Dell PowerProtect Cyber Recovery: Reference Architecture

October 2022

H18661.3

Reference Architecture

Abstract

This document describes the features and reference architecture of Dell PowerProtect Cyber Recovery—another layer of protection to customers' data protection infrastructure.

Dell Technologies

Copyright

Published in the USA October 2022 H18661.3.

Contents

Executive summary

Overview

As organizations become increasingly aware of the cybersecurity risks that threaten their mission-critical operations and their reputation, IT security has become an essential part of enterprise digital strategy. According to the Gartner 2020 Board of Directors Survey, cybersecurity-related risk is rated as the second-highest source of risk for the enterprise, following regulatory compliance risk.

According to Gartner, 40 percent of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member by 2025. Currently, only 10 percent of companies have this type of committee. This is one example of many organizational changes that Gartner expects to see at the board, management, and security team level in response to greater risk created by the expanded digital footprint of organizations.

Global business relies on the constant flow of data across interconnected networks, and digital transformation has increased the transfer of sensitive data. This increased data flow presents ample opportunity for cyber threats, exposure of data for ransom, corporate espionage, or even cyber warfare.

Dell Technologies and Dell PowerProtect Cyber Recovery protect business-critical data and minimize the impact of a cyberattack. The PowerProtect Cyber Recovery solution offers a higher likelihood of success in the recovery of business-critical systems.

Cyber Recovery provides proven, modern, and intelligent protection to isolate critical data, identify suspicious activity, and accelerate data recovery. This protection allows normal business operations to resume quickly after a cyber-attack.

Audience

This white paper is intended for Dell Technologies' customers, partners, and employees who would like to understand the PowerProtect Cyber Recovery solution.

Revisions

Date	Description
June 2021	Initial release
April 2022	Updated white paper content with Cyber Recovery 19.10 version
August 2022	Updated white paper content with Cyber Recovery 19.11 version
October 2022	Updated white paper content with Cyber Recovery 19.12 version

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Vinod Kumar

Note: For links to other documentation for this topic, see the PowerProtect Cyber Recovery Info Hub.

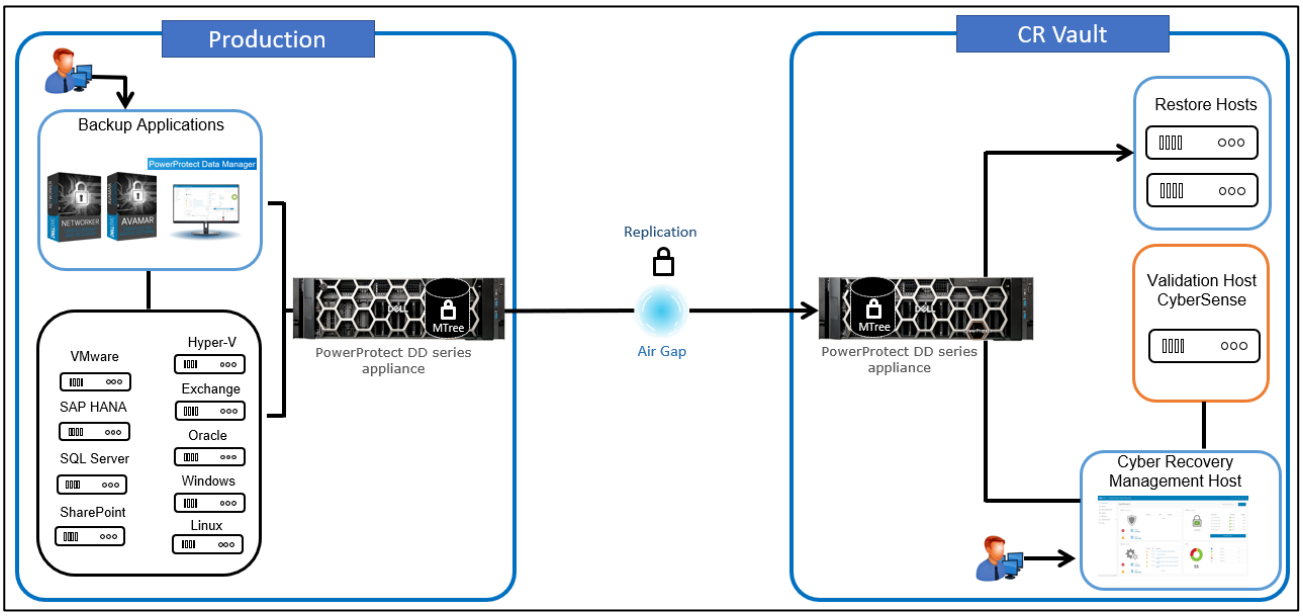
Introduction

Dell PowerProtect Cyber Recovery

PowerProtect Cyber Recovery enables automated workflows to augment data protection infrastructure with true data isolation, data forensics, analytics, and, most importantly, data recovery for increased business resiliency. Cyber Recovery combines multiple layers of protection and security into a turnkey solution to provide maximum protection for critical data.

The Cyber Recovery solution protects the backed-up mission-critical business data and technology configurations in a secure vault environment that can be used for data recovery. The management software also enables creation of writable sandbox copies for data validation and analytics.

The Cyber Recovery vault is disconnected from the production network through an automated air gap. The vault stores all critical data off-network to isolate it from attack. Cyber Recovery automates data synchronization between production systems and the vault by creating immutable copies with locked retention policies.

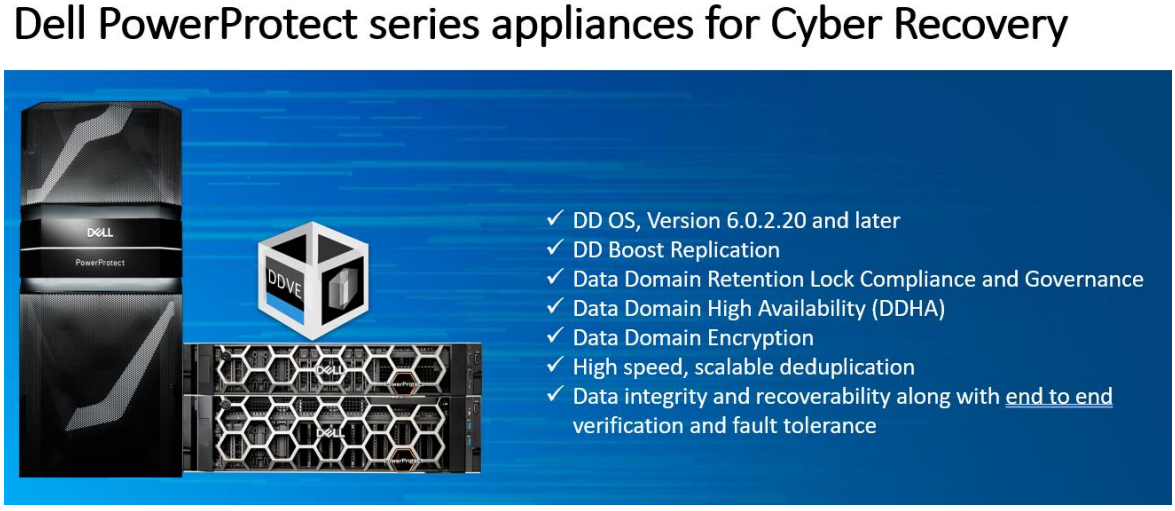


If a security breach occurs, the Security Officer or an admin user can manually secure the Cyber Recovery vault. During this time, the Cyber Recovery software does not perform any replication operations, even if they are scheduled. This action promotes business resiliency, provides assurance following extreme data loss or destruction, and includes both business and technology configuration data to enable rapid recovery of the environment and resumption of normal business operations.

Dell PowerProtect DD series appliances for Cyber Recovery

PowerProtect DD series appliances are fast, secure, and efficient data protection appliances that support the Cyber Recovery solution and accommodate a unique Cyber Recovery vault.

Cyber Recovery works with DD series MTree replication technology to move and retain the protected copies of critical data in the Cyber Recovery vault. Cyber Recovery supports up to five DD series in the Cyber Recovery vault.



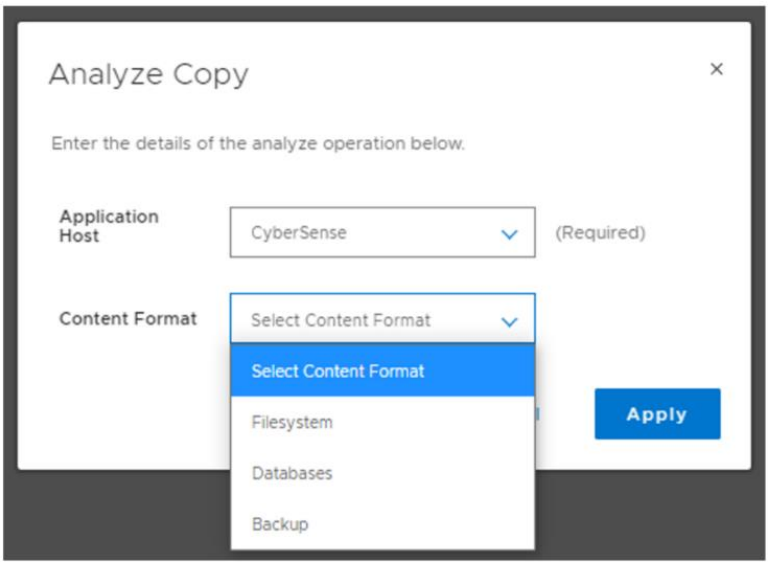
Required DD series licenses for Cyber Recovery include DD Boost, Replication, Retention Lock Governance, and Retention Lock Compliance.

Cyber Recovery features

The Cyber Recovery solution key features include:

- Secure data in an isolated network with an automated operational air gap
- Policy-based secure copy creation, management, and scheduling
- Integration with Index Engine CyberSense software to detect if the backup data has been compromised
- Robust REST API framework that enables analytics with artificial intelligence (AI) and machine learning (ML) for malware (including ransomware). Cyber Recovery REST API availability on Dell Marketplace and Stoplight
- Recovery assistance and the ability to export data to a recovery host easily
- Automated recovery options for the NetWorker and PowerProtect Data Manager applications
- Optional multifactor authentication enabled from the UI or command-line interface (CLI) to provide added protection for the Cyber Recovery software and its resources
- Informative dashboards that show system alerts, the state of the Cyber Recovery vault, and critical details
- Ability to transmit alerts through SMTP outside the Cyber Recovery vault
- Support for high availability (HA) on DD series in the Cyber Recovery vault
- Replication window enforcement that stops a sync operation if it runs longer than the replication window
- Automatic retention locking feature that allows setting of retention lock with no additional operation. Cyber Recovery deployments running DDOS 7.8 support replicating a Retention Lock Compliance replication on the production system to the Cyber Recovery vault
- Ability to create a Cyber Recovery policy by selecting multiple MTree replication contexts (multiple MTrees are only supported for a PowerProtect Data Manager policy)
- Cyber Recovery supports subscription licensing model along with evaluation or proof-of-concept license that is valid for 90 days
- Sheltered Harbor endorsement for achieving compliance with financial institution data vaulting standards and certification, planning for operational resilience and recovery, and protecting financial critical data
- On-demand cleanup from the Cyber Recovery UI by clicking the **Maintenance** tab under the gear icon in the masthead navigation
- A maximum of three simultaneous login sessions for the Security Office (crso) for enhanced security
- Notification if a user's email address is modified or if multifactor authentication is disabled

