Technical White Paper

Dell EMC PowerProtect Cyber Recovery-Automated Recovery of PowerProtect Data Manager

Abstract

This white paper explains the steps to recover Dell EMC™ PowerProtect Data Manager using Dell EMC PowerProtect Cyber Recovery.

July 2021

Revisions

Date	Description
October 2020	Initial release
July 2021	Document revised for PowerProtect Cyber Recovery 19.8 release

Acknowledgments

Author: Charu

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.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Table of contents

Executive summary

Data is one of the most important assets of the Internet economy and must be protected against any kind of technology crimes including ransomware and breaches. Continuous flow of data across interconnected networks and digital transformation tends to put sensitive information at risk. Such attacks destroy or steal the data and even backups are compromised. Hence, it becomes crucial to have backup secure if there is any attack. Dell EMC™ PowerProtect Cyber Recovery software provides this protection by replicating backup data from a production system to a secure air-gapped vault system. This white paper focuses on the steps to recover Dell EMC PowerProtect Data Manager using PowerProtect Cyber Recovery.

1 Introduction

Cyber Recovery keeps customers' business critical data and technology configurations in a secure air-gapped environment that can be used for recovery or analysis. The Cyber Recovery vault is isolated from unsecure system or network.

The Cyber Recovery solution enables access to the Cyber Recovery Vault only long enough to replicate data from the production system. At all other times, the Cyber Recovery Vault is secured and off the network. Deduplication process on Production Dell EMC PowerProtect DD series appliances expedites the replication process so that connection time to the Cyber Recovery Vault is as short as possible.

Within the Cyber Recovery Vault, the Cyber Recovery software creates point-in-time (PIT) retention-locked copies that can be validated and then used for recovery of the production system.

2 Pre-requisites for a PowerProtect Data Manager Recovery

Ensure that the following prerequisites are met before PowerProtect Data Manager recovery is initiated.

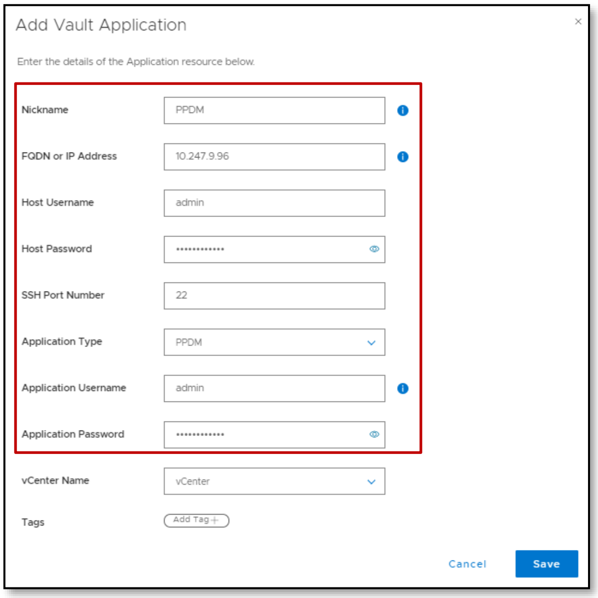
2.1 Requirements to be met in Production environment

- The PowerProtect Data Manager application is defined as an application asset in the Cyber Recovery software. Use either the Cyber Recovery User Interface (UI) or the CRCLI to add the application.
- Ensure that there are no snapshots of the PowerProtect Data Manager virtual machine that is deployed in the vCenter server.
- Ensure both client and PowerProtect Data Manager server backup is writing to production DD series.
- Replication context is configured for both data mtree and PowerProtect Data Manager server backup mtree.
- Perform a Secure Copy policy operation to copy data to the Cyber Recovery Vault environment.

2.2 Requirements to be met in Vault environment

- The Cyber Recovery Vault DD series system must be running DD Operating System (DDOS) Version 6.2 or later.
- Cyber Recovery virtual appliance is deployed in the Cyber Recovery Vault environment, and the PowerProtect Data Manager application is installed as the admin user.
- The UIDs that are associated with the production PowerProtect Data Manager DD Boost users are configured in the Cyber Recovery Vault DD series system. These UIDs must be available in the DD series system in the Cyber Recovery Vault.

