Technical White Paper

Multi-Cloud Data Services for Dell EMC PowerProtect

Abstract

This document explains how a data protection offering from Dell Technologies™ and Faction provides a fully managed service to protect on-premises and multi-cloud environments.

April 2021

Revisions

Date	Description
April 2021	Initial release

Acknowledgments

Authors: Vinod Kumaresan and Parimala Guruprasad

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

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

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

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

Table of contents

Executive summary

As public cloud services continue to grow, the competition between cloud providers drives innovation. As native cloud services evolve, they provide increasingly differentiated value propositions to organizations. A multi-cloud strategy allows users to select the cloud services that best meet their needs, unleashing competitive advantages and productivity gains that would be unattainable with a single cloud. However, with multi-cloud environments, organizations require an integrated data-protection strategy and seamless data movement across their various cloud ecosystems.

Customers are looking for cost efficiency and operational flexibility of their cloud ecosystem without compromising security, data protection, and data integrity that on-premises environments offer.

Multi-Cloud Data Services for Dell EMC™ PowerProtect is a fully managed data-protection-as-a-service solution. It enables customers to back up their workloads across public clouds to a PowerProtect DD series appliance that is hosted in a Faction data center.

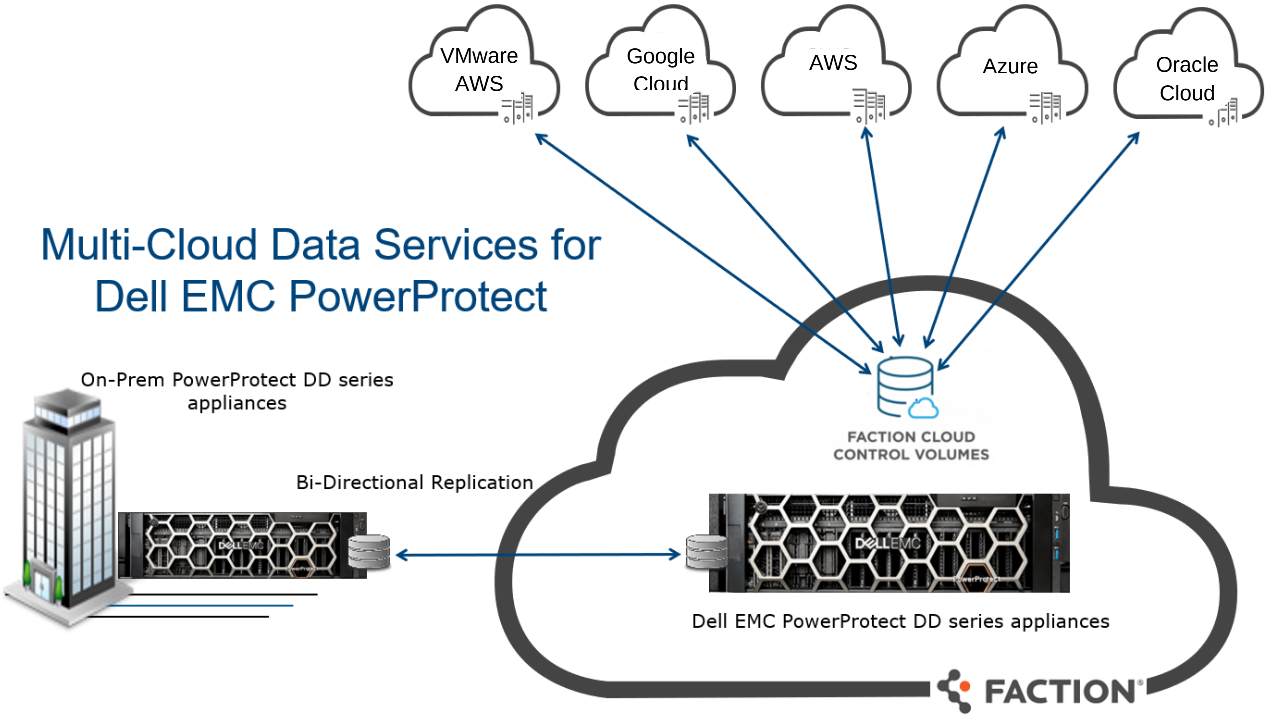
Multi-Cloud Data Services for Dell EMC PowerProtect also integrates with Dell EMC PowerProtect Cyber Recovery, enabling customers to protect their organization from ransomware, insider attacks, and other cyber threats. This solution provides an air-gapped and secure Cyber Recovery vault that is hosted in a Faction data center, providing physical isolation of critical customer data.

Audience

This white paper is intended for Dell Technologies customers, partners, and employees looking to protect their on-premises and public cloud workloads in a fully managed, nonpublic cloud destination.

1 Introduction

Multi-Cloud Data Services for Dell EMC PowerProtect is offered through Faction Cloud Control Volumes (CCV) and is backed by Dell EMC PowerProtect DD series appliances. The Multi-Cloud Data Services for Dell EMC PowerProtect solution provides centralized data protection for workloads across various public clouds and on-premises workloads.


VMware AWS
Google Cloud
AWS
Azure
Oracle Cloud
Multi-Cloud Data Services for Dell EMC PowerProtect
On-Prem PowerProtect DD series appliances
Bi-Directional Replication
FACTION CLOUD CONTROL VOLUMES
Dell EMC PowerProtect DD series appliances
FACTION

Multi-Cloud Data Services for Dell EMC PowerProtect is ideal for the following use cases:

- Backup target for public cloud workloads
- Replication target for on-premises PowerProtect DD series appliances or PowerProtect DD Virtual Edition (DDVE) deployed on the cloud
- Air-gapped, physically isolated vault environment for PowerProtect Cyber Recovery

Multi-Cloud Data Services for Dell EMC PowerProtect offers a low-latency connection (< 2 ms) to the major hyperscale cloud providers. This ability enables efficient backup, archiving, and disaster recovery of both cloud-based and on-premises data workloads.

1.1 Solution benefits

Multi-Cloud Data Services for Dell EMC PowerProtect offers the following benefits to enterprises that require protection for their hybrid-cloud or multi-cloud environments.

Simplified management:

- Enables managing multiple cloud backups in one location
- Removes the requirement to deploy and maintain a PowerProtect DD Virtual Edition (DDVE) appliance in each cloud if it is used as a primary backup target
- Eliminates the maintenance of a secondary data center for replication and Cyber Recovery vault
- Has a single IP, VLAN, or namespace across public clouds
- Deduplicates one copy of data globally across all clouds
- Provides governance and compliance management

Cost savings:

- Up to 75% lower egress cost with Faction contracts for Amazon Web Services (AWS), VMware® Cloud (VMC), and Google Cloud Platform (GCP)
- Zero egress cost for Microsoft® Azure® and Oracle®
- Industry-leading deduplication reduces storage cost[1]

Flexibility:

- Native read/write using DD Boost, CIFS, or NFS for various public clouds
- No limitations on quota for cloud-workload protection
- Application mobility across public clouds
- Ability to instantly restore to any multi-cloud provider
- Flexibility for customers to choose technologies from any cloud and not get locked in to one cloud provider

Trusted service:

- Certified Dell Cloud Service Provider
- High-speed access with low-latency connection to all major public clouds

[1] https://www.delltechnologies.com/en-us/data-protection/powerprotect-backup-appliances.htm

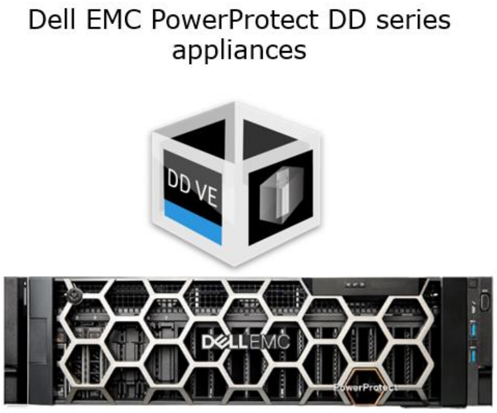
1.1.1 PowerProtect DD series appliances

The Dell EMC PowerProtect DD series offers the ultimate protection storage appliances that are the latest generation of Dell EMC Data Domain appliances. DD series delivers a fast, secure, and an efficient solution that is optimized for multi-cloud data protection and future demands.

The DD Operating System (DDOS) is the intelligence that powers DD series. It provides the agility, security, and reliability that enables DD series to deliver high-speed, scalable, and industry-leading multi-cloud protection storage for backup, archive, and disaster recovery[2].

DDOS software elements include the following:

- DD Boost
- DD VTL
- DD Replicator
- DD Cloud Tier
- DD Retention Lock
- DD Encryption
- DD Secure Multi-Tenancy
- DD High Availability
- DD System Manager
- DD Management Center



DD series can scale up to a physical capacity of 1.5 PB in a single rack, using minimal floor space and lowering power and cooling by up to 41%[2]. DD series provides up to an additional 2 PB of cloud capacity for long-term retention with Dell EMC Cloud Tier.

DD series consists of the DD9900, DD9400, DD6900, DD3300, and a software-defined appliance with PowerProtect DD Virtual Edition (DDVE).

DDVE uses the power of DDOS to deliver software-defined protection storage on-premises and in-cloud. DDVE is fast and simple to download, deploy, and configure, and can be up and running in minutes.

[2] https://www.delltechnologies.com/en-in/collaterals/unauth/data-sheets/products/data-protection/h17926-dellemc-powerprotect-dd-ds.pdf

You can deploy DDVE on any standard hardware, converged or hyperconverged, and run it in VMware vSphere®, Microsoft Hyper-V®, KVM. You can also run DDVE in the cloud with AWS, AWS GovCloud, VMware Cloud, Azure, Azure Government Cloud, and Google Cloud.

A single DDVE instance can scale up to 256 TB in-cloud (AWS, Azure, and Google Cloud) and up to 96 TB on-premises.

As part of Multi-Cloud Data Services for Dell EMC PowerProtect, customers can choose any of the PowerProtect DD series appliance models: DD6900, DD9400, and DD9900 with incremental scaling.

1.1.2 Faction Cloud

Faction, Inc. is a Dell Technologies Platinum Partner and Extended Technologies Complete partner, founded in 2006, and headquartered in Denver, Colorado.

Faction is a leading multi-cloud data-services provider. Faction pioneered cloud-adjacent storage that is powered by patented technology providing data access over low-latency, high-throughput connections to all the major clouds, including AWS, Azure, and Google Cloud Platform.

Faction is also a leading managed service provider for VMware Cloud on AWS, including disaster recovery and production deployments. Also, Faction was the first to offer cloud-attached storage solutions that integrate natively with VMware Cloud on AWS.

Faction Cloud Control Volumes (CCVs) are persistent cloud-attached storage volumes that can connect to public clouds through proprietary, patented network connectivity with ultralow latency. This technology enables organizations to minimize the high egress fees charged by cloud providers. Cloud-attached storage also enables seamless data portability between clouds and avoids vendor lock-in.

Faction services and data centers undergo annual Type II SOC1 and SOC2 and HIPAA compliance audits, with independent outside auditor attestations available under NDA. Faction can create BAA agreements with customers-subject to HIPAA.

The Faction difference:

- **Faction Internetwork Exchange (FIX):** A single IP and single namespace across all clouds and on-premises locations.
- **Application mobility across clouds:** Faction’s private and multi-cloud platforms give clients the ability to move, access, scale, and protect data between clouds, without the fear of cloud lock-in. Faction has data centers strategically located next to the public cloud providers (Azure, AWS, VMC, GCP, and OCI).
- **Balancing of cloud network costs:** Faction efficiently blends cloud-connect ports to offer a balance of high and low speeds, driving down TCO. Faction has negotiated contracts with each cloud vendor: $0 egress charges for Azure and Oracle Cloud.
- **Low-latency connections:** Managed data center locations to offer the lowest latency connectivity to multiple clouds. Faction has dark fiber connections to each of these data centers for low latency and fast connectivity.

Faction provides a portal that allows customers to manage connections to their DD series appliances that are hosted at the Faction data centers. Through the Faction Portal, customers can also provision new connections to cloud providers through the Faction Internetwork Exchange (FIX).

Faction operates seven cloud-service locations (see Figure 1) across the United States, in London, and in Frankfurt.

