DUMPSBOSS.

Dell PowerScale Deploy 2023

EMC D-PSC-DY-23

Version Demo

Total Demo Questions: 12

Total Premium Questions: 124

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Plan	23
Topic 2, Prepare	2
Topic 3, Install	3
Topic 4, Configure	64
Topic 5, Validate	2
Topic 6, Manage	30
Total	124

QUESTION NO: 1

When reconciling permissions (or clients using UNIX as well as Microsoft Windows systems, what describes the scope of the permissions?

A. Windows ACLs and POSIX bits have overlapping semantics, but neither completely reflects the other

B. POSIX bits have semantics that are a subset of Windows ACLs. but Windows ACLs are more extensive

C. Windows ACLs have semantics that are a subset of POSIX bits

D. POSIX bits and Windows ACLs are semantically equivalent

ANSWER: A

Explanation:

Windows ACLs and POSIX bits have overlapping semantics, but neither completely reflects the other. In a mixed UNIX and Windows environment, both permission models can express fundamental access decisions such as allowing or denying access to files and directories, and both can represent common read, write, and execute-style controls. This overlap enables OneFS to present and evaluate permissions for clients using either protocol. However, the models are not interchangeable. POSIX mode bits provide owner, group, and other classes with a limited set of permissions, while Windows NTFS ACLs use access control entries that can apply to individual users and groups, include allow and deny rules, support inheritance, and define a substantially richer set of access rights. Conversely, the effective behavior seen by UNIX clients is also affected by UNIX identity and permission semantics. Therefore, reconciliation is required because a direct, lossless representation of every permission from one model in the other is not possible. OneFS supports multiprotocol access and maintains the appropriate permission information so that access can be evaluated consistently according to the protocol and security model in use. See Dell's PowerScale authentication, identity management, and authorization guidance and the PowerScale OneFS documentation.

QUESTION NO: 2

In a Dell PowerScale environment, what is a requirement to join multiple, untrusted Active Directory (AD) authentication sources to an access zone?

A. All untrusted AD provider instances must exist in all access zones

B. Only one of the AD provider instances can exist in a zone at one time

C. A common / ' ifs tree is required for all access zones

D. Must only join Active Directory domains in the same forest

ANSWER: D

Explanation:

Must only join Active Directory domains in the same forest is correct because OneFS supports associating multiple Active Directory authentication-provider instances with an access zone only when the AD domains are members of one forest. A common forest provides the forest-wide directory and trust framework that OneFS relies on when it resolves identities and authenticates users across the configured domains. This allows OneFS to consistently obtain user and group information, including security identifiers and group membership, through the authentication configuration assigned to the zone.

In deployment planning, the forest boundary is therefore a key design constraint for an access zone that requires more than one AD provider. Administrators should identify the target AD forest, confirm that the required domains are part of that forest, and then configure the corresponding provider instances for the zone. This design also helps ensure that access-zone authentication behavior remains predictable for SMB clients and for authorization decisions based on AD identities. Dell's PowerScale documentation resources provide OneFS administration and identity-management guidance at Dell PowerScale OneFS documentation and the Dell Technologies Info Hub.

QUESTION NO: 3

An administrator deletes a large directory from the active file system. The directory was included in a SnapshotIQ snapshot that is still retained. The administrator expects the deletion to immediately return all of the directory capacity to the cluster.

What will occur?

A. The directory capacity is released when the next FlexProtect job completes.

B. The directory capacity remains in use until the snapshot no longer references the data.

C. The directory capacity is released when SnapshotIQ creates the next snapshot.

D. The directory capacity is moved automatically to the virtual hot spare reservation.

ANSWER: B

Explanation:

The deleted data blocks remain allocated while the retained snapshot references them. SnapshotIQ preserves a point-in-time view of the directory, so OneFS cannot release blocks that are required to present the deleted files through that snapshot. Capacity is reclaimed only after the relevant snapshots are deleted or expire.

The active namespace no longer displays the directory, but deleting it does not override the snapshot retention requirement. Running a FlexProtect job or changing the file protection level does not release snapshot-referenced blocks.

