

Dell PowerProtect Cyber Recovery: Reference Architecture

April 2023

H18661.4

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.

Copyright

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 © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Published in the USA April 2023 H18661.4.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary4

Introduction6

Cyber Recovery architecture15

Integrating vault storage and applications with Cyber Recovery25

MTree replication30

Infrastructure service recommendations.....33

Technical support and resources.....35

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	Part number/ revision	Description
June 2021	H18661	Initial release
April 2022	H18661.1	Updated for Cyber Recovery 19.10
August 2022	H18661.2	Updated for Cyber Recovery 19.11
October 2022	H19661.3	Updated for Cyber Recovery 19.12
April 2023	H18661.4	Updated for Cyber Recovery 19.13: <ul style="list-style-type: none"> • CyberSense multiple links • CyberSense 8.2.0 enhancements • Cyber Recovery reporting • Cyber Recovery alternate recovery option • Cyber Recovery on Amazon Web Services (AWS)

**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

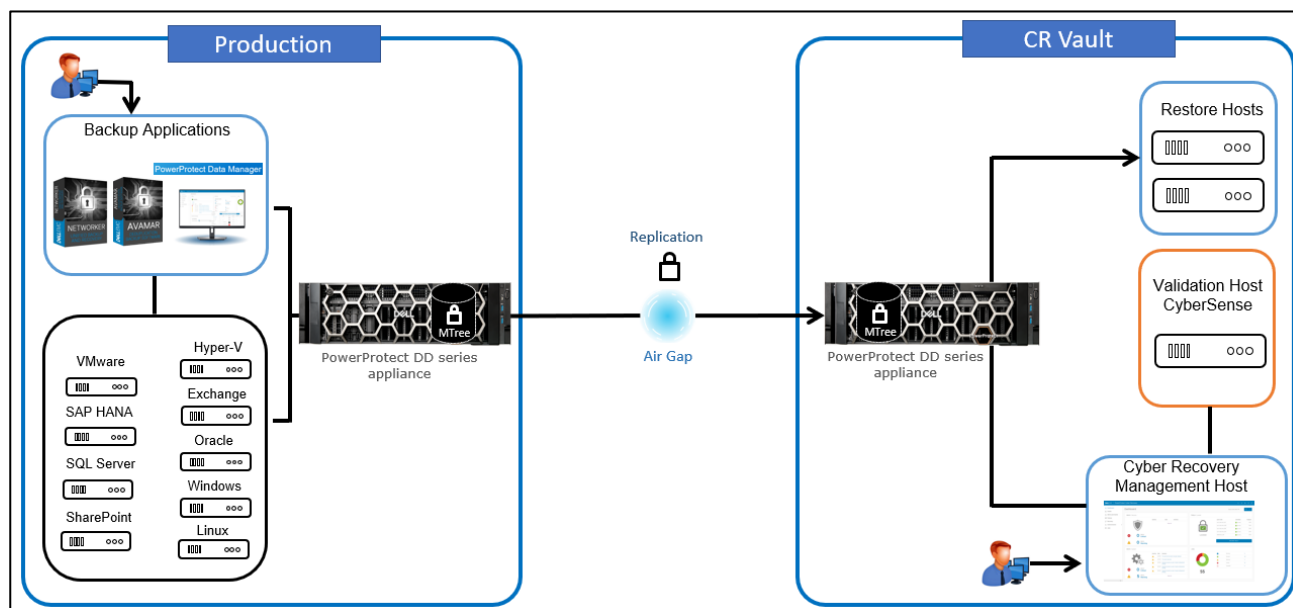
Dell PowerProtect Cyber Recovery

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.

Dell PowerProtect series appliances for Cyber Recovery

- ✓ DD OS, Version 6.0.2.20 and later
- ✓ DD Boost Replication
- ✓ Data Domain Retention Lock Compliance and Governance
- ✓ Data Domain High Availability (DDHA)
- ✓ Data Domain Encryption
- ✓ High speed, scalable deduplication
- ✓ Data integrity and recoverability along with end to end verification and fault tolerance

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

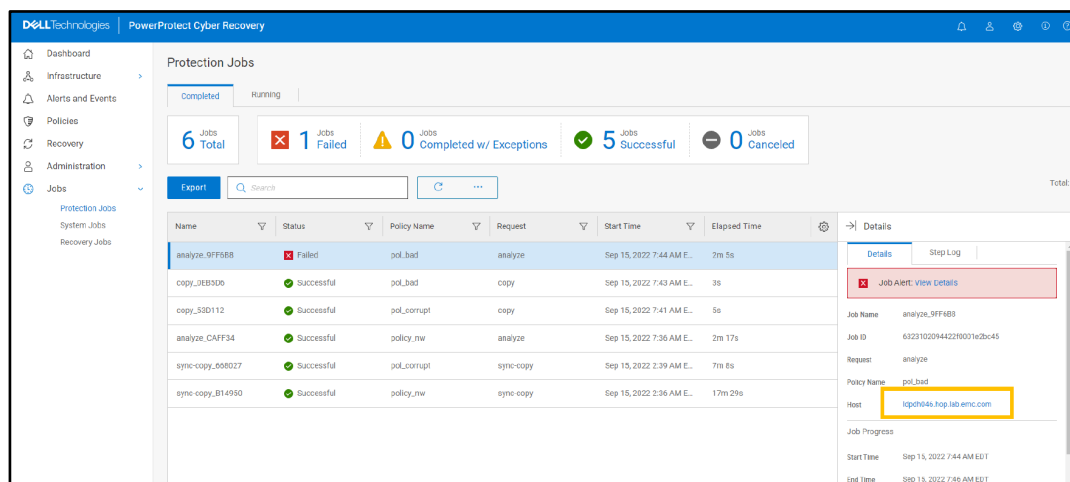
Cyber Recovery features

The Cyber Recovery solution key features include:

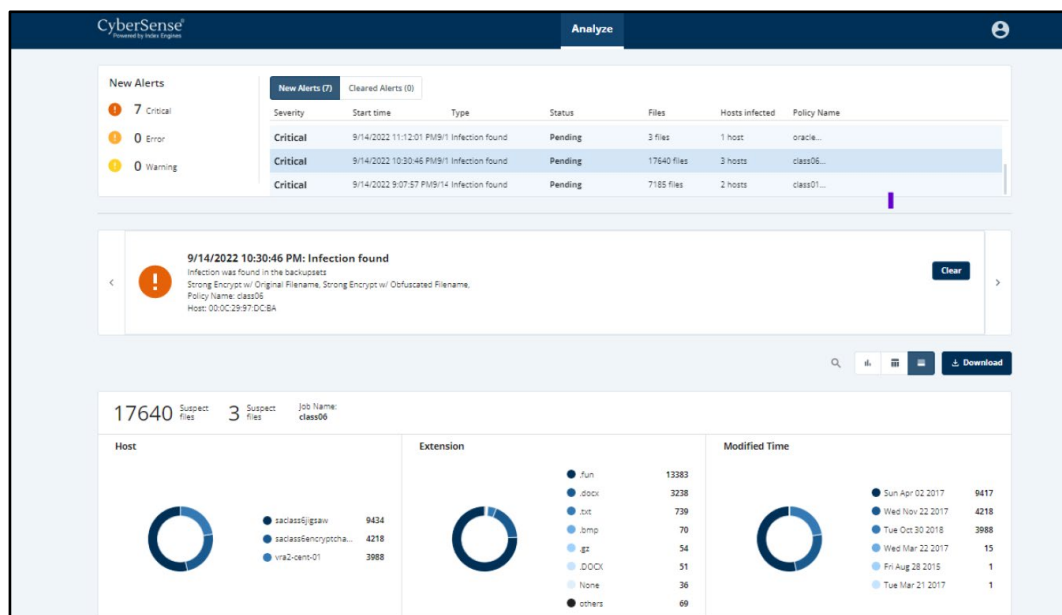
- Secure data in an isolated network with an automated operational air gap
- Policy-based secure copy creation, management, and scheduling
- Integration with Index Engine CyberSense software to detect if the backup data has been compromised
- Robust REST API framework that enables analytics with artificial 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 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