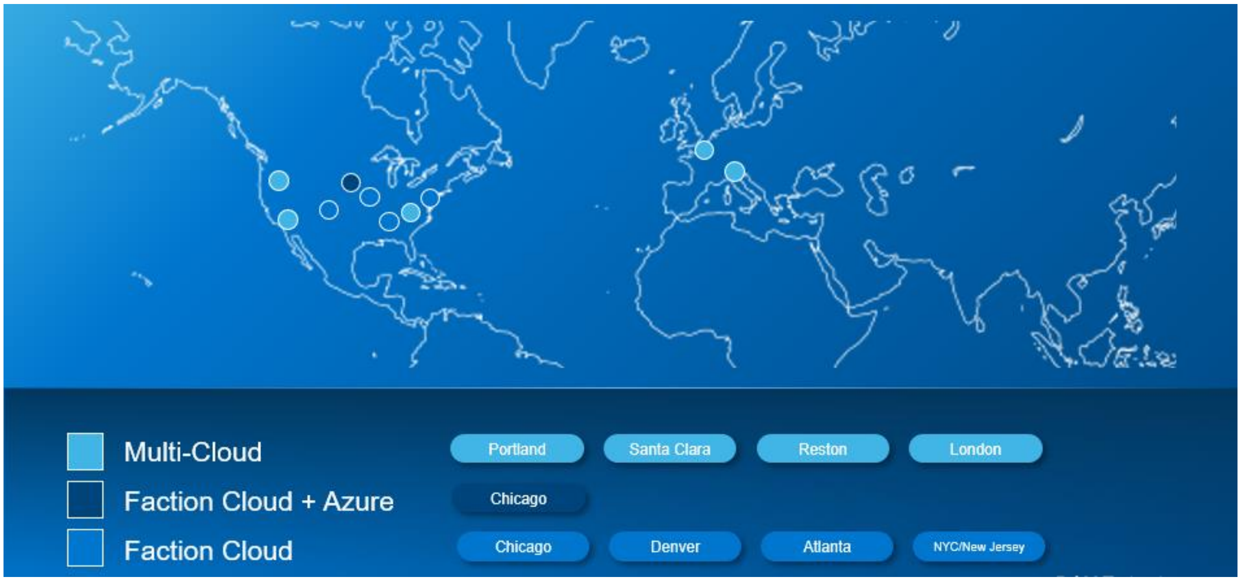
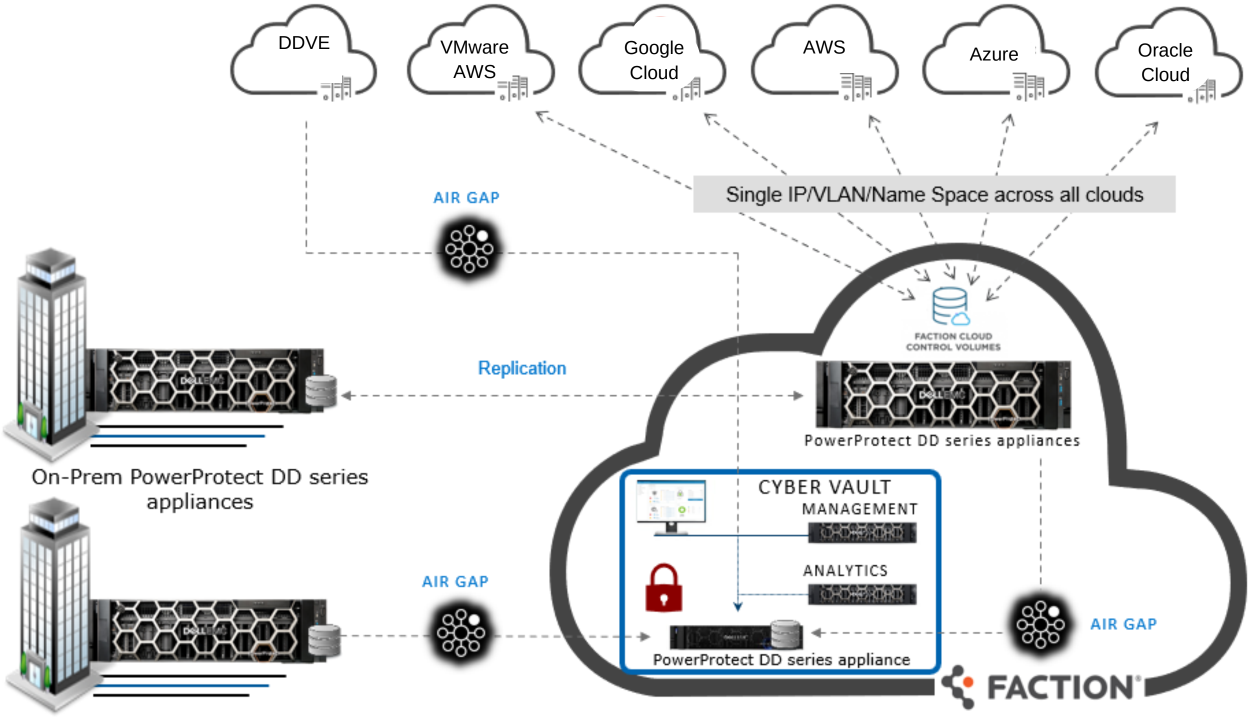


Figure 1 Faction Cloud locations

2 Use cases

Multi-Cloud Data Services for Dell EMC PowerProtect supports the following use cases:

- **Backup target**: Protection of public cloud data to DD series at Faction data centers with a single namespace across multiple clouds.
- **Replication target**: Replicate data from on-premises DD series or DDVE deployed in the cloud for long-term retention (LTR) to Faction data centers or to public clouds, and for Cloud Disaster Recovery.
- **PowerProtect Cyber Recovery**: Enables customers to replicate both on-premises and off-premises workloads to a physically isolated, air-gapped vault.


DDVE
VMware AWS
Google Cloud
AWS
Azure
Oracle Cloud
Single IP/VLAN/Name Space across all clouds
AIR GAP
FACTION CLOUD CONTROL VOLUMES
Replication
PowerProtect DD series appliances
On-Prem PowerProtect DD series appliances
CYBER VAULT
MANAGEMENT
ANALYTICS
AIR GAP
AIR GAP
PowerProtect DD series appliance
FACTION

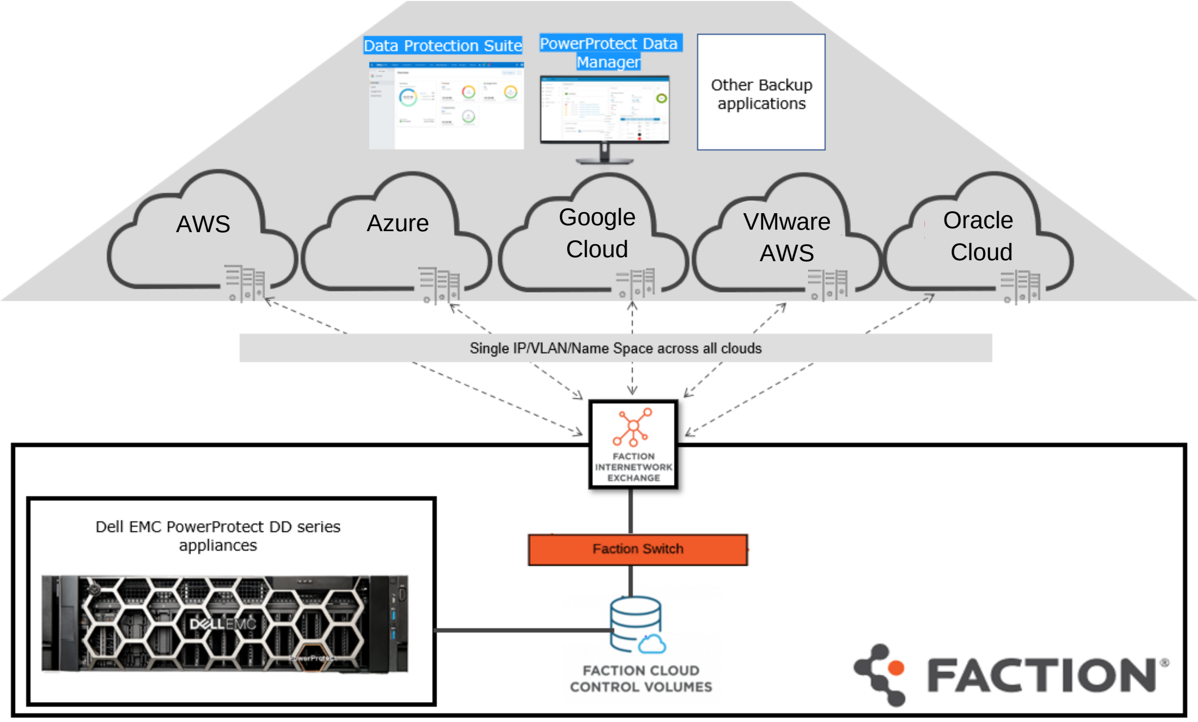
As part of the offer, customers have the option of long-term data retention in Faction's data center and can migrate or replicate data into public clouds. Multi-Cloud Data Services for Dell EMC PowerProtect makes disaster recovery possible using multi-cloud attached storage and compute that is ready in Faction or in supported the public cloud.

Cloud Disaster Recovery (CDR) allows enterprises to copy backed-up VMs from their on-premises environments to the public cloud (AWS and Azure) for the orchestration and automation of DR testing, DR failover and failback of Tier 2 workloads to or from the cloud in a disaster scenario.

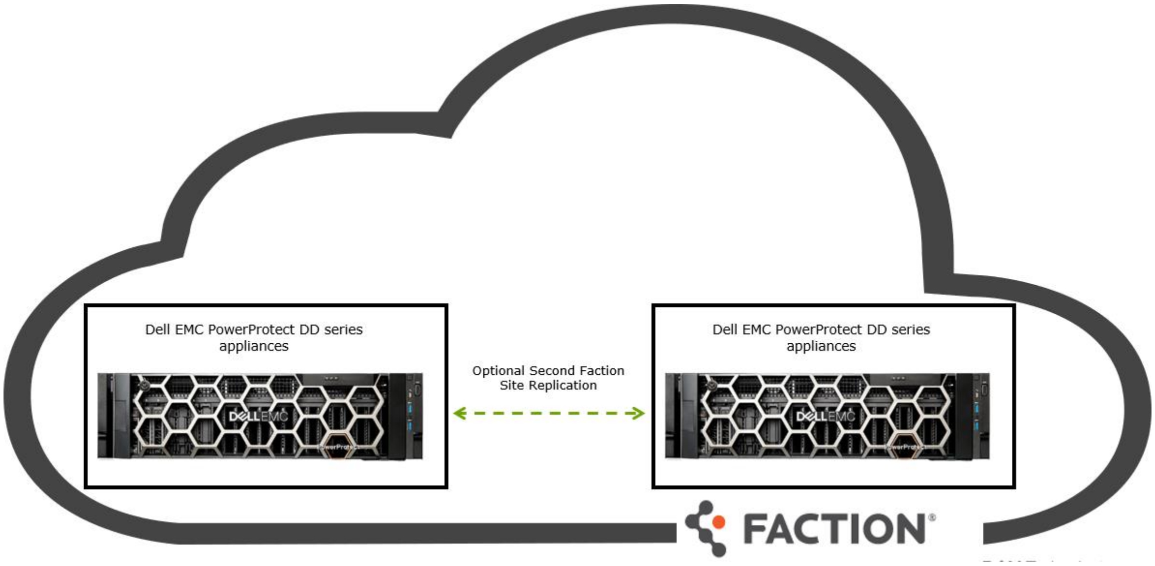
Long-Term Retention (Cloud Tier) is available for data on-premises, in the cloud, or both. Multi-Cloud Data Services for Dell EMC PowerProtect can be a remote site to protect data that must be retained for regulatory requirements (governance and compliance) and for workload migration.

2.1 Public cloud protection (backup target)

A DD series appliance at a Faction data center can be used as single backup target to protect workloads across multiple clouds. Using DD Boost, CIFS, and NFS protocols, backup applications can send data to a single DD series appliance at the Faction data center.

