

The science behind the report:

# Save time completing backups and restores with Dell PowerProtect Data Manager Appliance

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 [Save time completing backups and restores with Dell PowerProtect Data Manager Appliance](#).

We concluded our hands-on testing on October 31, 2022. 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 31, 2022 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: Time, in minutes, it took to deployment the backup and recovery solutions.

Task (minutes)	Dell™ PowerProtect Data Manager Appliance	Vendor V	Vendor W	Vendor X	Vendor Y
Time to deploy	15	33	24	15	34

Table 2: Summary of the time (in hh:mm:ss) it took to complete backup and restore tasks using the Dell Technologies and Vendor X solutions. Source: Principled Technologies.

Task (hh:mm:ss)	Dell PowerProtect Data Manager Appliance with Transparent Snapshots	Vendor X solution with VADP and NBD
Time to back up 500 VMs	9:32:07	17:48:34
Time to complete ten days of incremental backups	7:35:10	24:30:35
Time to restore one large VM	0:12:07	0:21:51
Time to restore five large VMs	0:30:57	0:44:20

Table 3: Minimum, maximum, and average disk activity, in throughput (IOPS) and latency (ms), of each solution while backing up a single VM running a workload. Higher is better for throughput; lower is better for latency. Source: Principled Technologies.

	Dell PowerProtect Data Manager Appliance with Transparent Snapshots	Vendor X solution with VADP and NBD
Latency (ms)		
Minimum	0.332	0.425
Maximum	0.366	2.769
Average	0.346	1.791
Read IOPS		
Minimum	7,992.66	1,073.81
Maximum	8,800.85	6,884.75
Average	8,434.79	1,933.08
Write IOPS		
Minimum	2,664.30	357.58
Maximum	2,916.77	2,297.74
Average	2,813.61	645.66

### VM read and write IOPS

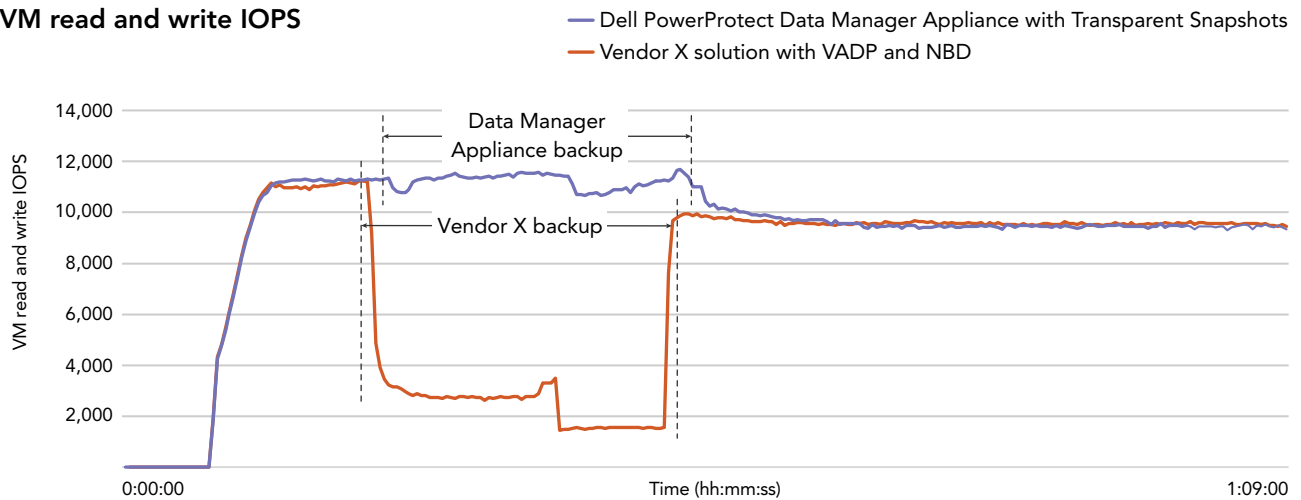


Figure 1: IOPS on the single VM for both solutions, before, during, and after a backup and while running a DISKSPD workload. Note: These backups did not run concurrently, but we plotted them on the same graph for ease of comparison. Higher is better. Source: Principled Technologies.

## System configuration information

Table 4: Detailed information on the Dell PowerProtect Data Manager Appliance we tested.

System component information	Dell PowerProtect Data Manager Appliance
Data protection software	Dell PowerProtect Data Manager
Model/version	DM5500/A00
Backup transport methods	Transparent Snapshot Data Mover with LWD
Backing storage	Dell Data Domain Virtual Edition
Storage capacity (TB)	95.3
PowerProtect Data Manager Appliance	
VMware ESXi™ server	7.0 Update 3-050 (Dell-EMC)
Processor vendor and model	Intel® Xeon® Gold 5218R
Core frequency (GHz)	2.10
Memory module(s)	
Total memory in system (GB)	384
PowerProtect Data Manager virtual machine	
vCPUs	14
RAM (GB)	32
OS	SUSE Linux® Enterprise Server 12 SP5 (x86_64) – Kernel 4.12.14-122.133-default
Disk	7

Table 5: Detailed information on the Vendor X solution we tested.

System component information	Vendor X solution
Capacity (TB)	96.4

## How we tested

From our lab at PT, we connected to Microsoft Windows VM jumpboxes running in a remote lab. From within those jumpboxes, we could access, verify, and control the lab environment, including multiple VMware vSphere™ clusters, VMs, and all storage and backup solutions under test. For these efforts, we used either a web-based GUI, SSH connections, or both.

For the solution deployment phase of our testing, we observed lab personnel performing the installations of each solution. The process for each solution followed the same three basic sets of steps: install the solution software, configure or customize each product for use in the lab's environment, and create and start an initial backup job of the same test VM. The lab personnel conducted the software installation phase via either a Windows 'setup' executable or through the deployment of an OVA. After the deployment completed and the solution presented the opportunity to log into its UI, lab personnel moved on to the next step, which included customizing the appliance for use in this particular lab environment. This customization included steps such as setting up user accounts, configuring networking addresses, and accepting any license agreements and other infrastructure requirements. Finally, lab personnel created policies that included a test VM and executed these policies to test the applications.

During all phases of the solution deployments, we kept running timers for each step of the process. We recorded the times to complete each phase. These timers suggest the overall effort required by a typical system administrator, and we used the times to compare solutions.

For our performance tests, we used the command line interface of a dedicated Ansible® server that provided orchestration. We executed scripts to simulate full and incremental backup solutions and could set the number of VMs. These scripts performed checks to validate that the solutions could back up and create VMs and write changes to those VMs. The scripts also verified that the VMs could access the backup solutions and storage APIs to execute backups on policy-defined groups of VMs and to collect responses from the solutions under test to capture execution and completion times. We logged all collected data for analysis.

For backups of VMs, we performed a full backup before executing incremental backups using similar scripted methods. For performance testing during the backup windows, we used PerfMon to capture disk performance metrics and isolate potential performance impacts a VM experienced. For VM recovery, we used a script that collected all data points automatically to ensure consistency across the data collections.

[Read the report here](#)

This project was commissioned by Dell Technologies.



**Facts matter.®**

Principled Technologies is a registered trademark of Principled Technologies, Inc. All other product names are the trademarks of their respective owners.

#### DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.