  For example, when a backup is done using PPDM, DD Boost user will be automatically created in the production DD series with a UID (say 528). So, when automated recovery of PowerProtect Data Manager is initiated, Cyber Recovery will try to create same DD Boost user on vault DD series system with the same UID (528). If that UID is assigned to some other user, recovery will fail. Hence it is required to keep that UID free in vault DD series system for a successful recovery.
- The PowerProtect Data Manager virtual appliance is deployed which will be used as vault application. While adding PowerProtect Data Manager application in the Cyber Recovery Vault, it must be configured with the same credentials used for the PowerProtect Data Manager application on the production system.



Add Vault Application

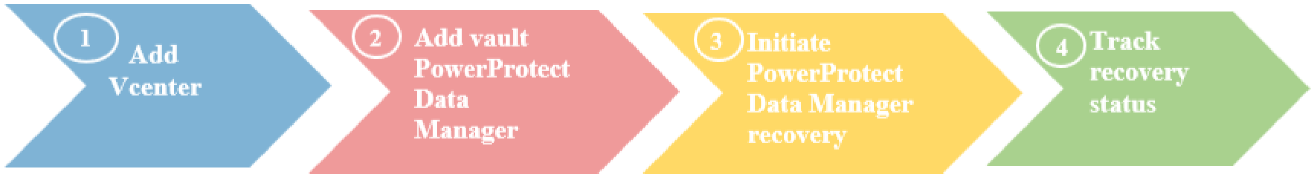
Enter the details of the Application resource below.

Nickname	PPDM
FQDN or IP Address	10.247.9.96
Host Username	admin
Host Password	•••••••••••••
SSH Port Number	22
Application Type	PPDM
Application Username	admin
Application Password	•••••••••••••
vCenter Name	vCenter
Tags	Add Tag +

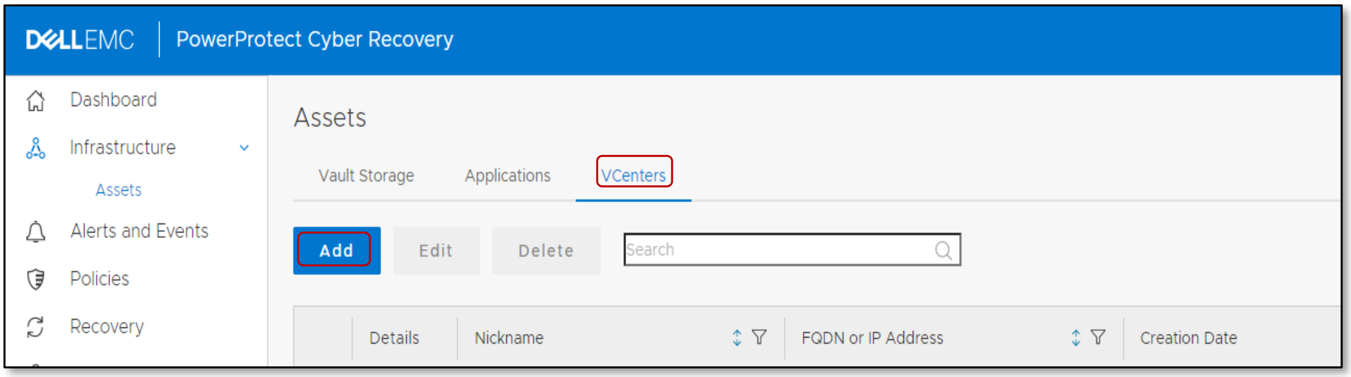
3 Steps to perform PowerProtect Data Manager automated recovery using the Cyber Recovery UI