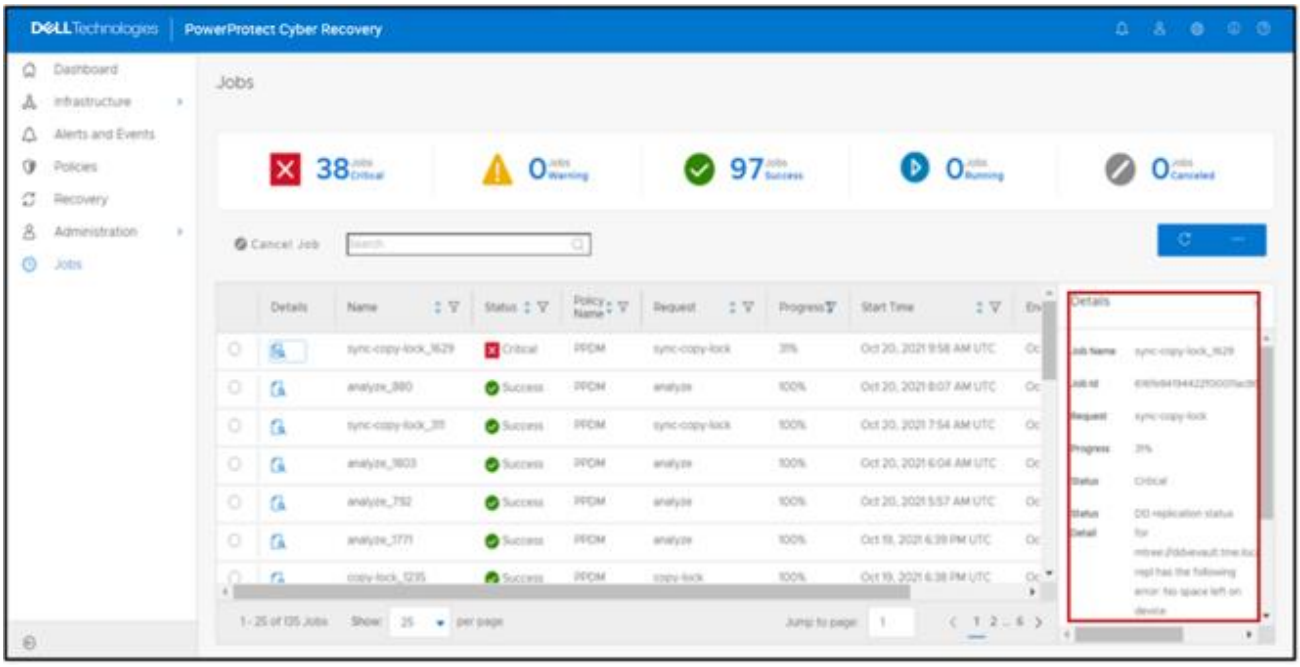
- Option to add a virtual Ethernet adapter to configure a separate IP address for SMTP communication from the Cyber Recovery vault if the Postfix mail transfer agent is used
- Support for recovery of PowerProtect Data Manager with Oracle, SQL, and file system workloads
- Option to provide the location of the latest bootstrap backup for a faster automated NetWorker recovery
- Support for the Cyber Recovery vault on Amazon Web Services (AWS), available from Amazon Marketplace using custom pricing
- Support for the Cyber Recovery software on a supported Linux operating system in a Microsoft Hyper-V environment
- Support for the analyze operation for PowerProtect Data Manager backups (Filesystem, VMware, and Oracle) is enabled
- Addition of REST API V6, which is backwards compatible with REST API V5 and V4. REST API V3 and earlier versions are no longer supported
- The "`crsetup.sh`" script to perform a readiness check before upgrading the Cyber Recovery software
- Support for multiple DDVE appliances for the Cyber Recovery vault on AWS—up to 5 DDVEs are supported
- CyberSense analysis report can be sent to additional email addresses
- Cyber Recovery telemetry feature sends telemetry information using one-way email to Dell Technologies for troubleshooting purposes. Telemetry can be run on demand using CRCLI or scheduled to run with frequency of minimum of one day and maximum of 30 days
- Cyber Recovery custom certificate support: users can generate a Certificate Signed Request (CSR), submit the CSR to Certificate Authority (CA) to apply for a CA signed certificate, and can add it to the Cyber Recovery system
- Secure reset option to regenerate the Cyber Recovery certificates – Starting with Cyber Recovery version 19.11, the `crsetup.sh` script includes an option that allows you to reset the Cyber Recovery root certificates and encryption keys when your deployment is compromised.
- From CRCLI and API, users have the option to:
  - Include or exclude files and file path from the analyze action
  - The content format of the MTree to be analyzed can be specified optionally, which is included as part of the CyberSense report for informational purposes



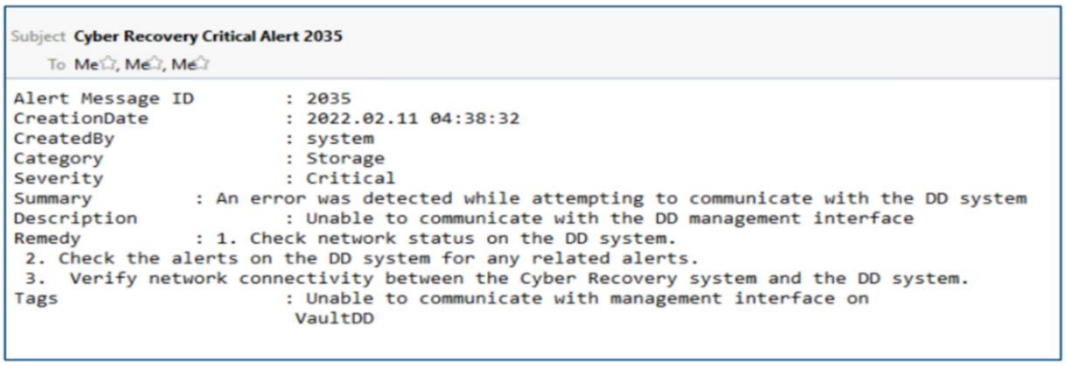
- Password expiration is set to 90 days by default; the value can be changed to a minimum of 30 days and a maximum of 180 days for all UI users

Cyber Recovery alert services

- DD series capacity alert
  - Cyber Recovery notifies a user if the Secure Copy/Sync operation fails due to space issues in Vault Data Domain. If the DD system in the Cyber Recovery vault generates a capacity alert, the Cyber Recovery software displays it as warning or critical alert on the dashboard and on the Alerts tab. The threshold capacity can be set on the DD system.



- Alert when one or more DD series is down:

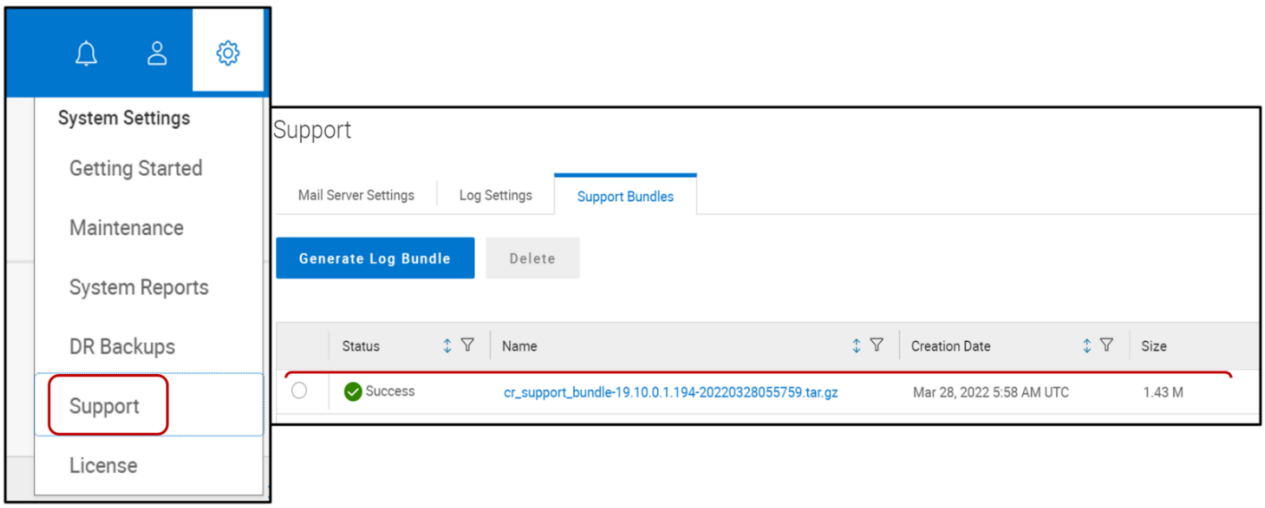


When a DD series in the Cyber Recovery vault is down, the Cyber Recovery software generates a critical alert that is displayed on the dashboard and on the Alerts tab. It also sends an email message to user accounts that are configured to receive email messages. The vault status is displayed as Degraded (orange icon) until the DD system is up and running again.

- Monitor Cyber Recovery services
  - Cyber Recovery 19.10 monitors its services in the background and alerts every hour after initial critical alert if one or more Cyber Recovery service is down. If a Cyber Recovery service stops, the Cyber Recovery software displays a critical alert on the dashboard and the Alerts tab. Use the `crsetup.sh` script to restart the service.

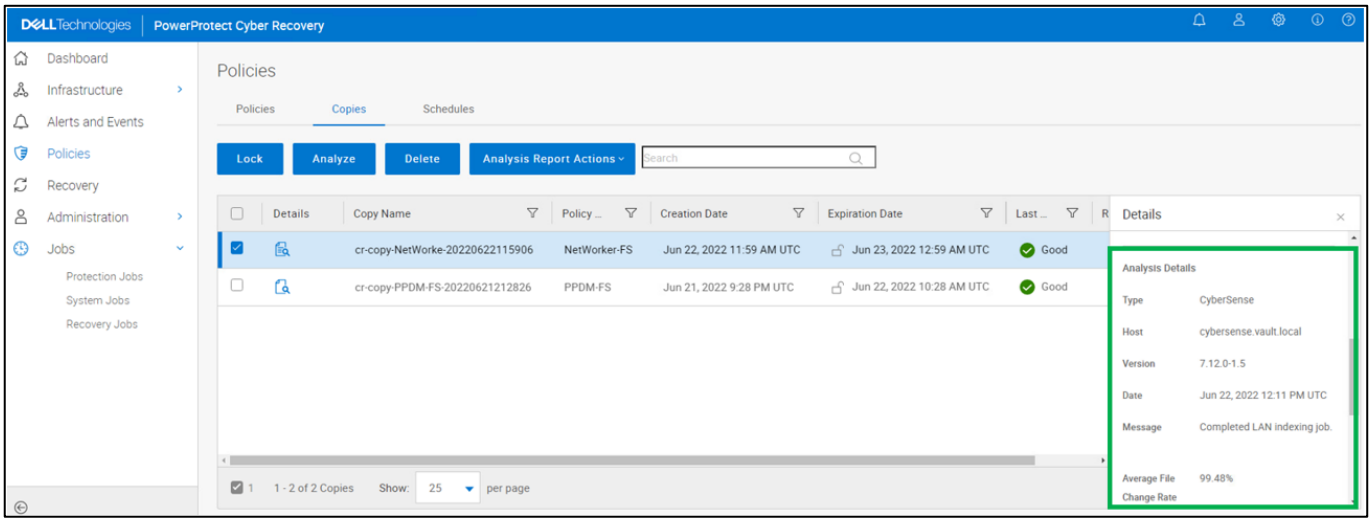
Cyber Recovery UI support menu

Cyber Recovery 19.10 provides a new support menu for users in Cyber Recovery UI. Users can generate and download the support bundle from Cyber Recovery UI.



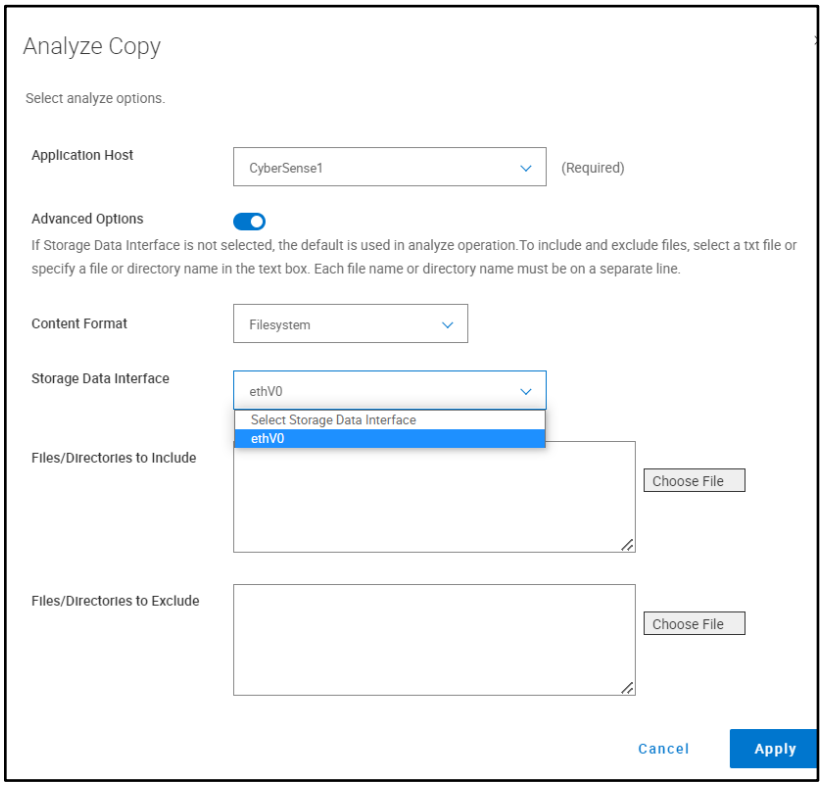
CyberSense host information in copy details

Cyber Recovery provides information about the analysis host which analyzed the copy in the copy details. This information helps users to identify the Cyber Sense details for environments with more than one CyberSense host.