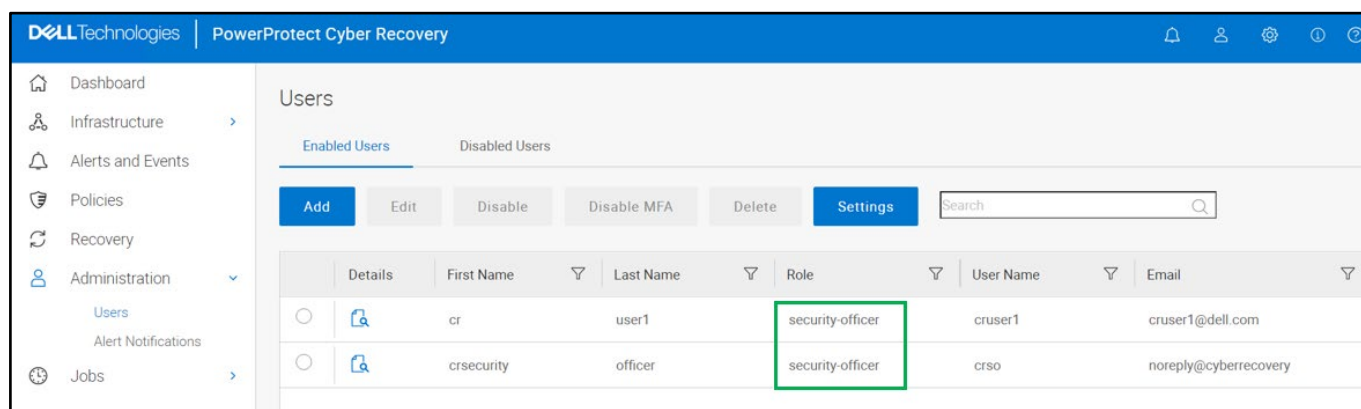
- **Policy network interfaces** - Users can use eth V1 for analysis or for Cyber Recovery policy but cannot use both at the same time. For example, only ethV0 is listed in the following figure because ethV1 is being used for the Cyber Recovery policy.
- **CyberSense analyze dashboard link from Cyber 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.

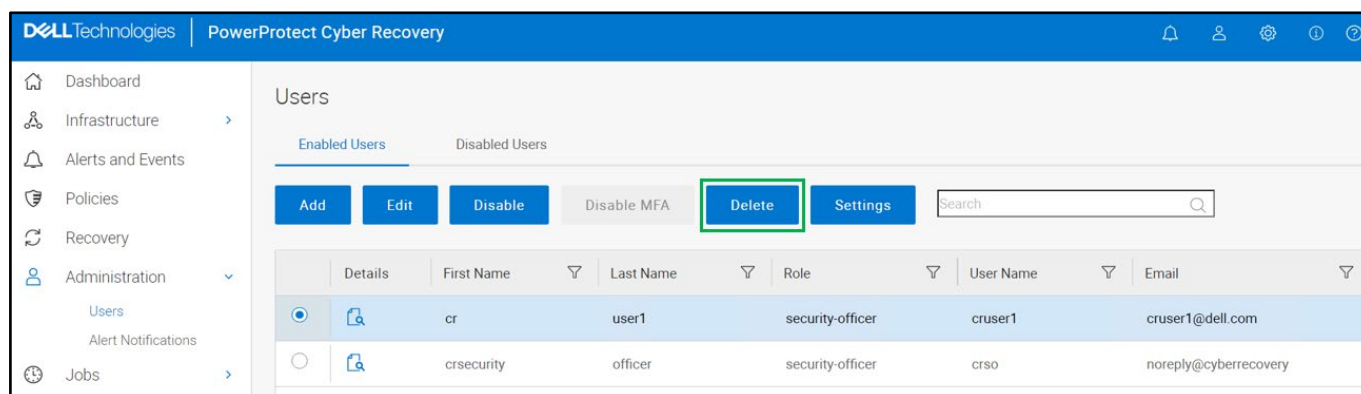


- **Cyber Recovery users and access management** - Multiple security officer roles: Starting with Cyber Recovery version 19.12, the Cyber Recovery security officer (crso) can create multiple security officer roles and manage those accounts. The security officer has the same permissions as the crso but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



Note: Security officer users can create other security officer users. The “Admin” role can no longer create users.

Deletion of users: 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.



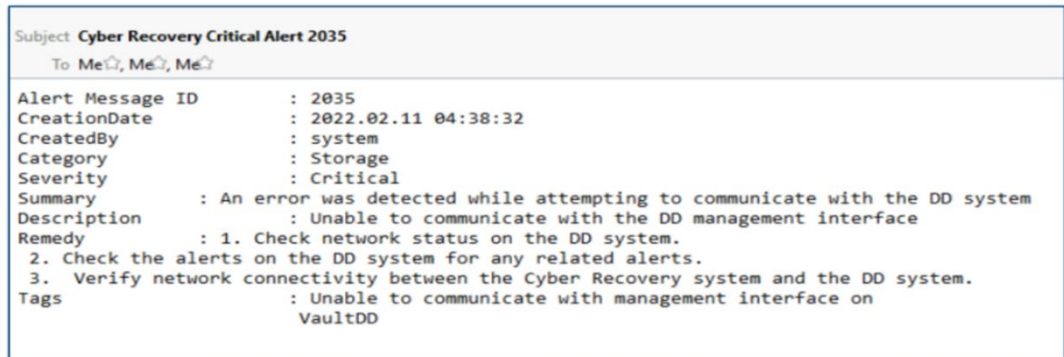
Note: One cannot add a user with the same username of a previously deleted user. Instead, add a user that has a different username.

- **Cyber Recovery 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.



- 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.

Protection Jobs

Completed | Running

6 Total | 1 Failed | 0 Completed w/ Exceptions | 5 Successful | 0 Canceled

Export | Search | Refresh | More

Name	Status	Policy Name	Request	Start Time	Elapsed Time
analyze_9FF688	Failed	pol_bad	analyze	Sep 15, 2022 7:44 AM E...	2m 5s
copy_DCB506	Successful	pol_bad	copy	Sep 15, 2022 7:43 AM E...	3s
copy_SSD112	Successful	pol_corrupt	copy	Sep 15, 2022 7:41 AM E...	9s
analyze_CAFF34	Successful	policy_nw	analyze	Sep 15, 2022 7:36 AM E...	2m 17s
sync-copy_666027	Successful	pol_corrupt	sync-copy	Sep 15, 2022 2:39 AM E...	7m 6s
sync-copy_B14950	Successful	policy_nw	sync-copy	Sep 15, 2022 2:36 AM E...	17m 29s

Details | Step Log

Job Name: analyze_9FF688
 Job ID: 63231020944220001e2bc45
 Request: analyze
 Policy Name: pol_bad
 Host: ldpd446.hop.lab.emc.com

Job Progress

Start Time: Sep 15, 2022 7:44 AM EDT
 End Time: Sep 15, 2022 7:46 AM EDT

- Configuring and managing multiple links for CyberSense**

Starting with Cyber Recovery version 19.13, you can define multiple links between a CyberSense host and one or more PowerProtect DD systems from the Cyber Recovery UI. CyberSense version 8.2 with Cyber Recovery version 19.13 provides the ability to configure links between network interfaces on the PowerProtect DD and network interfaces on the CyberSense host to improve network performance. The multilink feature provides significant performance improvements for all workloads. With Cyber Recovery version 19.13 and CyberSense version 8.2, you must configure the network interface links for each CyberSense host before you can analyze copies.