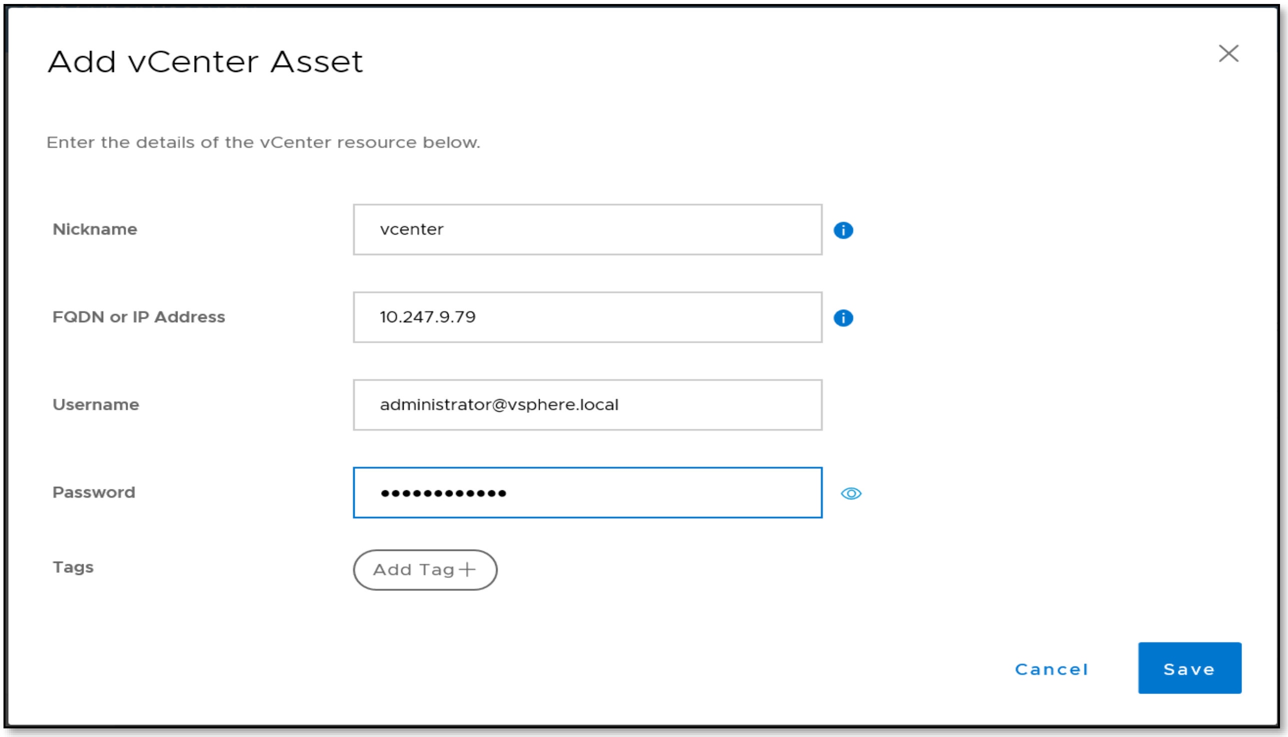
3.1 Performing a recovery job

The Cyber Recovery software prepares the environment which allows to run the recovery operation from the PowerProtect Data manager application console. Ensure that all the pre-requisites mentioned in the above section are met. The overall steps involved in the process are:


1 Add Vcenter
2 Add vault PowerProtect Data Manager
3 Initiate PowerProtect Data Manager recovery
4 Track recovery status

- **Add vCenter**: In the Cyber Recovery UI, add vCenter where vault PowerProtect Data Manager with the same hostname and IP is deployed. Vault PowerProtect Data Manager is a PowerProtect Data Manager deployed on the Cyber Recovery vault which is offline or air-gapped from the surface of attack.