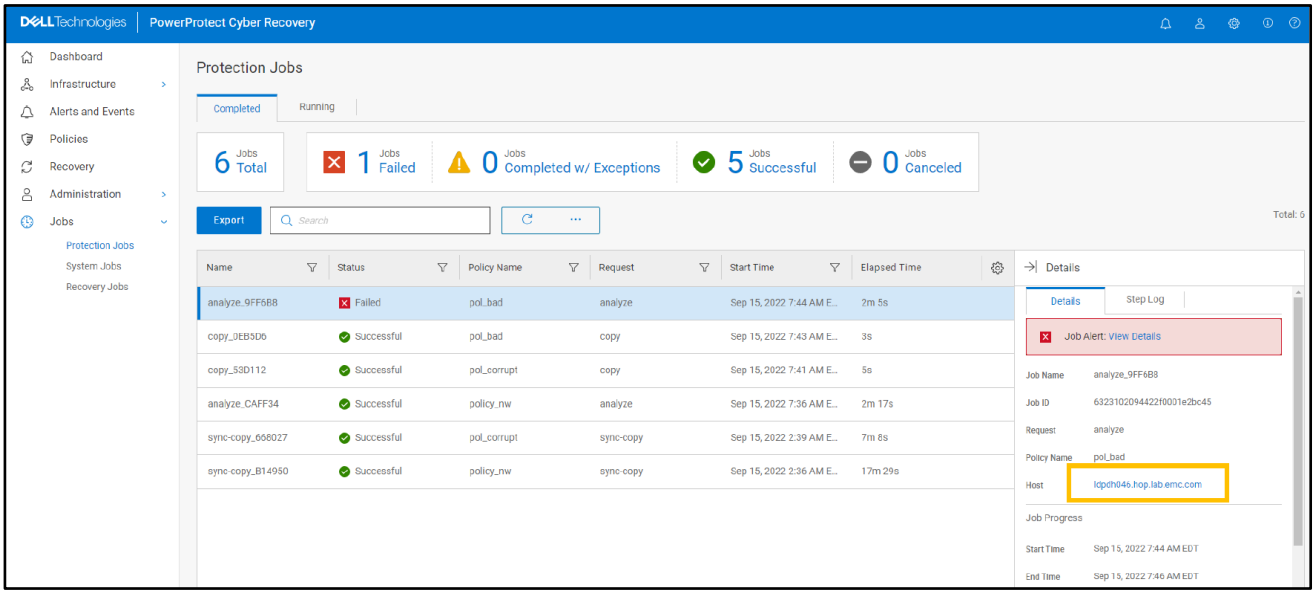
Policy network interfaces

Users can use eth V1 for analysis or for Cyber Recovery policy but cannot use both at the same time. For example, only ethV0 is listed in the following figure because ethV1 is being used for the Cyber Recovery policy.



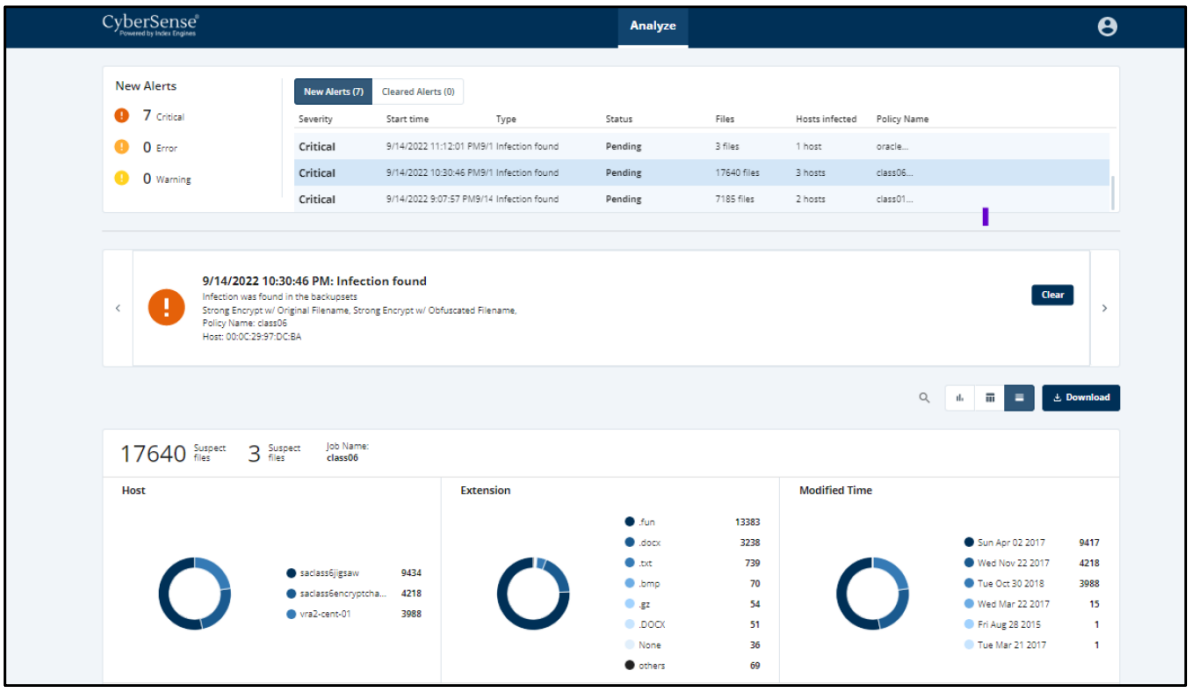
CyberSense analyze dashboard link from Cyber Recovery jobs

Starting with Cyber Recovery version 19.12, the job details section and policies/copies section have links that open the CyberSense analyze dashboard when a copy is found to be suspicious.



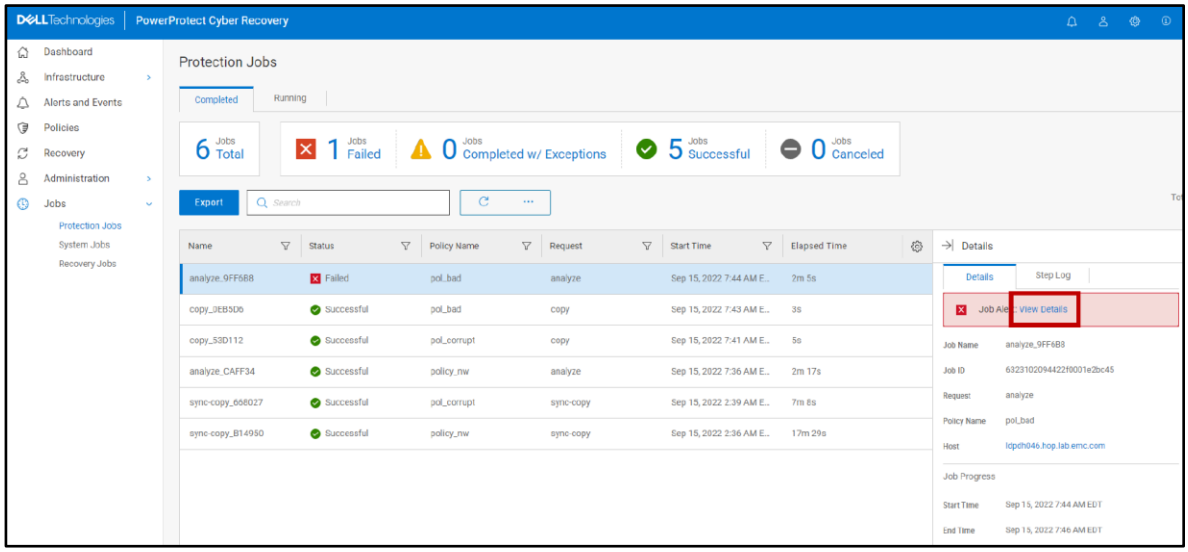
CyberSense analyze dashboard

CyberSense analyze dashboard is a UI that was designed specifically for CyberSense workflow. It provides the ability to scope and analyze a potential attack in a single dashboard.



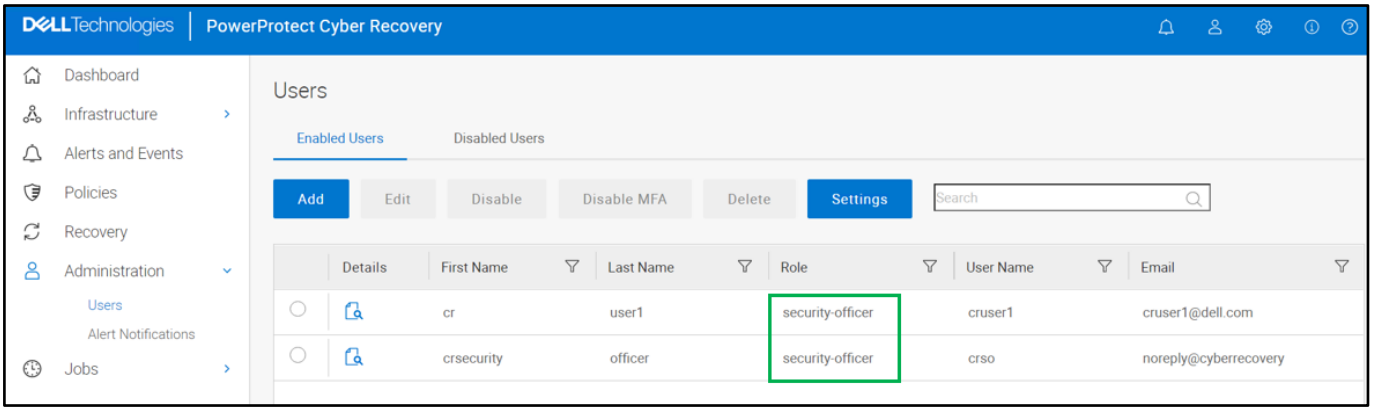
Links to the Alerts and Events page

Starting with Cyber Recovery version 19.12, any failed jobs that generated alerts have links to the "**Alerts and Events**" page and show the alert details.



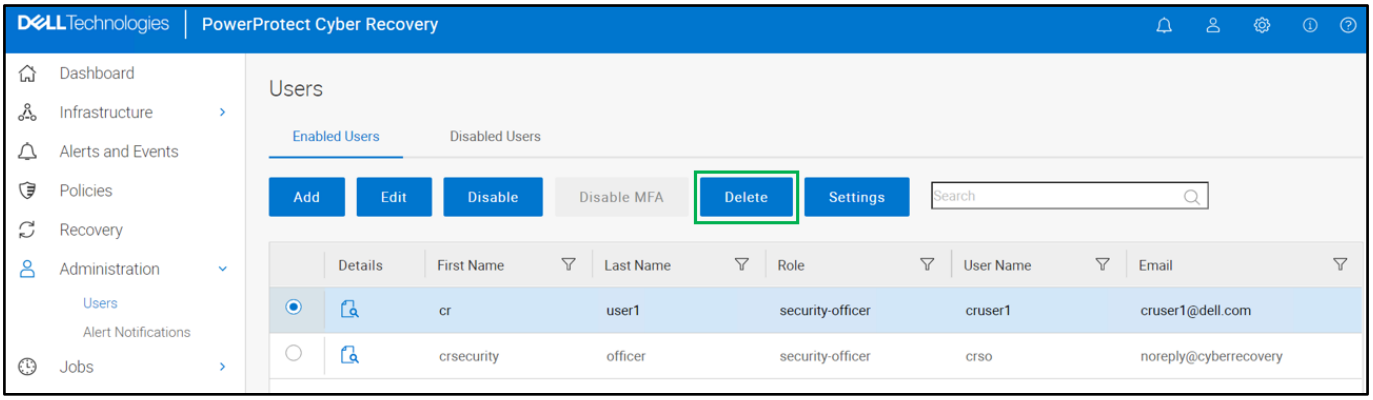
Cyber Recovery users and access management

Multiple security officer roles: Starting with Cyber Recovery version 19.12, the Cyber Recovery security officer (crso) can create multiple security officer roles and manage those accounts. The security officer has the same permissions as the crso but cannot manage the crso account.



Note: Security officer users cannot create other security officer users. The “Admin” role will no longer be able to create users.

