PowerProtect Data Manager 20.3

E-Lab Navigator Compatibility Guide

Report generated August 20, 2026

Contents

- DEPLOYMENT
- TARGETS
- LANGUAGE SUPPORT
- VMWARE
- MICROSOFT HYPER-V
- NUTANIX AHV
- GENERIC APPLICATION AGENT
- SQL
- EXCHANGE
- ORACLE
- DELL NATIVEEDGE
- SAP HANA
- STORAGE ARRAYS
- FILE SYSTEMS
- NAS
- CLOUD MARKETPLACES
- KUBERNETES
- EXTERNAL COMPONENTS & SERVICES

DEPLOYMENT

Web Browsers

PLATFORM	VERSION	COMMENTS
Google Chrome	151.0.x	All shipping versions supported
Microsoft Edge	151.0.x	All shipping versions supported

Deployments that use a vCenter OVA or a cloud machine image

PLATFORM	PLATFORM VERSION	COMMENTS
Operating System	SUSE Linux Enterprise Server (SLES) 15 SP4	Installed for both upgrade and new-installation scenarios.
VMware vCenter/ESXi	8.0, 8.0 U1, 8.0 U2b, 8.0 U3, 9.0, 9.1	Includes subsequent U2 and U3 patches.
Amazon Web Services (AWS)	AWS instance type: m5-2xlarge (8 vCPUs, 32 GB memory)	Subscribe via AWS Marketplace. Delivered via CloudFormation template.
Azure	Azure VM size: Standard D8s v5 (8 vCPUs, 32 GB memory)	Subscribe via Azure Marketplace. Delivered via Azure Resource Manager (ARM) template.
Google Cloud Platform (GCP)	GCP VM size: Customized (8 vCPUs, 32 GB memory)	Subscribe via GCP Marketplace. Delivered via Terraform.
VMware Cloud (VMC) on AWS	SDDC 1.22, 1.24, 1.26	Supported when deployed to a VMC on AWS vCenter or to the AWS native cloud.
Azure VMware Solutions (AVS)		For deployments in AVS, software is available from Dell Technologies (not the Marketplace). Subscribe via Azure Marketplace for DDVE deployment. Supported when deployed to an AVS vCenter or to the Azure native cloud
Google Cloud VMware Engine (GCVE)		For deployments in GCVE, software is available from Dell Technologies (not the Marketplace). Subscribe via GCP Marketplace for DDVE deployment. Supported when deployed to a GCVE vCenter or to the GCP native cloud.
Oracle Cloud VMware Solution (OCVS)		For deployments in OCVS, software is available from Dell Technologies (not the Marketplace).

NOTES:

• For PPDM Virtual Appliance (OVA) deployments, the underlying operating system utilizes an embedded Linux distribution which is licensed to Dell and is provided as an integrated component of the appliance. This embedded Linux is only authorized to be used to operate the Dell product and only the Dell product. Dell Technologies is responsible for PPDM OVA operating system maintenance, including security patches, kernel updates, and system hardening, which are delivered through supported PPDM software updates in accordance with the terms of the Dell standard support purchased with the product. Customers are responsible for applying Dell-provided PPDM updates and managing system access credentials in accordance with Dell support policies and terms.

• Supported datastores: vVols, vSAN, VMFS, and NFS.
• Includes VMware Cloud Foundation (VCF) versions that contain supported vCenter/vSphere versions.
• When deploying to a VMC on AWS, VMC on Dell, AVS, or GCVE vCenter, deploy PowerProtect Data Manager from the OVA and use the deployment wizard to select the corresponding configuration for this VMC environment.
• PowerProtect Data Manager supports only in-cloud VM image protection in the respective environments. Protection from in-cloud to on-premises environments, or from on-premises to in-cloud environments, is not supported.

Component resource requirements

COMPONENT	RESOURCE REQUIREMENTS
PowerProtect Data Manager	CPU—10 * 2 GHz, Memory—36 GB, Seven disks with the following capacities: Disk 1—100 GB, Disk 2—500 GB, Disks 3 and 4—10 GB each, Disks 5 through 7—5 GB each, 1 Gb VMXNET3 network interface card (NIC). 10 virtual sockets, 1 core for each socket.
PowerProtect Data Manager with Cloud DR	If you plan to use Cloud DR, the following requirements apply instead: CPU—14 * 2 GHz, Memory—40 GB, no changes to disk requirements 14 virtual sockets, 1 core for each socket.
External protection engine	Available sizes by protection workload: Kubernetes: Small. NAS: Small, Medium, Large. Default is Small. PowerMax: Medium Large. Default is Medium. Virtual machines: Small.
External protection engine (small)	CPU—4 * 2 GHz Memory—8 GB Two disks with the following capacities: Disk 1—59 GB Disk 2—100 GB SCSI controller—maximum of 4 1 Gb VMXNET3 NIC. 4 virtual sockets, 1 core for each socket.
External protection engine (medium)	CPU—8 * 2 GHz Memory—16 GB Two disks with the following capacities: Disk 1—59 GB Disk 2—200 GB SCSI controller—maximum of 4 1 Gb VMXNET3 NIC. 8 virtual sockets, 1 core for each socket.
External protection engine (large)	CPU—12 * 2 GHz Memory—24 GB Two disks with the following capacities: Disk 1—59 GB Disk 2—300 GB SCSI controller—maximum of 4 1 Gb VMXNET3 NIC. 12 virtual sockets, 1 core for each socket.
Search Engine node	CPU—4 * 2 GHz Memory—8 GB Four disks with the following capacities: Disks 1 through 3—50 GB each Disk 4—1 TB SCSI controller—maximum of 4 1 Gb VMXNET3 NIC. 4 virtual sockets, 1 core for each socket.
Reporting Engine	CPU—8 * 2 GHz Memory—16 GB Three disks with the following capacities: Disk 1—48 GB Disk 2—512 GB Disk 3—8 GB 1 Gb VMXNET3 NIC Operating system—SLES 15 SP4. 8 virtual sockets, 1 core for each socket.

NOTES:
• The PowerProtect Data Manager Administrator Guide provides more information about supported Internet Protocol versions and resource requirements.
• There are small, medium, and large protection engines. The specific protection workload determines both the default size and other sizes that can be optionally selected. Larger protection engines increase the performance of backup and restore operations but also require more resources. If the default size can be changed and you are unsure if you should change it, contact your Customer Support representative.
• Protected virtual machines must use the same protocol version as the protection engine. Virtual machines can use both IPv4 and IPv6, even though the protection engine cannot.
• The Search Engine node requirements apply to each node in the cluster.

Deployments that use an Install package

PLATFORM	PLATFORM VERSION	COMMENTS
Operating System	SLES 15 SP6, SP7, RHEL 9.6, 9.7, Rocky Linux 9.6	Installed for new-installation scenarios.