Interface Links

Select Data Domain and select Data Domain and CyberSense interfaces to pair each link.

Refresh

Data Domain: vault

Select a Data Domain to populate the table below with associated Data Domain interfaces.

Name	Status	IP Address	Speed	SUP
ethV0	Enabled		10Gbs	N/A

Show 25 per page

Select CyberSense interface: ldpd4250.hop.lab.emc.com

Name	Status	IP Address	Speed	SUP
ens161	Enabled		10Gbs	10
ens192	Enabled		10Gbs	10

Show 25 per page

Add Interface Link

Data Domain	DD Interface	CS Interface	Connectivity Status
vault	ethV0	ens161	Unknown

Show 25 per page

Note: You can use CyberSense versions earlier than version 8.2 with Cyber Recovery version 19.13; however, you cannot configure multiple links.

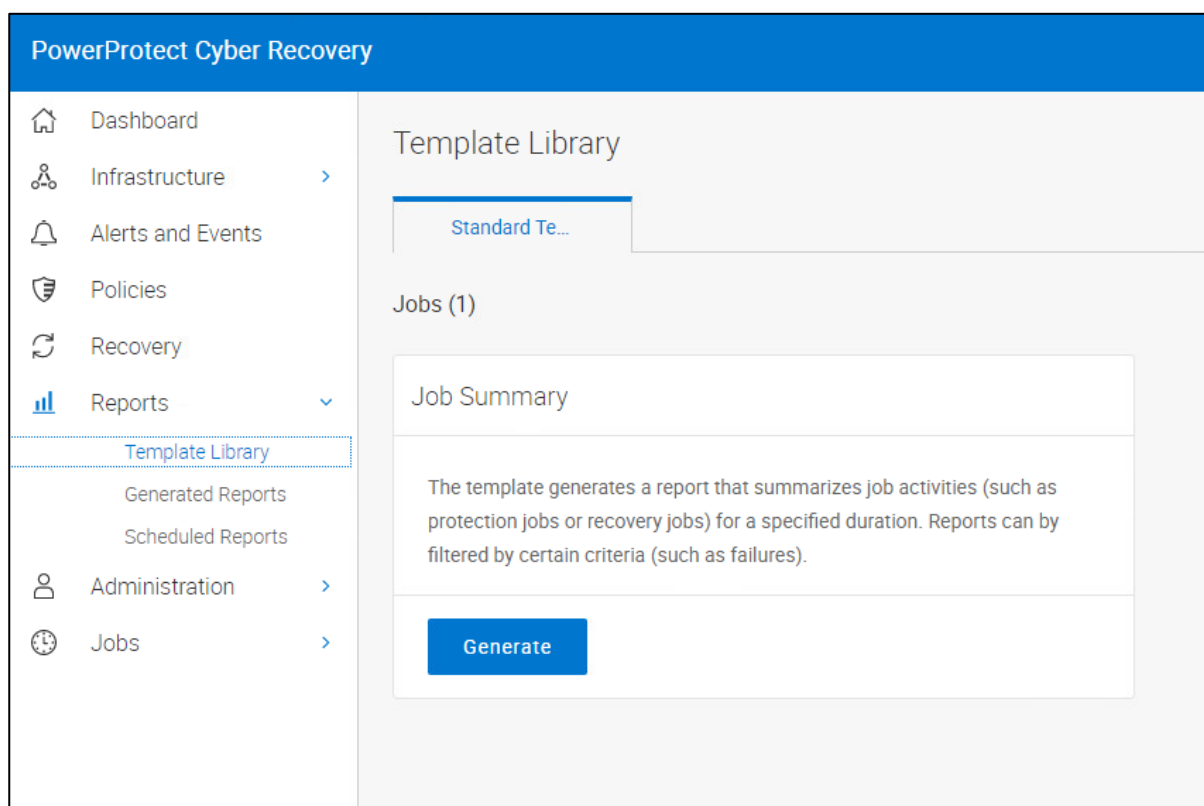
The multilink feature enables you to take advantage of multiple Ethernet interfaces on the CyberSense host and the PowerProtect DD systems. CyberSense Analyze operations read data from the PowerProtect DD system using both the NFS and DD Boost protocols. A multilink configuration improves performance for both NFS and DD Boost read operations by load-balancing traffic across all available links.

For more details about configuring multiple links, see the Dell PowerProtect Cyber Recovery Product Guide.

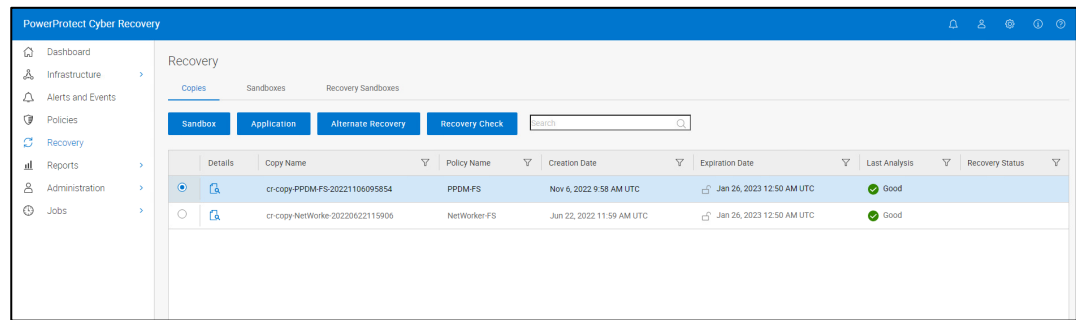
- **Cyber Recovery reporting**

The Cyber Recovery reporting feature in the Cyber Recovery UI enables you to create, run, and schedule reports that summarize job activities. The reporting feature includes a built-in job summary report template. A wizard provides access to a template library that contains predefined standard templates for various reporting categories. The wizard guides you through the template to create a report. Security officers and admin users can create report schedules or on-demand reports that provide information about Cyber Recovery activities. Scheduled reports are emailed, and on-demand reports can be downloaded and emailed.

For more details about Cyber Recovery reporting, see the Dell PowerProtect Cyber Recovery Product Guide.



- Starting with Cyber Recovery version 19.13, an **Alternate Recovery** option is available in the Cyber Recovery UI.



For more details about recovering data to an alternate DD series, see the Dell PowerProtect Cyber Recovery Product Guide.

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.

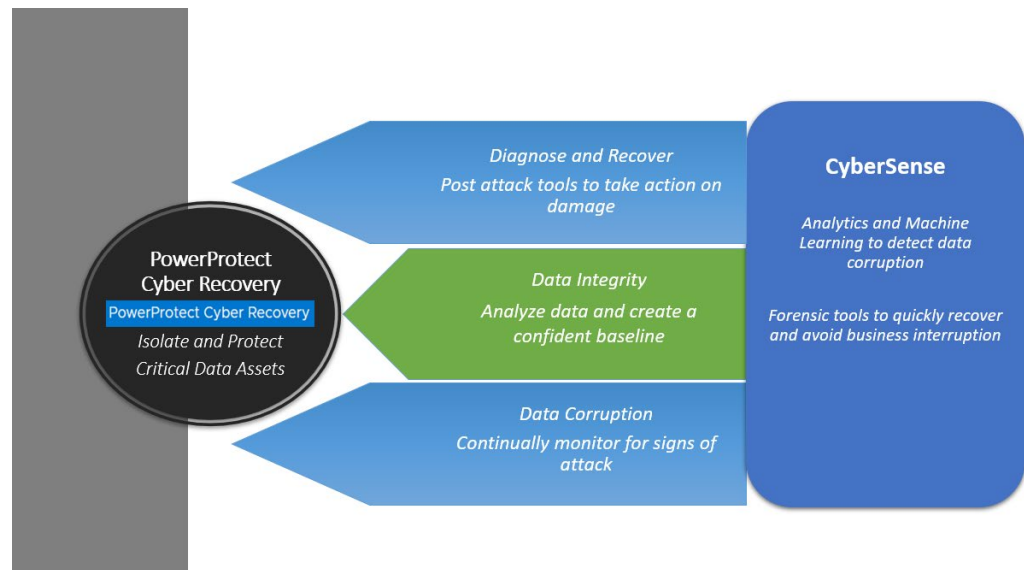
Cyber Recovery software—The Cyber Recovery software orchestrates synchronization, manages, locks the multiple data copies that are stored on the DD series in the Cyber Recovery vault, and orchestrates recovery. The software also governs the optional process of performing analytics on data that is stored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