Users’ deletion: Starting with Cyber Recovery version 19.12, the crso and security officer can delete security officer, admin, and dashboard users from the Cyber Recovery UI.



Note: One cannot add a user with the same username of a previously deleted user. Instead, add a user that has a different username.

Cyber Recovery support matrix

For details about compatibility, see the Dell PowerProtect Cyber Recovery Simple Support Matrix.

Cyber Recovery architecture

Production environment— For the production side of the solution, it is taken that the data to be protected as part of the Cyber Recovery solution is available in a format supported by the DD series and CyberSense. The data must be stored on a DD series MTree in the production environment.

Vault environment—The Cyber Recovery vault environment contains a DD series and the Cyber Recovery management host that runs the Cyber Recovery software. Data from the production environment enters the Cyber Recovery vault environment through DD series MTree replication. This environment can also contain various recovery and analytics/indexing physical or virtual hosts that integrate with the solution.

Cyber Recovery integrates with the Integrated Data Protection backup solution to maintain mission-critical business data in a secure vault environment for data recovery.

Server infrastructure is installed in the vault environment and is not shared with or connected to the production environment. Keeping vault server equipment separate from the production environment ensures that any ongoing issues (cyberattacks, operational issues, and so on) do not propagate into the vault environment.

Additional safeguards include an automated operational air gap that provides network isolation and eliminates management interfaces.

The server infrastructure in the Cyber Recovery vault can be deployed in multiple ways:

- Discrete physical servers
- Hyper-V, VMware ESXi with or without VSAN
- Dell VxRail appliance

Cyber Recovery solution components

The Cyber Recovery solution includes the following components:

Production DD series—The source DD series contains the production data that the Cyber Recovery solution protects.

Vault DD series—The DD series system in the Cyber Recovery vault is the replication target for the source DD series.

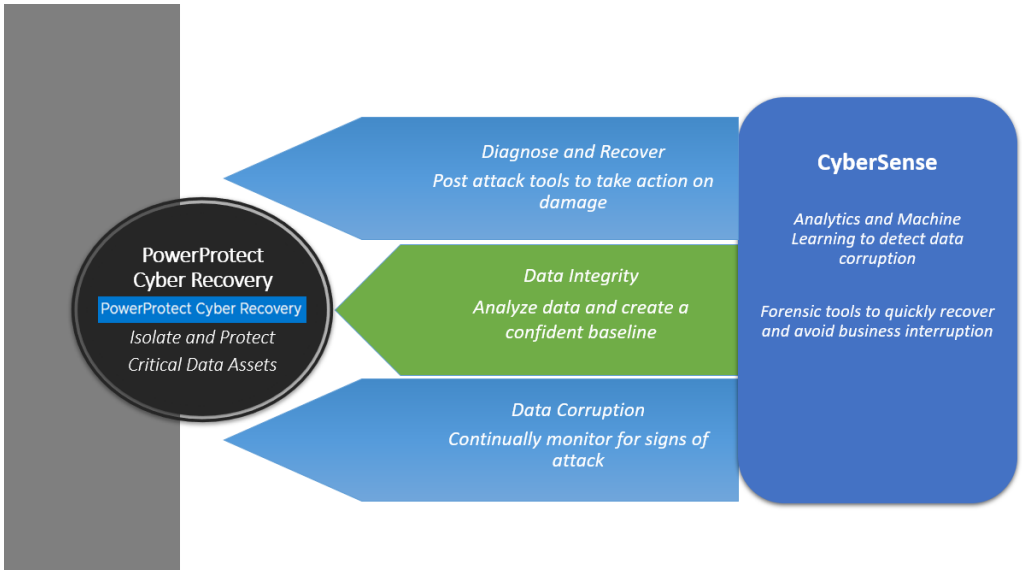
Cyber Recovery software—The Cyber Recovery software orchestrates synchronization, manages, locks the multiple data copies that are stored on the DD series in the Cyber Recovery vault, and orchestrates recovery. The software also governs the optional process of performing analytics on data that is stored on the DD series in the Cyber Recovery vault using the CyberSense feature.

Retention Lock (governance or compliance) software—Data Domain Retention Lock technology provides data immutability for a specified time. Retention Lock functionality is enabled based on Cyber Recovery policy configuration.

Cyber Recovery management host—Cyber Recovery software is installed on the management host. This server is installed in the vault environment.

Recovery hosts—The backup application recovery server is a designated server to which the backup application (NetWorker, Avamar, PowerProtect Data Manager, or other applications or combination of applications) and backup application catalog are recovered. Multiple servers can be deployed, depending on the recovery requirements of the solution. The backup application recovery server is sized so that all backup applications that are being protected by the Cyber Recovery solution can be recovered. If the Cyber Recovery solution is protecting a physical, single-node Avamar system in a production environment, a single-node Avamar system must also reside in the vault for recovery purposes.

Analytics/indexing host (CyberSense)—Cyber Recovery is the first solution to fully integrate with CyberSense. CyberSense adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. CyberSense is deployed on the Cyber Recovery vault environment. This innovative approach provides full content indexing. It uses machine learning (ML) to analyze the backup copies in the vault with over 100 content-based statistics and detects signs of corruption due to ransomware. CyberSense detects corruption with up to 99.5 percent confidence, identifies threats, and diagnoses attack vectors while protecting the business-critical content – all within the security of the vault.



Enhancements with CyberSense Version 7.9:

- Improved performance when indexing Dell Technologies backups on the PowerProtect DD server by using the DD Boost delta block API. CyberSense supports both performance Optimized and Capacity Optimized backups.
- Improved performance for the following workloads:
  - For Avamar - VMDK
  - For NetWorker - VMDK and file system Block Based Backup (BBB)
  - For PowerProtect Data Manager - VMDK, file system BBB, and Exchange

Enhancements with CyberSense Version 8.0:

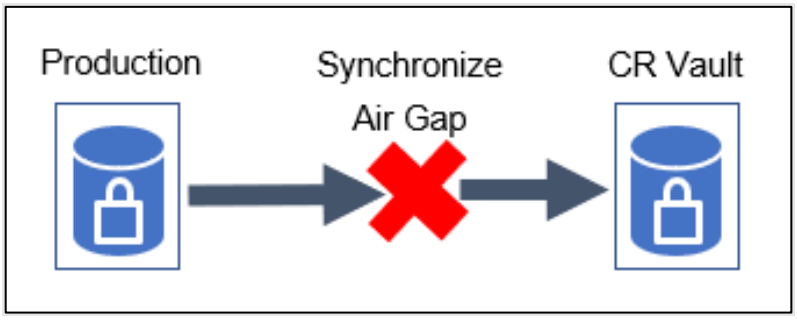
- An OVA deployment option is available.

- CyberSense support for SELinux Linux - SELinux can be set to “active” and “Enforcing” to meet STIGs requirement
- CyberSense can be deployed on AWS using an AMI which will be shared with customers’ AWS accounts by Dell Technologies
- Support for CyberSense migration from RHEL to SLES - Migrate data from a RHEL server to a SLES server
- CyberSense analyze dashboard - Provide a UI that was designed specifically for CyberSense workflow

Logical air gap

The term “air gap” implies physical isolation from an unsecure system or network. Logical air gap describes a physical connection but logical isolation from the network. The logical air gap provides another layer of defense by reducing the surface of attack.

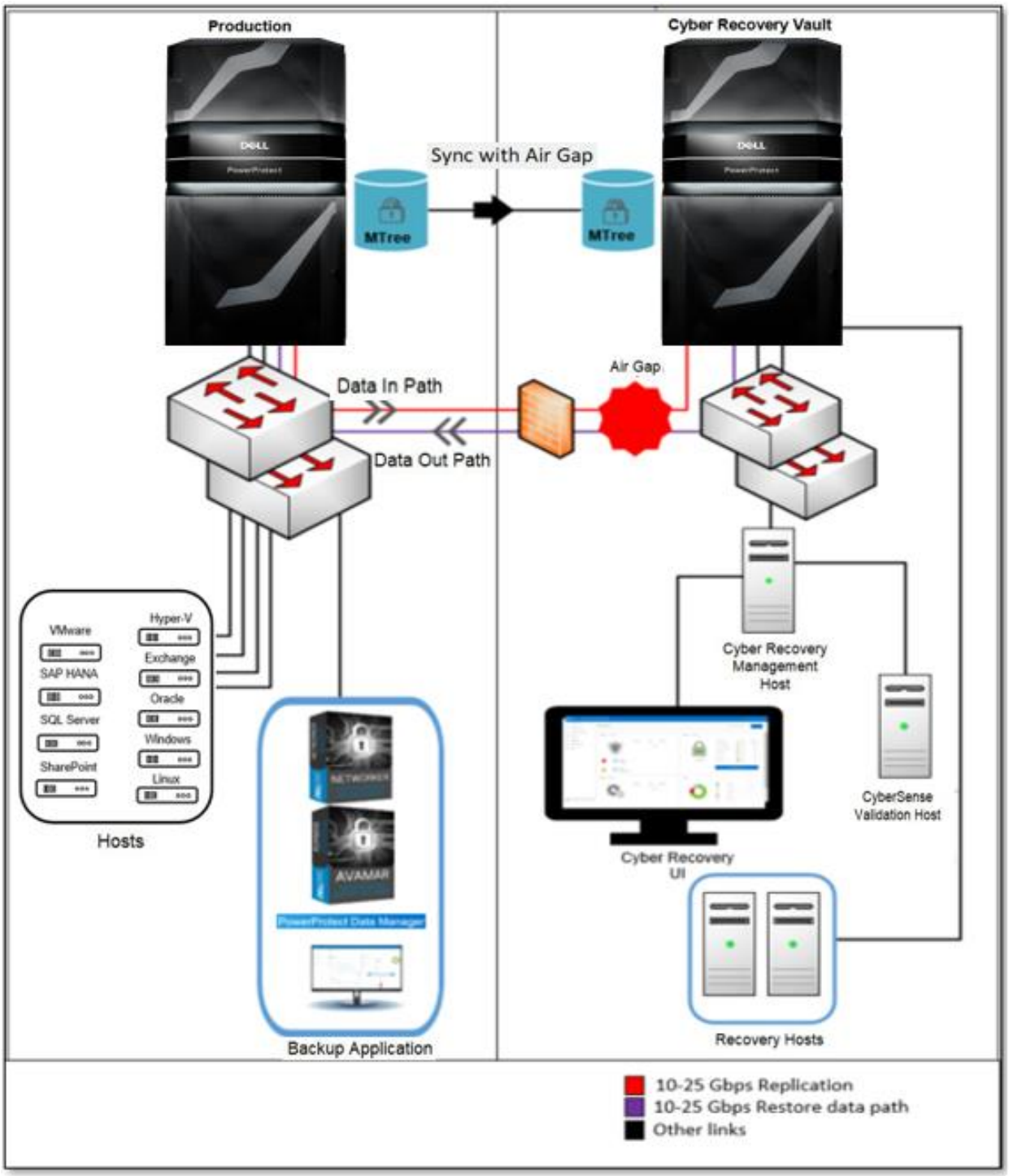
Cyber Recovery provides the air-gapped feature to keep the Cyber Recovery vault disconnected from the production network. The DD series in the Cyber Recovery vault is disconnected (air-gapped) from the production network most of the time and is only connected when Cyber Recovery triggers replication.



The DD series in the Cyber Recovery vault is connected to the production DD series only during the data synchronization operation.