PLATFORM	PLATFORM VERSION	COMMENTS
Host Resources (Core, 1x Search, Reporting)	At least 22 CPU cores (10+4+8), At least 84 GB memory (44+16+24 GB), At least 2338 GB storage (680+1090+568 GB)	Deploy PowerProtect Data Manager Core, Search Engine, and Reporting Engine on the same host. This host can be a physical server such as Dell PowerEdge, or a VMware, Microsoft Hyper-V, Nutanix AHV, or KVM virtual machine.
Host Resources (Core, 2x Search, Reporting)	At least 26 CPU cores (10+8+8), At least 100 GB memory (44+32+24 GB), At least 3428 GB storage (680+2180+568 GB)	Deploy PowerProtect Data Manager Core, Search Engine, and Reporting Engine on the same host. This host can be a physical server such as Dell PowerEdge, or a VMware, Microsoft Hyper-V, Nutanix AHV, or KVM virtual machine.
Host Resources (Core, 3x Search, Reporting)	At least 30 CPU cores (10+12+8), At least 116 GB memory (44+48+24 GB), At least 4518 GB storage (680+3270+568 GB)	Deploy PowerProtect Data Manager Core, Search Engine, and Reporting Engine on the same host. This host can be a physical server such as Dell PowerEdge, or a VMware, Microsoft Hyper-V, Nutanix AHV, or KVM virtual machine.
Host Resources (Core, 4x Search, Reporting)	At least 34 CPU cores (10+16+8), At least 132 GB memory (44+64+24 GB), At least 5608 GB storage (680+4360+568 GB)	Deploy PowerProtect Data Manager Core, Search Engine, and Reporting Engine on the same host. This host can be a physical server such as Dell PowerEdge, or a VMware, Microsoft Hyper-V, Nutanix AHV, or KVM virtual machine.
Host Resources (Core, 5x Search, Reporting)	At least 38 CPU cores (10+20+8), At least 148 GB memory (44+80+24 GB), At least 6698 GB storage (680+5450+568 GB)	Deploy PowerProtect Data Manager Core, Search Engine, and Reporting Engine on the same host. This host can be a physical server such as Dell PowerEdge, or a VMware, Microsoft Hyper-V, Nutanix AHV, or KVM virtual machine.
Microsoft Hyper-V (Azure Local)		Excludes block volume protection engine for PowerMax.
Nutanix Acropolis Hypervisor (AHV)		Excludes block volume protection engine for PowerMax.
Kernel-Based Virtual Machine (KVM)		

NOTES:

• For PPDM deployed on customer-managed infrastructure, Dell Technologies is responsible for the PPDM application software and associated product support in accordance with the terms of the Dell standard support purchased with the product. Customers are responsible for the underlying operating system, including operating system licensing, installation, configuration, patching, security maintenance, and lifecycle management
• A2O and NAS proxies are supported on all OSs listed
• SDNG proxy is only supported on SLES 15 SP6 and SP7, RHEL 9.6 and 9.7
• NDMP accelerator is only supported in SLES 15 SP6, SP7 and RHEL 9.6 and 9.7
• Migration from VMware vCenter deployment to Linux install package deployment is not supported.
• Deploy the install package with root privileges.
• The installation path must contain only English characters.

TARGETS

Backup – Data Domain (Physical & Virtual)

DATADOMAIN	VERSION
DDOS / DDMC / DDVE	8.0.x, 8.1.x, 8.3.x, 8.4.x, 8.5.x, 8.6.x, 8.7.x, 8.8.x, 8.9.x

NOTES:

- Review the Data Domain documentation for model-specific details.
- Review the Data Domain Cloud Tier Support documentation for a list of supported cloud providers.
- DDBoost library packaged in PowerProtect Data Manager: 8.9.0.0-1257697

Archive – Object Storage

CLOUD PROVIDER	CLOUD SERVICE	SUPPORTED ASSETS	SUPPORTED REGIONS
Dell	Elastic Cloud Storage (ECS)	VM, Filesystem Agent, SQL Agent, Oracle, DNAS	NA
Amazon	Amazon S3 (Standard)	VM, Filesystem Agent, SQL Agent, Oracle, DNAS	NA
Microsoft	Azure	VM, Filesystem Agent, SQL Agent, Oracle, DNAS	NA
Generic	S3 Compatible	VM, Filesystem Agent, SQL Agent, Oracle, DNAS	NA

NOTES:

- The file system agent supports Linux, Windows, and AIX operating systems.
- Active Directory granular level restore (ADGLR) is not supported.
- VM File-Level Restore (FLR) and VM Application Aware SQL are not supported.
- Wasabi with Dell ObjectScale is qualified only with VM protection engines.
- Software Packaged Proxy (SPP) supports RHEL 9.6, RHEL 9.7, SLES 15 SP6 & SP7 and Rocky Linux 9.6
- Only Oracle full backups along with dependent archive logs supported when sealed flag is True
- Only Oracle SBT copies supported
- Only NAS filebased copies are supported (No NDMP)
- Wasabi Dell ObjectScale solution is supported through S3 Compatibility.

LANGUAGE SUPPORT

Supported Asset Languages

CATEGORY	FULL SUPPORT	CONDITIONAL SUPPORT	LINUX DEPLOYMENTS
Languages / Details	English	Simplified Chinese, French, German, Italian (See Note 2), Japanese, Korean, Traditional Chinese (See Note 3), Spanish, Portuguese–Portugal, Portuguese–Brazil	All languages supported by PowerProtect Data Manager
Constraints		Protection of data in these language environments must observe the following considerations: (1) Application agents must be installed to the default location. (2) Names of assets such as files, folders, and databases can use characters in any supported language. (3) Hostnames, fully qualified domain names, and cluster names can only use the ASCII characters A-Z, a-z, 0-9, and hyphen. (4) The operating systems of the backup source and restore destination must use the same locale. (5) Only UTF-8 is supported for non-English assets.	

NOTES:

1. PowerProtect Data Manager and its user interface support only the ASCII characters A-Z, a-z, 0-9, and hyphen in the following functions:
1.a. APIs.
1.b. Character string input and output.
1.c. Configuration settings.
1.d. Exported logs.
1.e. Headings and fields.
1.f. Informational and error messages.
1.g. Local time and date formats.
1.h. Sorting, searching, and filtering.
2. For VMware virtual machines, Italian language support requires vSphere 8.0 and above.
3. Traditional Chinese language support is not available for Oracle.
4. Active Directory granular level restore (ADGLR) is supported only on English, German, and Simplified Chinese operating systems.
5. AHV is supported only on English & Japanese operating systems.

VMWARE

Platform support

PLATFORM	PLATFORM VERSION	COMMENTS
vCenter	8.0, 8.0 U1, 8.0 U2b, 8.0 U3, 9.0.x.y (See Note 1), 9.1.x.y	8.0, 8.0 U1 includes patch/letter releases. 8.0 U2b is the minimum supported build (includes subsequent U2 and U3 patches).
VMC on AWS	SDDC 1.22, 1.24, 1.26	Includes odd numbered optional releases.
Azure VMware Solutions (AVS)		
Google Cloud VMware Engine (GCVE)		
Oracle Cloud VMware Solutions (OCVS)		

NOTES:

• Supported datastores: vVol, vSAN, VMFS, NFS, vSAN ESA.
• Supported vSAN topologies: Standard Cluster, Stretched Cluster, Two-node Cluster, HCI Mesh.
• PowerProtect Data Manager supports in-cloud VM image protection in the respective environments. Protection from in-cloud to on-premises environments, or from on-premises to in-cloud environments, is not supported.
1. TSDM is not supported with vSphere 9.0 (ESXi and/or vCenter). VM asset protection falls back to VADP and VM protection engines are required to protect VM assets.

Hypervisor support

PLATFORM	PLATFORM VERSION	COMMENTS
ESXi	8.0, 8.0 U1, 8.0 U2b, 8.0 U3, 9.0.x.y (See Note 1), 9.1.x.y	8.0, 8.0 U1 includes patch/letter releases. 8.0 U2b is the minimum supported build (includes subsequent U2 and U3 patches).

NOTES:

1. TSDM is not supported with vSphere 9.0 (ESXi and/or vCenter). VM asset protection falls back to VADP and VM protection engines are required to protect VM assets.

