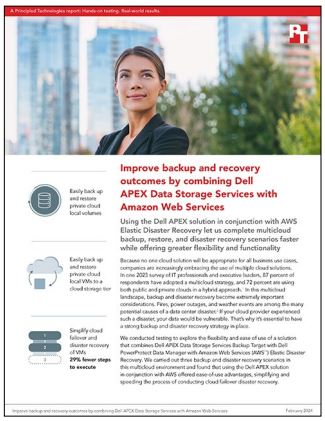

The science behind the report:

Improve backup and recovery outcomes by combining Dell APEX Data Storage Services with Amazon Web Services

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Improve backup and recovery outcomes by combining Dell APEX Data Storage Services with Amazon Web Services.

We concluded our hands-on testing on January 5, 2024. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on October 2, 2023 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Results of our testing.

	AWS and Dell	AWS
Steps to execute disaster recovery scenario	17	24

System configuration information

Table 2: Detailed information on the VxRail V670F we tested.

System configuration information	VxRail V670F
BIOS name and version	
Operating system name and version/build number	VMware® ESXi™, 8.0.1 - 21813344
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Platinum 8358
Core count (per processor)	32
Core frequency (GHz)	2.60
Stepping	64
Memory module(s)	
Total memory in system (GB)	512
Local storage (type A)	
Number of drives	2
Drive size (GB)	480
Drive information	BOSS
Number of drives	1
Drive size (TB)	1.46
Drive information (speed, interface, type)	NVMe®
Number of drives	6
Drive size (TB)	3.49
Drive information (speed, interface, type)	SATA
Network adapter	
Vendor and model	Broadcom® NetXtreme E-Series Advanced Dual-port 25Gb SFP28 Ethernet OCP 3.0 Adapter
Number and type of ports	2 x 25GbE
Vendor and model	Broadcom BCM57414 NetXtreme-E 10Gb/25Gb RDMA Ethernet Controller
Number and type of ports	2 x 25GbE

Table 3: Detailed information on the PowerStore 5000T we tested.

System configuration information	PowerStore 5000T
Number of storage controllers	2
OS version	3.5.0.1 Build 2083289
Number of Drives	4
Drive size (GB)	16.4
Drive information (speed, interface, type)	NVMe NVRAM
Number of drives	10
Drive size (TB)	14.7
Drive information	NVMe SSD

Table 4: Detailed information on the DD6900 we tested.

System configuration information	DD6900
OS version	7.7.5.20-1063368
Number of drives	45
Drive size (TB)	3.64
Drive information	HITACHI H0S726T4CLAR4000 SAS

How we tested

Testing overview

From our lab at PT, we connected to a VDI desktop. From the VDI desktop, we could access, verify, and control the lab environment, including VMware vCenter, VMs, PowerStore, DD, and the backup solution under test. For these efforts, we used either web-based GUI or SSH connections, or both.

In this study, we tested three scenarios:

1. We tested backing up local volume from Dell APEX Data Storage Services Block Storage (i.e., PowerStore) to a Dell APEX Data Storage Services Backup Target (i.e., DD appliance). We set up four block volumes to perform local backups. After the backups completed, we restored them back to the source storage array.
2. We tested local back up of four VMs to a Dell APEX Data Storage Services Backup Target (i.e., DD appliance). Then we enabled the Cloud tier feature of Dell PowerProtect Data Manager, configured the AWS account, and copied the backups to AWS via Data Manager Cloud tier. We then recalled the copies from AWS back to Dell PowerProtect Data Manager and restored them to on-prem vCenter.
3. We tested both the Cloud Disaster Recovery feature of Dell PowerProtect Data Manager and the Elastic Disaster Recovery feature of AWS. We simulated a disaster-recovery scenario with backup a VM to AWS, failover, then recovery back to on-prem vSphere. We found that the AWS EDR solution could restore VMs to local cloud, but must first failover VMs to AWS and then undergo an admin-involved failback process (boot to recovery ISO, transfer data from AWS). We captured and compared the number of steps required to fail back to on-prem using only AWS and the number of steps required when we integrated the Dell APEX Data Storage Services solution with AWS.

The following sections describe the steps we took to run the test cases.