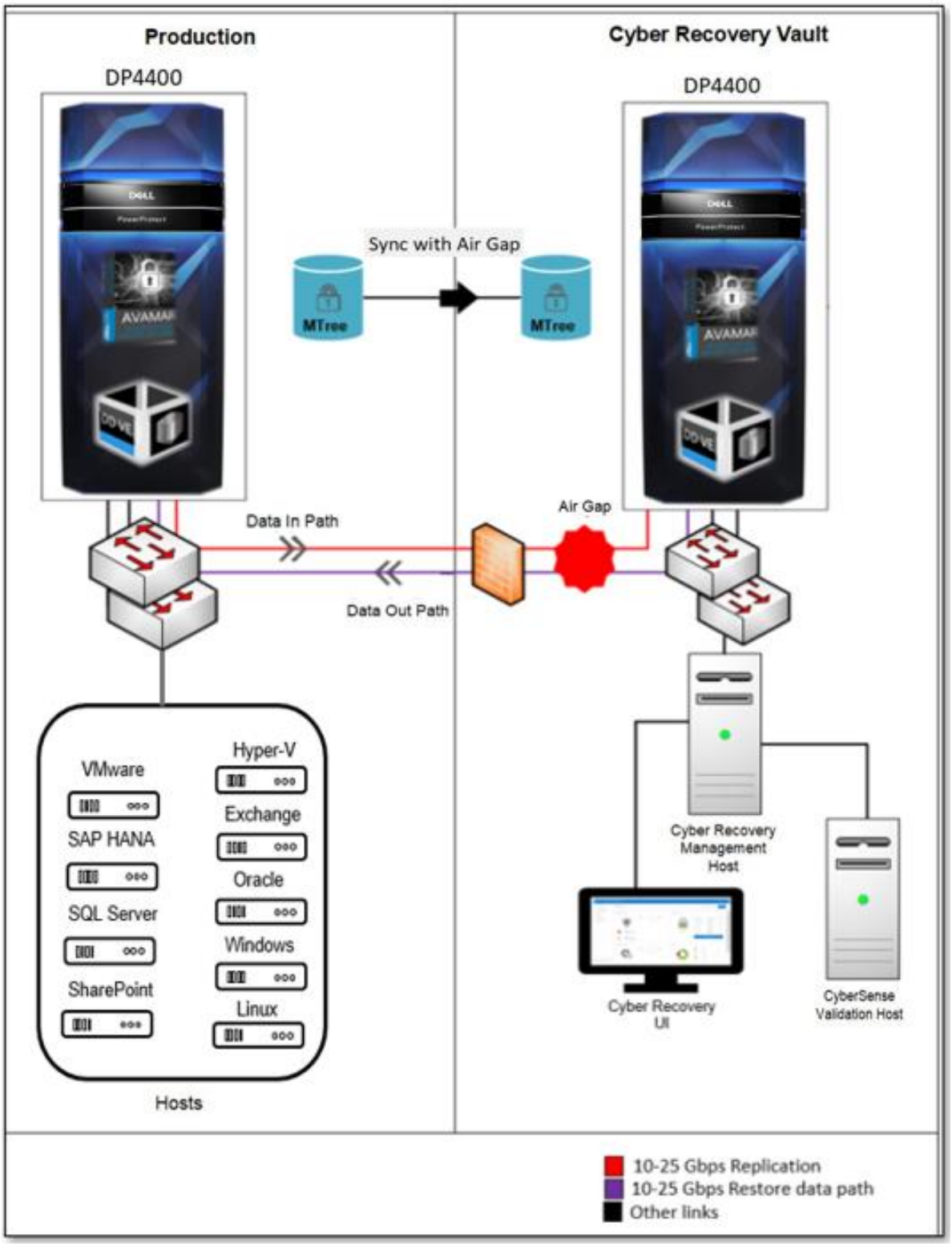
Cyber Recovery integration with DD series

The reference architecture below represents Cyber Recovery solution integration with DD series. The Cyber Recovery solution uses DD series to replicate data from the production system to the Cyber Recovery vault through a dedicated replication data link.



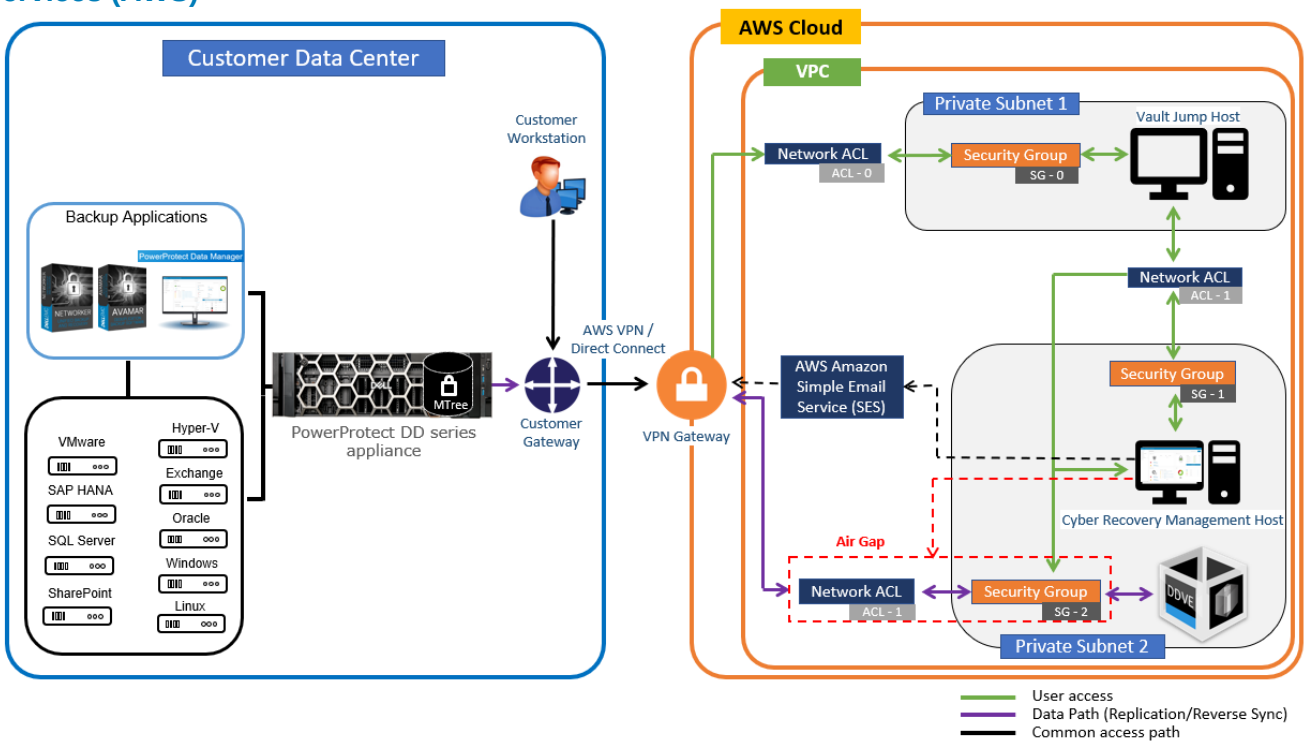
Cyber Recovery integration with the IDPA (DP4400)

The reference architecture below represents Cyber Recovery solution integration with IDPA.



Cyber Recovery on Amazon Web Services (AWS)

The Cyber Recovery vault is supported on AWS starting with Cyber Recovery 19.7 and later versions. The Cyber Recovery solution is also supported in AWS GovCloud.



The Cyber Recovery software is available as an Amazon Machine Image (AMI). To deploy the Cyber Recovery software to an Elastic Compute Cloud (EC2) instance in a Virtual Private Cloud (VPC), use an AWS CloudFormation template.

The CloudFormation template deploys all the components that the Cyber Recovery solution requires in the VPC on AWS. The template creates two private subnets: A private subnet that includes the jump host and a private subnet that includes the Cyber Recovery management host and DDVE. It also configures security groups, Access Control Lists (ACLs), inbound and outbound rules. The vault jump host can be accessed using a VPN gateway or an AWS Direct Connect.

Cyber Recovery software is also available as additional purchase option through AWS Marketplace using custom pricing.

AWS provides VPC security mechanisms for additional security measures for the Cyber Recovery vault:

- Security groups, which protect the instances deployed in the VPC
- Network access control list (ACL)

The Cyber Recovery software enables and disables access to a private subnet through a network access control list (network ACL) and enables and disables access to an instance through security groups.

CyberSense on AWS

Starting with Cyber Recovery version 19.12, Cyber Recovery vault on AWS supports the CyberSense software. With CyberSense version 8.0, CyberSense software can be integrated with Cyber Recovery vault on AWS to analyze your data.

CyberSense 8.0 can be deployed on AWS using an AMI. On request, Dell Technologies provides access to the AMI that is required to deploy the CyberSense software on AWS. The AMI must be deployed in the same subnet with the Cyber Recovery management host and the vault DDVE. The jump host, deployed by the CloudFormation template as part of the Cyber Recovery vault deployment on AWS, enables access to the CyberSense host.

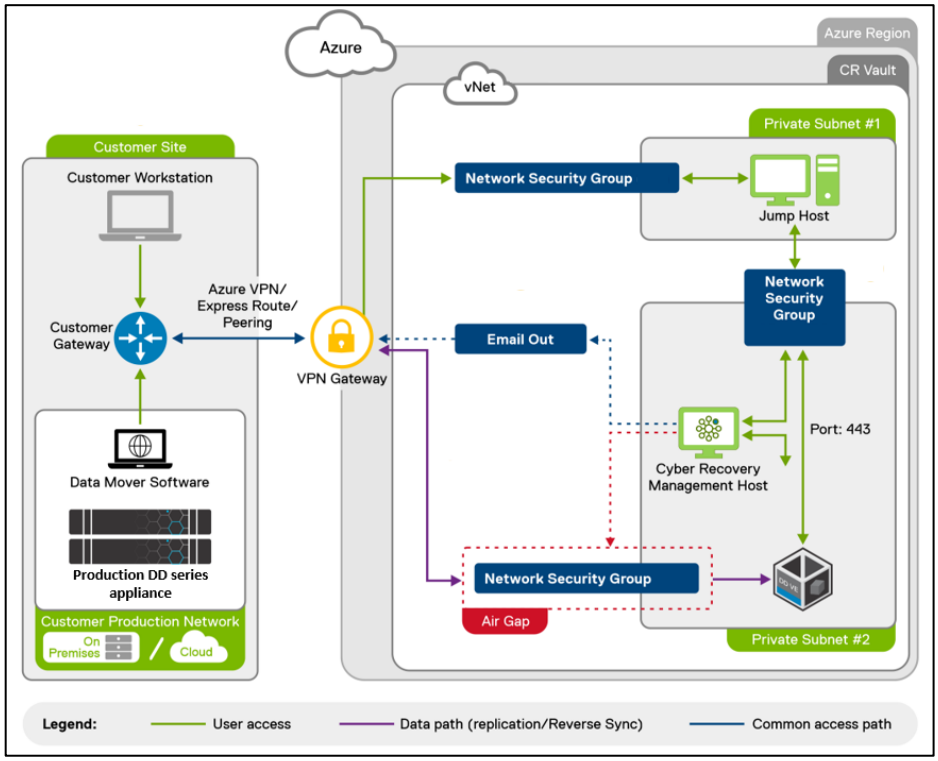
Note: Contact Dell Technologies team to deploy CyberSense on AWS.

For more details, see the Dell PowerProtect Cyber Recovery AWS Deployment Guide.

Cyber Recovery on Microsoft Azure

The Cyber Recovery solution is available on Microsoft Azure. The Cyber Recovery vault is deployed using the Azure Resource Manager (ARM) template.

The Cyber Recovery vault deployment is fully automated based on the template provided by Dell Technologies. On request, Dell Technologies provides access to the ARM template and VM Image that are required to deploy the Cyber Recovery solution. The ARM template deploys all the necessary Cyber Recovery vault components.



The ARM template creates:

- The Resource Group—The Resource Group includes all the components required for the Cyber Recovery solution.

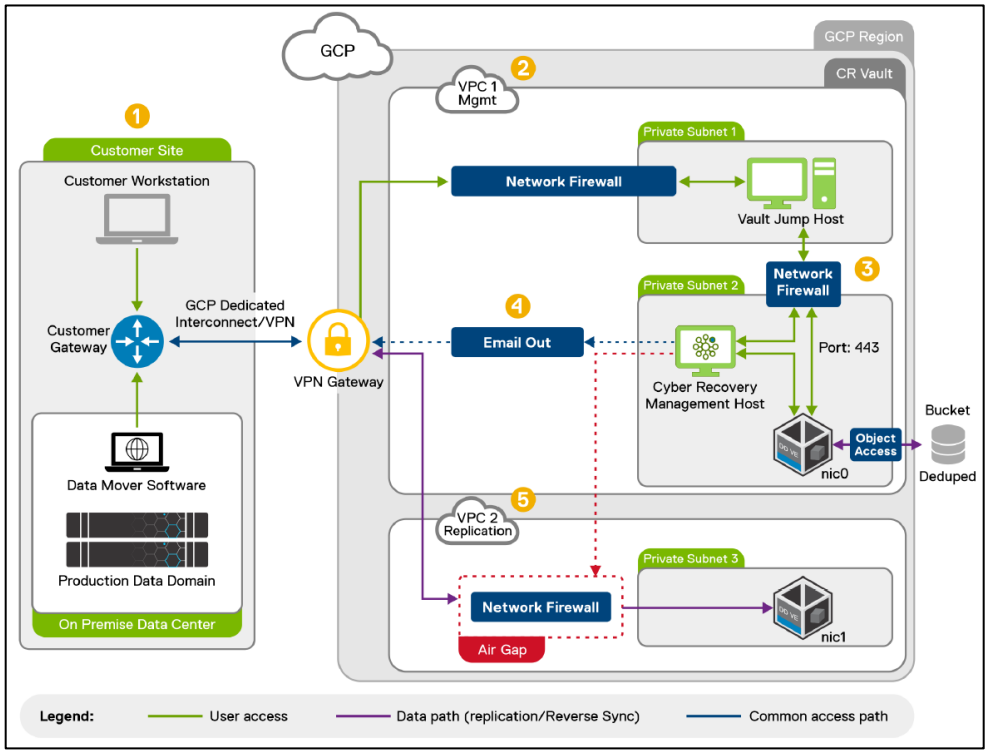
- The Virtual Network (VNet)—The network that the various components use to communicate with each other.
- Two subnets—The two private subnets include:
  - An Azure jump host on one subnet
  - The Cyber Recovery management host and DDVE on the other subnet
- Network Security Groups—The Network Security Groups and VMs provide a layer of security for the VNet that acts as a virtual firewall for controlling traffic in and out of the subnets.
- VNet endpoints—The VNet endpoints enable private connections between the VNet and supported Azure services.
- Identity and Access Management (IAM) roles—Along with the VNet endpoints, the roles provide access to Azure services for specific VMs.
- A storage account—The storage account includes a container for the DDVE storage.