Enhancements with CyberSense 8.2.0:

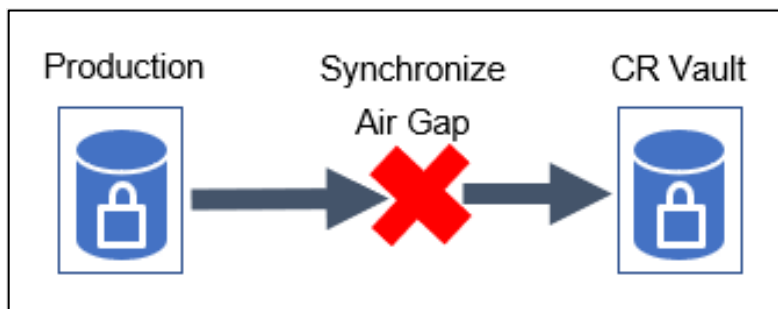
- CyberSense 8.2.0 supports Avamar backups of virtual machines running in a Microsoft Hyper-V environment.
- Before CyberSense 8.2.0, the host names in the CSV file attached to the CyberSense email that a customer received were obfuscated. The customer now receives a CSV file with the host names displayed, and the number of columns is reduced to only those columns that are of interest to the customer.

- For new deployments (CS OVA and CS package), you must provide a password (**iepasswd admin**) using a CLI command before you can log in to the CyberSense UI
- Before CyberSense 8.2.0 the licensed capacity of an index could not decrease; it could only increase if the amount of active data in the index increased. With the 8.2.0 release, high water mark licensing is eliminated. The licensed capacity of the index can decrease to reflect the amount of currently active data in the index.
- Before CyberSense 8.2.0, the CyberSense software identified files suspected of being attacked based on a fixed query for each attack class. With the 8.2.0 release, a new machine learning model that was trained with many real ransomwares identifies files that were likely attacked. This model increases the accuracy of identifying suspect files after an attack.
- The combination of CyberSense 8.2.0 and Cyber Recovery 19.13 provides the capability to create a storage configuration among the CyberSense servers and the Data Domain systems it connects with. This new configuration provides ongoing link integrity checking and improves the performance of indexing by introducing the ability to use multiple network links for accessing the Data Domain through the DDBoost protocol.
- When a ransomware attack is detected, the audit trail output that goes to the Linux syslog is enhanced with a message for each directory or folder that holds a file suspected of being attacked by the ransomware. This message contains a description of the detected attack, the host name, and the directory or folder that holds a suspect file.

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.

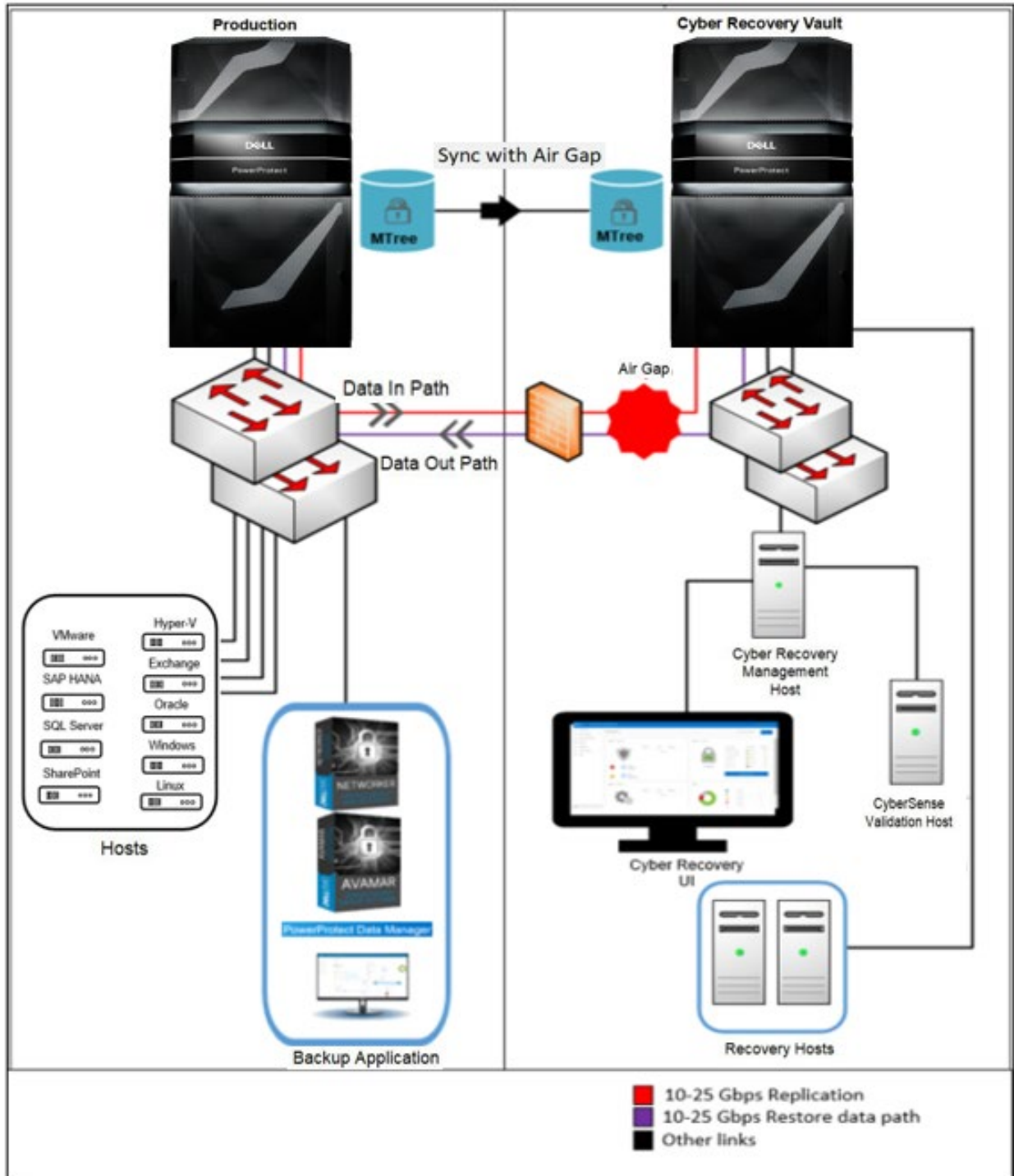
Cyber Recovery provides the air-gapped feature to keep the Cyber Recovery vault disconnected from the production network. The DD series in the Cyber Recovery vault is disconnected (air-gapped) from the production network most of the time and is only connected when Cyber Recovery triggers replication.