Management (vCenter Plugin)

PLATFORM	PLATFORM VERSION	COMMENTS
vCenter	8.0, 8.0 U1, 8.0 U2b, 8.0 U3, 9.0.x.y, 9.1.x.y	8.0 U2b is the minimum supported build (includes subsequent U2 and U3 patches).

Virtual Machines

PLATFORM	PLATFORM VERSION	COMMENTS
VMware Tools	11.x, 12.x, 13.x	Version 11.1 and later is required to perform Microsoft SQL Server application-aware protection.
Open VM Tools	11.x, 12.x, 13.x	For Linux platforms.

NOTES:

• All virtual machine operating systems supported by VMware.
• Anomaly Detection is supported for all supported VMware virtual machines

Transparent Snapshot Data Mover (TSDM)

SUPPORTED FEATURES & PRODUCTS	PLATFORM VERSION	COMMENTS
vSphere (ESXi and/or vCenter)	8.0 U1-U3, 9.1.x.y (See Notes 1)	8.0 U1 includes patch/letter releases. 8.0 U2b is the minimum supported build (includes subsequent U2 and U3 patches).
VMware Virtual Volumes (vVols)	vSphere 8	Includes Update releases
CyberSense		https://www.indexengines.com/cs
VMware Cloud Foundation (VCF)	5.0, 5.1.1, 5.2.x, 9.1.x.y	BOM contains vSphere 8.0 U2b (minimum version).
Oracle Cloud VMware Solution (OCVS)	vSphere 8	Includes Update releases
Google Cloud VMware Engine (GCVE)	vSphere 8	Includes Update releases
Microsoft SQL Application Aware Protection	vSphere 8	VM Application Aware Backup – SQL provides supported versions.
VMware Live Site Recovery (VLSR)	9.0.1 (and above)	vSphere Replication 9.0.1 or later is required.
		vSphere 8.0 U3 or later is required.
		Array-based replication is not supported.
		vSphere 9.x.y.z is not supported.

NOTES:

1. TSDM is supported with vSphere/VCF 9.1. Refer to the Dell PowerProtect Data Manager 20.2 VMware Virtual Machine User Guide for VIB download and deployment instructions.

Aria Data Protection Extension (DPE)

PLATFORM	PLATFORM VERSION	COMMENTS
VMware Aria Automation with Embedded Aria Automation Orchestrator	8.14.x, 8.16.x, 8.17.x, 8.18.x	Includes standalone and cluster deployments.

NOTES:

• Broadcom KB article 403297 provides more information about usage details - https://knowledge.broadcom.com/external/article?articleNumber=403297

VCF (on VxRail) Management Protection

PLATFORM	PLATFORM VERSION	COMMENTS
VMware Cloud Foundation	5.0, 5.1, 5.2	

NOTES:

• Includes VCF on vSAN Ready Nodes and VCF on VxRail.
• Configure protection for VCF management components with the ppdm-vcf-component-protection.sh script that you obtain through the UI by clicking > Downloads > VMware and then selecting VMware Cloud Formation (VCF) on VxRail.

VMWare Telco Cloud Platform

PLATFORM	VERSION	SUPPORTED STACK
Telco Cloud Platform (TCP)	3.0	VMware Tanzu Kubernetes Grid 2.1.x; ESXi and vCenter 8.0 (including patch releases)
Telco Cloud Platform (TCP)	4.0	VMware Tanzu Kubernetes Grid 2.5; ESXi and vCenter 8.0 U2b
Telco Cloud Platform (TCP)	5.0	VMware Tanzu Kubernetes Grid 2.5.2; ESXi and vCenter 8.0 U3

NOTES:

• For TCP components that require file-level protection, refer to the File Systems – Block Based Backup (BBB) and File Systems – File Based Backup (FBB) tables on pages 16 and 17 for supported file and operating systems.
• For TKGm workload clusters, refer to the Kubernetes table on page 22 for supported distributions.
• For more information, refer to the Dell Technologies PowerProtect Data Manager for VMware Telco Cloud Platform Solution Brief.

VM Application Aware Backup – SQL (General)

PLATFORM	PLATFORM VERSION	COMMENTS
VMware vSphere (ESXi and vCenter)	8.0, 8.0 U1, 8.0 U2b, 8.0 U3	8.0 U2b is the minimum supported build (includes subsequent U2 and U3 patches).
	9.0.x.y (See Note 1), 9.1.x.y	

VM Application Aware Backup – SQL (SQL Server Versions)

MICROSOFT SQL SERVER VERSION	MS SQL SERVER BITNESS	WINDOWS OS [64 BIT]
2016 Service Pack 3	64-bit	2016, 2019
2017 (supported up to CU31)	64-bit	2016, 2019, 2022
2019 (supported up to CU32)	64-bit	2016, 2019, 2022, 2025
2022 (supported up to CU23) (See Note 2)	64-bit	2016, 2019, 2022, 2025
2025 (supported up to CU2)	64-bit	2019, 2022, 2025

NOTES:

• Clustered and cluster-less AAG Quorum supports file share witness only.
• VMs with multi-writer/shared disks are not supported.
• VMware Tools: 11.x and later. Clustered AAG for pure IPv6 requires VMware Tools 12.x.
1. TSDM is not supported with vSphere 9.0 (ESXi and/or vCenter). VM asset protection falls back to VADP and VM protection engines are required to protect VM assets.
2. SQL Server 2022 below CU4 is not supported.

VM File Level Recovery

OPERATING SYSTEM	HARDWARE ARCHITECTURE	OS VENDOR	FILESYSTEMS	SEARCH AND INDEXING
Windows 10	64-bit	Microsoft	NTFS	Yes
Windows 11	64-bit	Microsoft	NTFS	Yes
Windows 2012	64-bit	Microsoft	NTFS, FAT32, ReFS	Yes (See Note 2)
Windows 2012 R2 (See Note 1)	64-bit	Microsoft	NTFS	Yes
Windows 2016	64-bit	Microsoft	NTFS	Yes
Windows 2019	64-bit	Microsoft	NTFS, FAT32, Dynamic	Yes
Windows 2022	64-bit	Microsoft	NTFS, ReFS, Dynamic	Yes (See Note 2)
Windows 2025	64-bit	Microsoft	NTFS, Dynamic	Yes
AlmaLinux 8.10, 9.7, 10.1	X64	AlmaLinux OS Foundation	XFS	Yes
CentOS 9 Stream	X64	CentOS	XFS, EXT4	Yes
CentOS 10 Stream	X64	CentOS	XFS, EXT2/3/4	
RedHat Enterprise Linux (RHEL) 7.8, 7.9	X64	Red Hat	XFS, EXT4, BTRFS (See Note 3)	Yes
RHEL 8.8 – 8.10	X64	Red Hat	XFS	Yes
RHEL 9.4 – 9.8	X64	Red Hat	XFS	Yes
RHEL 10.0 – 10.1	X64	Red Hat	XFS	Yes