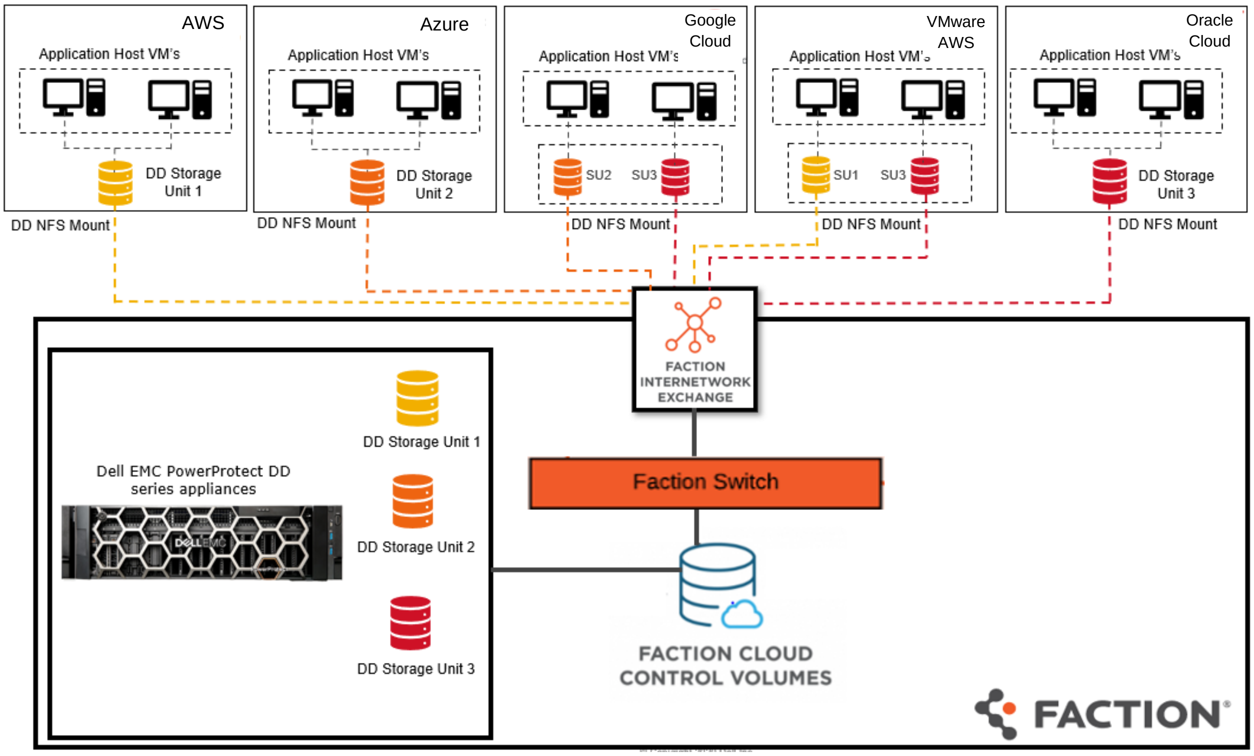

Data Protection Suite
PowerProtect Data Manager
Other Backup applications
AWS
Azure
Google Cloud
VMware AWS
Oracle Cloud
Single IP/VLAN/Name Space across all clouds
FACTION INTERNETWORK EXCHANGE
Dell EMC PowerProtect DD series appliances
Faction Switch
FACTION CLOUD CONTROL VOLUMES
FACTION

Customers can also use the optional secondary Faction DD series appliance for site replication.


Dell EMC PowerProtect DD series appliances
Optional Second Faction Site Replication
Dell EMC PowerProtect DD series appliances
FACTION

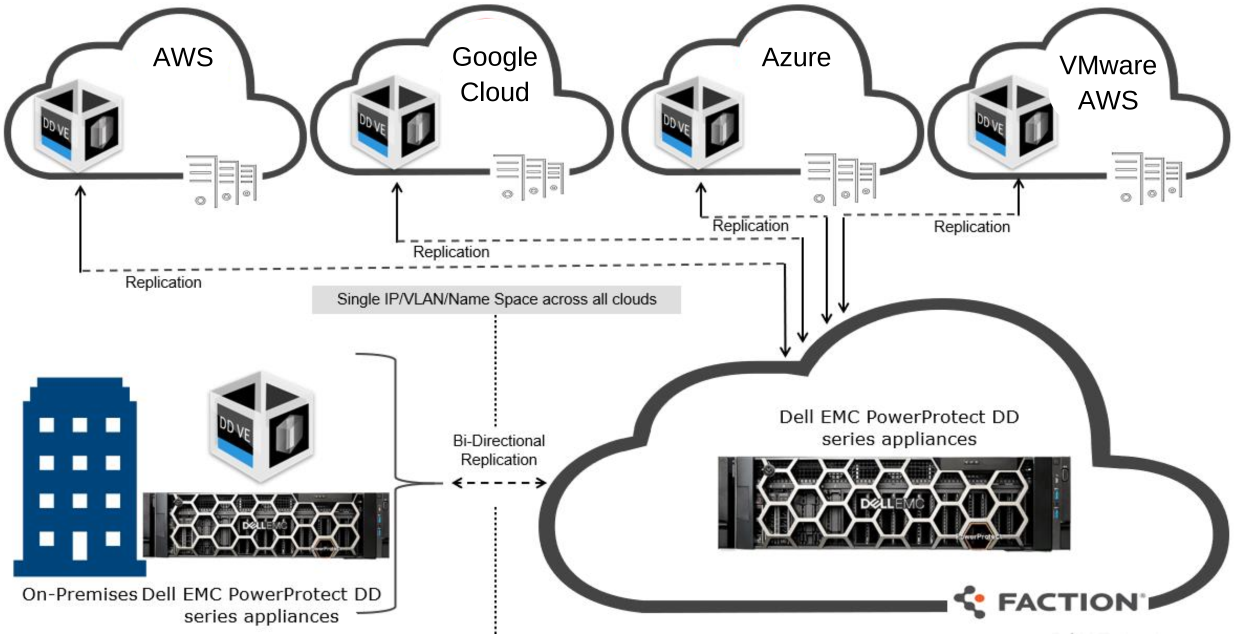
Databases and applications running on public clouds can save backups to the DD series appliances at Faction data centers by mounting the DD series storage unit on the cloud instances using BoostFS plug-in. With direct access to a BoostFS mount point, the application can use source-side deduplication, storage, and network efficiencies of the DD Boost protocol for backup and recovery.

Using DD BoostFS plug-in, the DD series storage unit can be simultaneously mounted on the multiple public cloud instances for data protection and recovery. See the BoostFS Compatibility Matrix (login required) for more details.



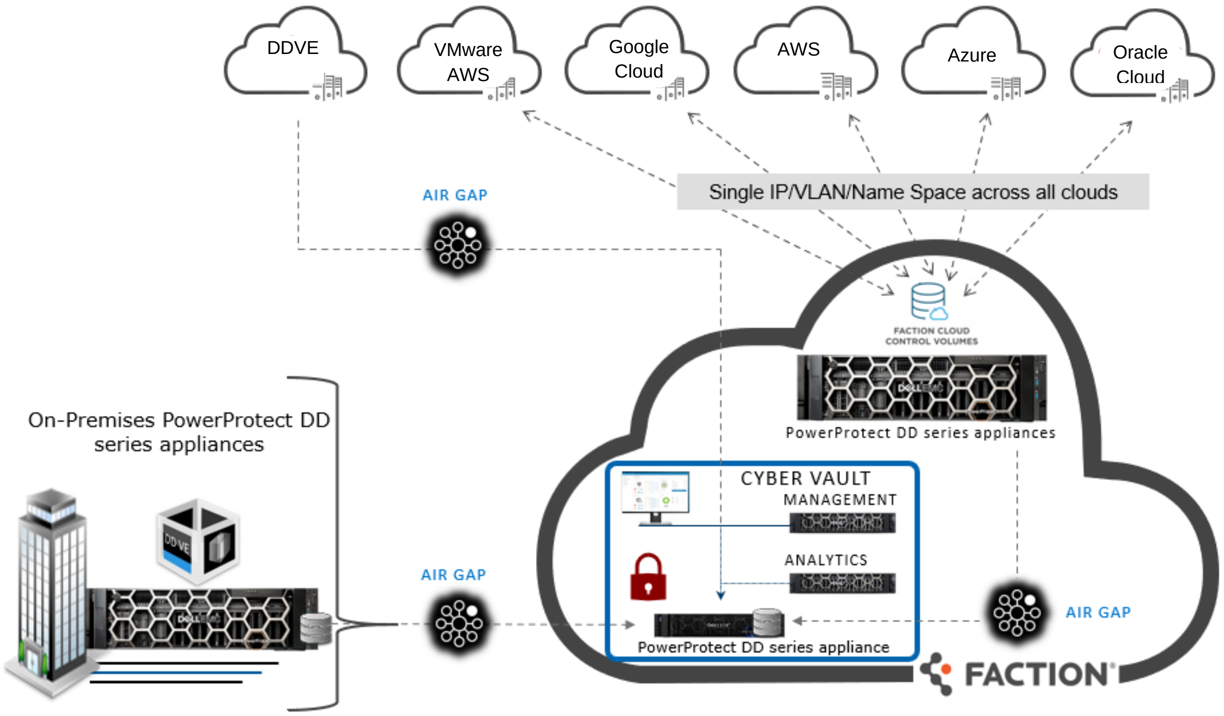
2.2 Replication target for on-premises DD series and DDVE in the cloud

Customers can replicate data from an on-premises DD series or a DDVE in the cloud to a single DD series provisioned in the Faction data centers. This solution eliminates the need for customers to maintain a secondary site for replication. This solution enables long-term retention and disaster recovery.


AWS
Google Cloud
Azure
VMware AWS
DD VE
Replication
Replication
Replication
Replication
Single IP/VLAN/Name Space across all clouds
Bi-Directional Replication
On-Premises Dell EMC PowerProtect DD series appliances
Dell EMC PowerProtect DD series appliances
FACTION

2.3 Cyber recovery

This secure data-vaulting service is physically and logically air-gapped and is built on secure, multi-cloud-enabled infrastructure that safeguards critical data from cyberattacks.


DDVE
VMware AWS
Google Cloud
AWS
Azure
Oracle Cloud
AIR GAP
Single IP/VLAN/Name Space across all clouds
FACTION CLOUD CONTROL VOLUMES
PowerProtect DD series appliances
On-Premises PowerProtect DD series appliances
CYBER VAULT
MANAGEMENT
ANALYTICS
AIR GAP
AIR GAP
PowerProtect DD series appliance
FACTION

Combined with the physical security and isolation of the vault, this solution includes an operational air gap. This air gap enables access to the vault only during replication.

At all other times, the vault is disconnected from the client's production environment. Immutable copies of user-selected data are created in the Cyber Recovery vault hosted in the Faction data center. Once a copy of the selected data is safely in the secure, isolated vault, the data cannot be altered, deleted, or otherwise changed for a prescribed duration.

PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense, which adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. This innovative approach provides full content indexing and uses machine learning to analyze over 100 content-based statistics and detect signs of corruption due to ransomware. CyberSense finds corruption with up to 99.5% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content—all in the security of the vault.