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

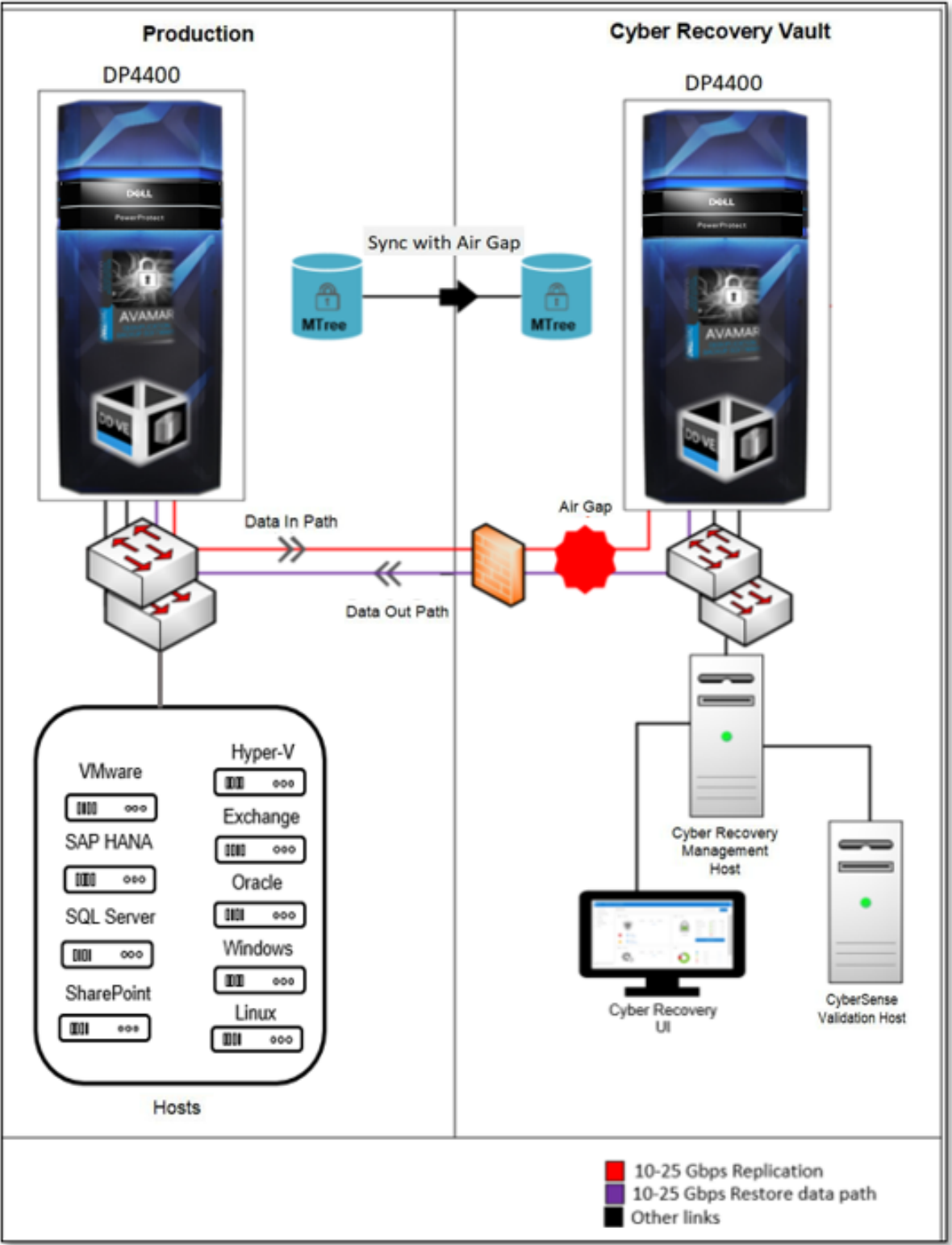
Cyber Recovery integration with DD series

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.



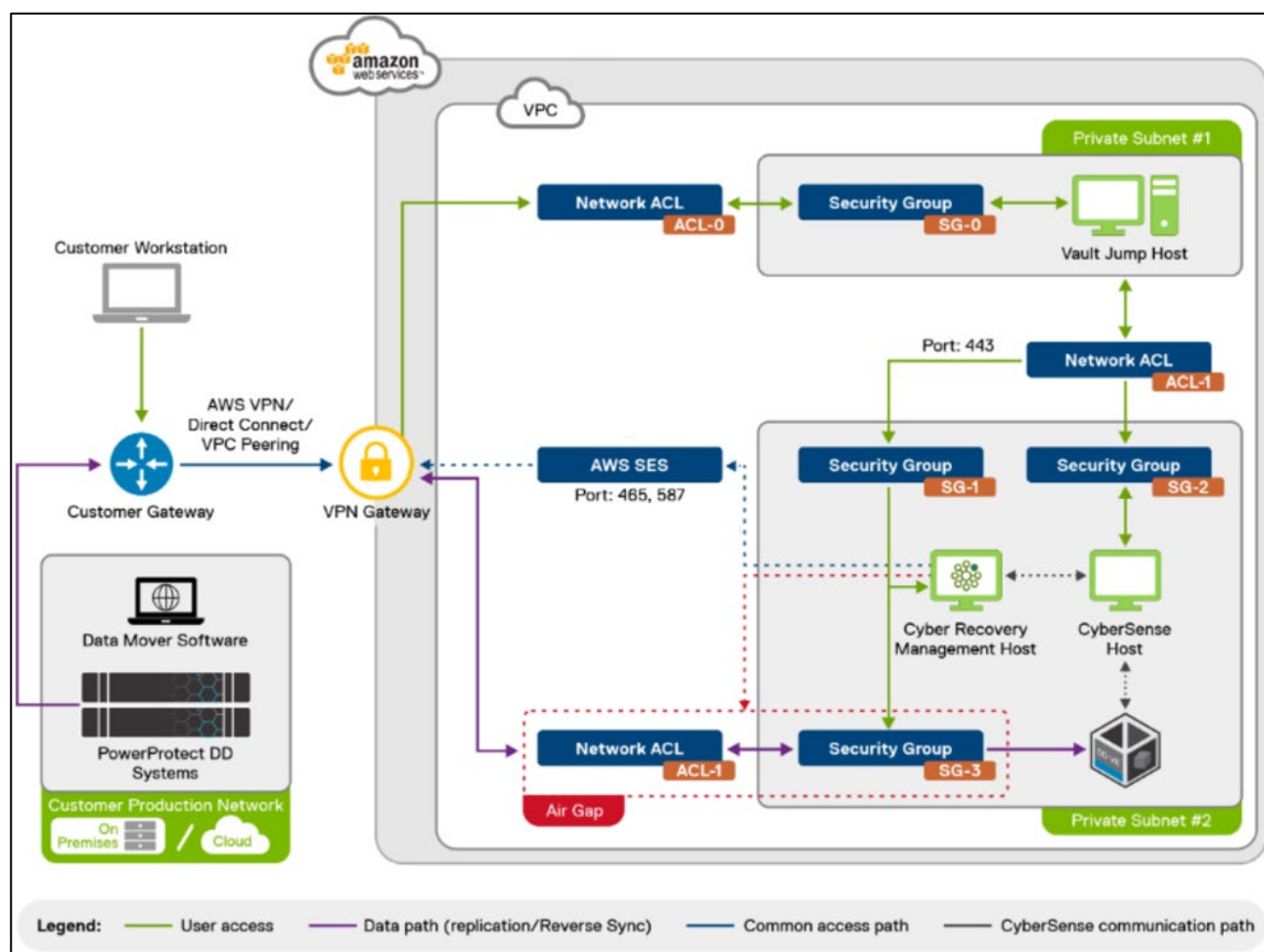
Cyber Recovery integration with the IDPA (DP4400)

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. Starting with Cyber Recovery version 19.13, the Cyber Recovery software supports multiple Cyber Recovery vaults in the same AWS region.

Beginning with Cyber Recovery version 19.13, Cyber Recovery supports PowerProtect Data Manager automated recovery in AWS. Adding a PowerProtect Data Manager asset inside an AWS Cyber Recovery vault is supported. A vCenter server is not required.

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.

