Dell EMC
D-PDM-DY-23
Dell PowerProtect Data Manager Deploy 2023

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

What unit of time does the "backup once every" field display when configuring a PowerProtect Data Manager disaster recovery backup?

A. Days
B. Weeks
C. Minutes
D. Hours

Answer: D

Explanation:
In Dell PowerProtect Data Manager (PPDM), protecting the application itself is a critical administrative task. This is handled through the Server Disaster Recovery (DR) backup configuration. When an administrator navigates to Infrastructure > Disaster Recovery to set up or edit the DR backup schedule, the system requires a frequency to be defined for the backup of the PPDM metadata and configuration database.
The Schedule Field: The specific field labeled "Backup Once Every" is designed to ensure that the system state is captured frequently enough to meet the Recovery Point Objective (RPO) of the management plane.
The Unit: According to the PPDM Administration Guide, this field is expressed in Hours. By default, it is often set to 8 or 12 hours, but it can be adjusted by the user within the allowed numerical range (typically 1 to 24 hours).
Storage Target: These DR backups are sent to a pre-configured PowerProtect DD (Data Domain) system to ensure that, in the event of a total PPDM VM failure, the environment can be restored using the ISO and the metadata stored on the protection storage.
Setting this in hours allows for a more granular protection cycle than "Days" or "Weeks," which would be insufficient for a dynamic environment where protection policies and assets change throughout the day.

Question: 2

Which two user roles can be used to initiate a successful Dell PowerStore file restore in PowerProtect Data Manager?

A. Backup Administrator
B. User
C. Restore Administrator
D. Administrator

E. Security Administrator

Answer: C, D

Explanation:
PowerProtect Data Manager utilizes Role-Based Access Control (RBAC) to ensure that only authorized users can perform specific tasks. When performing recovery operations, especially specialized ones like a PowerStore file-level restore, the system verifies the permissions associated with the logged-in account.
Administrator: This role has unrestricted access to the PowerProtect Data Manager system. It includes the ability to manage infrastructure, protection policies, and initiate any restore operation across all asset types.
Restore Administrator: This specific role is designed for users whose primary responsibility is data recovery. Users assigned this role can browse protected assets and initiate restore jobs, but they lack the permissions to change system-wide settings or security configurations.
Other roles like Backup Administrator are primarily focused on the creation and management of protection policies, while the Security Administrator manages certificates and user access but does not typically handle the data restoration workflow.

Question: 3

Which NAS devices can be protected by PowerProtect Data Manager?

A. Dell Unity and Dell ECS
B. Dell PowerFlex and Dell PowerVault
C. Dell PowerScale and Dell Unity
D. Dell PowerStore and Dell PowerFlex

Answer: C

Explanation:
Dell PowerProtect Data Manager provides high-performance, efficient protection for Network Attached Storage (NAS) environments. While PPDM continues to expand its compatibility matrix, its core NAS integration focuses on Dell's primary NAS platforms:
Dell PowerScale (Isilon): PPDM integrates with PowerScale to provide scalable protection, leveraging the platform's ability to handle massive amounts of unstructured data.
Dell Unity: PPDM supports protection for Unity NAS file systems, allowing for efficient snapshots and backups of file-based workloads.
While Dell PowerStore also has NAS capabilities that PPDM can protect, the specific pairing of PowerScale and Unity represents the foundational supported NAS assets highlighted in the PPDM Integration and Administration guides for specialized NAS protection workflows. Dell ECS is primarily an object storage platform, and PowerFlex is a Software-Defined Storage (SDS) platform primarily focused on block storage.

Question: 4

What is the default approximate slice size setting parameter of the PowerProtect Data Manager NAS Slicer?

A. 100 GB
B. 200 GB
C. 300 GB
D. 400 GB

Answer: A

Explanation:
To solve the challenges associated with backing up large NAS environments (which often contain millions of small files), PowerProtect Data Manager introduced Dynamic NAS (DNAS) Protection.
A key technology within DNAS is the NAS Slicer. Instead of treating a large NAS share as a single serial stream, the NAS Slicer breaks the file system down into smaller, manageable units called "slices."
Default Slice Size: By default, the NAS Slicer is configured to create slices of approximately 100 GB.
Parallelism: These 100 GB slices allow PPDM to distribute the backup workload across multiple protection engines (vProxies) simultaneously. This parallel processing significantly improves throughput and reduces the time required to complete the backup (the backup window).
Functionality: If a specific folder or subtree is larger than 100 GB, the slicer identifies logical break points to maintain these balanced units, ensuring that no single stream becomes a bottleneck for the entire protection job.

Question: 5

An administrator wants to design a PowerProtect Data Manager solution for a Kubernetes cluster. What are the design considerations?

A. A Kubernetes namespace resides on both CSI and non-CSI-based storage and can be backed up.
B. Kubernetes cluster can be discovered and backed up.
C. Kubernetes namespace can be discovered and backed up.

Answer: C

Explanation:
In Dell PowerProtect Data Manager, the primary unit of protection for Kubernetes is the Namespace. While the Kubernetes cluster itself is added as an Asset Source, the discovery process identifies the individual namespaces within that cluster as protectable assets.
Discovery and Protection: Once the Kubernetes cluster is connected using the discovery IP and credentials, PPDM communicates with the API server to list all namespaces. Administrators can then create protection policies targeting specific namespaces.
Storage Requirements: A critical design consideration is that PPDM requires Container Storage

Interface (CSI) drivers to facilitate volume snapshots. If a namespace contains volumes residing on non-CSI storage, those specific volumes cannot be backed up by PPDM. Therefore, ensuring the application uses CSI-compliant storage is a prerequisite for successful namespace protection.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/