapp_bbb:1612366663}
C:\Program Files\DPSAPPS\MSAPPAGENT\tmp\1325738711460494... {msapp_bbb:1612366661}

```

To complete the granular-level restore, you can use ItemPoint as described in [Browse and recover granular-level data with ItemPoint for Microsoft Exchange Server](#).

6 Replication and DD Cloud Tier

During the protection policy creation, you can add the replication to a remote PowerProtect DD series appliance as the replication target.

In a protection policy Click **Replicate** next to **Primary Backup**, **Primary Retention**, or **Extend Retention**. An entry for **Replicate** is created to the right of the primary or extended retention backup schedule. Under **Replicate**, click **Add**. The **Add Replication** dialog appears.

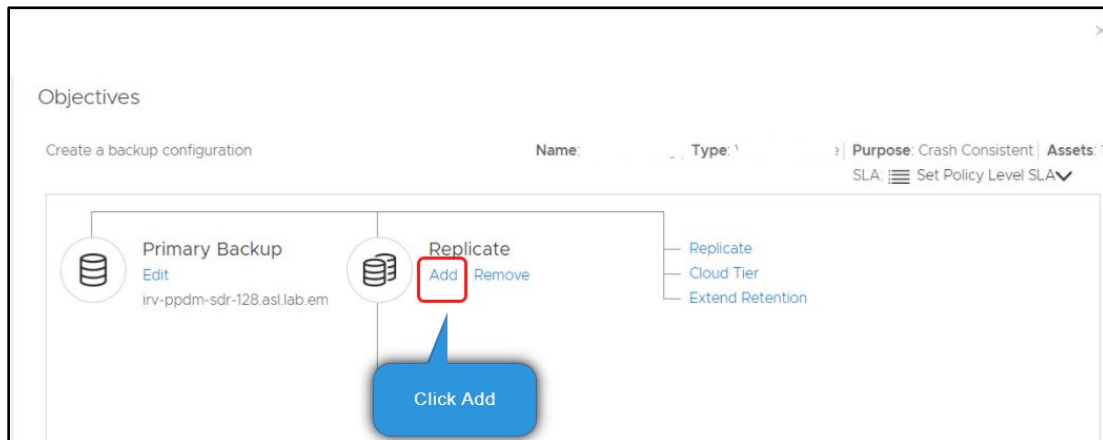


Figure 18 Replication Configuration

Complete the schedule details in the **Add Replication** dialog, and then click **Save** to save your changes.

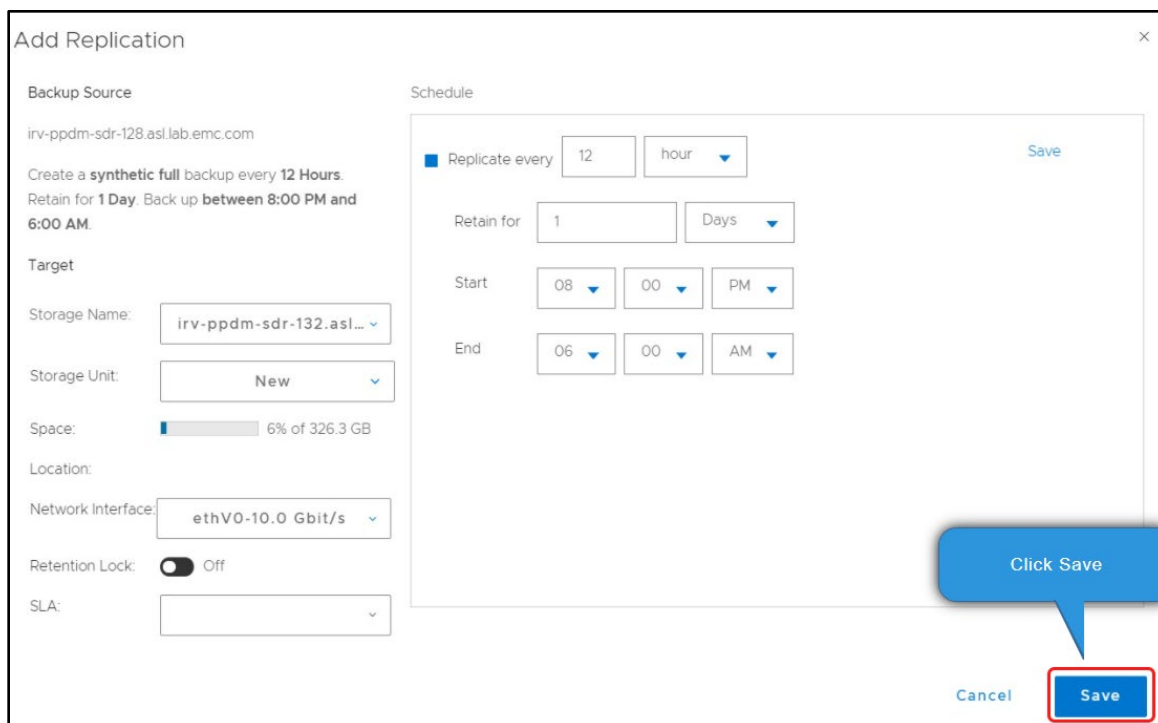


Figure 19 Replication Configuration

The Data Manager cloud tier feature works in tandem with the Data Domain Cloud Tier feature to move Data Manager backups from the PowerProtect DD series appliance to the cloud. This feature provides long-term storage of Data Manager backups by seamlessly and securely tiering data to the cloud. From the Data Manager UI, you configure the replication to move data to another PowerProtect DD series appliance and also configure cloud tier to move Data Manager backups from PowerProtect DD series appliance to the cloud. You can also perform seamless recovery of these backups. DD cloud storage units must be preconfigured on the PowerProtect DD series appliance before they are configured for cloud tier in the Data Manager UI. See the [DD OS Administration Guide](#) for more information.