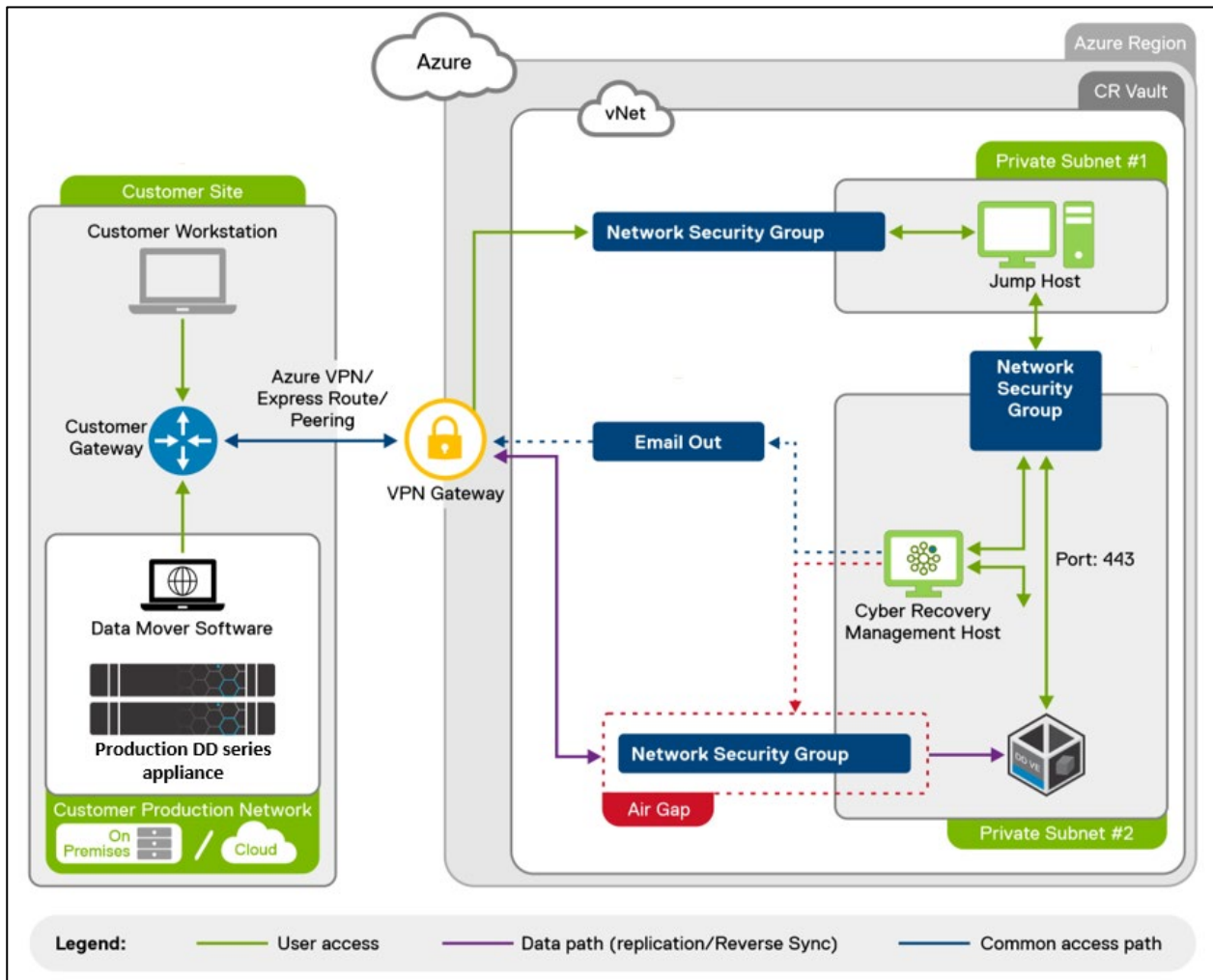
Note: Contact Dell Technologies team to deploy CyberSense on AWS.

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.

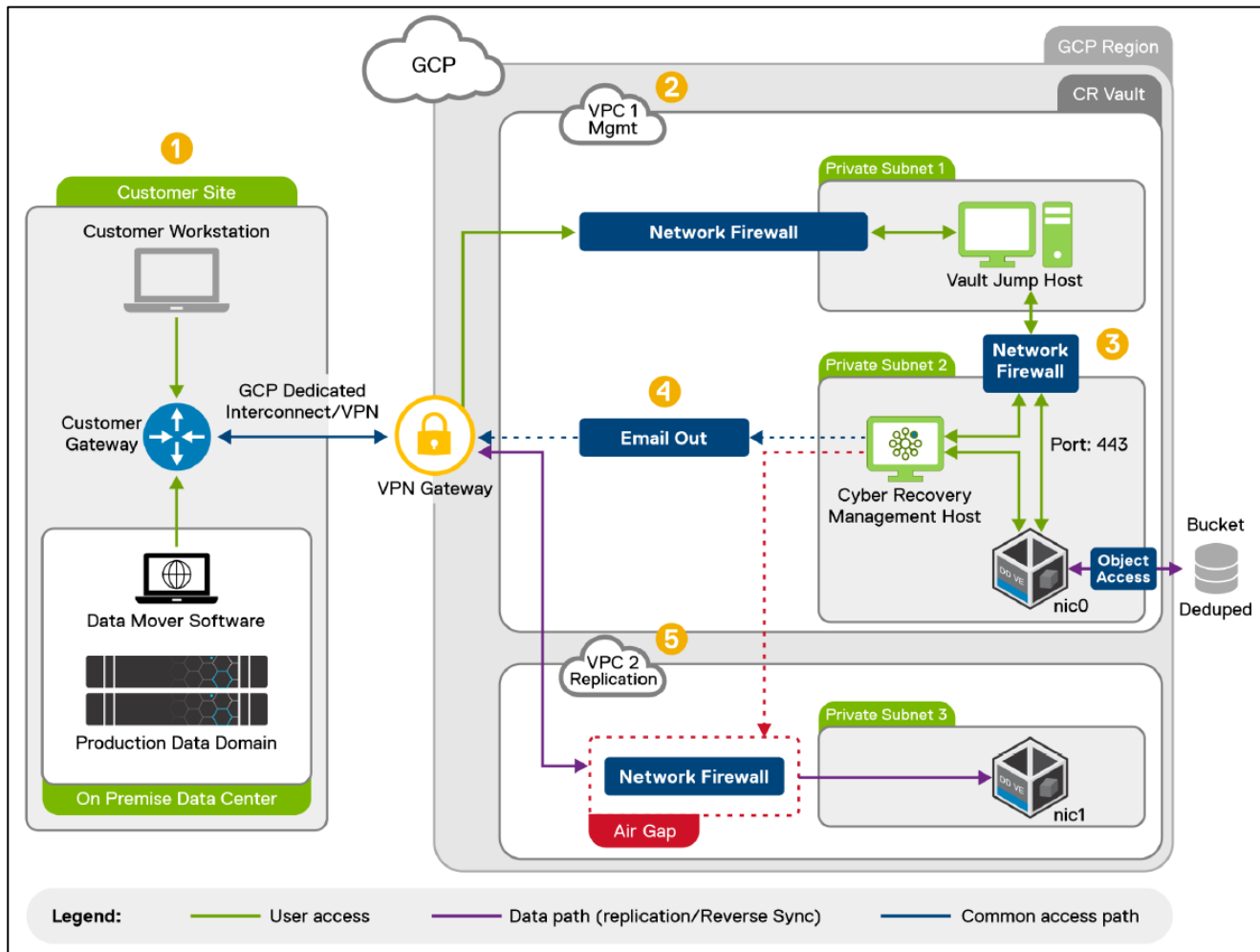
- A storage account—The storage account includes a container for the DDVE storage.

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.

