PassQueen
a.k.a dumpsqueen.com

Specialist - Systems Administrator PowerProtect DD Exam

EMC DES-DD33

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, PowerProtect DD Concepts	22
Topic 2, PowerProtect DD Configuration	21
Topic 3, PowerProtect DD Administration	9
Topic 4, PowerProtect DD Data Protection	15
Topic 5, PowerProtect DD Security	10
Topic 6, PowerProtect DD Maintenance	2
Total	79

QUESTION NO: 1

Which DD Boost capabilities can be used by supported backup applications to optimize backup and replication workflows? (Choose all that apply.)

A. Distributed segment processing

B. Managed file replication

C. Client-direct backup

D. CIFS session persistence

E. VTL tape emulation

ANSWER: A B C

Explanation:

Distributed segment processing allows the backup host to identify duplicate segments before sending data to the PowerProtect DD system, reducing backup-network traffic. **Managed file replication** allows supported backup applications to control replication between PowerProtect DD systems. **Client-direct** backup enables supported clients to send backup data directly to the PowerProtect DD system while the backup application retains control of the job.

CIFS and NFS are standard file-access protocols rather than DD Boost optimization capabilities. VTL emulation is a separate tape-oriented feature. Dell provides DD Boost information through the PowerProtect DD Boost overview.

QUESTION NO: 2

An administrator is preparing a PowerProtect DD system for integration with a backup application through DD Boost.

Which actions are required on the PowerProtect DD system? (Choose all that apply.)

A. Enable DD Boost

B. Create a DD Boost storage unit

C. Create an NFS export

D. Enable VTL

E. Create a CIFS share

ANSWER: A B

Explanation:

DD Boost must be enabled on the PowerProtect DD system before a supported backup application can use the DD Boost protocol. The administrator must also create a DD Boost storage unit, which provides the logical target that is configured in the backup application.

An NFS export or CIFS share is not required for a DD Boost storage-unit deployment because DD Boost uses its own application integration protocol. VTL configuration is also unrelated to DD Boost file-based backup operations. Dell documents DD Boost configuration and storage-unit management in the PowerProtect DDOS Administration Guide.

QUESTION NO: 3 - (SIMULATION)

What is the correct sequence of steps to configure storage for Dell EMC Cloud Tier in the DD System Manager?

ANSWER: See the explanation for the answer

Explanation:

Correct sequence:

1. In DD System Manager, open **Data Management > File System > Cloud Tier** (the exact menu can be shown as **Administration > Cloud Tier** in some DDOS releases).
2. Create or select the **cloud provider profile**. Enter the provider type and its authentication information, such as the access key/secret, tenant credentials, endpoint, and certificate details if required.
3. Create a **Cloud Unit**. Select the provider profile, then specify the target cloud storage location (bucket/container), region/endpoint, and the required storage class.
4. Configure Cloud Unit protection options, including **encryption** and the associated key-management settings when encryption is required, then validate/test the connection and save the Cloud Unit.
5. Configure the **data-movement policy** for the Cloud Tier (for example, age/space threshold and schedule) and enable/run data movement to tier eligible data to the newly created Cloud Unit.

In short: `Provider credentials/profile → Cloud Unit (bucket or container) → encryption/connection validation → data-movement policy → tier data.`

A Cloud Unit cannot be created until the cloud provider credentials/profile and target object-storage location are available. Creating the Cloud Unit makes the cloud storage available to the DD file system; the data-movement policy controls when eligible data is moved to Cloud Tier.

QUESTION NO: 4

What is the maximum number of concurrently active MTrees that are supported on any PowerProtect DD appliance with DDOS 7.3?

A. 64

B. 100

C. 256

D. 512

ANSWER: C

Explanation:

256 is the maximum number of concurrently active MTrees supported by any PowerProtect DD appliance running DDOS 7.3. An MTree is a logical partition of the DD filesystem used to separate data, apply retention and replication policies, and organize protection workloads. The concurrent-active-MTree limit is specifically the number of MTrees that can be active at the same time, rather than merely created or configured in the filesystem.