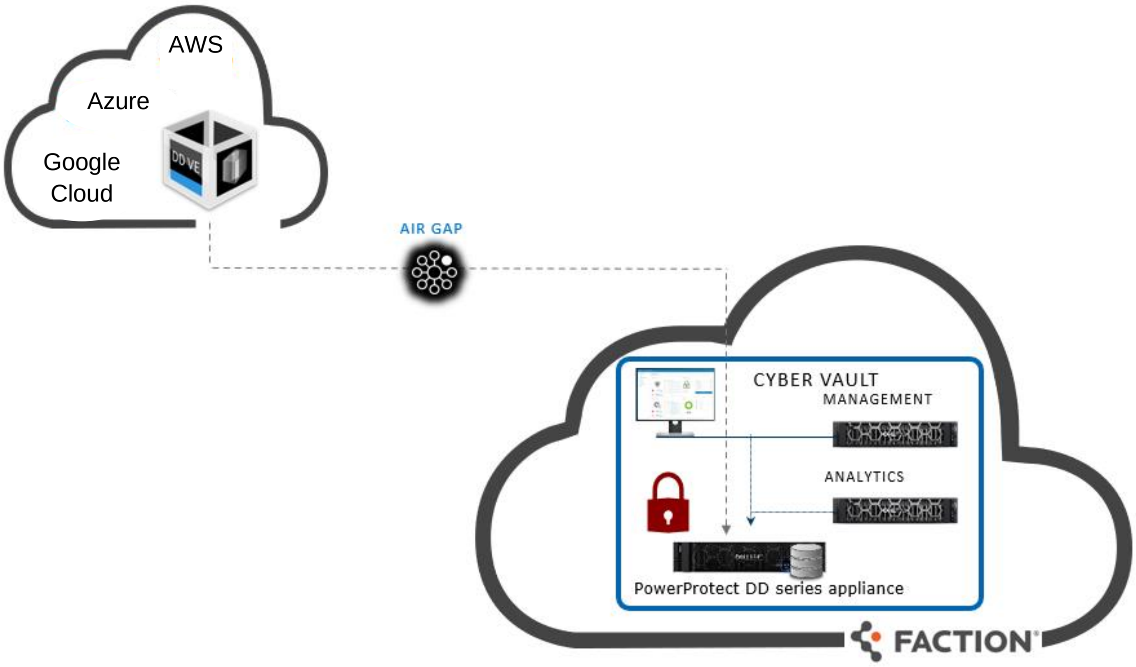
When data recovery is required, the data from the Cyber Recovery vault can be restored to AWS, VMC on AWS, Microsoft Azure, Google Cloud, Oracle Cloud, or back to the on-premises environment.

Data in DD series appliances can be replicated to a Cyber Recovery vault in the Faction data center from the following:

- Public cloud
- On-premises
- Within the Faction cloud

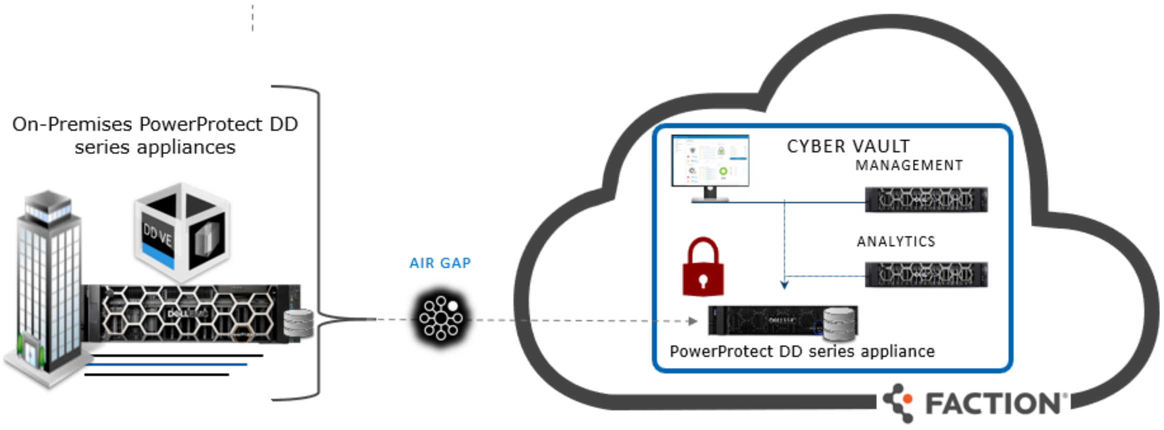
2.3.1 Replicate from DDVE on public cloud to Cyber Recovery vault in the Faction data center

For cloud-native applications using DDVE, the Cyber Recovery vault service enables customers to replicate critical data to a secure Cyber Recovery vault at a Faction data center.



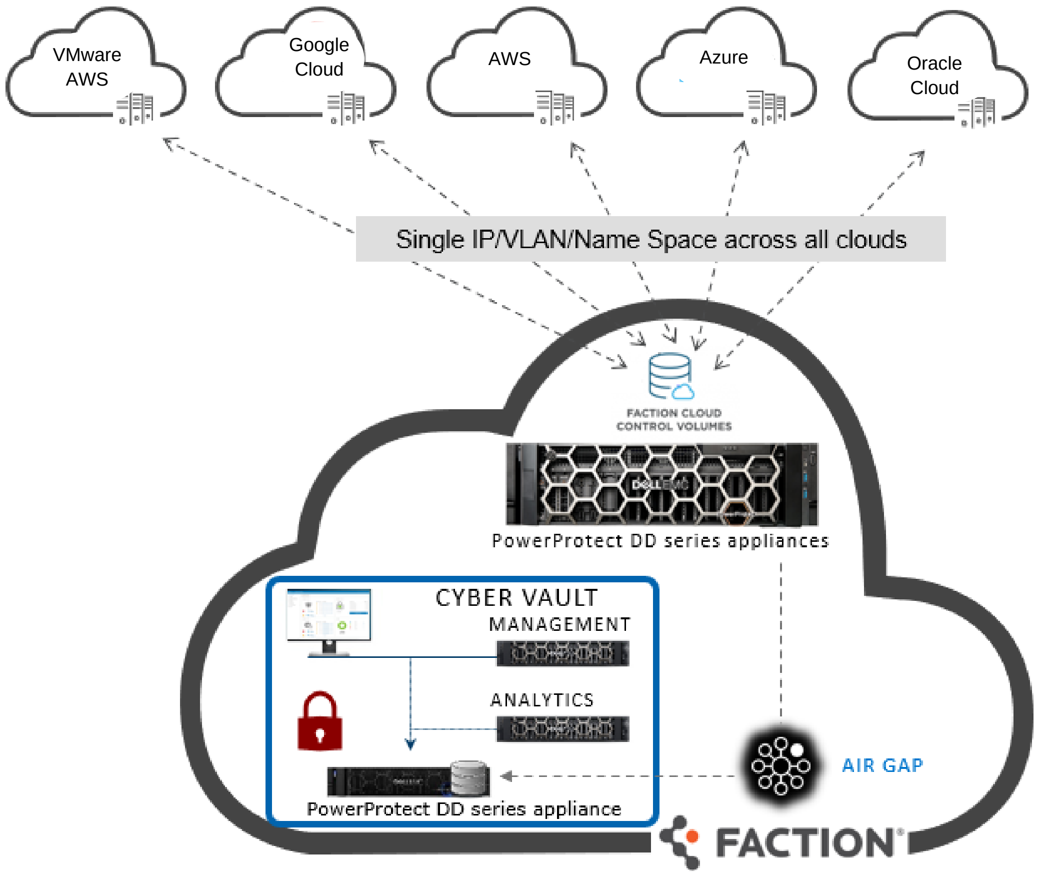
2.3.2 Replicate from on-premises DD series to Cyber Recovery vault in Faction data centers

Customers can replicate data from an on-premises DD series appliance to a Cyber Recovery vault in the Faction data center.


On-Premises PowerProtect DD series appliances
DD VE
AIR GAP
CYBER VAULT
MANAGEMENT
ANALYTICS
PowerProtect DD series appliance
FACTION

2.3.3 Replicate within Faction data centers

Data residing in any public cloud can be backed up to the DD series appliance in a Faction data center as a primary target. These backups can be replicated to a secure Cyber Recovery vault in a Faction data center.


VMware AWS
Google Cloud
AWS
Azure
Oracle Cloud
Single IP/VLAN/Name Space across all clouds
FACTION CLOUD CONTROL VOLUMES
PowerProtect DD series appliances
CYBER VAULT
MANAGEMENT
ANALYTICS
PowerProtect DD series appliance
AIR GAP
FACTION

2.3.4 Compute resource at Faction for Cyber Recovery:

Compute resources required for Cyber Recovery are deployed on a dedicated VMware ESXi™ host or hosts. This VMware compute environment includes the following:

- Required ESXi host to support management VMs
  - Available resources: 50 GHz, 250 GB RAM, 22 TB storage
- Optional ESXi CyberSense analytics host or hosts
  - Available resources: 95 GHz, 635 GB RAM, 14 TB storage

The number of analytics hosts required varies based on the amount of data to be analyzed.

All VMware licensing is included in the cost of these hosts. Customers are provided VMware vCenter® access to install and manage all VMs that run in the VMware compute environment.

Cyber Recovery and the optional CyberSense analytics licenses must be purchased separately.

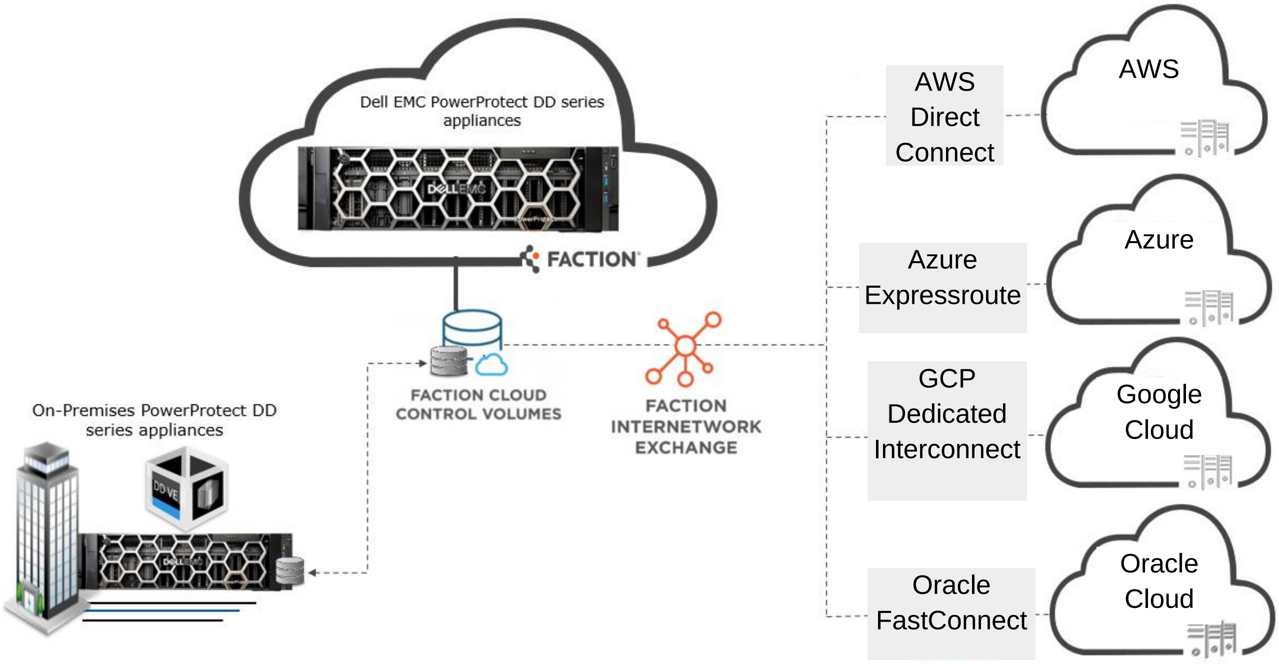
3 Client connectivity

Faction can terminate both Fibre Channel and copper cross-connects in supported facilities, and most other common connections. There are two replication transport options to move data from a customer on-premises data center to the Faction data center:

VPN: Faction can supply an Internet endpoint for replication and client network connectivity over VPN. Also, Faction can terminate IPsec VPNs from compatible equipment for encryption in transit. The VPN must be managed by Faction if the customer does not have a compute environment in the Faction cloud.

Dedicated circuit: Large-scale customers can opt for a dedicated connection for replication traffic between their facility and Faction. These customers can use a VPN temporarily since lead times for dedicated circuits can be in the 90+ day range. Customers may also use a VPN for redundancy to a dedicated link. Faction can source and manage the dedicated link, or the client can work with their carrier directly.

It is the customer's responsibility to manage the network between their on-premises data center and the Faction data center.