OPERATING SYSTEM	HARDWARE ARCHITECTURE	OS VENDOR	FILESYSTEMS	SEARCH AND INDEXING
SUSE Linux Enterprise Server (SLES) 12 SP5	X64	SUSE	XFS, EXT4	Yes
SLES 15 SP3 – 15 SP7, SLES 16	X64	SUSE	XFS, EXT4, BTRFS (See Note 3)	Yes
Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (Server)	X64	Canonical	EXT4, XFS	Yes
Ubuntu 22.04 (Desktop)	X64	Canonical	EXT4, XFS	Yes
Debian 11.3 – 11.10	X64	Debian	EXT4	Yes
Debian 12.0 – 12.2, 12.5 – 12.6, 12.8, 12.9, 12.11 – 12.12	X64	Debian	EXT4	Yes
Oracle Linux 7.7	X64	Oracle	XFS, EXT4	Yes
Oracle Linux 7.9	X64	Oracle	XFS, EXT4, BTRFS (See Note 3)	Yes
Oracle Linux 8.3 – 8.4	X64	Oracle	XFS, BTRFS (See Note 3)	Yes
Oracle Linux 8.5 – 8.10	X64	Oracle	XFS, EXT4, BTRFS (See Note 3)	Yes
Oracle Linux 9.0 – 9.6, 10	X64	Oracle	XFS, EXT4	Yes
OpenSUSE Leap 15.6	X64	openSUSE	EXT4, BTRFS (See Note 3)	Yes
Fedora Linux 41 - 43	X64	Fedora	XFS	Yes
Rocky Linux 8.10, 9.6, 10.0	X64	Rocky Enterprise Software	XFS	Yes

NOTES:

• Indexing of LVM thin-pool logical volumes is not supported.
• Indexing of RAID5 volumes is not supported.
• Indexing of Windows Storage Pool configurations is not supported.
• PowerProtect Data Manager does not support file-level restore to a target VM that is protected using VMware Live Site Recovery (VLSR) or vSphere Replication (VR).
• The target VM for the restore should support the same filesystem type, version, and options as the source backup. For example, the versions of xfsprogs on the target and source VMs must be compatible.
1. Includes Extended Security Update (ESU) from Microsoft (https://docs.microsoft.com/en-US/lifecycle/faq/extended-security-updates).
2. Indexing of ReFS is not supported.
3. Restore of files from BTRFS sub-volumes is not supported, only image-level recovery.

MICROSOFT HYPER-V

Protection

PLATFORM	PLATFORM VERSION	COMMENTS
Hyper-V Server	2016, 2019	
Windows Server	2016, 2019, 2022, 2025	Applies to both GUI and Core OS version.
Azure Local (Azure Stack HCI)	23H2, 24H2 (2411)	Applies to both GUI and Core OS version.

NOTES:

- Hyper-V is supported for all the PPDM supported Languages
- For non-English locales, Hyper-V agents must be installed in the default location.
- If Windows Defender Application Control (WDAC) is enabled, configure Hyper-V WDAC Supplemental Policy.
- Anomaly Detection is supported for Hyper-V workloads.
- Compatible with Dell AX Systems: 15G AX, 16G AX
- Does not support Azure Local Hyper-V cluster configuration with Azure Arc-enabled

Microsoft Hyper-V File Level Recovery

OPERATING SYSTEM	HARDWARE ARCHITECTURE	OS VENDOR	FILESYSTEMS	SEARCH AND INDEXING
Windows 11	64-bit	Microsoft	NTFS	Yes
Windows 2016	64-bit	Microsoft	NTFS, ReFS, FAT32	Yes (See Note 1)
Windows 2019	64-bit	Microsoft	NTFS	Yes
Windows 2022	64-bit	Microsoft	NTFS	Yes
Windows 2025	64-bit	Microsoft	NTFS	Yes

NOTES:

- Indexing Windows Storage Pool configurations is not supported.
- Indexing Windows VMs with AVHDX file (Checkpoint files) is not supported.
- Indexing Windows VMs with VHD format is not supported.

1. Indexing of VMs with ReFS is not supported.

NUTANIX AHV

Protection

PLATFORM	PLATFORM VERSION	COMMENTS
Prism Central	2024.2, 2024.3, 7.3	
Acropolis Operating System (AOS)	6.10, 7.0, 7.3	

NOTES:

• AHV is supported only on English & Japanese operating systems.

Nutanix AHV File Level Recovery (Mount)

OPERATING SYSTEM	HARDWARE ARCHITECTURE	OS VENDOR	FILESYSTEMS	SEARCH AND INDEXING
Windows 11	64-bit	Microsoft	NTFS	Yes
Windows 2016	64-bit	Microsoft	NTFS, ReFS, FAT32	Yes (See Note 1)
Windows 2019	64-bit	Microsoft	NTFS	Yes
Windows 2022	64-bit	Microsoft	NTFS	Yes
Windows 2025	64-bit	Microsoft	NTFS	Yes

NOTES:

1. Indexing of VMs with ReFS is not supported.

• FLR workflows not supported on Non-HCI clusters. Target VMs should reside on HCI nodes

GENERIC APPLICATION AGENT

Generic Application Agent

APPLICATION AND VERSION	OS	HARDWARE ARCHITECTURE	OS VENDOR	OS VENDOR VERSION
PostgreSQL 13, 14, 15, 16, 17, 18	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x, 10.x, SLES 12 SP5, SLES 15 SPx
MariaDB	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x, 10.x ,SLES 12 SP5,SLES 15 SPx
MySQL	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x,10.x, SLES 12 SP5,SLES 15 SPx
MongoDB	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x,10.x, SLES 12 SP5,SLES 15 SPx
PaaS	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x,10.x. SLES 12 SP5,SLES 15 SPx
Redis	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x, 10.x, SLES 12 SP5,SLES 15 SPx
Sybase	Linux	X64	RHEL, SUSE	RHEL 8.x, 9.x,10.x, SLES 12 SP5,SLES 15 SPx

NOTES:

• The Generic Application Agent supports all combinations of operating system vendors, applications, and their respective versions listed in this table, provided that the application is compatible with the operating system.

• Co-existence of the file system and generic application agents for all the operating systems mentioned in the table.

SQL

MS SQL Server

MICROSOFT SQL SERVER VERSION	SERVER BITNESS	OS	HARDWARE ARCHITECTURE	OS VENDOR	OS VENDOR VERSION
SQL Server 2017	64-bit	Windows	X64	Microsoft	2016, 2019, 2022
SQL Server 2019	64-bit	Windows	X64	Microsoft	2016, 2019, 2022, 2025
SQL Server 2022	64-bit	Windows	X64	Microsoft	2016, 2019, 2022, 2025
SQL Server 2025	64-bit	Windows	X64	Microsoft	2019, 2022, 2025

NOTES:

• Application Agent for MS SQL supports:

• MS SQL clustering for AAG (except distributed AAG, which is not a supported configuration, as this Availability Group spans two separate Availability groups configured on on-premise SQL Server instances or Azure VMs or AWS EC2) and FCI configurations.

• MS SQL clusterless AAG configurations (except clusterless AAG over FCI, which is not a supported configuration).

  • All combinations of OS and application versions in this table, provided that the OS is supported by the application.

  • All file systems shown in the table, provided that these file systems are supported by the application.

  • All Windows Server editions and all Service Packs (SP) for a given release, provided that the combination is supported by the application.

  • All SQL server, editions such as Standard, Enterprise, Express, Workgroup, and Web that are supported by the application release.

• SQL Server Management Studio 2012 through 19.x versions in SQL Servers is based on Microsoft compatibility.