Dell's PowerProtect DD platform specifications identify 256 as the applicable upper bound for concurrently active MTrees on systems supporting DDOS 7.3. This appliance-wide maximum is important during capacity and workload planning: administrators should account for all protection applications, tenants, replication targets, and operational workflows that may require MTrees to be active simultaneously. Keeping the design within this limit helps ensure the configuration remains within the supported operating envelope for DDOS 7.3.

See Dell's PowerProtect DD technical specifications and the PowerProtect DD documentation library for platform documentation and release-specific guidance.

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

What are the steps to configure the Retention Lock Compliance?

Select and Place:

ANSWER:

Explanation:

Retention Lock Compliance is enabled through an ordered, security-controlled workflow because it establishes a configuration intended to protect retained data from alteration or deletion before its retention period expires. Start by creating iDRAC users. iDRAC provides the required out-of-band platform management access used as part of preparing the appliance for this compliance-capable configuration. Next, add one or more security officer users. These users provide the separated security authority required for sensitive Retention Lock Compliance operations.

After the required identities exist, configure the system to use DD Retention Lock Compliance. This prepares the DD system for the Compliance operating model before the irreversible compliance capability is switched on. The next action is to enable security officer authorization. Enabling this authorization ensures that protected configuration actions require the designated security-officer control, rather than relying only on a standard administrative session. This is a key safeguard for the compliance workflow and supports the separation of duties expected when retention settings must be protected.

Only after the platform users, security officers, system configuration, and security-officer authorization are in place should DD Retention Lock Compliance be enabled on the system. At that point, the system has the necessary management access and authorization controls to activate the feature safely. Dell describes PowerProtect DD as a data-protection platform with capabilities for secure retention and governance; see the Dell PowerProtect DD Series page and the Dell PowerProtect DD documentation portal for product documentation and administration resources.

QUESTION NO: 6

A source PowerProtect DD system replicates an MTree to a destination system over a WAN link.

How does PowerProtect DD reduce the amount of data sent during replication?

A. Only unique segments not present on the destination are transferred

B. All files are copied as full images

C. Only compressed files are transferred

D. The destination retrieves data directly from the backup client

ANSWER: A

Explanation:

PowerProtect DD replication is deduplication-aware and transfers only unique segments that are not already available on the destination system. Segment references and metadata are used for data that the destination already has, reducing WAN bandwidth consumption and replication time.

This behavior is a key advantage of replicating between PowerProtect DD systems. The source and destination systems maintain the information necessary to reconstruct the replicated files while avoiding repeated transfer of duplicate data. Dell describes PowerProtect DD replication capabilities in the PowerProtect DD appliance overview.

QUESTION NO: 7

What is a requirement to use the PowerProtect DD HA feature?

A. A single set of shared storage

B. Dual set of shared storage configuration

C. Head units and notes require an active/active configuration

D. Each head unit requires its own FS25 shelf

ANSWER: B

Explanation:

A dual set of shared storage configuration is required for PowerProtect DD High Availability. PowerProtect DD HA is designed as a two-controller, active/standby solution in which the controller pair must be able to access the storage needed to preserve data availability through a controller failover. The shared-storage design provides the common capacity and data access foundation that lets the standby controller assume service when the active controller is unavailable, while maintaining the DD system's protection and availability characteristics. HA deployment also requires compatible, supported hardware and software configurations, plus the appropriate network and cabling design, but the dual shared-storage arrangement is the fundamental storage requirement described by this answer. Dell's PowerProtect DD platform information identifies high availability as an enterprise resiliency capability, and Dell documentation should be consulted for the precise supported HA hardware combinations, shelf layouts, and DDOS release requirements before implementation. See the Dell PowerProtect DD Series overview and the Dell PowerProtect DD documentation portal for current platform-specific configuration documentation.