Dell EMC PowerProtect DD series appliances
FACTION
FACTION CLOUD CONTROL VOLUMES
FACTION INTERNETWORK EXCHANGE
On-Premises PowerProtect DD series appliances
DD VE
AWS Direct Connect
AWS
Azure Expressroute
Azure
GCP Dedicated Interconnect
Google Cloud
Oracle FastConnect
Oracle Cloud

For public clouds, customers can establish private connectivity between the respective cloud providers and Faction data center through the following:

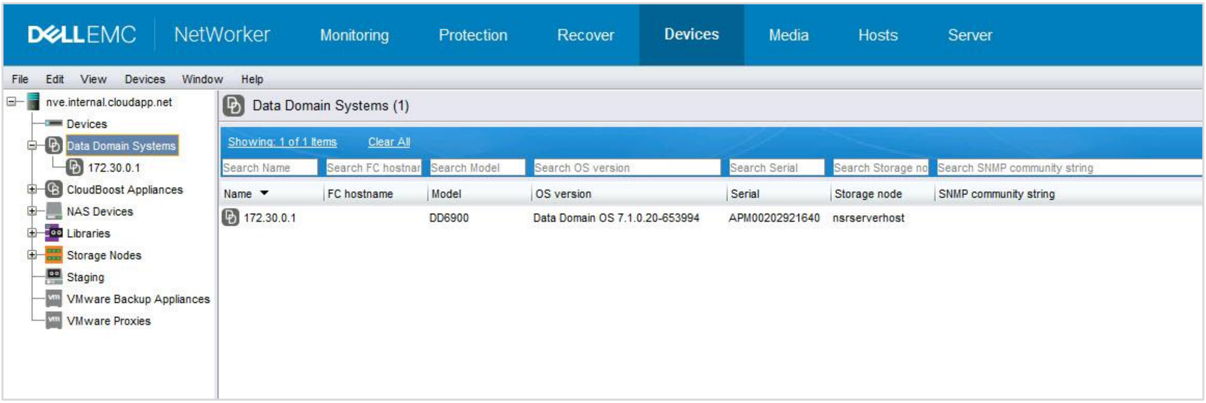
- AWS Direct Connect
- Azure ExpressRoute
- Google Cloud Platform Dedicated Interconnect
- Oracle FastConnect

4 Example scenarios

4.1 DD series appliance at Faction as the primary backup target for cloud workloads

In this example, NetWorker Virtual Edition (NVE) is used to back up and restore Azure workloads. A DD series appliance at a Faction data center (DC) is used as the primary backup target.

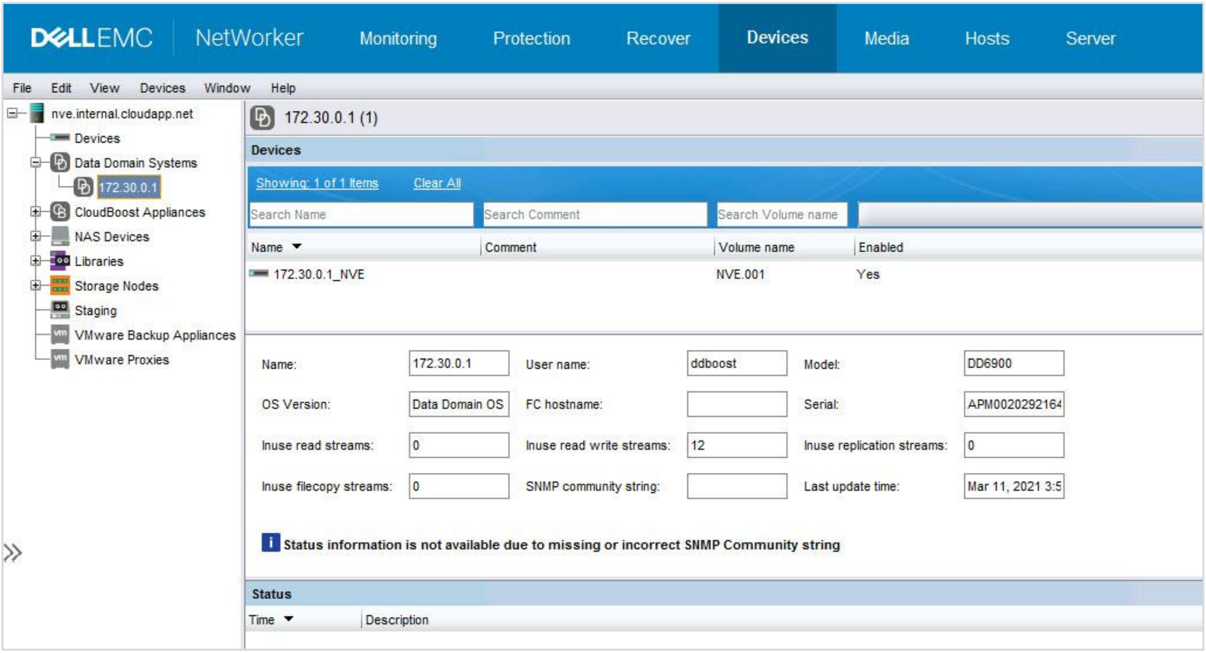
1. Integrate a DD series appliance at a Faction DC with NetWorker using a ddboost user.



Data Domain Systems (1)

Name	FC hostname	Model	OS version	Serial	Storage node	SNMP community string
172.30.0.1		DD6900	Data Domain OS 7.1.0.20-653994	APM00202921640	nsrserverhost	

2. Create and configure a new device with the DD series appliance at the Faction DC.



172.30.0.1 (1)

Devices

Name	Comment	Volume name	Enabled
172.30.0.1_NVE		NVE.001	Yes

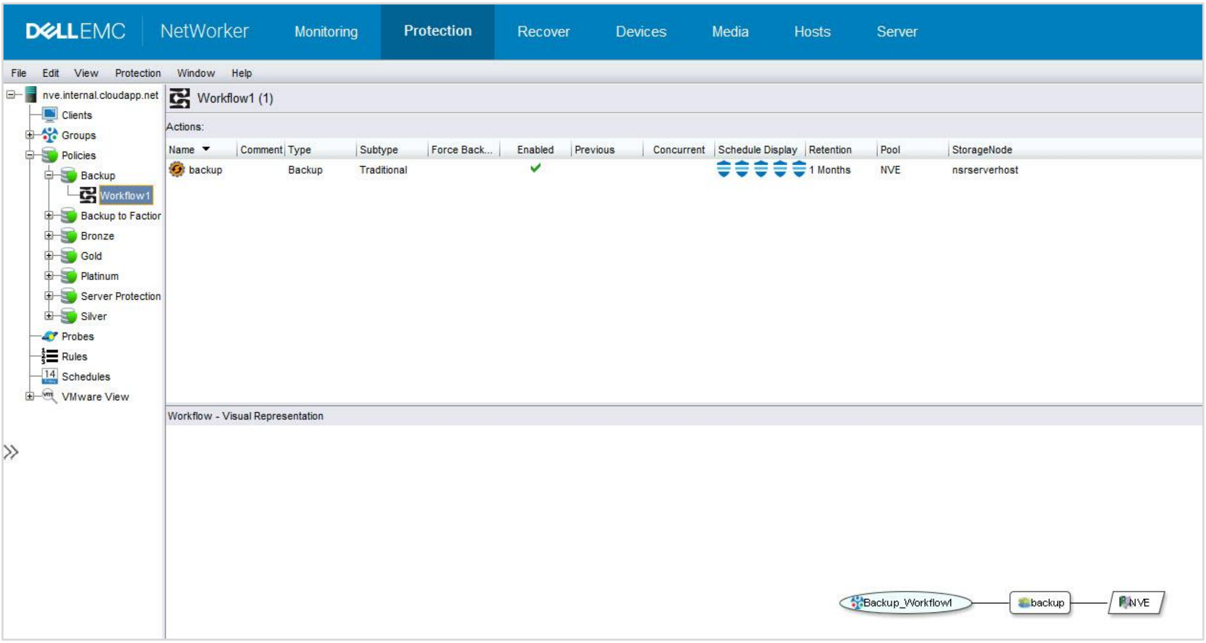
Name:	172.30.0.1	User name:	ddboost	Model:	DD6900
OS Version:	Data Domain OS	FC hostname:		Serial:	APM0020292164
Inuse read streams:	0	Inuse read write streams:	12	Inuse replication streams:	0
Inuse filecopy streams:	0	SNMP community string:		Last update time:	Mar 11, 2021 3:5

Status information is not available due to missing or incorrect SNMP Community string

Status

Time	Description

3. Configure a backup workflow with the created backup pool, and initiate the policy workflow.



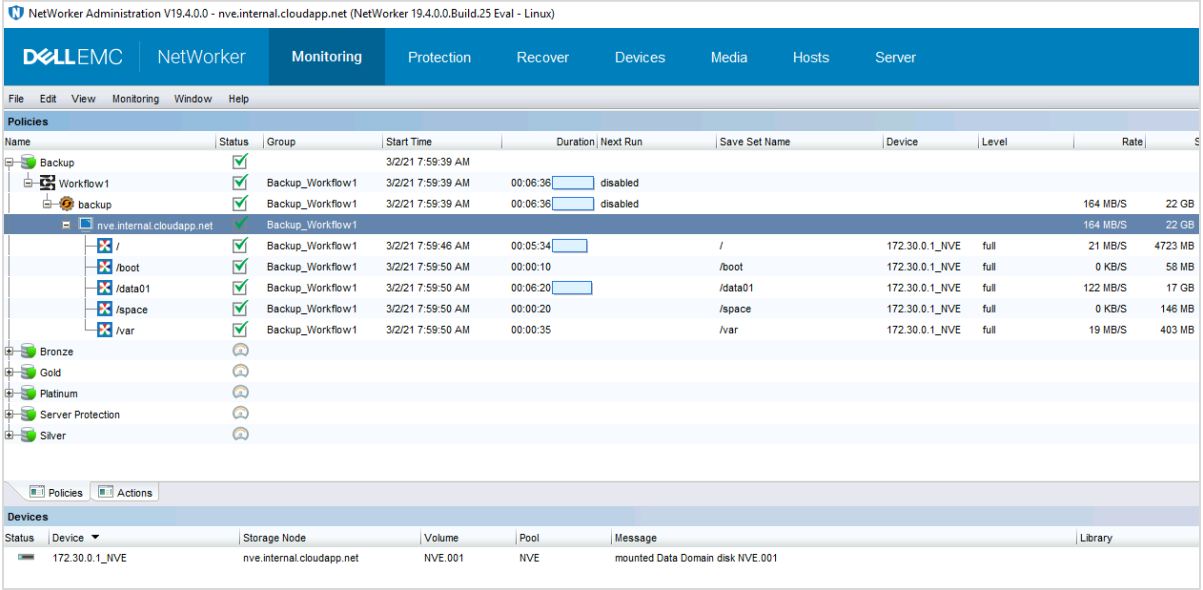
Workflow1 (1)

Actions:

Name	Comment	Type	Subtype	Force Back...	Enabled	Previous	Concurrent	Schedule Display	Retention	Pool	StorageNode
backup		Backup	Traditional		✓				1 Months	NVE	nsrserverhost

Workflow - Visual Representation

4. An Azure workload backup completes successfully using the DD series appliance at the Faction DC as the primary backup target.