EXCHANGE

Microsoft Exchange

MICROSOFT EXCHANGE VERSION	SERVER BITNESS	OS	HARDWARE ARCHITECTURE	OS VENDOR	OS VENDOR VERSION
2016	64-bit	Windows	X64	Microsoft	2012, 2012 R2, 2016
2019	64-bit	Windows	X64	Microsoft	2019, 2022, 2025
Subscription Edition	64-bit	Windows	X64	Microsoft	2019, 2022, 2025

NOTES:

- Application Agent for Exchange supports:
  - All combinations of OS and application versions in the table, provided that the OS is supported by the application.
  - All virtualization environments (such as VMware) at the guest level, provided that the application and database app agent running on this guest OS natively support this OS.
  - All Cumulative Updates (CU) and Update Rollups (UR) for the application versions listed in this table unless explicitly stated otherwise.
- PowerProtect Data Manager for Exchange supports only Windows Server 2022 from Exchange 2019 CU11 and above.
- Because Outlook cannot be installed on Windows Server Core Editions, ItemPoint is not supported directly on Windows Server Core Edition. Instead, use the proxy server method for ItemPoint operations.
- Co-existence of the Exchange agent is supported only with the file system agent.
- Installing ItemPoint for Granular-Level Recovery requires 32-bit Outlook.
- Co-existence of the Exchange agent and the Windows Platform RMAN agent is not supported.
- PowerProtect Data Manager for Exchange supports Windows Server 2025 only from Exchange 2019 CU15 to SE.
- Exchange Granular-Level Recovery (GLR) supports Microsoft Outlook versions up to Outlook 2024.

ORACLE

Oracle Server Versions

ORACLE VERSION	OS
12c R2	Windows - 2016,2019,2022. RHEL & Oracle Enterprise Linux - 7, 8 SLES - 12, 15 AIX - 7.2
18c	RHEL & Oracle Enterprise Linux - 7 SLES - 12 AIX - 7.2
19c	Windows - 2016, 2019, 2022, 2025. RHEL & Oracle Enterprise Linux - 7, 8, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 SLES - 12, 15 AIX - 7.2, 7.3
21c	Windows - 2016, 2019, 2022 RHEL & Oracle Enterprise Linux - 7, 8, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 SLES - 15
26 AI	RHEL - 8.6, 9.2 SLES - 15 SP5

NOTES:

- PowerProtect Data Manager for Oracle supports:
  - Oracle Server when installed and configured on one of the following systems:
    - Stand-alone configuration.
    - Oracle RAC in active/active configuration.
    - Oracle RAC in active/passive configuration.
    - Data Guard configuration.
    - Data Guard Heterogeneous (Linux+Windows).
    - Oracle Exadata Oracle Linux.
    - RHEL 9 supports patch versions of 19c (19.19 and above).
    - Oracle ODA ACFS is supported.
  - Oracle RAC on all Cluster File Systems supported by Oracle.
  - Oracle Single-Node Appliance X7, X8 and X10-HA models supported
  - Oracle on Exadata Cloud Oracle 19c and above with Linux (RHEL/OEL) supported
  - All OS and application versions in the table, provided that the OS is supported by the application.
  - All Fix Packs/Patch Sets for all application versions in this table.
  - All Service Packs, Updates, Patches, etc. of all OSs listed in this table, provided that the update is supported by the application (for example, stated support for Oracle Linux 7 also implies support for Oracle Linux 7 Update 5).
  - Raw devices and all file systems shown in the table, provided that these file systems are supported by the application.
  - All virtualization environments (such as VMware, LPAR) at the guest level, provided that the application and database app agent running on this guest OS natively supports this OS.
  - Oracle Incremental Merge (OIM) is supported only on Linux and AIX (NFS protocol) platforms.
  - Oracle database single-node appliance X7, X8 and X10-HA models.
- PowerProtect Data Manager for Oracle on AIX supports AIX 7.2 TL2 SP1 or later, and AIX 7.3 until TL4.
- PowerProtect Data Manager for Oracle supports Oracle 19c and above with Linux (RHEL/OEL) on Exadata Cloud at Customer (ExaCC).
- PowerProtect Data Manager for Oracle does not support:
  - An Oracle database installation in a High Availability (active/passive) OS cluster configuration.
  - Enabling Oracle Application-Optimized compression through the UI for mobile storage units on system pools using DDMC 8.1 & later versions.

DELL NATIVEEDGE

Dell NativeEdge

PLATFORM	DELL AUTOMATION PLATFORM ORCHESTRATOR	NATIVEEDGE OS
Dell NativeEdge	1.1.0.0	4.0.0.0 (and above)
Dell NativeEdge	1.2	4.1
Dell NativeEdge	2.0	4.2

SAP HANA

SAP HANA

SAP HANA VERSION	SAP HANA BITNESS	OS	HARDWARE ARCHITECTURE	OS DISTRIBUTION	OS VENDOR VERSION
2.x	64-bit	Linux	X64	RHEL	7.x, 8.x, 9.x
2.x	64-bit	Linux	X64	SLES	12.x, 15.x

NOTES:

- Application Agent for SAP Hana supports:
  - All combinations of OS and application versions in the table, provided that the OS is supported by the application.
  - All Fix Packs/Patch Sets for all application versions in this table.
- All Service Packs, Updates, Patches, etc. of all OSs listed in this table, provided that the update is supported by the application.
  - Support covers all SAP HANA 2.0 patch releases up to and including SPS 08.
  - Raw devices and all file systems shown in the table, provided that these file systems are supported by the application.
  - All virtualization environments (such as VMware) at the guest level, provided that the application and database app agent running on this guest OS natively support this OS.
- SAP HANA High Availability (HA) configurations are currently not supported by PowerProtect Data Manager.

STORAGE ARRAYS

PowerStore

DELL POWERSTORE MODELS	STORAGE ARRAY OPERATING SYSTEM VERSION	VENDOR
500T, 1000T, 1200T, 3000T, 3200T, 5000T, 5200T, 7000T, 9200T	3.5.0.x; 3.6.0.x; 4.0.0.x; 4.0.1.x; 4.1.0.x; 4.2.0.x, 4.3.0.x, 4.4.0.x, 5.0.0.x	Dell

NOTES:

• This table applies for protection of block volume and volume group data.
• The PowerStore appliance communicates with PowerProtect DD over IP (DD Boost). Storage array protection supports physical PowerProtect DD appliances, including HA models, as well as DDVE on-premises and in a public AWS, GCP, and Azure cloud.
• Block volume protection policies do not support PowerStore Metro volumes
• If a volume or volume group is already part of a PowerStore Manager protection policy, the volume or volume group cannot be protected by PowerProtect Data Manager, and conversely.
• A PowerProtect DD storage unit that is configured as a remote system for a PowerStore Manager protection policy cannot be shared with a PowerProtect Data Manager protection policy, and conversely.
• There is no specific hard limit on the number of PowerStore clusters or appliances that can be managed by a single instance of PowerProtect Data Manager. However, other PowerProtect Data Manager limitations may impose such limits.
• Anomaly Detection is supported for PowerStore snapshots using the Fiber Channel & iSCSI protocol on NTFS, FAT, BTRFS, ext2/3/4 and XFS file systems.