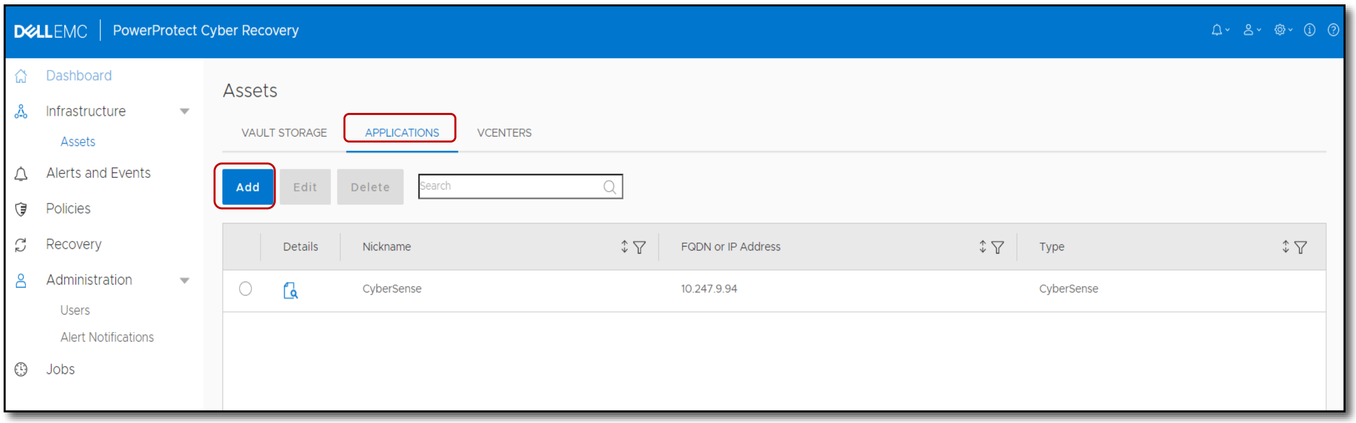
Add vCenter Asset

Enter the details of the vCenter resource below.

Nickname	vcenter
FQDN or IP Address	10.247.9.79
Username	administrator@vsphere.local
Password	•••••••••••••
Tags	Add Tag +

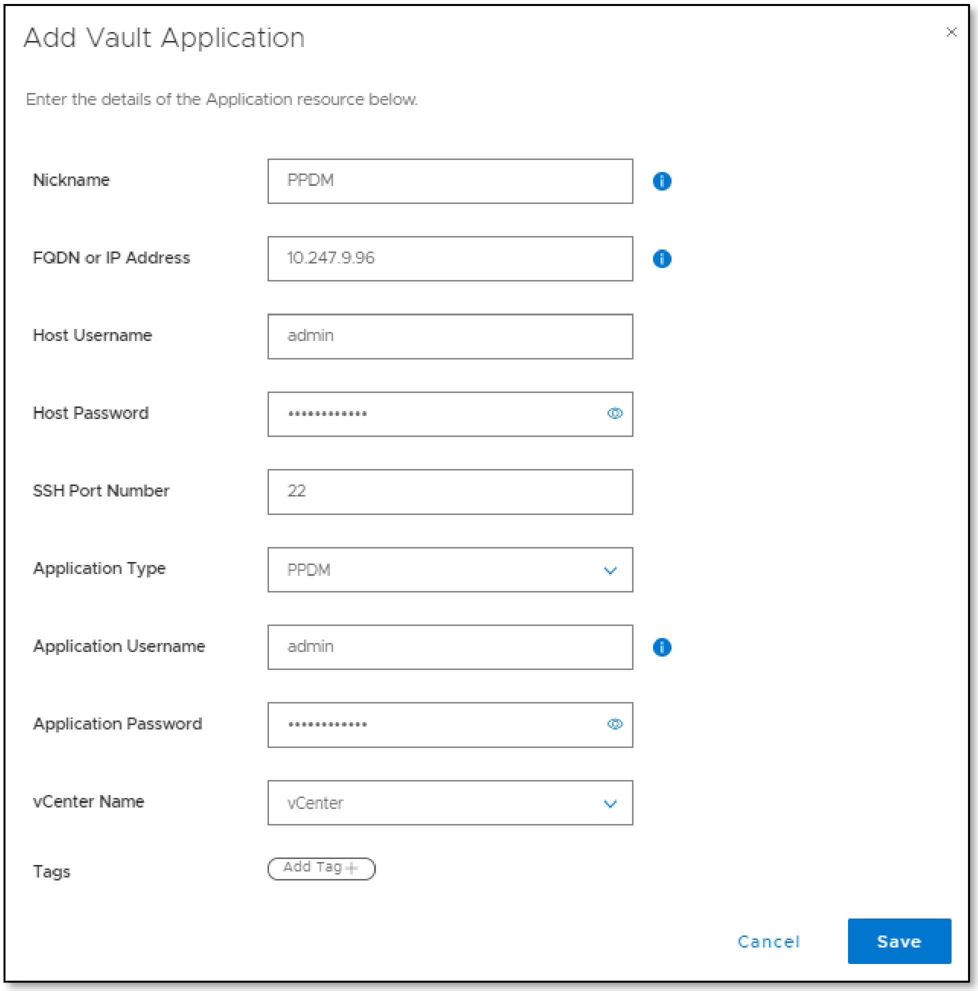
- **Add vault PowerProtect Data Manager**: Add vault PowerProtect Data Manager application asset in the Cyber Recovery UI.