QUESTION NO: 4

What is the maximum supported node limit with a Dell PowerScale Gen 6 cluster running OneFS 9.4?

A. 400 nodes

B. 252 nodes

C. 144 nodes

D. 288 nodes

ANSWER: B

Explanation:

The maximum supported cluster size is **252 nodes** for a Dell PowerScale Gen 6 cluster running OneFS 9.4. Dell documents platform and release-specific scalability limits in the OneFS support and configuration documentation; the supported maximum is a cluster-level limit, not merely a count based on a particular node type or pool. This limit applies to the complete PowerScale/Isilon cluster and must be considered during initial architecture, node-addition planning, capacity forecasting, and SmartPools tier design. Remaining within the documented node-count limit is important because OneFS distributes metadata, protection, and cluster-management functions across the entire node membership, and Dell qualification defines the supported operational boundary for that software release and hardware generation. Before expanding an installed environment, administrators should also validate the precise hardware mix, OneFS release, and upgrade path against the applicable Dell support matrix and release documentation. Dell's PowerScale documentation portal provides the authoritative documentation set for OneFS 9.4, including support information and release materials: Dell PowerScale OneFS 9.4 documentation. Dell's PowerScale product documentation landing page is also a central source for current and historical platform documentation: Dell PowerScale documentation.

QUESTION NO: 5

An administrator wants to create an S3 bucket in a non-System access zone using the CLI What Information is required to perform this operation?

A. Bucket path, bucket name, and access zone

B. Bucket name, access zone, and ACLs

C. Bucket path, access zone, and ACLs

D. Bucket name, bucket path, and bucket owner

ANSWER: D

Explanation:

Bucket name, bucket path, and bucket owner is correct. When an S3 bucket is created through the OneFS CLI, the administrator supplies a unique bucket name and the OneFS filesystem path that will store the bucket's objects. The bucket path establishes the backing directory in /ifs and must be suitable for the access zone's data-access configuration. A bucket owner is also required for a bucket in a non-System access zone. The owner associates the bucket with an identity that belongs to the applicable access zone, allowing OneFS to determine the access-zone context and apply the appropriate authentication and authorization behavior for S3 requests. In this workflow, the access zone is established through the owner's identity and its configured zone membership rather than being provided as a separate bucket-create requirement. ACL settings can be applied to control bucket access after creation, but they are not part of the core identifying information required to create the bucket. Dell's PowerScale S3 documentation describes the relationship between S3 buckets, their filesystem paths, and access-zone-aware identities. See the Dell PowerScale OneFS S3 and S3-compatible object storage guide and the Dell PowerScale S3 configuration guide.

QUESTION NO: 6

In addition to the policy name, what information is required to create a new file pool policy on a Dell Power Scale cluster?

A. Storage target only

B. File matching criteria and storage target

C. File matching criteria only

D. Storage target and snapshot target

ANSWER: B

Explanation:

File matching criteria and storage target is correct because a PowerScale file pool policy must define both the files to which the policy applies and the destination pool in which those files should reside. The matching criteria identify the files based on attributes such as path, filename pattern, file type, owner, access time, modification time, size, or user-defined metadata. The storage target identifies the file pool that is selected for those matching files. A file pool represents a logical storage tier built from one or more node pools, allowing SmartPools to place data on storage with the desired performance, protection, and capacity characteristics. Together, these details make the policy actionable: PowerScale can evaluate files against the criteria and then use the selected pool as the placement objective during file-pool evaluation, restriping, or related SmartPools operations. The policy name is simply the identifier used to manage and prioritize the policy; it does not establish either file selection or intended placement. Dell's PowerScale documentation describes file pool policies as rules consisting of matching criteria and a target file pool. See the Dell PowerScale SmartPools technical overview and the Dell PowerScale OneFS documentation portal for configuration guidance.

QUESTION NO: 7

Which data access pattern uses a highly aggressive prefetch caching algorithm?