Both Exchange centralized and self-service protection policies support replication and cloud tiering. You can create the cloud tier schedule from both primary and replication stages. Schedules must have a minimum weekly recurrence and a retention time of 14 days.

Click **Cloud Tier** next to **Primary Backup** or **Extend Retention** or, if adding a cloud stage for a replication schedule that you have added, click **Cloud Tier** under **Replicate**. An entry for **Cloud Tier** is created to the right of the primary or extended retention backup schedule, or below the replication schedule.

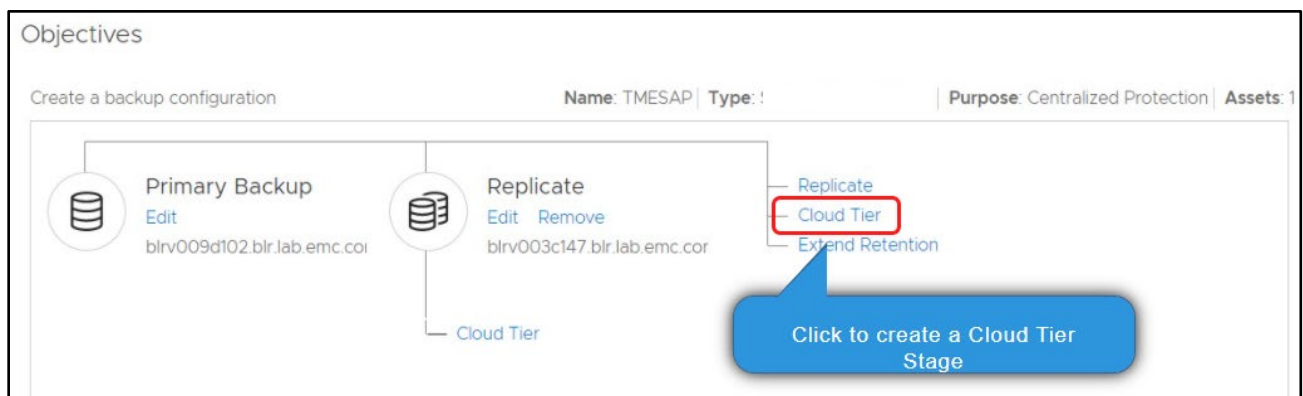


Figure 20 Cloud Tier Configuration

Under the entry for **Cloud Tier**, click **Add**.