Installing and configuring Dell PowerProtect Data Manager

1. Download a PowerProtect Data Manager .ova file from https://www.dell.com/support/home/en-us/product-support/product/enterprise-copy-data-management/drivers.
2. Log into the vCenter. From the Actions menu, select Deploy OVF Template.
3. On the Select an OVF template page, select Local File, and select the ova file you just downloaded. Click Next.
4. On the Select a name and folder page, specify the name for the appliance, and leave folder as default. Click Next.
5. On the Select a computer resource page, select the destination compute resource, and click Next.
6. On the Select storage page, select the datastore that will host the configuration and disk files. Click Next.
7. On the Select Networks page, select the network you will use for testing.
8. On the Customize template page, specify the network IP address, gateway, netmask, and DNS server. Click Next.
9. To start deployment, click Finish.
10. After the deployment completes, log into the PowerProtect Data Manager UI as admin.
11. On the left panel, click Infrastructure → Asset Sources.
12. On the Virtual Machine box, click Enable Source.
13. To add the vCenter Server, click Add.
14. Specify Name, FQDN/IP, and credentials for the vCenter, and click Save to add the vCenter to PowerProtect Data Manager.
15. On the left panel, click Infrastructure → Asset Sources.
16. On the Storage Arrays box, click Enable Source.
17. On the Storage Array tab, click Add.
18. Specify Name, FQDN/IP, port, and credentials for the PowerStore. For Asset Types, select Block Volume.
19. To add the PowerStore to PowerProtect Data Manager, click Save.
20. On the left panel, click Storage, and click Add.
21. On the Add Storage screen, select Data Domain System, and specify name, address, port, and credentials for the DD6900.
22. To add Data Domain to PowerProtect Data Manager, click Save.

Backing up a block volume in PowerProtect Data Manager

1. Log into the PowerProtect Data Manager UI as admin user.
2. On the left panel, select protection → Protection Policies, and click Add.
3. On the Type page, enter a name and description, select Block Volume as the type of system to back up, and click Next.
4. On the Purpose page, select Crash Consistent as the purpose of the new policy, and click Next.
5. On the Assets page, select one or more block volumes the new policy will protect, and click Next.
6. On the Objectives page, under Primary Backup, click Add. In the Add Primary Backup Dialog, fill out the Target and Schedules fields, and click Save.
7. On the Summary page, click Finish to create the new policy.
8. Select Protect → Protection Policies.
9. Select the protection policy you have just created.

10. Click Protect Now to manually start a backup job.
11. Select Job → Protection Jobs to monitor the progress of the backup job.
12. Select one volume from the list, and click Restore.
13. Select a copy from the Copy Selection screen, and click Next.
14. Select Restore to origin, and click Next.
15. To start the restore job, click Restore.

Restoring a block volume in PowerProtect Data Manager

1. Log into the PowerProtect Data Manager UI as admin user.
2. On the left panel, select Restore → Assets.
3. Click the Block Volume tab.
4. Select one volume from the list, and click Restore.
5. Select a copy from the Copy Selection screen, and click Next.
6. Select Restore to origin, and click Next.
7. To start the restore job, click Restore.

Backing up a virtual machine in the PowerProtect Data Manager Cloud Tier

1. Log into the PowerProtect Data Manager UI as admin user.
2. On the left panel, select protection → Protection Policies, and click Add
3. On the Type page, enter a name and description, select Virtual Machine as the type of system to back up, and click Next.
4. On the Purpose page, select Crash Consistent as the purpose of the new policy, and click Next.
5. On the Assets page, select one or more VMs to be protected by the new policy, and click Next.
6. On the Objectives page, under Primary Backup, click Add. On the Add Primary Backup dialog, fill out the Target and Schedules fields, and click Save.
7. Next to Primary Backup, click Cloud Tier.
8. Under the entry for Cloud Tier, click Add.
9. In the Add Cloud Tier Backup dialog, select the appropriate cloud unit from the Cloud Target list. Set Tier After to be 14 days or more, and click Save.
10. On the Options page, select the appropriate options, and click Next.
11. On the Summary page, click Finish to create the new policy.