A. Parallel

B. Concurrency

C. Random

D. Streaming

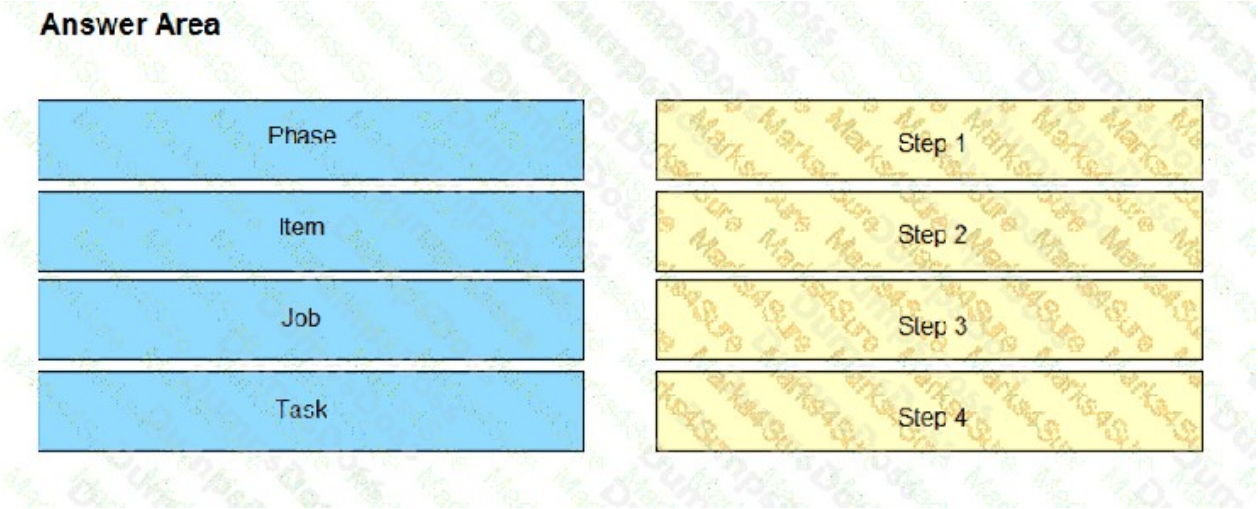
ANSWER: D

Explanation:

Streaming is the data access pattern that uses a highly aggressive prefetch caching algorithm. It is intended for workloads that read a file sequentially, generally from beginning to end, such as media playback, video processing, backup reads, large-file analytics, and other throughput-oriented operations. After OneFS recognizes sequential reads, the streaming access pattern proactively brings subsequent portions of the file into cache before the client explicitly requests them. This aggressive read-ahead behavior reduces wait time for later reads and helps sustain high sequential-read throughput. The setting is therefore appropriate when the workload has predictable forward read behavior and can benefit from having upcoming file data ready in memory. Dell PowerScale documentation describes access-pattern controls as mechanisms for tuning caching and read-ahead behavior to the expected application I/O pattern; administrators should apply Streaming when observed workload behavior is predominantly sequential. See the Dell PowerScale OneFS documentation portal at Dell PowerScale OneFS Documentation and Dell Technologies Info Hub resources at Dell Technologies Info Hub.

QUESTION NO: 8 - (SIMULATION)

What is the correct hierarchy of the Job elements structure?



ANSWER: See the explanation for the answer

Explanation:

The correct Job Engine element hierarchy, from highest level to lowest level, is:

Therefore, place **Job** in Step 1, **Phase** in Step 2, **Task** in Step 3, and **Item** in Step 4.

A job is divided into phases; each phase contains tasks; and tasks process individual work items.

QUESTION NO: 9

What is the recommended number of SmartConnect zone delegations on a cluster?

A. 8

B. 1

C. 2

D. 16

ANSWER: C

Explanation:

The recommended number of SmartConnect zone delegations on a PowerScale cluster is **2**. This design provides separate delegated namespaces for the cluster's SmartConnect service while supporting a resilient and manageable name-resolution configuration. A SmartConnect zone delegation lets the authoritative parent-domain DNS infrastructure direct client queries for the delegated PowerScale namespace to the cluster's SmartConnect service IP addresses. SmartConnect then returns an appropriate pool IP address according to the configured connection-balancing policy and the state of the nodes in that pool.