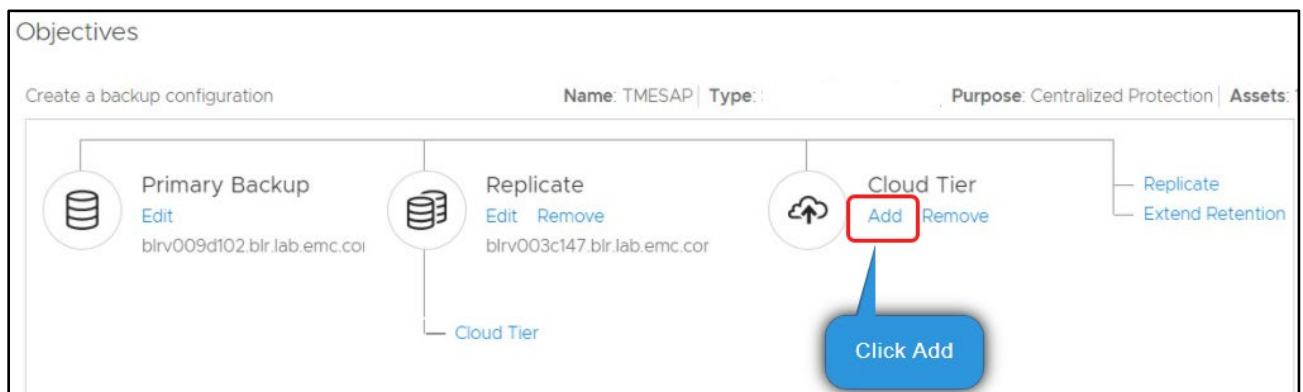
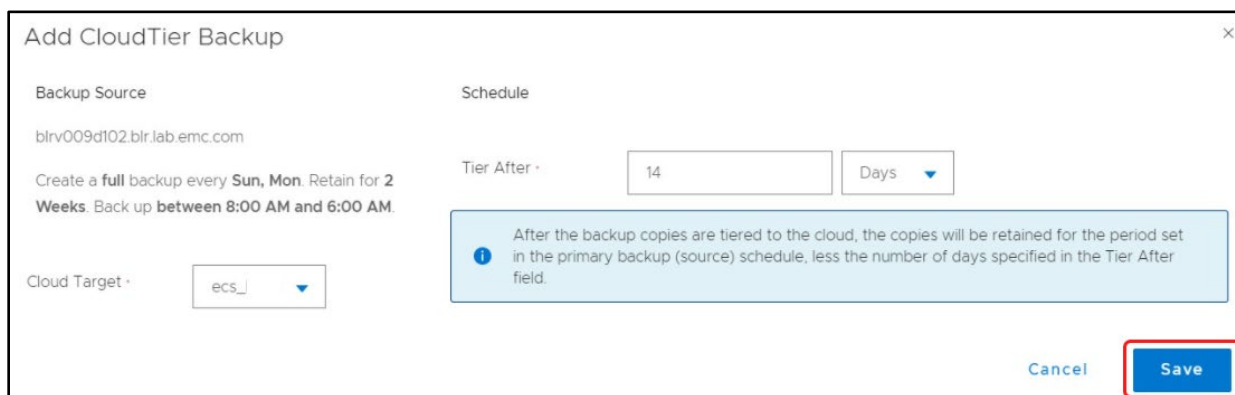


Figure 21 Cloud Tier Configuration

The **Add Cloud Tier Backup** dialog appears, with summary schedule information for the parent node to indicate whether you are adding this cloud tier stage for the primary backup schedule, the extended retention backup schedule, or the replication schedule.

Complete the schedule details in the **Add Cloud Tier Backup** dialog, and then click **Save** to save your changes



The dialog box titled "Add CloudTier Backup" contains the following fields and information:

- Backup Source:** blrv009d102.blr.lab.emc.com
- Schedule:** Create a **full** backup every **Sun, Mon**. Retain for **2 Weeks**. Back up **between 8:00 AM and 6:00 AM**.
- Tier After:** 14 Days
- Cloud Target:** ecs_
- Information:** After the backup copies are tiered to the cloud, the copies will be retained for the period set in the primary backup (source) schedule, less the number of days specified in the Tier After field.
- Buttons:** Cancel and Save (highlighted with a red box).

Figure 22 Cloud Tier Configuration

Protection Policy summary Lists **Replicate** and **Cloud Tier**.