The Cyber Recovery management host and vault DDVE are deployed on an isolated subnet and the jump host is deployed on a separate subnet. The Cyber Recovery management host and vault DDVE can be accessed only through the jump host.

For more details on how to deploy the Cyber Recovery solution on Azure, see the Dell PowerProtect Cyber Recovery Azure Deployment Guide.

Cyber Recovery on Google Cloud Platform

The Cyber Recovery vault is supported on Google Cloud Platform starting with Cyber Recovery 19.12 and later versions.



The Cyber Recovery software is made available as a VM image. The basic Cyber Recovery solution on Google Cloud Platform architecture includes a single region, two Virtual Private Clouds (VPCs), and a single availability zone (AZ).

To deploy the Cyber Recovery software in Google Cloud Platform, use a Terraform template.

The Terraform template creates:

- Two Cyber Recovery VPCs: The VPCs include all the components required for the Cyber Recovery solution.
- Three subnets: The three private subnets include:
  - A subnet with the Google Cloud Platform jump host
  - A subnet with the Cyber Recovery management host and DDVE
  - A subnet with a second DDVE network interface that is used for replication

Note: The production workstation cannot access the Cyber Recovery management host directly. The Windows-based jump host is available in the VPC to access the Cyber Recovery and DDVE instances. The management path is through the jump host.

- Firewall rules

The Terraform template also deploys a Google Cloud Platform jump host. The Windows-based jump host is available in the VPC to access the Cyber Recovery and DDVE instances. The management path is through the jump host.

Back up data is stored in a storage bucket with a high level of deduplication.

The Cyber Recovery deployment using Terraform does not include a VPN. We strongly recommend that you:

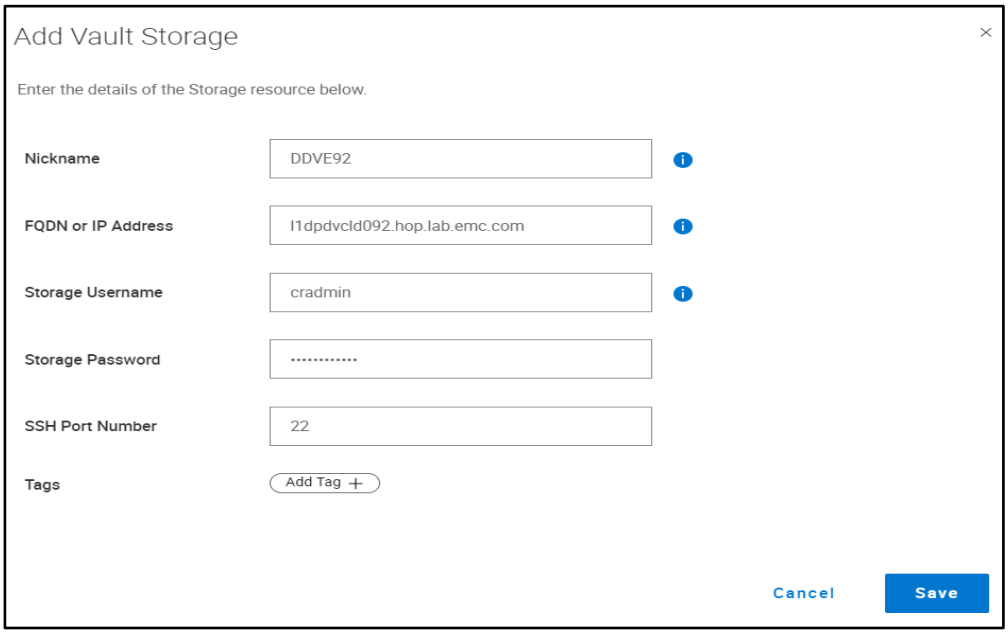
- Set up a VPN.
- Use a VPN gateway or Google Cloud Interconnect to access the jump host.

For more details on how to deploy the Cyber Recovery solution on Google Cloud Platform, see Dell PowerProtect Cyber Recovery on Google Cloud Platform Deployment Guide.

Integrating vault storage and applications with Cyber Recovery

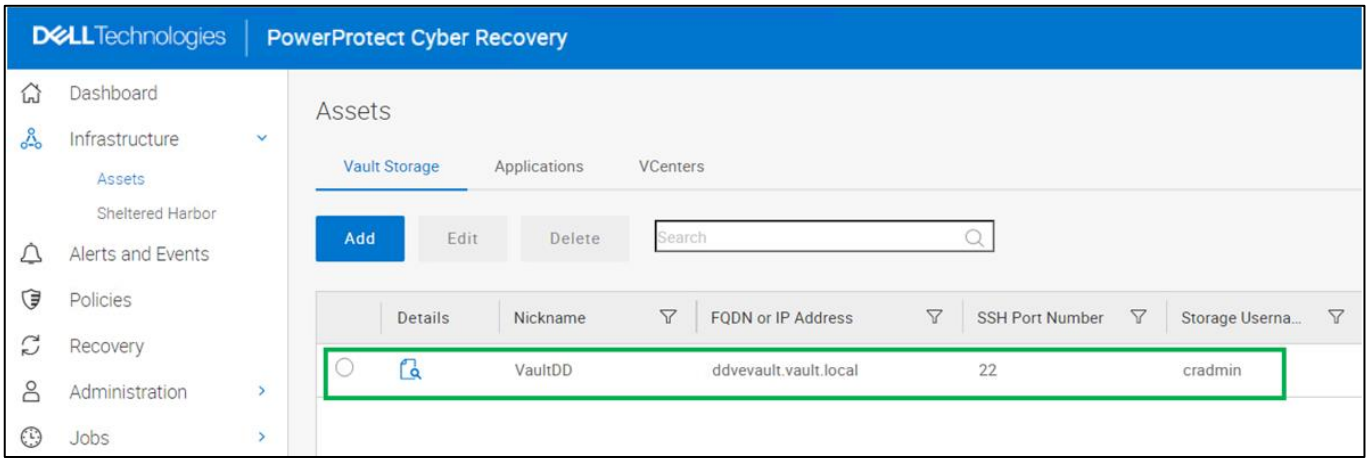
Adding vault storage with Cyber Recovery

1. From the Main Menu, select Infrastructure > Assets.
2. Click VAULT STORAGE at the top of the Assets content pane.
3. Click Add.
4. Complete the following fields in the dialog box:



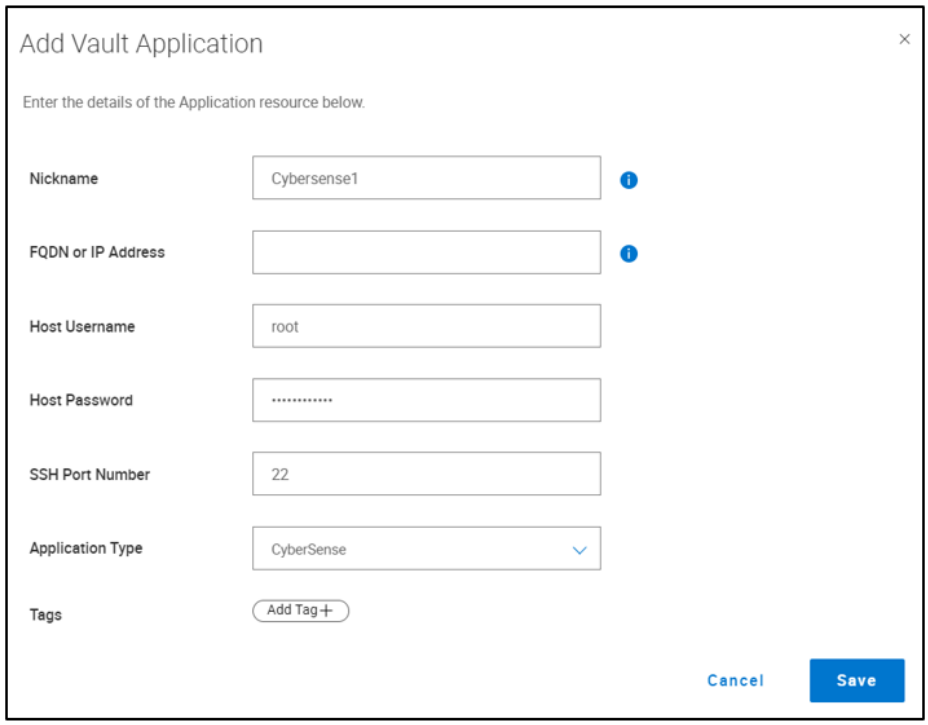
5. Click **Save**.

The Vault Storage table lists the storage object:



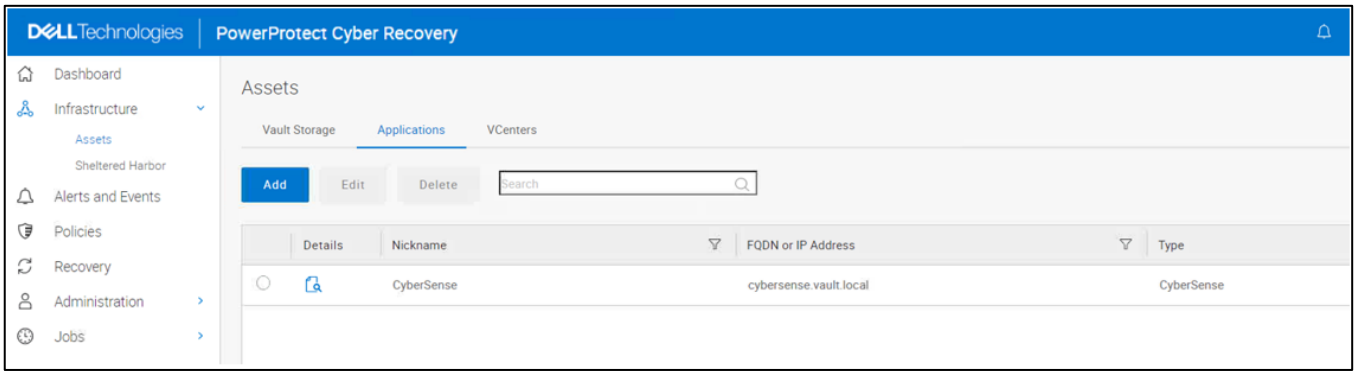
Adding CyberSense with Cyber Recovery

1. From the Main Menu, select **Infrastructure** > **Assets**.
2. Click **APPLICATIONS** at the top of the **Assets** content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box:



5. Click **Save**.

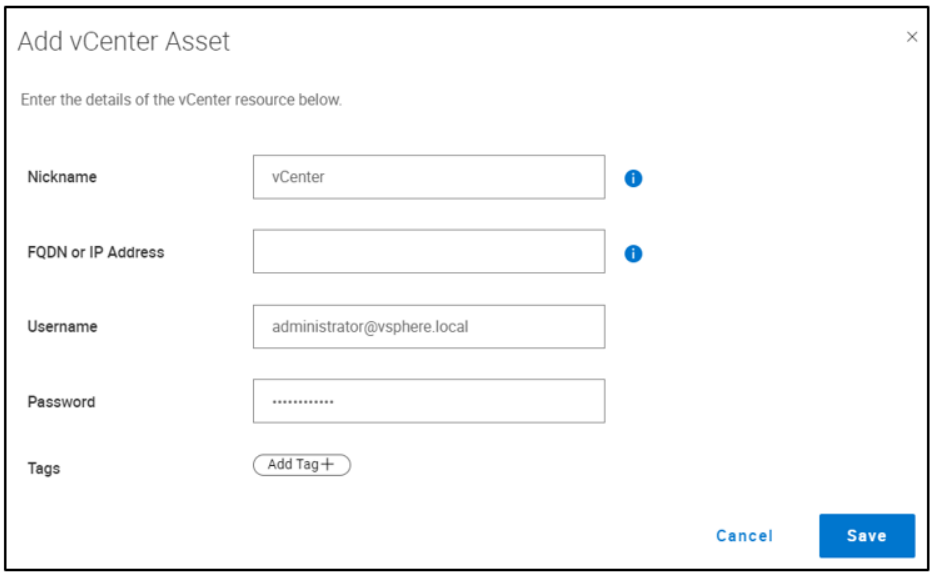
The Applications table lists the CyberSense application:



Adding PowerProtect Data Manager with Cyber Recovery

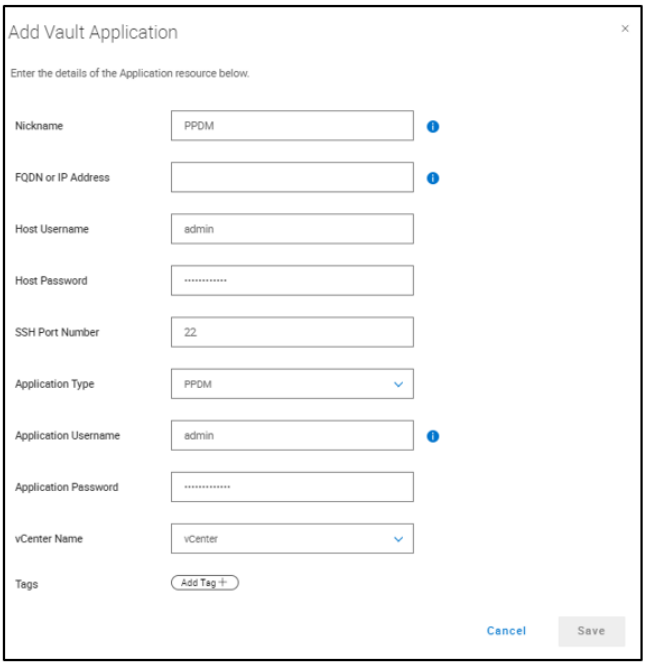
Adding vCenter

1. From the Main Menu, select **Infrastructure** > **Assets**.
2. Click **vCenters** at the top of the **Assets** content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.



Adding PowerProtect Data Manager

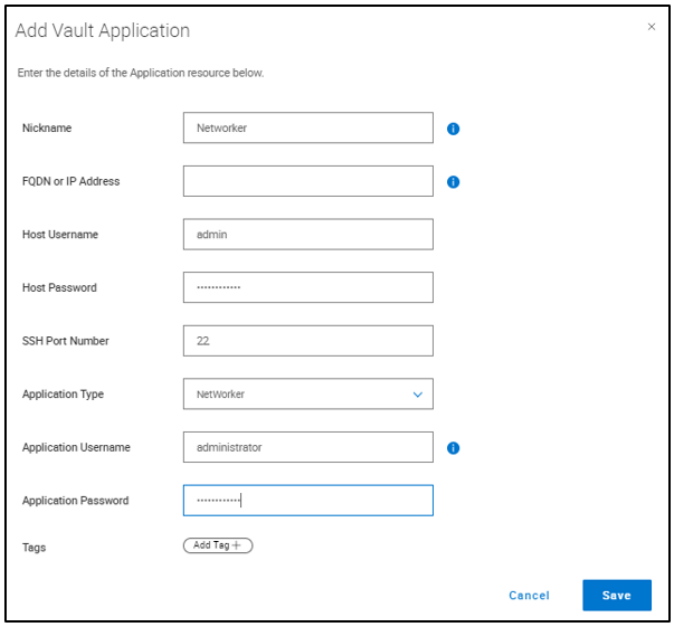
1. From the Main Menu, select **Infrastructure > Assets**.
2. Click APPLICATIONS at the top of the Assets content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.



Adding NetWorker with Cyber Recovery

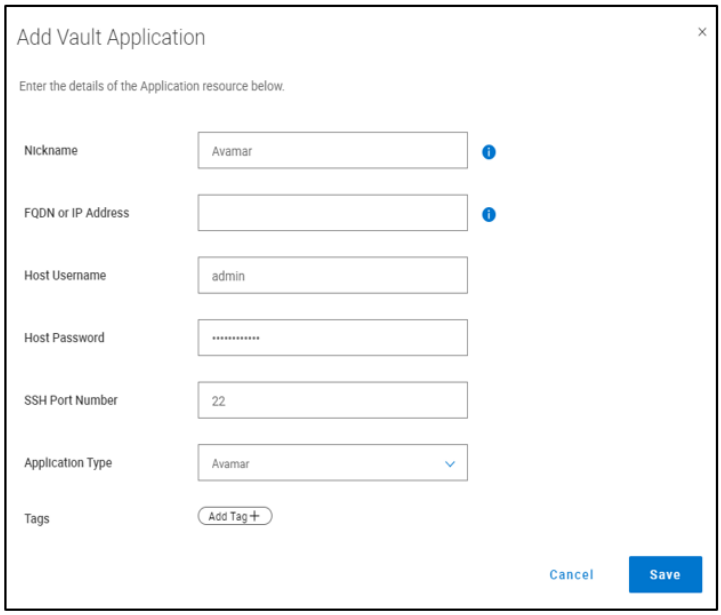
1. From the Main Menu, select Infrastructure > Assets.
2. Click APPLICATIONS at the top of the Assets content pane.

3. Click Add.
4. Complete the following fields in the dialog box and click Save.



Adding Avamar with Cyber Recovery

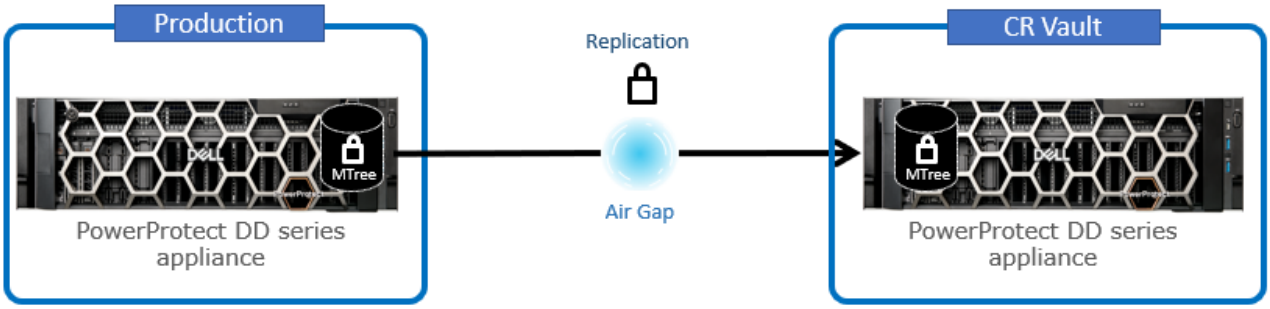
1. From the Main Menu, select **Infrastructure > Assets**.
2. Click APPLICATIONS at the top of the Assets content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.



MTree replication

MTree replication is a DD series feature that copies unique data from the production DD series MTree to the DD series MTree in the Cyber Recovery vault.

MTree replication synchronizes data between the production environment and the air-gapped Cyber Recovery vault. Immutable protection points are created in the Cyber Recovery vault. They can be used for recovery and analytics after being copied to a read/write DD series MTree.

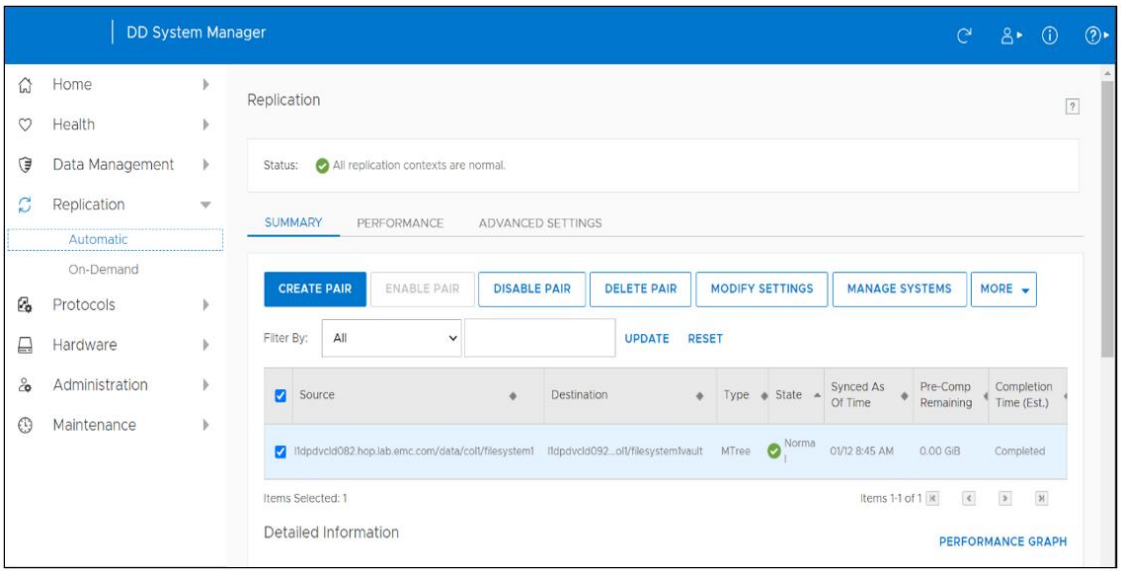


The Cyber Recovery software controls data synchronization from the production environment to the vault environment by DD series MTree replication. After the datasets and associated MTrees to be protected by the Cyber Recovery solution are determined, replication contexts are set up between the production and vault DD series.

MTree replication is designed so that all data within an MTree is replicated securely between two DD series appliances. After the initial synchronization is completed and all data is copied to the vault DD series, each subsequent synchronization operation copies only new and changed data segments.

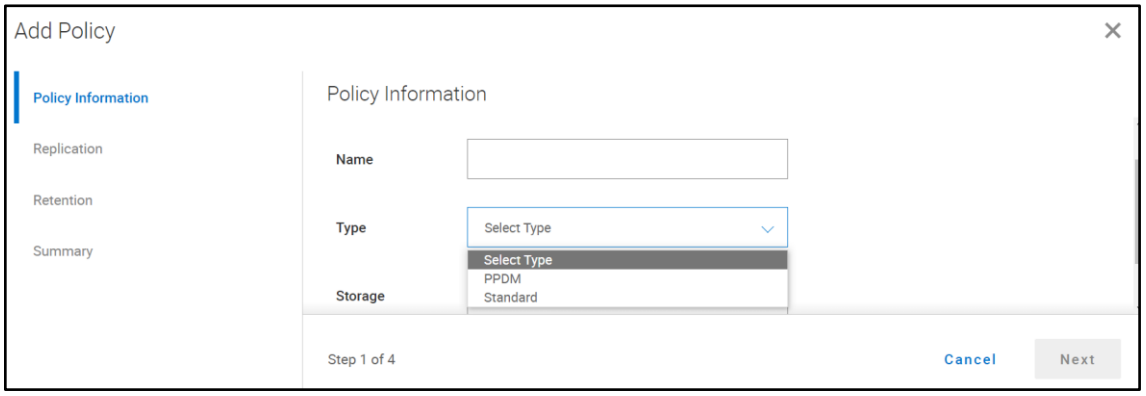
Creating the MTree replication context on DD series

Replication contexts must be created and initialized between DD series. The policy for the replication is created on the Cyber Recovery management host.