PowerMax

DELL POWERMAX MODEL	STORAGE ARRAY OPERATING SYSTEM VERSION (POWERMAX OS)	STORAGE ARRAY MANAGEMENT INTERFACE (UNISPHERE FOR POWERMAX)
2500, 8500	10.1.0.4 (plus hotfix 10443), 10.1.0.5 or higher, 10.2.0.0 or higher, 10.3.0.0 or higher, 10.3.1.0 or higher	10.1.0.5 or higher, 10.2.0.0 or higher, 10.3.0.0 or higher, 10.4.0.0 or higher
2000, 8000	5978.714.714 or higher	10.1.0.5 or higher, 10.2.0.0 or higher, 10.3.0.0 or higher, 10.4.0.0 or higher

NOTES:

• This table row applies for protection of PowerMax block storage located on PowerMax v4 systems.
• Open a PowerMax Service Request to have the required PowerMax hotfix installed. All other PowerMax OS versions not explicitly listed in this table need an approved RPQ to determine the mandatory PowerMax OS hotfix. Failure to apply the hotfix can have a critical impact on the PowerMax system.
• PowerMax protection requires the deployment of protection engines.
• This integration supports protection of storage group volumes that are provisioned via SCSI over FC. Volumes that are provisioned with NVMe over FC, NVMe over TCP, and iSCSI are not supported.
• PowerProtect Data Manager supports only storage groups with FBA emulation alone.
• Dell recommends using an external Unisphere for PowerMax instead of embedded, for better performance. For PowerMax 2000 and 8000, only external Unisphere is supported.
• Dell recommends using VMware native multipathing for ESXi where a protection engine is deployed.
• PowerProtect Data Manager is not aware of the SRDF/A, SRDF/S & SRDF/Metro replica states. Such volumes are treated as local. Only restore to alternate non-SRDF storage group is supported.
• The PowerProtect Data Manager Storage Array User Guide provides detailed information about solution scalability and limitations.
• The software installer proxy supports only SLES 15 SP6, SLES 15 SP7, RHEL 9.6 and RHEL 9.7

FILE SYSTEMS

Block Based Backup

OPERATING SYSTEM	KERNEL VERSION
Windows 2025	NA
Windows 2022	NA
Windows 2016	NA
Windows 2019	NA
Windows 10	NA
Windows 11	NA
RHEL 8.0	4.18.0-80
RHEL 8.1	4.18.0-147
RHEL 8.2	4.18.0-193
RHEL 8.3	4.18.0-240
RHEL 8.4	4.18.0-305
RHEL 8.5	4.18.0-348
RHEL 8.6	4.18.0-372
RHEL 8.7	4.18.0-425.3.1
RHEL 8.8	4.18.0-477.10.1
RHEL 8.9	4.18.0-513.5.1
RHEL 8.10	4.18.0-553
RHEL 9.0	5.14.0-70
RHEL 9.1	5.14.0-162.6.1
RHEL 9.2	5.14.0-284.11.1
RHEL 9.3	5.14.0-362.8.1
RHEL 9.4	5.14.0-427.13.1
RHEL 9.5	5.14.0-503.11.1
RHEL 9.6	5.14.0-570.12.1
SLES 12 SP3	4.4.73-5
SLES 12 SP4	4.12.14-94.41
SLES 12 SP5	4.12.14-120

OPERATING SYSTEM	KERNEL VERSION
SLES 15 SP1	4.12.14-195
SLES 15 SP2	5.3.18-22
SLES 15 SP3	5.3.18-57
SLES 15 SP4	5.14.21-150400.22
Oracle Linux 9.1	5.15.0-3.60.5.1
Oracle Linux 9.2	5.15.0-101.103.2.1
Oracle Linux 9.3	5.15.0-200.131.27
Oracle Linux 9.4	5.15.0-205.149.5.1

NOTES:

- The file system agent supports Microsoft failover clustering for both CSV and cluster volumes configurations.
- Filesystem agent support only x64 or 64bit architecture
- For Linux operating systems where the file system agent does not support BBB, use --skip-driver during agent installation to skip the BBB driver.
- Kernel versions are applicable for BBB, that is, for image-level backups only.
- The file system agent uses BBB if there are no exclusion filters associated with a protection policy. If a protection policy is associated with one or more exclusion filters, the file system agent performs backups using FBB instead.
- Only LVM-based volumes are supported for protection. Backups of non-LVM/physical disks are not supported with BBB.
- The only filesystem supported for BBB are Windows (NTFS, ReFS) & Linux (ext3, ext4, xfs)
- The only filesystem supported for indexing BBB based copies are Windows (NTFS) & Linux (ext3, ext4, xfs)
- The file system agent supports Microsoft Distributed File System (DFS).

File Based Backup

OPERATING SYSTEM
Windows 2025
Windows 2022
Windows 2016
Windows 2019
Windows 10
Windows 11
RHEL 8.x
RHEL 9.x
RHEL 10.x
RockyLinux 8.x
RockyLinux 9.x
RockyLinux 10.x

OPERATING SYSTEM
SLES 12.x
SLES 15.x
SLES 16
Ubuntu 16.x
Ubuntu 18.x
Ubuntu 20.x
Ubuntu 22.x
Ubuntu 24.x
Ubuntu 25.x
Oracle Linux 7.x UEK
Oracle Linux 8.x UEK
Oracle Linux 9.x UEK
Debian 11.x
Debian 12.x
Alma Linux 8.x
Alma Linux 9.x
Alma Linux 10.x
AIX 7.2 TL2 SP1
AIX 7.2 TL3
AIX 7.2 TL4
AIX 7.2 TL5
AIX 7.3 TL0
AIX 7.3 TL1
AIX 7.3 TL2 SP1
AIX 7.3 TL2 SP2
AIX 7.3 TL3
AIX 7.3 TL4
AIX 7.3 TL4 SP1

NOTES:

- Backups using FBB are independent of the operating system kernel version.
- The file system agent on AIX requires the xlc runtime environment 16.1.0.7 or later.
- Filesystem agent support only x64 or 64bit architecture

- The only filesystem supported for indexing BBB based copies are Windows (NTFS) & Linux (ext3, ext4, xfs)
- Supported filesyste are Windows (NTFS, ReFS), Linux (ext3, ext4, xfs, btrfs, acfs, ocfs2) & AIX (jfs, jfs2)
- The file system agent supports:
    - Microsoft failover clustering for both CSV and cluster volumes configurations.
    - Microsoft Distributed File System (DFS).
    - Active Directory Granular-Level Restore from BMR/SSR backups for Windows Server 2016, 2019, and 2022 only.
    - Disaster recovery backups, which consist of bare metal recovery (BMR) backup and system state recovery (SSR) backup, for Windows only and uses FBB.
- Anomaly Detection is supported for FBB workloads.

NAS

Dynamic NAS

STORAGE ARRAY	STORAGE VENDOR	SUPPORTED PROTOCOLS
Unity 5.0.x, 5.1.x, 5.2.x, 5.3.x, 5.4.x, 5.5	Dell	Share options: CIFSv1, CIFSv2, CIFSv3, NFSv3, NFSv4.x
PowerStore 3.0, 3.2, 3.5, 3.6, 4, 4.1, 4.2	Dell	Share options: CIFSv1, CIFSv2, CIFSv3, NFSv3, NFSv4.x
PowerScale OneFS 9.5.0.5, 9.7.x, 9.8, 9.9, 9.10, 9.12, 9.13	Dell	Share options: CIFSv1, CIFSv2, CIFSv3, NFSv3, NFSv4.x
NetApp ONTAP 9.12, 9.13, 9.14, 9.15, 9.16, 9.17	NetApp	Share options: CIFSv1, CIFSv2, CIFSv3, NFSv3, NFSv4.x
Generic NAS protection workflow	*	Share options: CIFSv1, CIFSv2, CIFSv3, NFSv3, NFSv4.x

NOTES:

- The generic NAS protection workflow involves backing up a live mount of the target share, without taking a snapshot.
- The generic NAS protection workflow supports all NAS appliances and file servers.
- Dynamic NAS supports only standalone configurations of NAS appliances. Replicated and stretched configurations of NAS appliances are not supported.
- The release schedule of each storage array in this table may differ from that of PowerProtect Data Manager. Contact Customer Support before you deploy a storage array release that is not listed in this table.
- The NAS protection engine installer supports SLES 15 SP6, SLES 15 SP7, RHEL 9.6, RHEL 9.7 and Rocky Linux 9.6
    - Additional virtualization platforms such as Nutanix AHV, Microsoft Hyper-V, and KVM are also supported, where the protection engine can be deployed.
- Version parity is maintained with the PowerProtect Data Manager software with all platforms and OS versions for deployment.
- Anomaly Detection is supported for NAS workloads.