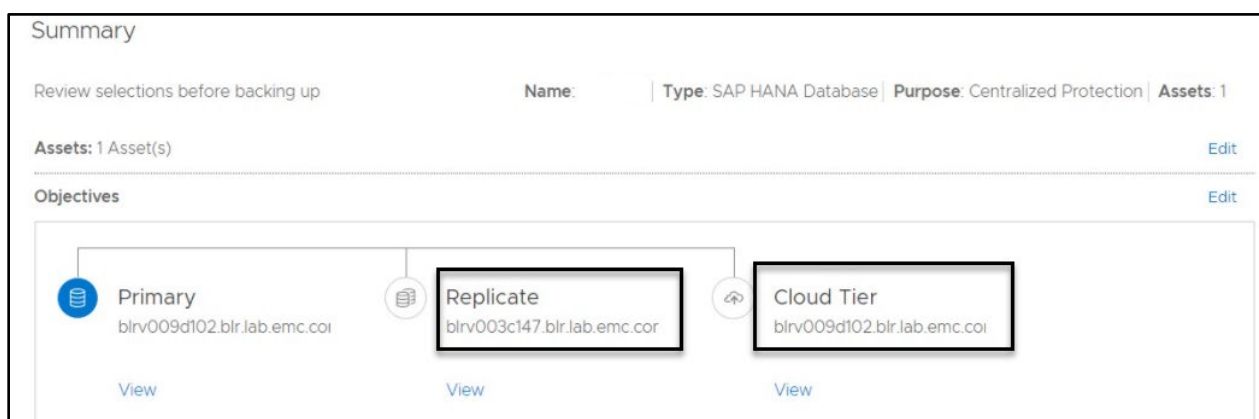


Figure 23 Replication and Cloud Tier Configured

Note : For detailed steps for replication and cloud tier see [PowerProtect Data Manager Administration and User Guide](#).

7 Disaster recovery of Exchange Server

When a disaster scenario occurs, the Microsoft application agent can provide disaster recovery of data that is on both a PowerProtect DD series appliance server and Data Domain Cloud Tier.

Follow these steps to perform a disaster recovery on the new disaster recovery host.

- Start the Exchange Server application and the required services.
- Create the databases that existed before the disaster and ensure that the databases are in the mounted state.
- Perform a restore of the databases.

7.1 Perform disaster recovery from the DD Cloud Tier

The Microsoft application agent provides a command-line tool to complete disaster recovery of save sets that are in a Data Domain Cloud Tier. After an MTree is recovered according to the disaster recovery procedure, you must restore the backup indexes from the Data Domain Cloud Tier.

When the Microsoft application agent moves a backup to the cloud, the index files are maintained on the active tier. A copy of the index files is created and moved to the cloud tier for long-term retention.

After an MTree is restored during a disaster recovery, all the files that resided only on the active tier are lost and unavailable. Only the file that were moved to the cloud are available. In this case, you must run **msagentadmin** administration with the **--dr-recall** parameter to restore the indexes.

After the indexes are recalled to the active tier, the data save sets for the same time range are also recalled unless you type **n** when prompted and browse to the recall of the found save sets [y/n]. If you choose to not recall the save sets, you can manually recall the save sets later.

Use the **msagentadmin** administration command with the following syntax to recall the indexes to the active tier:

```
msagentadmin.exe administration --dr-recall --ddhost "<Data_Domain_server_name>"
--ddpath
"<name_and_path_of_storage_unit>" --dduser "<DDBoost_username>" --appID
<application_ID>
```

- **--dr-recall:**
Specifies an operation to recall save sets for disaster recovery. You can use the **-M** alias for the **--dr-recall** parameter.
- **--ddhost "<name>":**
Specifies the name of the PowerProtect DD series appliance server that contains the storage unit, to which you backed up the databases.
- **--ddpath "/<storage_unit_name_and_path>":**
Specifies the name and the path of the storage unit, to which you backed up the databases.
- **--appID "<application_ID>→":**
Specifies the application ID (namespace) to locate backups. Specify **msapp_bbb** for Exchange Server. You can use the **-n** alias for the **--appID** parameter

Consider the following example commands to perform disaster recovery of Exchange Server with data on a PowerProtect DD Series Appliance Cloud.

Tier device:

- Cloud tier disaster recovery recall command without a configuration file:

```
msagentadmin administration --dr-recall --tier --after 1481104962 --before  
1481105533 -appID msapp_bbb --ddhost "10.70.102.111" --ddpath "/mt1" --dduser  
"ost" --confirm -client myDD.msapp.com --debug 9
```

- Cloud tier disaster recovery recall command with a configuration file:

```
msagentadmin.exe administration --dr-recall --tier --after 1481104962 --before  
1481105533 --appID msapp_bbb --confirm --config c:\temp\config_pp.txt --debug 9
```

8 Conclusion

Dell EMC PowerProtect Data Manager enables complete control of Microsoft Exchange database backup and disaster recovery to backup administrators. The advanced integration between Data Manager and Microsoft Exchange provides a fast and efficient database backup and restore solution.

A Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.

[Storage and data protection technical white papers and videos](#) provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

A.1 Related resources

- [PowerProtect Data Manager Microsoft Application Agent Exchange Server User Guide](#)
- [PowerProtect DD Series Appliance Operating System Administration Guide](#)
- [PowerProtect Data Manager Administration and User Guide](#)