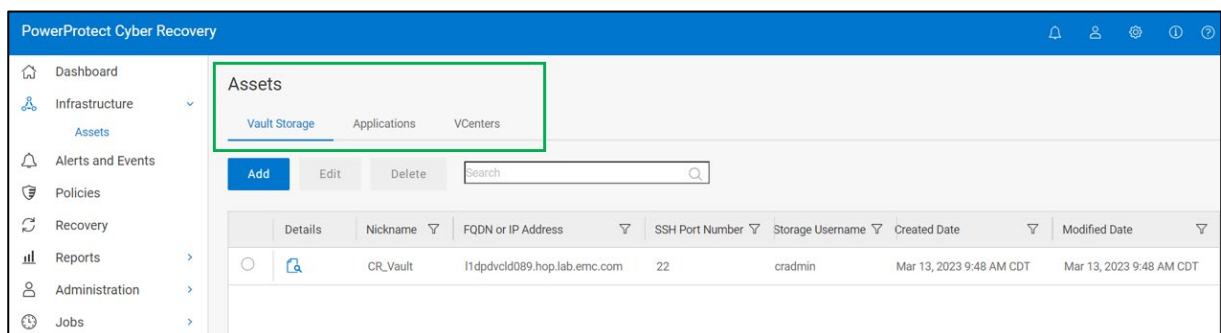
The Cyber Recovery deployment using Terraform does not include a VPN. We strongly recommend that you:

- 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

Assets in the Cyber Recovery vault are represented as storage, application, and vCenter server objects. When you install an application in the Cyber Recovery vault, you must present the application to the Cyber Recovery software. Applications can include the Avamar, NetWorker, PowerProtect Data Manager and the CyberSense application.



Adding vault storage with Cyber Recovery

A DD series in the Cyber Recovery vault serves as the repository for the data that is replicated from the production system and protected by the Cyber Recovery solution. The vault storage can be added from **Infrastructure > Assets > Vault Storage** in the Cyber Recovery UI.

Add Vault Storage

Enter the details of the Storage resource below.

Nickname

CR_Vault

FQDN or IP Address

l1dpdvcl089.hop.lab.emc.com

Storage Username

cradmin

Storage Password

SSH Port Number

22

Tags

Add Tag +

Cancel

Save

The Vault Storage table lists the storage object:

PowerProtect Cyber Recovery

Dashboard

Infrastructure

Assets

Alerts and Events

Policies

Recovery

Reports

Administration

Jobs

Assets

Vault Storage

Applications

VCenters

Add

Edit

Delete

Search

	Details	Nickname	FQDN or IP Address	SSH Port Number	Storage Username	Created Date	Modified Date
		CR_Vault	l1dpdvcl089.hop.lab.emc.com	22	cradmin	Mar 13, 2023 9:48 AM CDT	Mar 13, 2023 9:48 AM CDT

**Adding
CyberSense with
Cyber Recovery**

The CyberSense application can be added from **Infrastructure > Assets > Applications** in the Cyber Recovery UI.

Add Vault Application

Application Information

Host Authentication

Application Summary

Application Information

Enter the details of the Application resource below.

Nickname

CyberSense

FQDN or IP Address

Application Type

CyberSense

Tags

Add Tag +

Step 1 of 3

Cancel

Next

Dell Technologies | PowerProtect Cyber Recovery

Dashboard

Infrastructure

Assets

Sheltered Harbor

Alerts and Events

Policies

Recovery

Administration

Jobs

Assets

Vault Storage

Applications

VCenters

Add

Edit

Delete

Search

Details

Nickname

FQDN or IP Address

Type

CyberSense

cybersense.vault.local

CyberSense

**Adding
Applications
with Cyber
Recovery**

Adding PowerProtect Data Manager with Cyber Recovery

The PowerProtect Data Manager application can be added as a vault application from **Infrastructure > Assets > Applications** in the Cyber Recovery UI.

Add Vault Application

Application Information

Host Authentication

Application Authentication

Application Summary

Application Information

Enter the details of the Application resource below.

Nickname

PowerProtectDataManager

FQDN or IP Address

l1dpdvcl085.hop.lab.emc.com

Application Type

PPDM

Tags

Add Tag +

Step 1 of 4

Cancel

Next

Adding NetWorker with Cyber Recovery

The NetWorker application can be added as a vault application from **Infrastructure > Assets > Applications** in the Cyber Recovery UI.

Add Vault Application

Application Information

Host Authentication

Application Authentication

Application Summary

Application Information

Enter the details of the Application resource below.

Nickname

NetWorker

FQDN or IP Address

l1dpdvcl088.hop.lab.emc.com

Application Type

NetWorker

Tags

Add Tag +

Step 1 of 4

Cancel

Next

Adding Avamar with Cyber Recovery

The Avamar application can be added as a vault application from **Infrastructure > Assets > Applications** in the Cyber Recovery UI.

Add Vault Application

Application Information
Enter the details of the Application resource below.

Nickname: Avamar

FQDN or IP Address: l1dpdvcl086.hop.lab.emc.com

Application Type: Avamar

Tags: Add Tag +

Step 1 of 3

Cancel Next

Adding vCenter with Cyber Recovery

When you install a vCenter server in an on-premises Cyber Recovery vault, you must present it to the Cyber Recovery software.

Note: A vCenter server is not required for a Cyber Recovery deployment on Amazon Web Services (AWS).

Add vCenter Asset

Enter the details of the vCenter resource below.

Nickname: vCenter

FQDN or IP Address: l1dpdvcl079.hop.lab.emc.com

Username: administrator@vsphere.local

Password: [masked]

Tags: Add Tag +

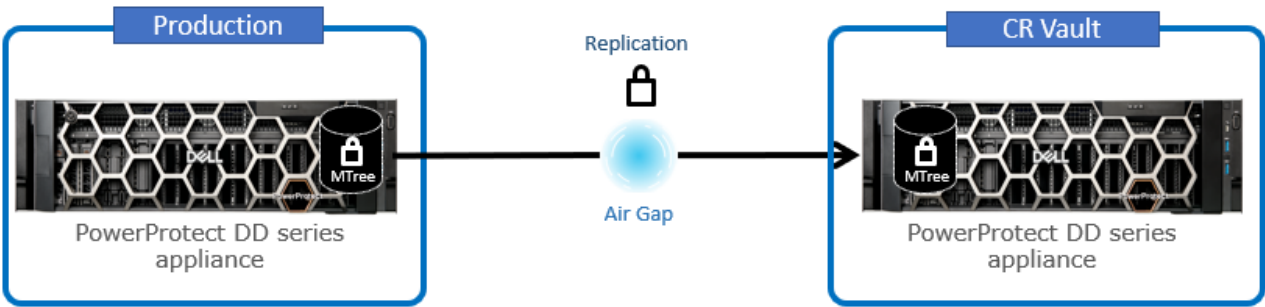
Cancel Save

For more details on configuring/managing storage and applications, see Dell PowerProtect Cyber Recovery Product Guide.

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.

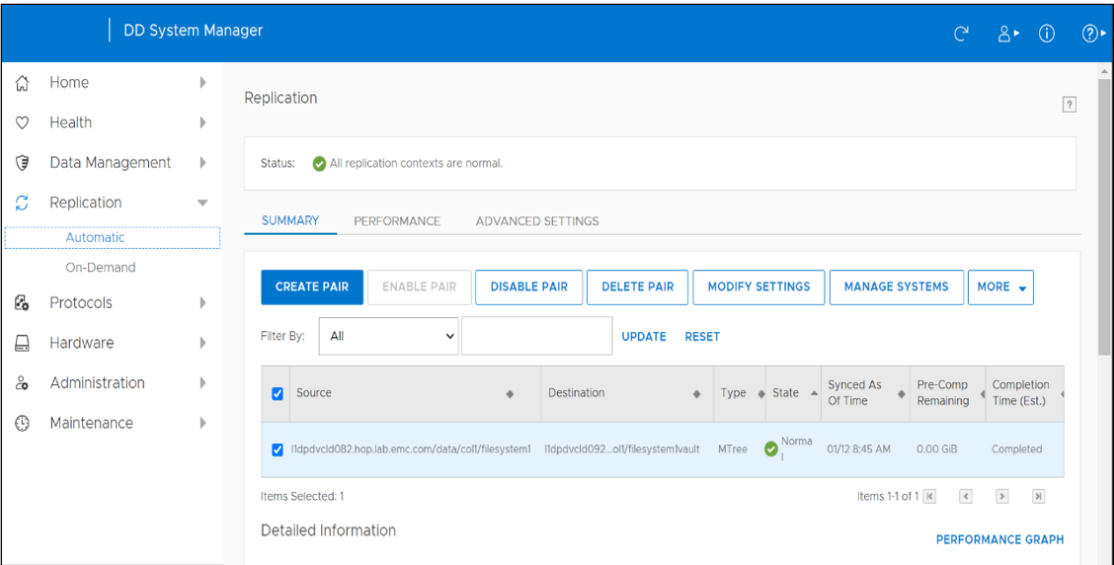


The Cyber Recovery software controls data synchronization from the production environment to the vault environment by DD series MTree replication. After the datasets and associated MTrees to be protected by the Cyber Recovery solution are determined, replication contexts are set up between the production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