  Note: Before adding vault PowerProtect Data Manager, user needs to launch the vault PowerProtect Data Manager console and edit **/etc/ssh/sshd_config** file and change the **PasswordAuthentication** field to **yes**. Restart of sshd service on vault PowerProtect Data Manager is required after this.



	Details	Nickname	FQDN or IP Address	Type
○		CyberSense	10.247.9.94	CyberSense

Add the Vault PowerProtect Data Manager details with the same credentials which were used for PowerProtect Data Manager in production environment. Cyber Recovery will automatically push these credentials to vault PowerProtect Data Manager during the recovery.

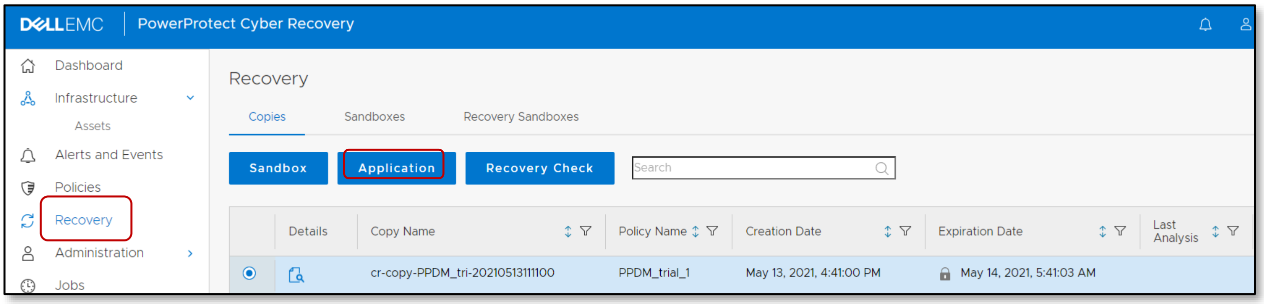


Add Vault Application

Enter the details of the Application resource below.

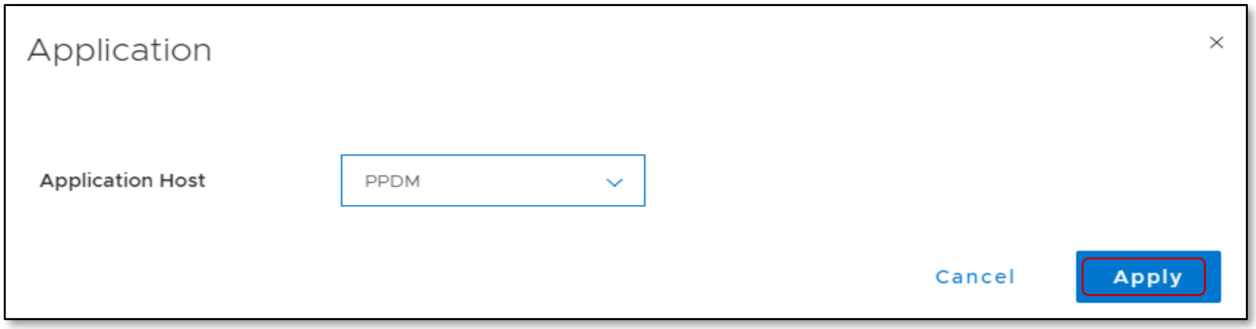
Nickname	PPDM
FQDN or IP Address	10.247.9.96
Host Username	admin
Host Password	•••••••••••••
SSH Port Number	22
Application Type	PPDM
Application Username	admin
Application Password	•••••••••••••
vCenter Name	vCenter
Tags	Add Tag +

- **Initiate PowerProtect Data Manager recovery**: Select the appropriate good copy that is to be recovered for the PowerProtect Data Manager policy and start the recovery process.