NDMP

STORAGE ARRAY	STORAGE VENDOR	SUPPORTED PROTOCOLS
NetApp ONTAP 9.12, 9.13, 9.14, 9.15, 9.16, 9.17	NetApp	NDMP v4
PowerStore 4, 4.1, 4.2	Dell	NDMP v4
PowerScale OneFS 9.8, 9.9, 9.10, 9.12, 9.13	Dell	NDMP v4

NOTES:

- The accelerator node installer supports SLES 15 SP6 and SP7, RHEL 9.6 and 9.7 with the following hardware configuration:
- 4 vCPUs/cores, 64 GB RAM, 2 TB disk space. (100 GB for / and 1900 GB for /data01)

CLOUD MARKETPLACES

Cloud Providers

CLOUD PROVIDER	CLOUD SERVICE	SUPPORTED ASSETS	SUPPORTED REGIONS
Amazon	AWS, AWS Glacier Instant Retrieval (IR)	SQL, Oracle, SAP HANA, and file system agents, and Kubernetes asset sources are supported. VM protection is available for VMs in VMC for AWS (SDDC 1.16, 1.18, 1.20).	[DDOS 7.4.0.5 onwards]: ca-central-1 (Canada - Central), eu-south-1 (EU - Milan), me-south-1 (Middle East - Bahrain) [From DDOS 6.0 onwards]: us-east-1, us-west-1, us-west-2, eu-west-1, ap-northeast-1, ap-southeast-1, ap-southeast-2, sa-east-1 (South America - Sao Paulo), ap-south-1 (Asia Pac - Mumbai), ap-northeast-2 (Asia Pac - Seoul), eu-central-1 (EU - Frankfurt)
Amazon	AWS GovCloud/C2S	SQL, Oracle, SAP HANA, and file system agents, and Kubernetes asset sources are supported. VM protection is available for VMs in VMC for AWS (SDDC 1.16, 1.18, 1.20).	[DDOS 7.2 onwards]: us-gov-east-1, us-gov-west-1
Microsoft	Azure	SQL, Oracle, SAP HANA, and file system agents, and Kubernetes asset sources are supported. VM protection is available for VMs in Azure VMware Solution.	All regions listed under General Purpose storage class. Azure Gov requires DDOS 6.1.1.x or later.
Microsoft	Azure Government Cloud	SQL, Oracle, SAP HANA, and file system agents, and Kubernetes asset sources are supported. VM protection is available for VMs in Azure VMware Solution.	US Gov Arizona, US Gov Texas, US Gov Virginia
Google	GCP	SQL, Oracle, SAP HANA, and file system agents, and Kubernetes asset sources are supported. VM protection is available for VMs in Google Cloud VMware Engine.	us, eu, asia, northamerica-northeast1, us-central1, us-east1, us-east4, us-west1, southamerica-east1, europe-north1, europe-west1, europe-west2, europe-west3, europe-west4, asia-east1, asia-northeast1, asia-south1, asia-southeast1, australia-southeast1

NOTES:

• Enabling Cloud DR and Search functionality is not supported in PowerProtect Data Manager instances running in the public cloud. This restriction does not apply to PowerProtect Data Manager instances running in VMware in Cloud.

CLOUD DISASTER RECOVERY

END OF SALE	END OF SUPPORT
January 31, 2026.	January 31, 2028.

NOTES:

• Cloud Disaster Recovery feature will be End of Support Jan 2028

VMware Infrastructure

PLATFORM	PLATFORM VERSION
VMware vCenter/ESXi	8

Cloud Vendor Support

VENDOR NAME	CLOUD SERVICE
Amazon	AWS (Amazon Web Services) & AWS GovCloud
Microsoft	Microsoft Azure & Azure Government Cloud

AWS Target Supported Virtual Machine Operating Systems

WINDOWS 64-BIT	LINUX OR UNIX
Microsoft Windows Server 2012 Standard, Datacenter. 64-bit only.	Ubuntu 14.04, 14.10, 16.04, 16.10
Microsoft Windows Server 2012 R2 Standard, Datacenter. 64-bit only. Nano Server installation not supported.	Red Hat Enterprise Linux 6.1–6.9, 7.0–7.3, 8, 9
	(6.0 lacks required drivers)
Microsoft Windows Server 2016 Standard, Datacenter. 64-bit only.	SUSE Linux Enterprise Server 15 SP3 and SP4
Microsoft Windows Server 2019 Standard, Datacenter. 64-bit only.	CentOS 7
Microsoft Windows 10 Professional, Enterprise, Ultimate. US English. 32-and 64-bit.	Oracle Linux 6.1–6.6, 7.0–7.1
Microsoft Windows Server 2022 Standard, Datacenter. 64-bit only.	

AWS Regions & AWS GovCloud Regions

REGION NAME	REGION ID	SUPPORTED
US East (Ohio)	us-east-2	Yes
US East (N. Virginia)	us-east-1	Yes
US West (N. California)	us-west-1	Yes
US West (Oregon)	us-west-2	Yes
Africa (Cape Town)	af-south-1	Yes
Asia Pacific (Hong Kong)	ap-east-1	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes

REGION NAME	REGION ID	SUPPORTED
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Jakarta)	ap-southeast-3	Yes (Windows only)
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Paris)	eu-west-3	Yes
Europe (Stockholm)	eu-north-1	Yes
Europe (Milan)	eu-south-1	Yes
Middle East (Bahrain)	me-south-1	Yes
South America (Sao Paulo)	sa-east-1	Yes

Azure Cloud Supported Virtual Machine OSs

WINDOWS (64-BIT ONLY)	LINUX OR UNIX
Microsoft Windows Server 2012 Standard, Datacenter.	Ubuntu 14 and 16
Microsoft Windows Server 2016 Standard, Datacenter.	Red Hat Enterprise Linux 6–9
	(DR supported only for the registered machines)
Microsoft Windows 10 Professional, Enterprise, Education. US English.	CentOS 7
Microsoft Windows Server 2019 Standard, Datacenter.	Oracle Linux 6.4 – 7 (non-UEK3 and up)
Microsoft Windows Server 2022 Standard, Datacenter.	Debian 9, 10, 11. SLES 15 SP3 and SP4.

Azure Regions

REGION NAME	REGION ID	SUPPORTED
Central US	us-central	Yes
East US	us-east	Yes
East US 2	us-east-2	Yes

REGION NAME	REGION ID	SUPPORTED
North Central US	us-north-central	Yes
South Central US	us-south-central	Yes
West Central US	us-west-central	Yes
West US	us-west	Yes
West US 2	us-west-2	Yes
North Europe	europe-north	Yes
West Europe	europe-west	Yes
East Asia	asia-pacific-east	Yes
Southeast Asia	asia-pacific-southeast	Yes
Japan East	japan-east	Yes
Japan West	japan-west	Yes
Brazil South	brazil-south	Yes
Australia East	australia-east	Yes
Australia Southeast	australia-southeast	Yes
Central India	central-india	Yes
South India	south-india	Yes
West India	west-india	Yes
Canada Central	canada-central	Yes
Canada East	canada-east	Yes
UK South	united-kingdom-south	Yes
UK West	united-kingdom-west	Yes
France Central	france-central	Yes
France South	france-south	Yes
Korea Central	korea-central	Yes
Korea South	korea-south	Yes
South Africa North	south-africa-north	Yes
UAE North	uae-north	Yes

Azure Government Cloud Regions

REGION NAME	REGION ID	SUPPORTED
Virginia	US-Gov-Virginia	Yes

NOTES:

• Cloud DR is not supported as part of PowerProtect Data Manager when deployed in AWS, Azure, or GCP.