NetWorker Administration V19.4.0.0 - nve.internal.cloudapp.net (NetWorker 19.4.0.0.Build.25 Eval - Linux)

Policies

Name	Status	Group	Start Time	Duration	Next Run	Save Set Name	Device	Level	Rate	S
Backup	✓		3/2/21 7:59:39 AM							
Workflow1	✓	Backup_Workflow1	3/2/21 7:59:39 AM	00:06:36	disabled					
backup	✓	Backup_Workflow1	3/2/21 7:59:39 AM	00:06:36	disabled				164 MB/S	22 GB
nve.internal.cloudapp.net	✓	Backup_Workflow1							164 MB/S	22 GB
/	✓	Backup_Workflow1	3/2/21 7:59:46 AM	00:05:34		/	172.30.0.1_NVE	full	21 MB/S	4723 MB
/boot	✓	Backup_Workflow1	3/2/21 7:59:50 AM	00:00:10		/boot	172.30.0.1_NVE	full	0 KB/S	58 MB
/data01	✓	Backup_Workflow1	3/2/21 7:59:50 AM	00:06:20		/data01	172.30.0.1_NVE	full	122 MB/S	17 GB
/space	✓	Backup_Workflow1	3/2/21 7:59:50 AM	00:00:20		/space	172.30.0.1_NVE	full	0 KB/S	146 MB
/var	✓	Backup_Workflow1	3/2/21 7:59:50 AM	00:00:35		/var	172.30.0.1_NVE	full	19 MB/S	403 MB
Bronze										
Gold										
Platinum										
Server Protection										
Silver										

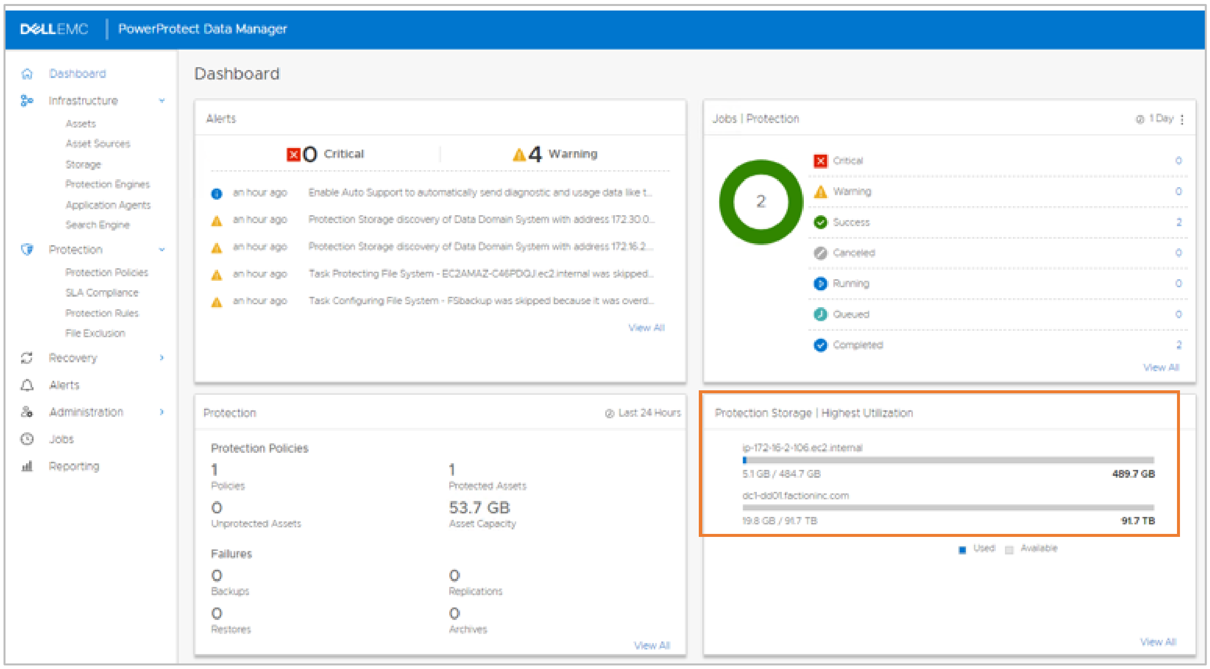
Devices

Status	Device	Storage Node	Volume	Pool	Message	Library
	172.30.0.1_NVE	nve.internal.cloudapp.net	NVE.001	NVE	mounted Data Domain disk NVE.001	

4.2 DD series appliance at Faction as the replication backup target for DDVE deployed on public cloud

In this example, a PowerProtect Data Manager deployed in AWS is used to back up and replicate the AWS workloads. DDVE is deployed in AWS as the primary backup target, and the DD series appliance at the Faction DC is the replication target.

1. Deploy DDVE in AWS, and add a DD series appliance at the Faction DC as Protection Storage in PowerProtect Data Manager.



Dashboard

Alerts

0 Critical | 4 Warning

an hour ago	Enable Auto Support to automatically send diagnostic and usage data like t...
an hour ago	Protection Storage discovery of Data Domain System with address 172.30.0...
an hour ago	Protection Storage discovery of Data Domain System with address 172.16.2...
an hour ago	Task Protecting File System - EC2AMAZ-C46PDQJ.ec2.internal was skipped...
an hour ago	Task Configuring File System - FSbackup was skipped because it was overd...

View All

Jobs | Protection — 1 Day

2

Critical	0
Warning	0
Success	2
Canceled	0
Running	0
Queued	0
Completed	2

View All

Protection — Last 24 Hours

Protection Policies

1 Policies — 1 Protected Assets

0 Unprotected Assets — 53.7 GB Asset Capacity

Failures

0 Backups — 0 Replications

0 Restores — 0 Archives

View All

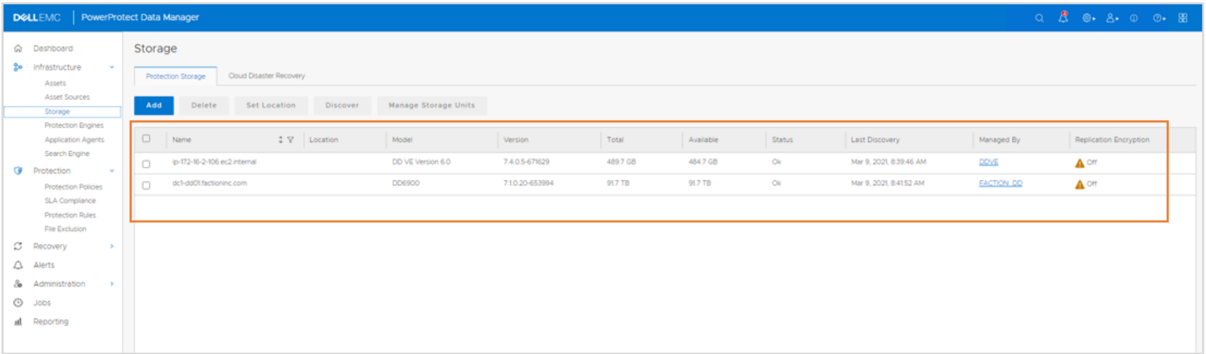
Protection Storage | Highest Utilization

ip-172-16-2-106.ec2.internal
5.1 GB / 484.7 GB — 489.7 GB

dc1-dd01.factioninc.com
19.8 GB / 91.7 TB — 91.7 TB

■ Used ▨ Available

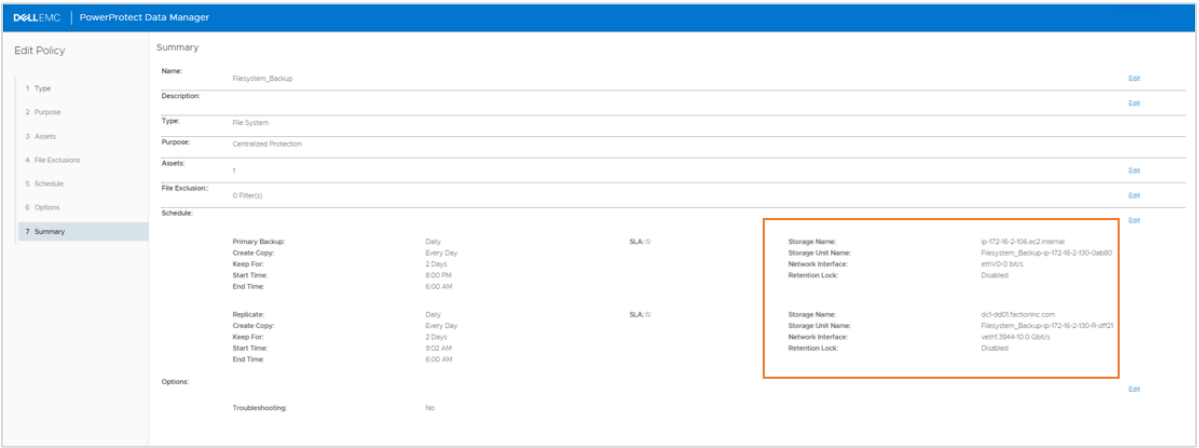
View All



Storage

□	Name	Location	Model	Version	Total	Available	Status	Last Discovery	Managed By	Replication Encryption
□	ip-172-16-2-106.ec2.internal		DD VE Version 6.0	7.4.0.5-671629	489.7 GB	484.7 GB	Ok	Mar 9, 2021, 8:39:46 AM	DDVE	Off
□	dc1-dd01.factioninc.com		DD6900	7.1.0.20-653994	91.7 TB	91.7 TB	Ok	Mar 9, 2021, 8:41:52 AM	FACTION_DD	Off

2. Create a protection policy, select the DDVE deployed in AWS as the primary backup target, and select the DD series appliance at the Faction DC as the replication target.



Name:	Filesystem_Backup
Description:	
Type:	File System
Purpose:	Centralized Protection
Assets:	1
File Exclusion::	0 Filter(s)

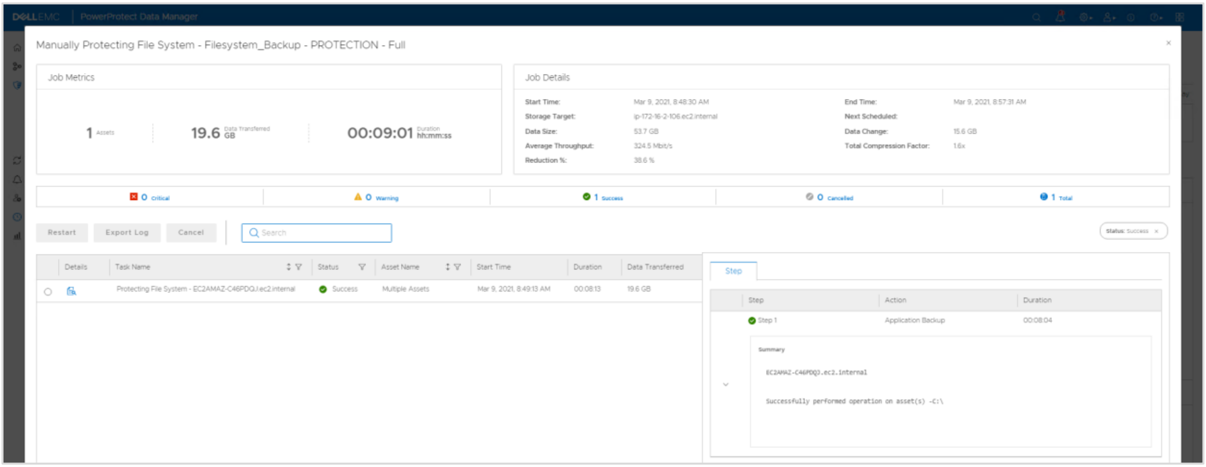
Schedule:

Primary Backup:	Daily	SLA:	Storage Name:	ip-172-16-2-106.ec2.internal
Create Copy:	Every Day		Storage Unit Name:	Filesystem_Backup-ip-172-16-2-130-0ab80
Keep For:	2 Days		Network Interface:	ethV0-0 bit/s
Start Time:	8:00 PM		Retention Lock:	Disabled
End Time:	6:00 AM			
Replicate:	Daily	SLA:	Storage Name:	dc1-dd01.factioninc.com
Create Copy:	Every Day		Storage Unit Name:	Filesystem_Backup-ip-172-16-2-130-R-dff21
Keep For:	2 Days		Network Interface:	veth1.3944-10.0 Gbit/s
Start Time:	9:02 AM		Retention Lock:	Disabled
End Time:	6:00 AM			

Options:

Troubleshooting: No

3. The policy runs, and the backup and replication jobs complete successfully.



Manually Protecting File System - Filesystem_Backup - PROTECTION - Full

Job Metrics

1 Assets | 19.6 GB Data Transferred | 00:09:01 Duration hh:mm:ss

Job Details

Start Time:	Mar 9, 2021, 8:48:30 AM	End Time:	Mar 9, 2021, 8:57:31 AM
Storage Target:	ip-172-16-2-106.ec2.internal	Next Scheduled:	
Data Size:	53.7 GB	Data Change:	15.6 GB
Average Throughput:	324.5 Mbit/s	Total Compression Factor:	1.6x
Reduction %:	38.6 %		