	Details	Copy Name	Policy Name	Creation Date	Expiration Date	Last Analysis
●		cr-copy-PPDM_tri-20210513111100	PPDM_trial_1	May 13, 2021, 4:41:00 PM	🔒 May 14, 2021, 5:41:03 AM	

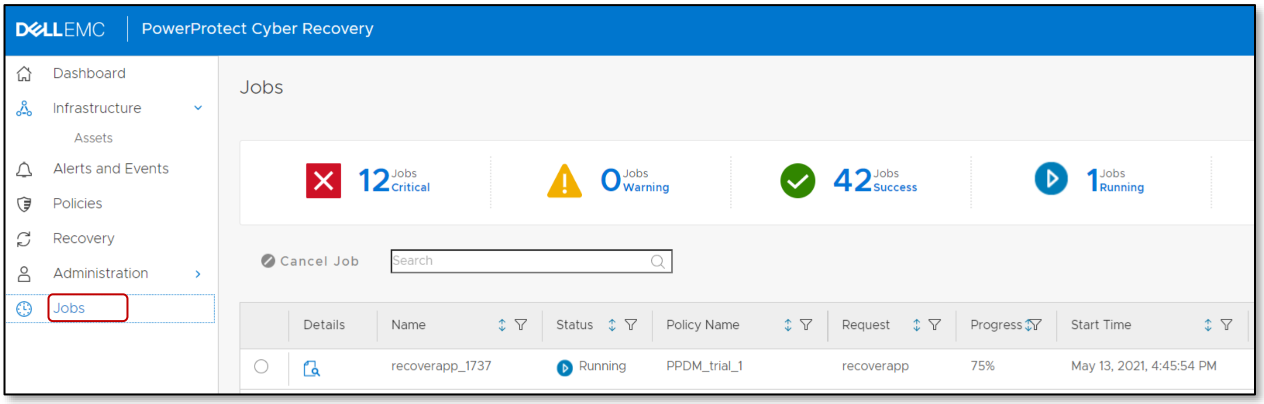
Select PPDM as application host and continue.



Application

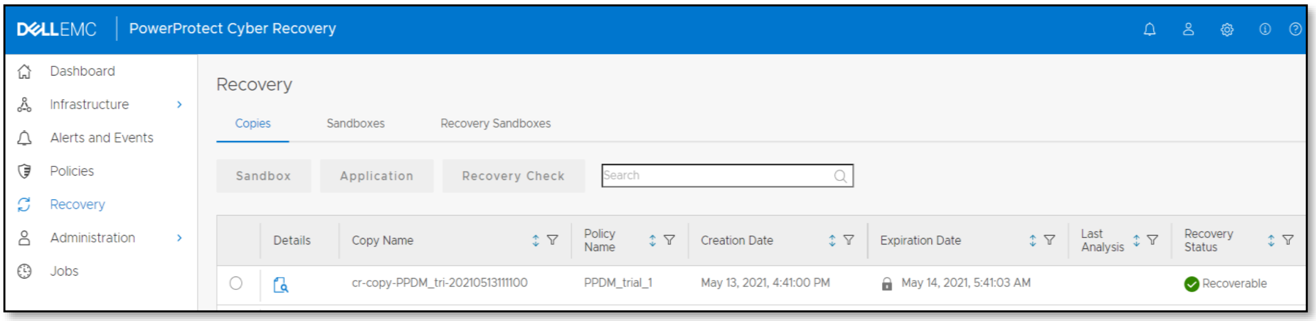
Application Host: PPDM

- **Recovery Progress**: The recovery can be monitored from the Jobs section and would take approximately 15 to 20 minutes. A recovery sandbox is created for the PowerProtect data manager application. A sandbox is a kind of security mechanism which provides an isolated environment for diminishing the system failures and software vulnerabilities from spreading.



Details	Name	Status	Policy Name	Request	Progress	Start Time
	recoverapp_1737	Running	PPDM_trial_1	recoverapp	75%	May 13, 2021, 4:45:54 PM

- **Recovery status**: Appropriate status will be shown after the completion of the recovery test.



Details	Copy Name	Policy Name	Creation Date	Expiration Date	Last Analysis	Recovery Status
	cr-copy-PPDM_tri-20210513111100	PPDM_trial_1	May 13, 2021, 4:41:00 PM	May 14, 2021, 5:41:03 AM		Recoverable

There are three recovery statuses:

- **Recoverable -** Copy passed the recovery test and recovery is complete
- **Not Recoverable -** Copy did not pass the recovery test and recovery is not complete
- **Failed -** Recovery Job failed for some reason

3.2 Canceling a recovery job

If recovery process is to be canceled after initiating the recovery for PowerProtect Data Manager, follow this procedure:

- Select **Jobs** from the main menu
- Select the running recovery job
- Click **Cancel job**