Add Policy

Policy Information

Replication

Retention

Summary

Name

Type

Select Type

PPDM

Standard

Storage

Step 1 of 4

Cancel Next

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.

Add Policy

Name: P1aystem

Policy Type: Standard

Storage: DDVULT

Context: Context (Selected), Ethernet Port

Rsystemhault

Replication Window: 0 Hours

Retention Lock Type: Governance

Retention Lock Minimum: Governance

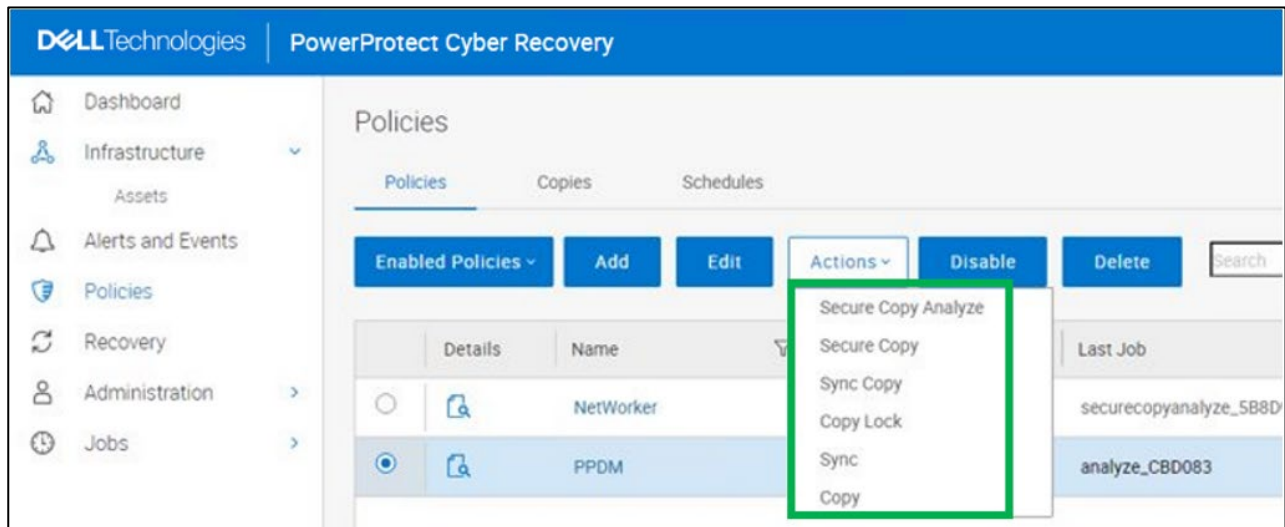
Retention Lock Maximum: Governance

Retention Lock Duration: Compliance

Tags: + Add Tag

Cancel Save

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	<ul style="list-style-type: none"> 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.

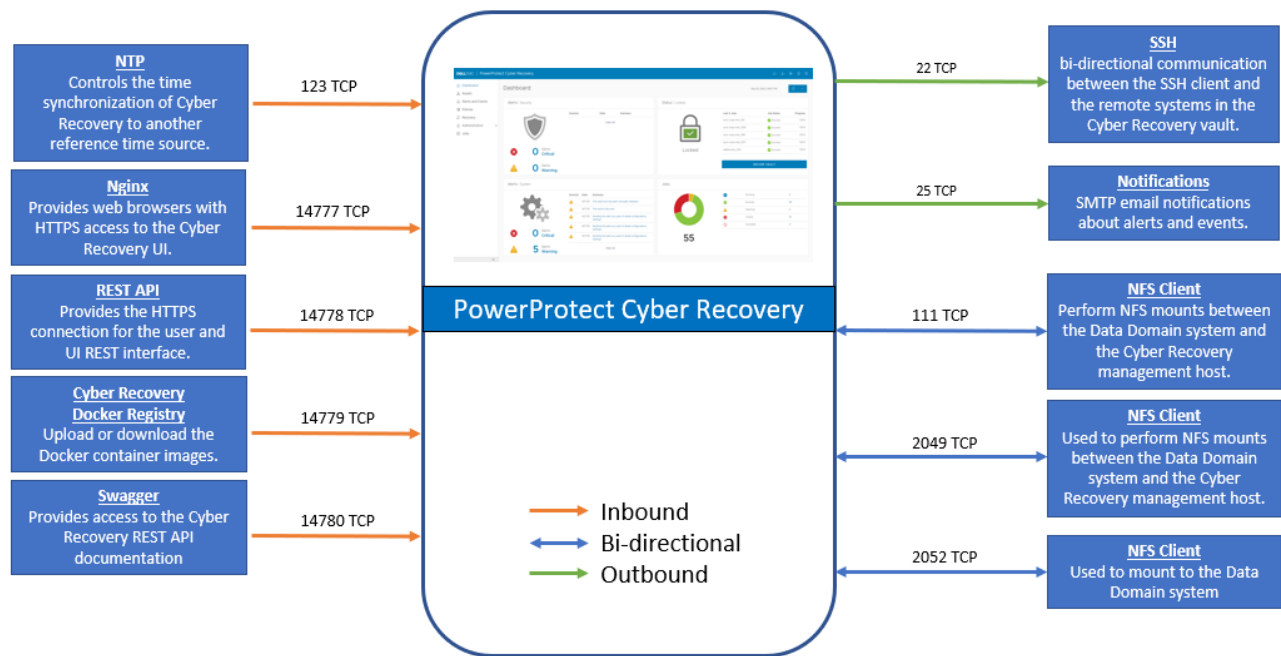
To secure the network links that connect the vault environment to the production environment, or any other network, installing a firewall or other packet inspection tool on both the DD series replication link and the SMTP link is recommended. It is recommended not to make use of packet inspection if 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

Technical support

The [Dell Technologies support page](#) is focused on meeting customer needs with proven services and support.

Related resources

The [Cyber Recovery product documentation set on Dell Support](#) includes:

- [Dell PowerProtect Cyber Recovery Product Guide](#)
- [Dell PowerProtect Cyber Recovery Installation Guide](#)
- [Dell PowerProtect Cyber Recovery AWS Deployment Guide](#)
- [Dell PowerProtect Cyber Recovery Azure Deployment Guide](#)
- [Dell PowerProtect Cyber Recovery Google Cloud Platform](#)

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

Additional documentation includes:

- [Dell PowerProtect Cyber Recovery Simple Support Matrix](#)
- [Dell PowerProtect Cyber Recovery Solution Guide](#)
- [Dell PowerProtect Cyber Recovery Solution Brief](#)

For more information, see the [PowerProtect Cyber Recovery Info Hub](#).

The [Dell Technologies Data Protection Info Hub](#) provides expertise that helps to ensure customer success on Dell Technologies data protection platforms.