☒ 0 Critical | ⚠ 0 Warning | ✓ 1 Success | 0 Cancelled | 1 Total

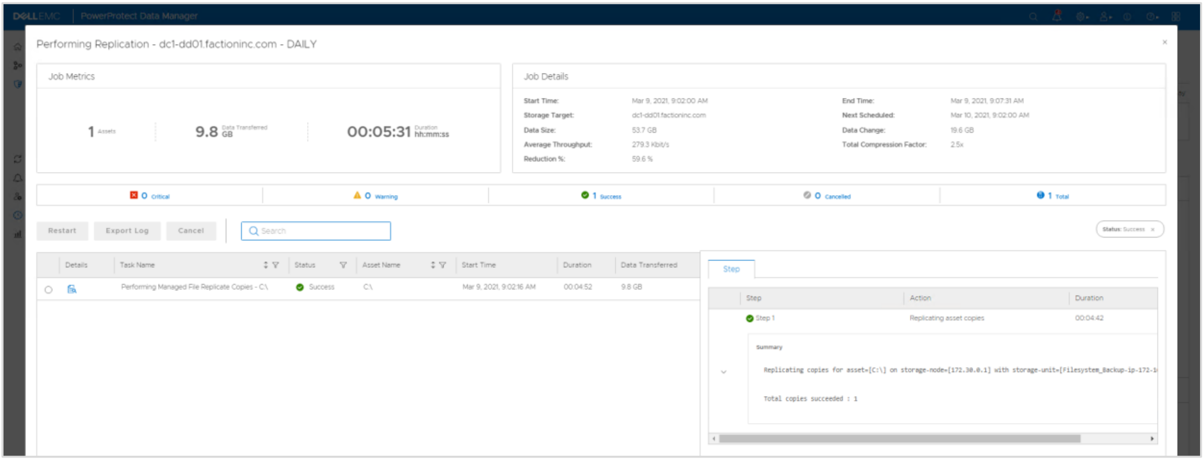
Status: Success ×

Details	Task Name	Status	Asset Name	Start Time	Duration	Data Transferred
	Protecting File System - EC2AMAZ-C46PDQJ.ec2.internal	Success	Multiple Assets	Mar 9, 2021, 8:49:13 AM	00:08:13	19.6 GB

Step	Action	Duration
Step 1	Application Backup	00:08:04

Summary

```
EC2AMAZ-C46PDQJ.ec2.internal

Successfully performed operation on asset(s) -C:\
```



Performing Replication - dc1-dd01.factioninc.com - DAILY

Job Metrics

1 Assets | 9.8 GB Data Transferred | 00:05:31 Duration hh:mm:ss

Job Details

Start Time:	Mar 9, 2021, 9:02:00 AM	End Time:	Mar 9, 2021, 9:07:31 AM
Storage Target:	dc1-dd01.factioninc.com	Next Scheduled:	Mar 10, 2021, 9:02:00 AM
Data Size:	53.7 GB	Data Change:	19.6 GB
Average Throughput:	279.3 Kbit/s	Total Compression Factor:	2.5x
Reduction %:	59.6 %		

☒ 0 Critical | ⚠ 0 Warning | ✓ 1 Success | 0 Cancelled | 1 Total

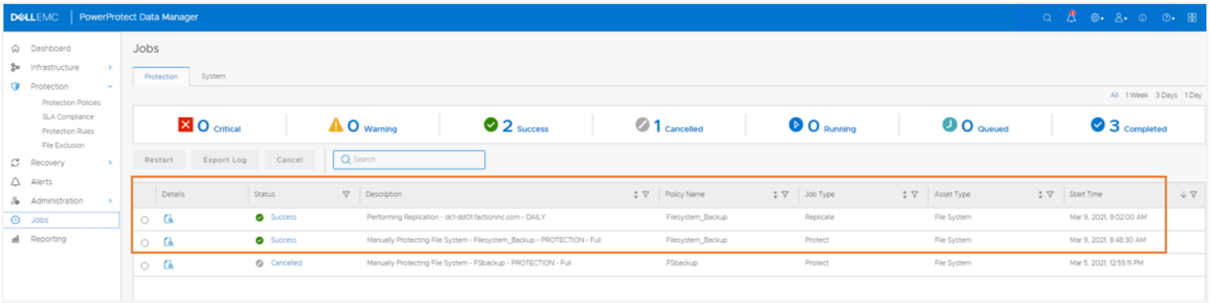
Status: Success ×

Details	Task Name	Status	Asset Name	Start Time	Duration	Data Transferred
	Performing Managed File Replicate Copies - C:\	Success	C:\	Mar 9, 2021, 9:02:16 AM	00:04:52	9.8 GB

Step	Action	Duration
Step 1	Replicating asset copies	00:04:42

Summary

```
Replicating copies for asset=[C:\] on storage-node=[172.30.0.1] with storage-unit=[Filesystem_Backup-ip-172-1

Total copies succeeded : 1
```

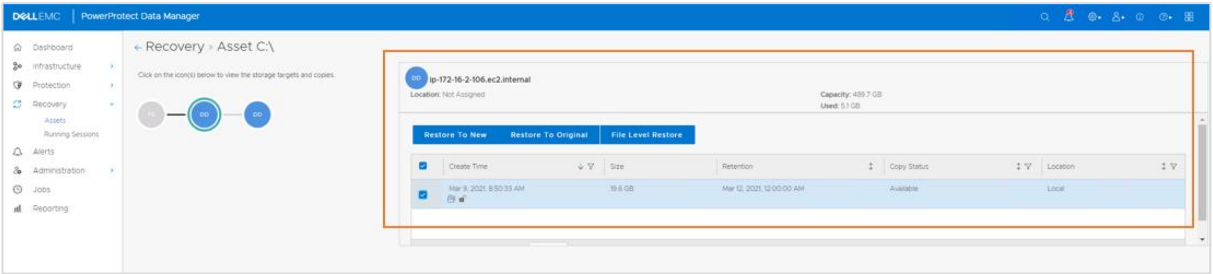


Jobs

0 Critical | 0 Warning | 2 Success | 1 Cancelled | 0 Running | 0 Queued | 3 Completed

Details	Status	Description	Policy Name	Job Type	Asset Type	Start Time
○	Success	Performing Replication - dc1-dd01.factioninc.com - DAILY	Filesystem_Backup	Replicate	File System	Mar 9, 2021, 9:02:00 AM
○	Success	Manually Protecting File System - Filesystem_Backup - PROTECTION - Full	Filesystem_Backup	Protect	File System	Mar 9, 2021, 8:48:30 AM
○	Cancelled	Manually Protecting File System - FSbackup - PROTECTION - Full	FSbackup	Protect	File System	Mar 5, 2021, 12:55:11 PM

4. The primary backup copy is available on the DDVE at AWS.



← Recovery › Asset C:\

Click on the icon(s) below to view the storage targets and copies.

ip-172-16-2-106.ec2.internal

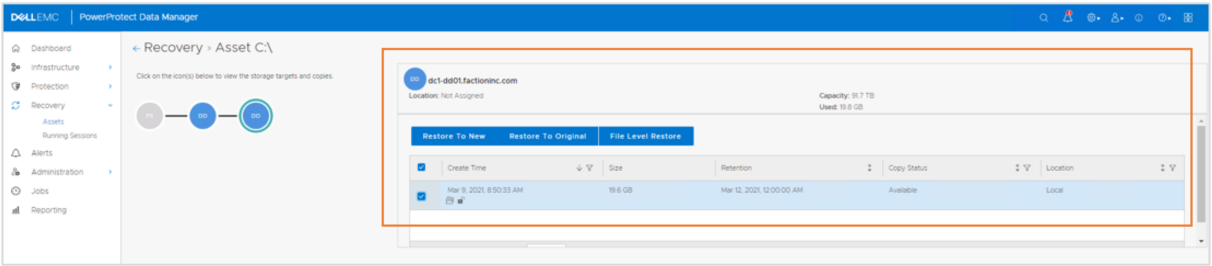
Location: Not Assigned

Capacity: 489.7 GB

Used: 5.1 GB

☑	Create Time	Size	Retention	Copy Status	Location
☑	Mar 9, 2021, 8:50:33 AM	19.6 GB	Mar 12, 2021, 12:00:00 AM	Available	Local

5. The replicated backup copy is available on the DD series appliance at the Faction DC.



← Recovery › Asset C:\

Click on the icon(s) below to view the storage targets and copies.

dc1-dd01.factioninc.com

Location: Not Assigned

Capacity: 91.7 TB

Used: 19.8 GB

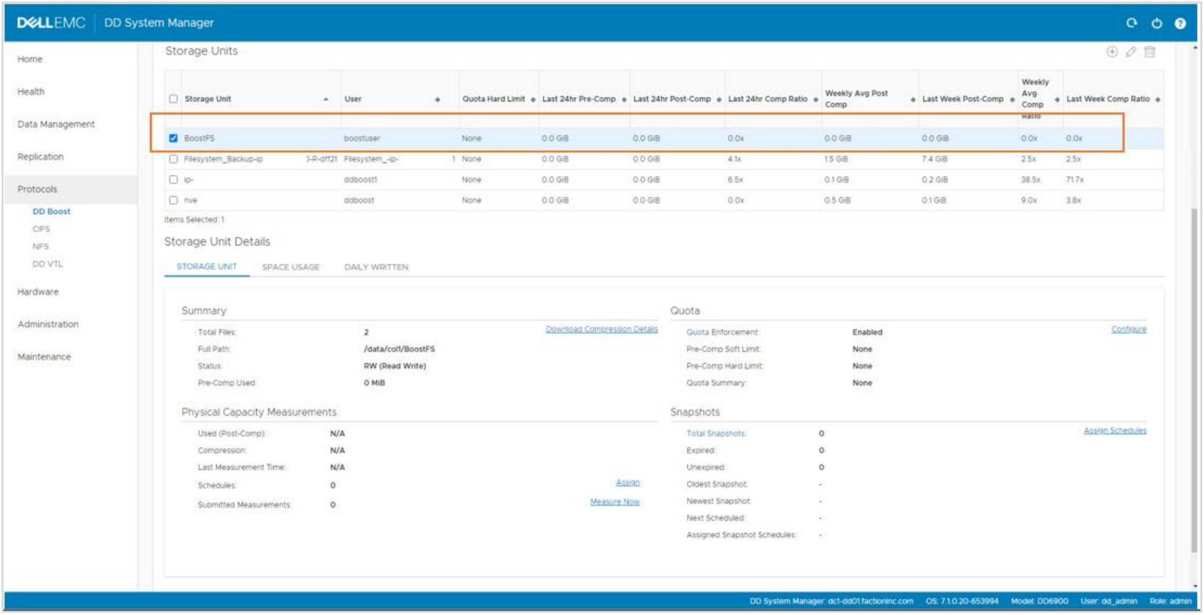
☑	Create Time	Size	Retention	Copy Status	Location
☑	Mar 9, 2021, 8:50:33 AM	19.6 GB	Mar 12, 2021, 12:00:00 AM	Available	Local

4.3 Mount Faction DD series storage unit on VMs running in multiple cloud environments using BoostFS

In this example, a Storage Unit is created on the DD series appliance at the Faction DC, and it is mounted simultaneously on AWS and Azure virtual machines using the BoostFS plug-in.