KUBERNETES

Distributions

SUPPORTED DISTRIBUTIONS	VERSIONS
All Cloud Native Computing Foundation (CNCF) certified Kubernetes distributions	1.33 – 1.35

Vendor Support

VENDOR DISTRIBUTIONS VALIDATED AND TESTED BY DELL	VERSIONS
Upstream Kubernetes	1.33 – 1.35
RedHat OpenShift	4.14 (OADP 1.3.0) (See Note 1, 2)
RedHat OpenShift	4.15, 4.16 (OADP 1.4.3) (See Note 1, 2)
RedHat OpenShift	4.17 (OADP 1.4.3) (See Note 1, 2)
RedHat OpenShift	4.18 (OADP 1.4.3) (See Note 1, 2)
RedHat OpenShift	4.19 (OADP 1.5.x) (See Note 1, 2)
RedHat OpenShift	4.20 (OADP 1.5.x) (See Note 1, 2)
RedHat OpenShift	4.21 (OADP 1.5.x) (See Note 1, 2)
Tanzu Platform, VMware Tanzu Kubernetes Grid Integrated (TKGi)	1.21 and 1.24
VMware Tanzu Kubernetes Grid (Standalone)	2.5.x
VMware Kubernetes Service (VKS)	3.0.x - 3.3.2 (vSphere 8.0, 8.0 U1, 8.0 U2, 8.0 U3) (See Note 3)
VMware Kubernetes Service (VKS)	3.3.3 (vSphere 8.0 U3g) (See Note 3)
SUSE Rancher Kubernetes Engine (RKE)	1, 2
SUSE K3s on SLE Micro	
Google Anthos (On-Premises)	
Nutanix Kubernetes Platform (NKP)	2.13.x, 2.17.x

NOTES:

• Compatibility assumes patch releases of the above versions unless stated otherwise.
• Restore to another cluster is not supported in OpenShift for namespaces using integrated registry.
• vSphere with Tanzu Supervisor Clusters is not supported for protection.
1. vSphere CSI driver storage classes with volume binding mode of WaitForFirstConsumer are not supported (for all distributions).
2. The PowerProtect Data Manager for Kubernetes User Guide provides instructions to update the OADP version.
3. Validated using: Velero vSphere Operator Version 1.6.x, 1.8.x, respectively. Velero Plugin for vSphere Version 1.4.x - 1.6.x, respectively.

Virtualization

DISTRIBUTIONS VALIDATED AND TESTED BY DELL	VERSIONS
OpenShift Virtualization	4.14 – 4.18 (OADP 1.4.3)
OpenShift Virtualization	4.19 (OADP 1.5.x)
OpenShift Virtualization	4.20 (OADP 1.5.x)
OpenShift Virtualization	4.21 (OADP 1.5.x)
SUSE Virtualization (open-source project: Harvester)	1.5.x, 1.6.x, 1.7.x

Cloud Distributions

DISTRIBUTIONS VALIDATED AND TESTED BY DELL	VERSIONS
Microsoft Azure Kubernetes Service (AKS)	
Google Kubernetes Engine (GKE)	
Amazon Elastic Kubernetes Service (EKS)	

Storage

SUPPORTED STORAGE	CSI DRIVERS
Any on-prem or cloud CSI driver with snapshot support, version 1.0 or higher	
Any on-prem or cloud storage Container Storage Interface (CSI) driver with snapshot support, version 1.0 or higher.	
*List of available CSI drivers: https://kubernetes-csi.github.io/docs/drivers.html	
*CSI support matrix for Dell Technologies storage: https://dell.github.io/csm-docs/docs/csidriver/	

CSI Drivers Validated and Tested by Dell

CSI DRIVERS VALIDATED AND TESTED BY DELL	VSPHERE VERSIONS	NOTES
vSphere Cloud Native Storage (CNS) storage for Tanzu Kubernetes guest clusters	7.0u3 (d-h), 8.0	vSphere CSI driver 2.6 to 3.1.x using FCD snapshots[1]
vSphere CNS for native K8s clusters		vSphere CSI driver 2.6 to 3.0.x using FCD snapshots[1]
OpenShift Data Foundation (ODF)		CEPH-FS[2], CEPH-RBD
PowerFlex		
PowerScale[3]		
PowerStore		

CSI DRIVERS VALIDATED AND TESTED BY DELL	VSPHERE VERSIONS	NOTES
CSI drivers without snapshot support		Example: vSAN File Services; Controller Configuration Key = k8s.ppdm.csi.nonsnapshot.storageclasses

NOTES:

• For NFS-based CSI storage, storage class with root client access enabled is required for backup. See the PowerProtect Data Manager for Kubernetes User Guide for information about protection of root squashed persistent volumes.

1. vSphere CSI driver storage classes with volume binding mode of WaitForFirstConsumer are not supported.
2. Limited support for CEPH-FS persistent volumes. Protection may fail for volumes greater than 25 GB.
3. CSI driver version for PowerScale must be 1.5 or higher and the user provided must additionally have ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE privileges. See CSI Driver for PowerScale Installation Guide for more information. The storage classes in the Kubernetes cluster should use only one PowerScale access zone.

Container Images

IMAGE	REPOSITORY	TAG
dellemc/powerprotect-k8s-controller	https://hub.docker.com/r/dellemc/powerprotect-k8s-controller/tags	20.2.0.0-14
dellemc/powerprotect-cproxy	https://hub.docker.com/r/dellemc/powerprotect-cproxy/tags	20.2.0.0-14
dellemc/powerprotect-velero-dd	https://hub.docker.com/r/dellemc/powerprotect-velero-dd/tags	20.2.0.0-14
velero/velero	https://hub.docker.com/r/velero/velero/tags	v1.18.0

EXTERNAL COMPONENTS & SERVICES

Authentication

TYPE	SUPPORTED AUTHENTICATORS AND PROVIDERS
Multi-factor authentication (MFA)	RSA SecureID, Microsoft Authenticator, Google Authenticator
Single sign-on (SSO)	Okta, AzureFS (EntraID), PingOne

Avamar

AVAMAR VERSION	INTEGRATED DATA PROTECTION APPLIANCE VERSION
19.7 – 19.12	2.7.9

NOTES:

• Avamar and IDPA is End of Life

SupportAssist

GATEWAY	GATEWAY VERSION
SCG	5.10 and higher

NOTES:

• SRS and SAE gateways are not supported by SupportAssist 4.0 and higher. Update these gateways to SCG before you update PowerProtect Data Manager.

• Alternatively, you can configure SupportAssist by connecting directly to the backend.

Syslog Forwarding

PROTOCOL	RSYSLOG VERSION
UDP	8.24.0 - 8.2406.0
TCP	8.24.0 - 8.2406.0
TLS	8.24.0 - 8.2406.0

NOTES:

• When you use TLS, the installed versions of rsyslog-gnutls and rsyslog must match.

PowerProtect Data Manager E-Lab — Compatibility Guide

This document was generated automatically by PowerProtect Hub.

© 2026 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.