Using two delegations is a documented deployment best practice because it provides redundancy in DNS referral and avoids relying on a single delegation path for client access. The delegations should be configured in the parent DNS zone and should point to SmartConnect service IP addresses that are reachable by clients and DNS resolvers. This approach complements SmartConnect's role in distributing client connections and helping clients reconnect to available nodes when cluster membership or node availability changes. For implementation and DNS delegation guidance, see the PowerScale OneFS Networking documentation and Dell's SmartConnect DNS delegation knowledge-base guidance.

QUESTION NO: 10

How many Active Directory provider instances can be configured per access zone?

A. 1

B. 2

C. 3

D. 4

ANSWER: A

Explanation:

Exactly **1** Active Directory provider instance can be configured for an individual PowerScale access zone. In OneFS, an access zone creates a defined authentication and namespace boundary, and its authentication providers are configured in the context of that zone. The Active Directory provider supplies AD domain authentication and identity services for clients and users associated with the access zone. Limiting a zone to one AD provider ensures that the zone has one unambiguous AD-domain configuration for operations such as user and group lookups, Kerberos-based authentication, SID-to-UID/GID mapping, and domain-controller discovery. If an environment needs separate AD domain configurations or separate authentication contexts, the normal design approach is to create and configure additional access zones, each with its own provider configuration, rather than attach multiple AD provider instances to one zone. This model supports tenant, department, workload, or security-boundary separation while preserving predictable identity resolution within each zone. Dell's OneFS administration documentation describes access-zone authentication-provider configuration and the Active Directory provider model: Dell PowerScale OneFS Web Administration Guide. See also Dell's PowerScale documentation portal: PowerScale OneFS Info Hubs.

QUESTION NO: 11

A Dell PowerScale administrator wants to create a new SMB share on an existing directory structure. The directory contains migrated production data and has an active NFS export What will happen if the administrator selects the Apply Windows default ACLs option during creation?

A. Existing mode bit rights are overwritten by the Windows default ACLs

B. Creation of the SMB share fails due to the existing mode bit rights

C. Windows default ACLs are merged with the existing mode bit rights

D. Windows default ACLs are overwritten by the existing mode bit rights

ANSWER: A

Explanation:

Existing mode bit rights are overwritten by the Windows default ACLs is correct. In OneFS, selecting *Apply Windows default ACLs* when creating an SMB share applies the Windows-style default security descriptor to the share's existing root directory. This is significant when the target directory already contains migrated production data and is used through NFS, because the directory may currently have POSIX mode-bit permissions rather than a Windows access-control list. Applying the Windows defaults replaces the directory's existing permissions representation with the Windows default ACL, allowing SMB clients to use Windows ACL semantics at that share root. The operation is not merely a display setting for the new share; it modifies the permissions on the existing directory that is selected as the share path. Administrators should therefore evaluate the impact on cross-protocol access before enabling it, particularly where NFS clients rely on the existing ownership and mode permissions. Dell's PowerScale documentation describes SMB share configuration and Windows ACL behavior in its OneFS protocol documentation: Dell PowerScale OneFS documentation. General Dell PowerScale product and support resources are available at Dell PowerScale.

QUESTION NO: 12

Which is statistics subcommand is used to display the most commonly accessed flics and directories in a file system?

A. system

B. heat

C. history

D. current

ANSWER: B

Explanation:

The **heat** subcommand is used with the OneFS `isi statistics` command to identify the most frequently accessed files and directories in a file system. In this context, "heat" represents access activity: OneFS gathers and presents file-system access information so an administrator can see which paths are receiving the greatest demand. This is useful when investigating workload behavior, locating heavily used data, and making informed decisions about performance tuning or data-placement policies. The command can report access patterns for files and directories, helping distinguish broad directory-level activity from concentrated activity on specific files. Because this information is based on observed protocol access activity, it provides practical operational insight into active data rather than merely displaying system-wide counters or historical configuration information. Dell documents `isi statistics` as the OneFS CLI facility for viewing statistical data and includes heat-related reporting among its file-system analysis capabilities. Refer to the Dell OneFS CLI Administration Guide and Dell's PowerScale technical documentation resources for the applicable command syntax and release-specific output details.