PassQueen
a.k.a dumpsqueen.com

Expert - PowerMax and VMAX All Flash Solutions

EMC DEE-1111

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, PowerMax and VMAX All Flash Concepts	10
Topic 2, PowerMax and VMAX All Flash Configuration	5
Topic 3, PowerMax and VMAX All Flash Management	25
Topic 4, PowerMax and VMAX All Flash Local Replication	5
Topic 5, PowerMax and VMAX All Flash Remote Replication	29
Total	74

QUESTION NO: 1

An organization has PowerMax systems on three sites. They plan to implement SRDF/Star to provide remote protection.

What is a restriction for an SRDF/Star configuration?

A. The asynchronous PowerMax requires twice the SRDF directors compared to the two synchronous arrays

B. All the SRDF Groups must be defined and in suspended state

C. SRDF Groups cannot be shared between SRDF/Star configurations

D. All SRDF/Star device pairs must be of the same geometry and size

ANSWER: D

Explanation:

All SRDF/Star device pairs must be of the same geometry and size. SRDF/Star provides three-site disaster-recovery protection by combining concurrent SRDF relationships: a synchronous relationship from the production array to the synchronous target and an asynchronous relationship to the third, remote target. During an SRDF/Star operation, the involved devices represent corresponding copies of the same application data across the participating arrays. Matching device geometry and capacity are therefore required so that each track address and extent represented at one site maps consistently to its counterparts at the other sites. This consistency is essential when SRDF/Star transitions its protection state following a site failure, because the configuration must preserve a recoverable, restartable copy of the application data at the appropriate target array. Before establishing the SRDF/Star environment, administrators should provision equivalent devices on each array and ensure that the RDF pairing is built using devices with identical sizes and compatible geometry. Dell documents SRDF/Star requirements and operational behavior in the Solutions Enabler SRDF Family CLI User Guide. Dell's PowerMax and VMAX All Flash SRDF overview and best practices also provides context on SRDF replication designs and consistency requirements.

QUESTION NO: 2

A host HBA is replaced during a server maintenance activity. The host continues to use the same PowerMax devices and Storage Group, but it can no longer access the volumes after the replacement. The new HBA WWPNs are correctly zoned to the intended PowerMax front-end ports.

What should be updated on the PowerMax array?

A. The Storage Resource Pool associated with the Storage Group

B. The Initiator Group in the Masking View

C. The Service Level assigned to the Storage Group

D. The TDAT allocation of the presented devices

ANSWER: B

Explanation:

The Initiator Group in the Masking View should be updated with the new HBA initiator identifiers. Zoning provides SAN connectivity, but PowerMax presentation is controlled by the Masking View. The Initiator Group must contain the active host initiators for the array to present the Storage Group devices through the associated Port Group.

Recreating the Storage Group or changing the Service Level does not add the new host initiators to the presentation configuration. Modifying the Storage Resource Pool affects device capacity placement and is unrelated to host access.

QUESTION NO: 3

A compliance team requires a point-in-time copy to be retained for 30 days. Storage administrators must not be able to terminate the copy accidentally before the retention period expires.

Which SnapVX capability should be used?

A. Create a standard snapshot and link it to a target

B. Create an SRDF/A cycle for the Storage Group

C. Create a copy-mode linked target

D. Create a Secure Snapshot with the required expiration time

ANSWER: D

Explanation:

Create a Secure Snapshot with the required expiration time is correct. Secure Snapshots provide retention protection for a defined period and prevent premature termination of the snapshot. This supports workflows in which the snapshot must remain available for compliance, investigation, or recovery purposes.

A regular snapshot can be terminated by an authorized administrator before the required retention period. A linked target provides host access to snapshot data but does not itself enforce immutable snapshot retention. An SRDF/A cycle provides remote replication consistency and is not a local snapshot-retention control.

QUESTION NO: 4

An SRDF/Metro device pair was in an ActiveActive state. A link failure between arrays occurs. The application continues running on the R1 side, and the link failure is addressed.

What is the current state of the Metro device pair?

A. Suspended

B. Active Bias

C. Active Active

D. Partitioned

ANSWER: B

Explanation:

Active Bias is the current SRDF/Metro state. SRDF/Metro normally presents both sides of a pair as read/write accessible while it is operating in ActiveActive mode. When the SRDF link between the two arrays fails, the Metro personality uses its configured bias to prevent simultaneous, independent writes at both sites. In this scenario, the R1 side is the biased side and remains ready and writable, allowing the application to continue without interruption. The R2 side is made not ready to its hosts, so it cannot accept writes while inter-array communication is unavailable. This controlled outcome is represented by the Active Bias Metro state: one side remains active based on the pair's bias setting, while the other side is unavailable for host I/O. The state protects data consistency and avoids a split-brain condition during the communication outage. Dell PowerMax documentation describes SRDF/Metro behavior and its high-availability design in the PowerMax documentation library. Additional Dell SRDF/Metro technical resources are available through the SRDF/Metro overview.

QUESTION NO: 5

An administrator is trying to view the SLO Compliance Report but is unable to find data for an issue that occurred 7 months ago.

What is the maximum retention period?