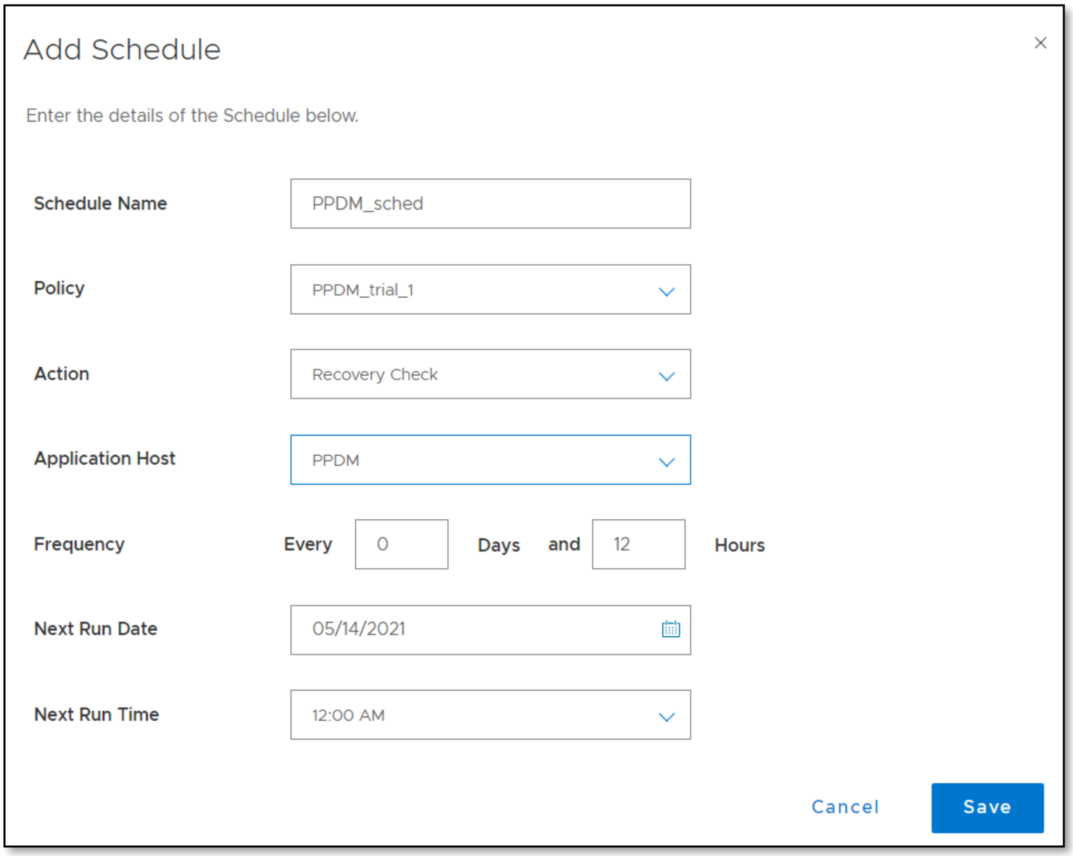
The recovery job is canceled, and the Cyber Recovery software automatically deletes the sandbox, reverts the VM back to the virtual snapshot, and the DD series system shows the status of the MTree that was associated with the sandbox is deleted.

4 Recovery check

Instead of running actual recovery, a copy can be verified by performing the recovery check option to see if the copy is recoverable. The recovery check process can be run on demand or can be scheduled.

4.1 Schedule a recovery check

- Select **Policies** from the Main Menu
- Click **SCHEDULES** at the top of the Policies content pane
- Click **Add** and complete the fields in the dialog box



Add Schedule

Enter the details of the Schedule below.