Recalling and restoring a virtual machine from the PowerProtect Data Manager Cloud Tier

1. Log into the PowerProtect Data Manager UI as admin user.
2. On the left panel, select infrastructiure → Assets.
3. On the Assets page, select the VMs you want to recall from Cloud, and click View Copies.
4. Click the DD icon, select one available cloud copy from the list, and click Recall from Cloud.
5. In the Retain Until box, specify how long you want to keep the copy in the primary tier, and click OK to start the recall job.
6. When the Recall job is complete, select Restore → Assets from the PowerProtect Data Manager UI.
7. Select the VM to be restored, and click Restore.
8. Click Choose copy, and click the DD icon. Select the local copy that PowerProtect Data Manager has recalled from Cloud, and click OK.
9. Click Next.
10. In the Purpose page, select the appropriate purpose, and click Next.
11. In the Restore page, select the appropriate Restore Type, and click Next.
12. In the Options page, select the appropriate options, and click Next.
13. Select the appropriate Network for the restored VM, and click Next.
14. Review the Summary, and click Restore to start the restore job.

Deploying and configuring Cloud Disaster Recovery in PowerProtect Data Manager to back up and restore virtual machines

1. Log into the PowerProtect Data Manager UI as admin user.
2. On the left panel, select Protection → Protection Policies, and select a policy.
3. Click the Cloud DR link next to the Primary Backup. The Cloud DR option is available next to the Primary Backup.
4. Click Add. The Add CDR Backup dialog displays.
5. From the Cloud Target list, select the appropriate cloud target, and click Save to add the new cloud target.
6. Click Next, and select the appropriate options.
7. Click Next. The Summary page appears.

8. Review the summary, and click Finish. Wait until backup copies synchronize to AWS.
9. On the left panel of PowerProtect Data Manager UI, select Restore → Assets. The Restore page displays all the assets with copies.
10. In the Virtual Machines tab, select the checkbox next to the virtual machine you want to restore, and click View Copies.
11. Click the CDR tab, select the check box next to the VM copy you want to recover, and click Failover.
12. In the Network section on the cloud account, select the applicable virtual network, and click Next.
13. In the Security Groups section, select a security group to attach to the recovered instance, and click Next. The Summary page displays.
14. Click Start Failover.
15. Select Infrastructure → Storage → Cloud Disaster Recovery.
16. In the Cloud Disaster Recovery Server pane, the public address of the Cloud DR Server hostname appears. To open the Cloud DR Server UI in a new tab, click the server hostname link.
17. From the Cloud DR Server UI, select Recovery → DR Activities, select a running failover, and click Failback to start the failback process.

Deploying and configuring Elastic Disaster Recovery in AWS to backup and restore virtual machines

1. Connect to the source server via SSH.
2. Download the replication agent installer:

```
wget -O ./aws-replication-installer-init https://aws-elastic-disaster-recovery-<REGION>.s3.<REGION>.amazonaws.com/latest/linux/aws-replication-installer-init
```

3. Run the installer script:

```
chmod +x aws-replication-installer-init; sudo ./aws-replication-installer-init
```

4. When prompted, enter your AWS Region Name.
5. Enter your AWS Access Key ID.
6. Enter your AWS Secret Access Key.
7. The installer identifies volumes for replication. It displays the identified disks and prompt you to choose the disks you want to replicate.
8. The installer downloads and installs the replication agent on the source server. Wait until the source server is synchronized to AWS and in Ready status.
9. Select the source server, click the Initiate recovery job menu, and select Initiate recovery.
10. Select a point in time to recover, and click Initiate recovery. Wait until the recovery job completes successfully.
11. Download the failback client iso file from https://aws-elastic-disaster-recovery- {REGION}.s3.{REGION}.amazonaws.com/latest/failback_livecd/aws-failbacklivecd-64bit.iso
12. Upload the iso file to a datastore in the vCenter.
13. Create a new VM in the vCenter, and make sure that the VM has an equal or greater number of volumes as the recovery instance and each volume size is equal to or larger than the ones on the recovery instance.
14. Attach the iso to the new VM, and power it on.
15. When prompted, enter your AWS region Name.
16. Enter your AWS access key ID.
17. Enter your AWS secret access key.
18. When prompted with volume mapping, type `Y` to accept the mapping between the recovery instance and the failback client.
19. The client then installs replication software on the source server and initiates replication between the recovery instance and the source server.
20. Log into AWS EDR console.
21. Click Recovery instances, and select the instance to continue the failback process.
22. Click the Failback settings tab, and edit Network bandwidth throttling and Use private IP settings.
23. To save the settings, click Save.
24. To start the failback, click Failback.

Read the report at https://facts.pt/iTWLsl9

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®