A. Last month

B. Last 2 weeks

C. 6 months

D. 3 months

ANSWER: C

Explanation:

6 months is the maximum retention period available for SLO Compliance Report data in Unisphere for PowerMax. The report uses the array's stored performance and compliance history to show whether a storage group met the response-time target associated with its service-level objective over the selected reporting interval. This historical reporting capability is limited to a six-month window. Consequently, an event that occurred seven months ago has aged out of the SLO compliance reporting history and cannot be retrieved through that report. Administrators investigating older events should rely on records retained outside this reporting window, such as exported reports, monitoring-platform history, operational logs, or incident documentation. For current and recent investigations, the SLO Compliance Report remains the appropriate Unisphere feature for reviewing compliance trends and identifying periods in which workload behavior did not meet the configured objective. Dell's Unisphere for PowerMax documentation and product-support documentation provide the applicable reporting and monitoring guidance: Dell Unisphere for PowerMax documentation and Dell PowerMax storage overview.

QUESTION NO: 6 - (SIMULATION)

Match Dual Personally SRDF device to its usage SRDF role.

ANSWER: See the explanation for the answer

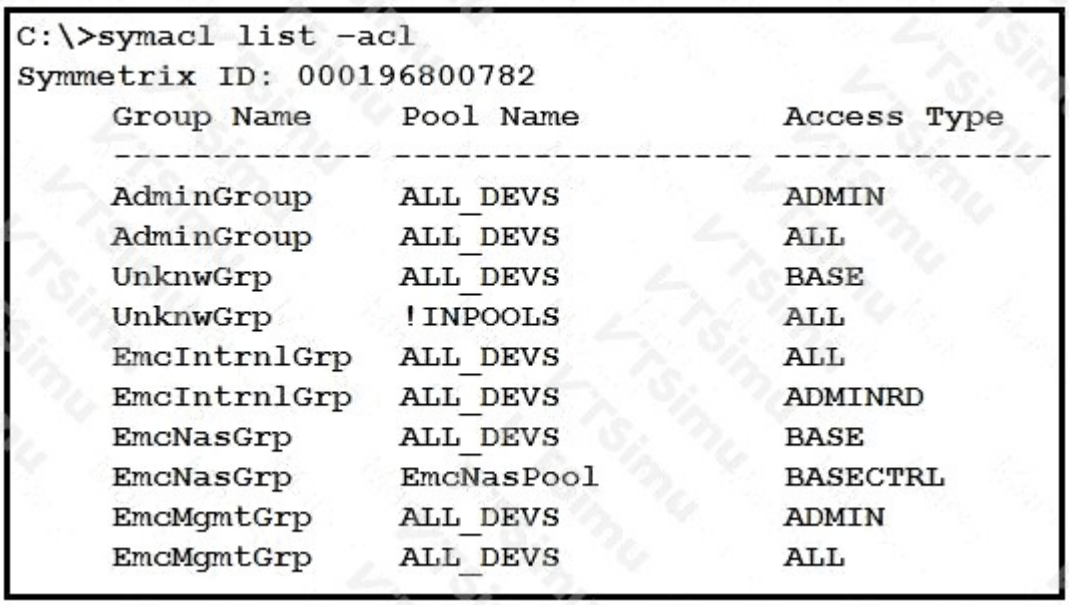
Explanation:

Match the dual-personality SRDF device types as follows:

SRDF device used for Concurrent SRDF environments: `R11`
SRDF device used for SRDF/Star environments: `R22`
SRDF device used for Cascaded SRDF environments: `R21`

`R11` has two R1 personalities for concurrent replication. `R22` has two R2 personalities and is used by SRDF/Star. `R21` is an R2 in one RDF relationship and an R1 in another, enabling the intermediate array role in cascaded SRDF.

QUESTION NO: 7



```
C:\>symacl list -acl
Symmetrix ID: 000196800782
     Group Name     Pool Name           Access Type
     -------------- ------------------- --------------
     AdminGroup     ALL_DEVS            ADMIN
     AdminGroup     ALL_DEVS            ALL
     UnknwGrp       ALL_DEVS            BASE
     UnknwGrp       !INPOOLS            ALL
     EmcIntrnlGrp   ALL_DEVS            ALL
     EmcIntrnlGrp   ALL_DEVS            ADMINRD
     EmcNasGrp      ALL_DEVS            BASE
     EmcNasGrp      EmcNasPool          BASECTRL
     EmcMgmtGrp     ALL_DEVS            ADMIN
     EmcMgmtGrp     ALL_DEVS            ALL
```

Refer to the exhibit.

Which correctly describes a possible configuration created by SYMACL?

A. Only BASECNTROL access type

B. Hosts that are part of AdminGrp proup

C. Only ADMINRD access type

D. Physical hosts that are part of EmcMgmtGrp group

ANSWER: B

Explanation:

Hosts that are part of AdminGrp proup is the possible SYMACL configuration described by the exhibit. SYMACL is the access-control mechanism used by SYMCLI to authorize management operations originating from client hosts. Its authorization model associates client hosts with named authorization groups and assigns an access type to each group. Consequently, a host that is defined as a member of *AdminGrp* receives the permissions granted to that group when it runs SYMCLI commands against the array.

The exhibit's presence of the named *AdminGrp* authorization group therefore supports a configuration in which client hosts are members of that group. This is a normal use of SYMACL: administrators organize management hosts into groups, then grant the group the appropriate level of Symmetrix/PowerMax command authorization. Group membership provides a manageable, consistent way to apply the same administrative authorization policy to multiple hosts rather than managing each host independently. Dell Technologies PowerMax documentation and support resources covering management and security configuration are available from the PowerMax documentation page and the Dell Technologies support knowledge base.