Cyber Recovery policies and actions

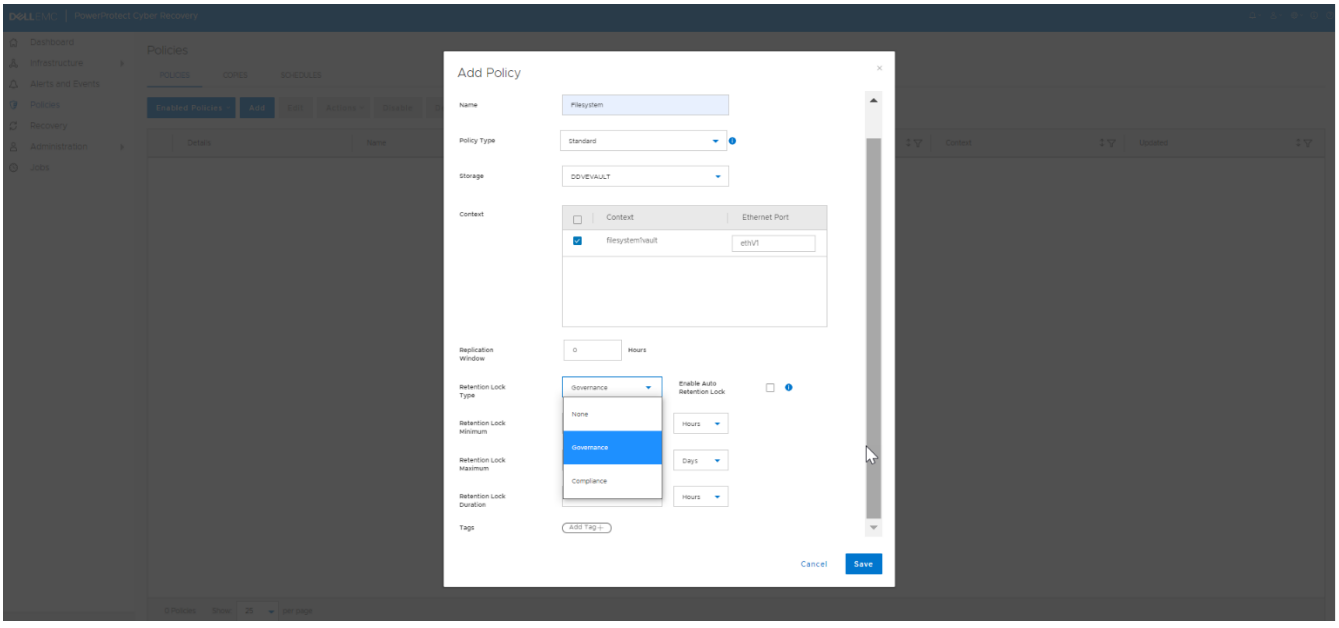
The UI displays the available policy types: Standard and PPDM.



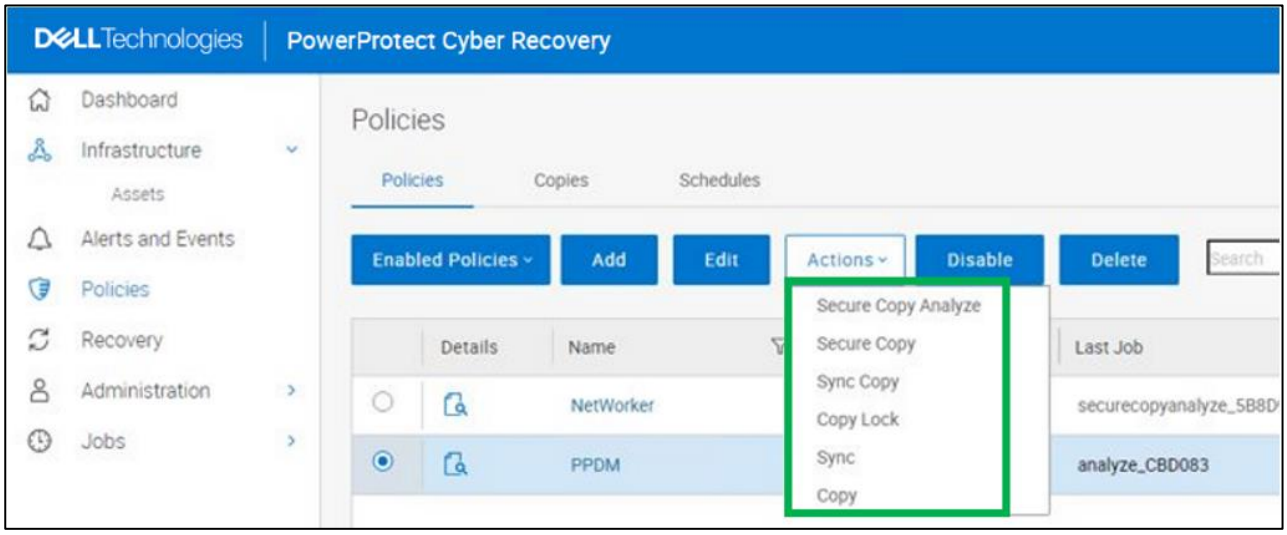
For backup software other than PowerProtect Data Manager, select the policy **Type** as **Standard**. The Cyber Recovery software supports DD Boost backup recovery, in addition to NFS backup recoveries, for PowerProtect Data Manager Version 19.10. Starting with Cyber Recovery version 19.12, Cyber Recovery software supports up to 32 Cyber Recovery policies.

Note: Backup and Recovery Design Center (BRDC) will help in assisting with the number of supported Cyber Recovery policies in your environment. Contact DPADBRDC@emc.com for information about the actual number of policies supported for your environment.

In the policy type menu. Sheltered Harbor is not enabled by default. When Sheltered Harbor is enabled on the system, it is then displayed in the menu.



The following actions are available for all policy types except for the Sheltered Harbor policy type:



- **Sync Copy** (Sync the data and create a fast copy)
- **Secure Copy** (Performs a replication, creates a PIT copy, and then retention locks all files in the PIT copy)
- **Secure Copy Analyze** (Performs a replication, creates a PIT copy, retention locks all files in the PIT copy and runs an analysis on the resulting PIT copy)

Note: The “Secure Copy Analyze’ action is available only if a CyberSense application is configured. If the “Analyze” operation of the schedule still runs when the next schedule starts and gets to the “Analyze” operation, it will fail because there can only be a single active “Analyze” operation for each Cyber Recovery policy.

- **Sync** (Sync the data)
- **Copy** (Create a fast copy of data that is already on PowerProtect DD series appliance in the vault environment)
- **Copy Lock** (Locks all files in the PIT copy)

For a Sheltered Harbor policy type, the only action available is Sheltered Harbor Copy (Sync, Verify, Copy, Certify, Lock, Report).

Infrastructure service recommendations

The following table shows infrastructure service recommendations:

Table 1. Infrastructure service recommendations

Service	Scope	Required	Notes
AD/LDAP	In-vault	Recommended	Stores Credentials. Can provide access controls and other functions.
DNS	In-vault	Recommended	Highly recommended when multiple hosts are in the vault.
Cyber Recovery UI	In-vault	Recommended	
Extended CR UI	Inbound/ outbound	Recommended	A firewall, jump-server or other techniques can be used for further hardening.
Jump server	Inbound/ outbound	Recommended	• Allows software and other critical maintenance. • Allows remote access for testers.
NTP	In-vault/ inbound	Required	A reliable time source is required to prevent clock skew. In-vault NTP can be provided
Physical lockbox/vault	In-vault	Recommended	Use a two-key lockbox to store a written copy of Data Domain system password. Open only in an emergency.
SMTP	Outbound	Required for some services	Allows vault services to send information out of the vault.
SMTP relay server	Outbound		Software packages are available from Microsoft and others.
SNMP	Outbound	Not recommended	Consider using SYSLOG. Data Domain supports both SNMP and SYSLOG, both are disabled by default.
Syslog	Outbound		Also consider Rsyslog.

Recommended network speed for DD series interfaces

The Cyber Recovery software enables and disables the replication Ethernet interface and the replication context on the DD series in the Cyber Recovery vault to control the flow of data from the production environment to the vault environment. The Cyber Recovery software manages the replication link, and the connection is only enabled when new data must be ingested by the DD series in the Cyber Recovery vault.

The replication link on the DD series in the Cyber Recovery vault uses its own unique Ethernet interface. For the replication link that connects the production DD series to the DD series in the Cyber Recovery vault, using the fastest link speed possible, preferably 10 Gb/s Ethernet (GbE) is recommended and supported up to 25 Gb/s.

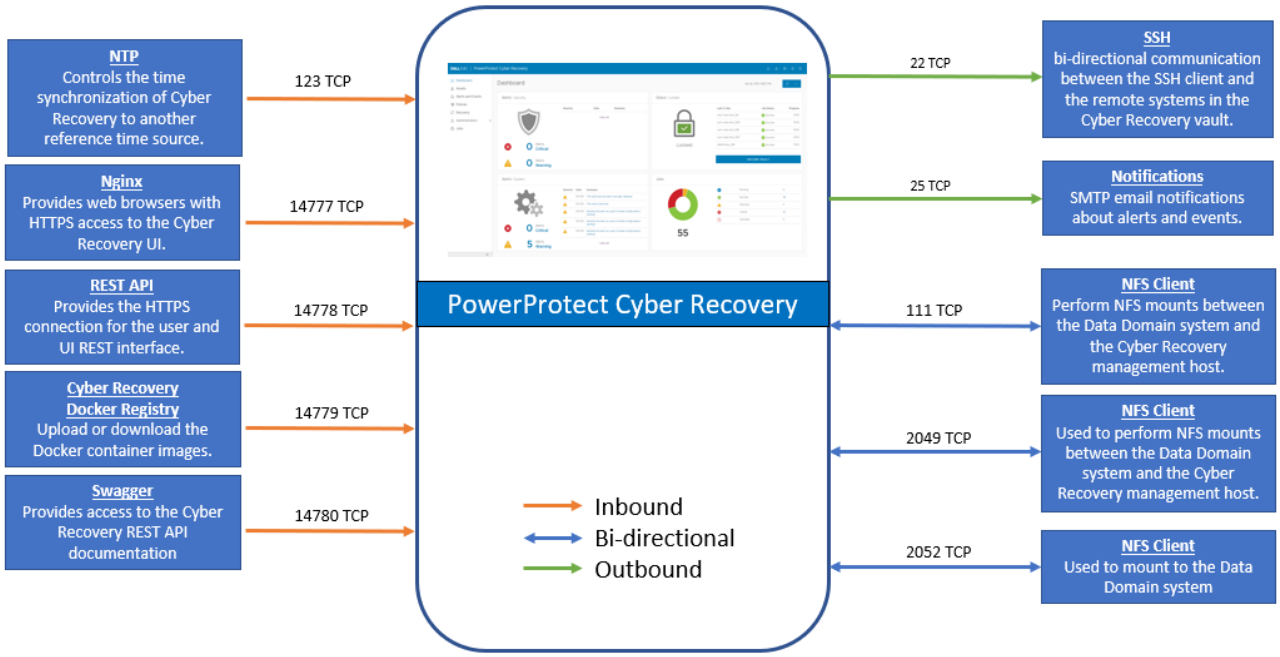
To secure the network links that connect the vault environment to the production environment, or any other network, installing a firewall or other packet inspection tool on both the DD series replication link and the SMTP link is recommended. It is recommended not to make use of packet inspection if a firewall is placed in the replication path. The cost of firewall will be very high, and the deep packet inspection would slow the process down.

If a hyperconverged VMware appliance is installed in the Cyber Recovery vault, the VMware NSX Distributed Firewall (DFW) is a satisfactory firewall option to reduce complexity in the vault environment and protect VMware-based infrastructure. Additionally, the DFW is a potential software-defined option for protecting the Data Domain replication link between production and vault DD series at near wire speed.

The Cyber Recovery software does not support adding Ethernet interfaces to a Cyber Recovery virtual appliance deployment.

Cyber Recovery network ports

The following figure lists the network ports that Cyber Recovery functions require:



Recommended connections between DD series

The Cyber Recovery software works with a replication data link between the vault-environment and production-environment DD series. The Cyber Recovery software communicates with all DD series appliances using SSH.

The production and vault environment networks are not directly connected to each other, except for a replication data link between the DD series in the two environments. The replication data link can be connected directly or through a dedicated switch to the DD series in the vault environment. We recommend using the dedicated replication switches.

Technical support and resources

The Dell Technologies support page is focused on meeting customer needs with proven services and support.

The Dell Technologies Info Hub provides expertise that helps to ensure customer success on Dell Technologies data protection platforms.

Related resources

The Cyber Recovery product documentation set includes:

- PowerProtect Cyber Recovery Info Hub
- Dell PowerProtect Cyber Recovery Product Guide
- Dell PowerProtect Cyber Recovery Installation Guide
- Dell PowerProtect Cyber Recovery Solutions Guide
- Dell PowerProtect Cyber Recovery AWS Deployment Guide
- Dell PowerProtect Cyber Recovery Azure Deployment Guide
- Dell PowerProtect Cyber Recovery Google Cloud Platform
- Dell PowerProtect Cyber Recovery Solution Brief
- Dell PowerProtect Cyber Recovery Simple Support Matrix

Note: Access to these documents might depend on your login credentials.