1. As a prerequisite, install the BoostFS plug-in, and configure the lockbox on the virtual machines.

2. Create a Storage Unit on the DD series appliance at the Faction DC.



Storage Units

□	Storage Unit	User	Quota Hard Limit	Last 24hr Pre-Comp	Last 24hr Post-Comp	Last 24hr Comp Ratio	Weekly Avg Post Comp	Last Week Post-Comp	Weekly Avg Comp Ratio	Last Week Comp Ratio
☑	BoostFS	boostuser	None	0.0 GiB	0.0 GiB	0.0x	0.0 GiB	0.0 GiB	0.0x	0.0x
□	Filesystem_Backup-ip)-R-dff21	Filesystem_-ip- 1	None	0.0 GiB	0.0 GiB	4.1x	1.5 GiB	7.4 GiB	2.5x	2.5x
□	ip-	ddboost1	None	0.0 GiB	0.0 GiB	6.5x	0.1 GiB	0.2 GiB	38.5x	71.7x
□	nve	ddboost	None	0.0 GiB	0.0 GiB	0.0x	0.5 GiB	0.1 GiB	9.0x	3.8x

Items Selected: 1

Storage Unit Details

STORAGE UNIT | SPACE USAGE | DAILY WRITTEN

Summary

Download Compression Details

Total Files:	2
Full Path:	/data/col1/BoostFS
Status:	RW (Read Write)
Pre-Comp Used:	0 MiB

Quota

Configure

Quota Enforcement:	Enabled
Pre-Comp Soft Limit:	None
Pre-Comp Hard Limit:	None
Quota Summary:	None

Physical Capacity Measurements

Used (Post-Comp):	N/A	
Compression:	N/A	
Last Measurement Time:	N/A	
Schedules:	0	Assign
Submitted Measurements:	0	Measure Now

Snapshots

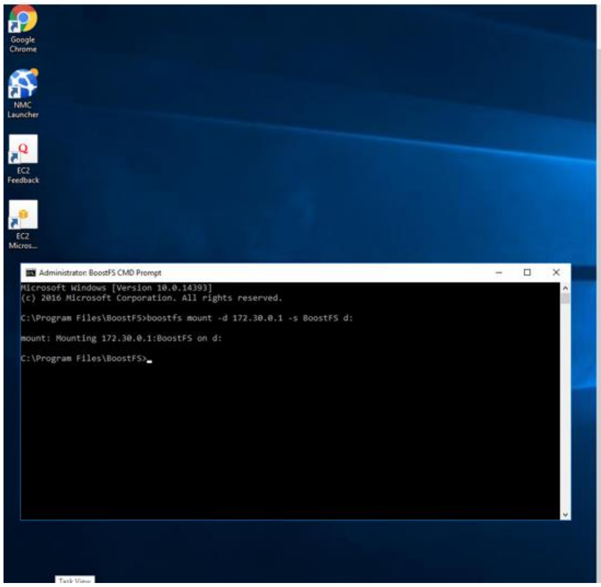
Assign Schedules

Total Snapshots:	0
Expired:	0
Unexpired:	0
Oldest Snapshot:	-
Newest Snapshot:	-
Next Scheduled:	-
Assigned Snapshot Schedules:	-

DD System Manager: dc1-dd01.factioninc.com OS: 7.1.0.20-653994 Model: DD6900 User: dd_admin Role: admin

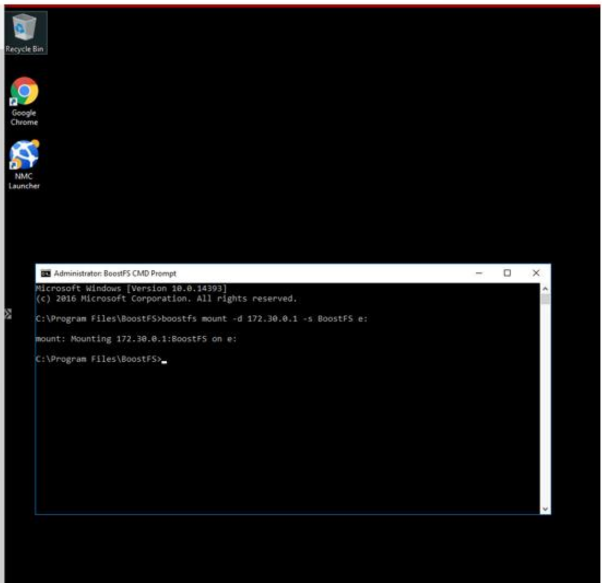
3. Using the boostfs mount command, mount the DD series Storage Unit on the virtual machines.

AWS



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS d:

mount: Mounting 172.30.0.1:BoostFS on d:

C:\Program Files\BoostFS>_
```

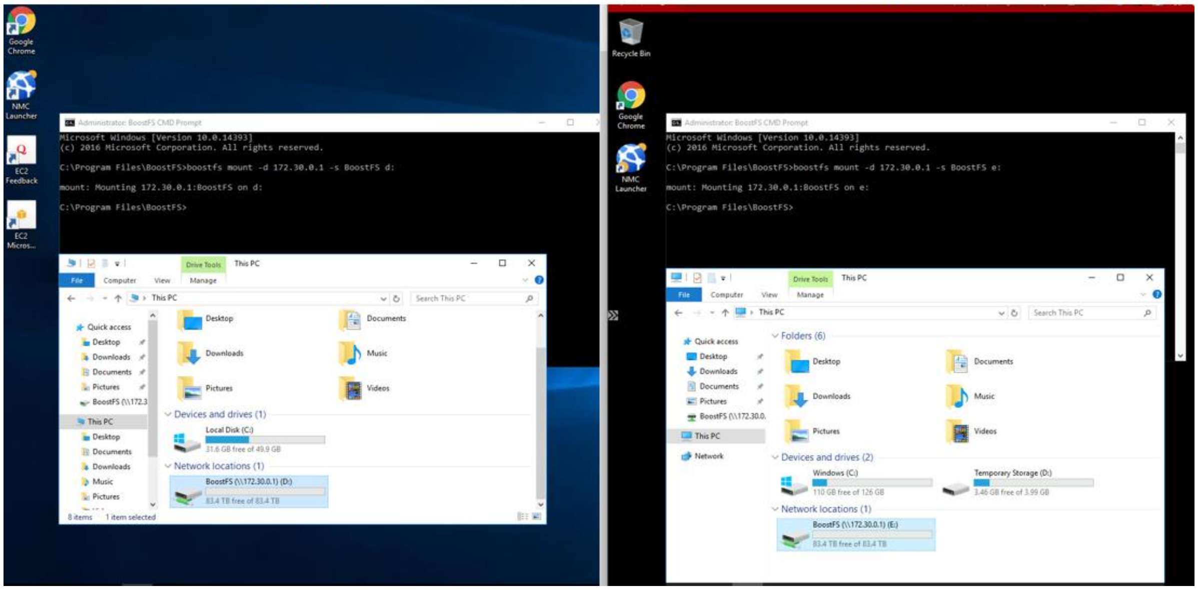
Azure



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS e:

mount: Mounting 172.30.0.1:BoostFS on e:

C:\Program Files\BoostFS>_
```

4. The Storage Unit created on the DD series appliance at the Faction DC is successfully mounted on the AWS and Azure VMs.

AWS	Azure



AWS:

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS d:

mount: Mounting 172.30.0.1:BoostFS on d:

C:\Program Files\BoostFS>
```

Local Disk (C:) 31.6 GB free of 49.9 GB

BoostFS (\\172.30.0.1) (D:) 83.4 TB free of 83.4 TB

Azure:

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS e:

mount: Mounting 172.30.0.1:BoostFS on e:

C:\Program Files\BoostFS>
```

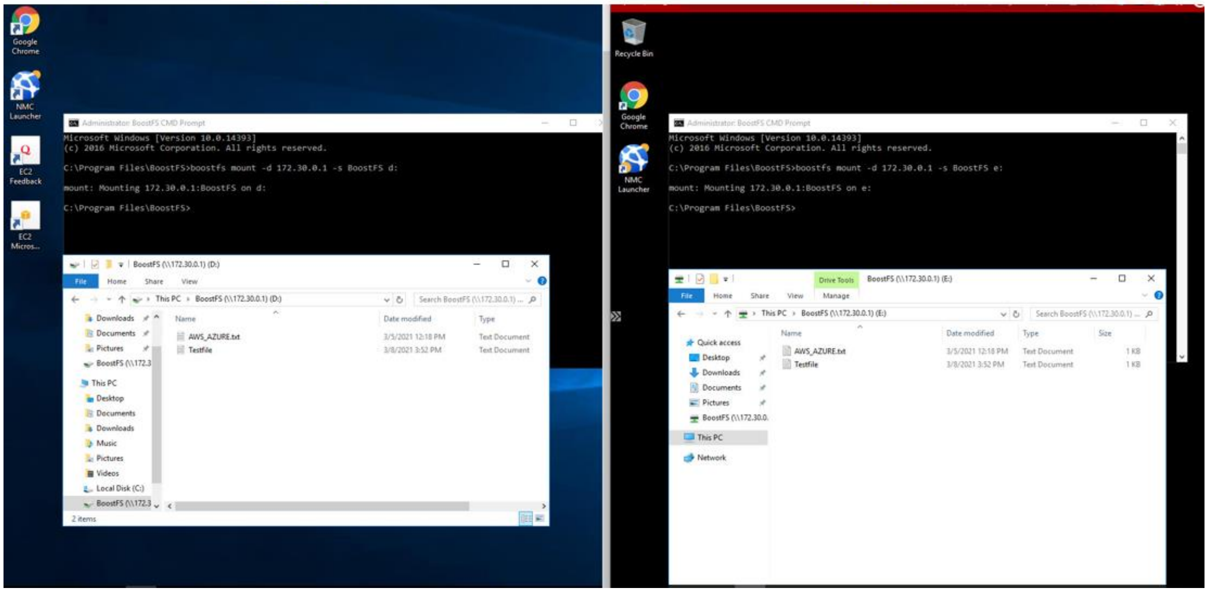
Windows (C:) 110 GB free of 126 GB

Temporary Storage (D:) 3.46 GB free of 3.99 GB

BoostFS (\\172.30.0.1) (E:) 83.4 TB free of 83.4 TB

5. The same set of files is available on both VMs using the BoostFS plug-in.

AWS	Azure



AWS:

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS d:

mount: Mounting 172.30.0.1:BoostFS on d:

C:\Program Files\BoostFS>
```

BoostFS (\\172.30.0.1) (D:)

Name	Date modified	Type
AWS_AZURE.txt	3/5/2021 12:18 PM	Text Document
Testfile	3/8/2021 3:52 PM	Text Document

Azure:

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs mount -d 172.30.0.1 -s BoostFS e:

mount: Mounting 172.30.0.1:BoostFS on e:

C:\Program Files\BoostFS>
```

BoostFS (\\172.30.0.1) (E:)

Name	Date modified	Type	Size
AWS_AZURE.txt	3/5/2021 12:18 PM	Text Document	1 KB
Testfile	3/8/2021 3:52 PM	Text Document	1 KB

5 Onboarding process and support

5.1 Implementation

The Service Order Form (SOF) or the Statement of Work (SOW) contains the detailed implementation process. Implementation includes the following high-level steps:

1. Solution design and proposal
2. Service order and MSA are signed
3. Introduction and project kickoff meeting
4. Solution design audit and project timeline creation
5. Ready-for-implementation signoff, and install timeline is committed
6. Solution build begins
7. Quality assurance testing and validation
8. Client access provided
9. User acceptance testing (UAT)
10. Close project: Handoff meeting with 24x7 Faction Support team

5.2 Support

The Faction NOC provides first-call support for client circuit issues. If Faction staff cannot resolve the issue, it may be escalated to the vendor for further support and troubleshooting. While Faction remains engaged, clients should be prepared and have resources available to work directly with the vendors to resolve issues.

Description	**Client**	**Faction**
Client premise connectivity (Layer 1 beyond the carrier demark)	Primary	
Client premise logical connectivity	Primary	Secondary
Faction premise connectivity		Primary
Faction premise logical connectivity	Primary	Secondary
First-call support		Primary
Middle-mile troubleshooting	Primary	Secondary
Maintenance notification (pass-through from provider only)		Primary

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage and data protection technical documents and videos provide expertise to ensure customer success with Dell EMC storage and data protection products.

A.1 Related resources

Access to the following documents may require login credentials.

- Multi-Cloud Data Services for Dell EMC PowerProtect
- Data Protection Multi-Cloud Innovations
- Multi-Cloud Data Services for Dell EMC PowerProtect (solution brief)
- Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect
- Multi-cloud Data Protection
- Data Protection Solution powered by Cloud Control Volumes (CCV)
- Faction CCV
- Dell EMC PowerProtect DD Series Appliances
- Dell EMC PowerProtect DD Series Appliances (spec sheet)
- Dell EMC PowerProtect DD Series Appliances (data sheet)
- Dell EMC Data Protection Suite
- Dell EMC Cloud Disaster Recovery
- Dell EMC PowerProtect Cyber Recovery Solution