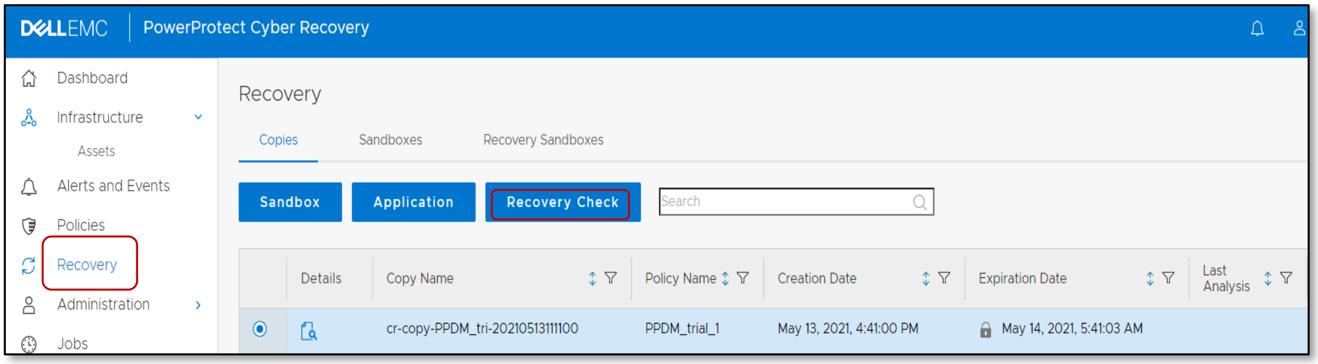
Schedule Name	PPDM_sched
Policy	PPDM_trial_1
Action	Recovery Check
Application Host	PPDM
Frequency	Every 0 Days and 12 Hours
Next Run Date	05/14/2021
Next Run Time	12:00 AM

- Click **Save**

The recovery check runs using the values that were defined in the recovery check schedule.

4.2 Run an on-demand recovery check

- Select **Recovery** from the Main Menu
- Under **Copies**, select a copy
- Click **Recovery Check**



	Details	Copy Name	Policy Name	Creation Date	Expiration Date	Last Analysis
●		cr-copy-PPDM_tri-20210513111100	PPDM_trial_1	May 13, 2021, 4:41:00 PM	🔒 May 14, 2021, 5:41:03 AM	

5 Post recovery steps for a PowerProtect Data Manager Recovery

The post recovery steps to be performed once the PowerProtect Data Manager has been recovered are as follows:

- Delete the sandbox that was created when PowerProtect Data Manager recovery was initiated.
    - From the Main Menu, click **Recovery** and then click **RECOVERY SANDBOXES** from the top of the **Recovery** pane
    - Select the recovery sandbox
    - Click **Cleanup**

  The sandbox is deleted, and the Cyber Recovery software reverts the PowerProtect Data Manager software to the snapshot that was created when the recovery was initiated.

- To validate success, click **Launch App** to access the PowerProtect Data Manager UI in the Cyber Recovery Vault.

  The **Welcome to PowerProtect Data Manager** window appears.

- Optionally, on the DD series system, run the file sys clean command.

  This step deletes the DD Boost storage unit. If this step is not performed, the DD Boost storage unit is deleted during the next scheduled cleaning operation.

- To verify the recovery for SQL, Oracle, and file system workloads:
    - For Windows deployments:
        a. Go to C:\Program Files\DPSAPPS\AgentService.
        b. Run the unregister.bat command to unregister the agent.
        c. If necessary, delete the ssl folder from the Agent Service folder.
        d. Run the register.bat command to register the host with PowerProtect Data Manager again.
        e. From the PowerProtect Data Manager Main Menu, go to **Protection** > **Protection Policies**. Select the policy and click **Set Lockbox** to run the configuration job again.
    - For Linux deployments:
        a. Go to /opt/dpsapps/agentservice.
        b. Run the unregister.bat command to unregister the agent.
        c. If necessary, delete the ssl folder from the Agent Service folder.
        d. Run the register.bat command to register the host with PowerProtect Data Manager again.
        e. From the PowerProtect Data Manager Main Menu, go to **Protection** > **Protection Policies**. Select the policy and click **Set Lockbox** to run the configuration job again.

6 Conclusion

PowerProtect Cyber Recovery provides a convenient and simplistic interface for PowerProtect Data Manager recovery. It also provides the provision to do a recovery check on the copies without performing an actual recovery which makes it easier for the users to analyze the copies and be prepared in case the need for recovery arises.

A Technical support and resources

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

- Cyber Recovery Installation Guide
  Dell EMC PowerProtect Cyber Recovery Installation Guide

- Cyber Recovery Product Guide
  Dell EMC PowerProtect Cyber Recovery Product Guide

- Cyber Recovery Solution Brief
  Dell EMC PowerProtect Cyber Recovery