PassQueen
a.k.a dumpsqueen.com

Dell XtremIO Operate Achievement

EMC D-XTR-OE-A-24

Version Demo

Total Demo Questions: 8

Total Premium Questions: 83

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, XtremIO Concepts	38
Topic 2, XtremIO Administration	41
Topic 3, XtremIO Maintenance	1
Topic 4, XtremIO Troubleshooting	3
Total	83

QUESTION NO: 1

After the volumes are created, which steps are required to provision the XtremIO volumes to the servers?

A. Host configuration, RAID groups, SAN connectivity, and volumes mapping

B. Host configuration, create pools, SAN connectivity, and volumes mapping

C. Host configuration, SAN connectivity, encryption, and volumes mapping

D. Host configuration, SAN connectivity, Initiator group, and volumes mapping

ANSWER: D

Explanation:

Host configuration, SAN connectivity, Initiator group, and volumes mapping are required to make XtremIO volumes available to a server. First, the server must be configured with supported Fibre Channel or iSCSI initiators and the appropriate multipathing configuration so it can reliably use multiple paths to the XtremIO X-Brick storage controllers. SAN connectivity must then be established, including appropriate switch zoning for Fibre Channel environments, so the host initiators can communicate with the XtremIO target ports. Within XtremIO, the host initiator identifiers are associated with an initiator group (also called an Initiator Group or IG). This provides the access-control object used to identify which server-side initiators are permitted to access storage. Finally, the created volumes are mapped to that initiator group. The mapping operation presents the volumes to every host initiator in the group, normally with a consistent logical unit number, after which the operating system can rescan its storage adapters and discover the new devices. This sequence ensures both physical connectivity and controlled logical access to the provisioned XtremIO storage. Dell documentation describes host connectivity, initiator groups, and volume mapping as core elements of XtremIO host provisioning. See the Dell XtremIO X2 documentation library and the Dell XtremIO Host Configuration Guide.

QUESTION NO: 2

A new application host must access only six XtremIO volumes. Other hosts in the same SAN fabric must not gain access to those volumes.

What should the administrator configure before mapping the volumes?

A. Create a consistency group containing the six volumes

B. Create a scheduler for the six volumes

C. Create an alert definition for the application host

D. Create an initiator group containing the application host initiators

ANSWER: D

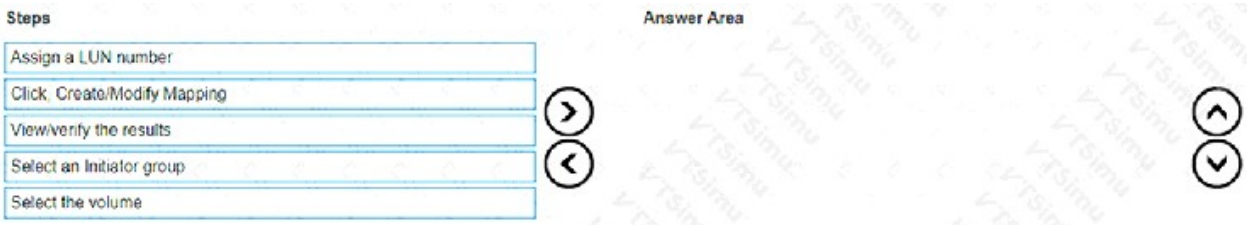
Explanation:

Create an initiator group containing the application host initiators is correct. An XtremIO initiator group associates the host initiator identities that are permitted to access mapped volumes. Mapping the six volumes to this initiator group restricts presentation to the intended application host initiators.

Creating a consistency group coordinates snapshot operations across related volumes but does not control host access. A scheduler automates operations and does not provide LUN masking. An alert definition controls notifications and has no effect on volume presentation.

QUESTION NO: 3 - (SIMULATION)

When using the XtremIO WebUI, what is the correct sequence of steps to map a volume to a host?



ANSWER: See the explanation for the answer

Explanation:

Correct sequence:

This sequence first identifies the XtremIO volume, then the host-facing Initiator Group, defines the host LUN ID, and commits the mapping. Finally, verify that the mapping was created successfully.

QUESTION NO: 4

A systems administrator has been informed that a new backup policy has been put in place for 500 production volumes on an XtremIO X2-R array. The 500 production volumes

must be backed up four times a day at 8 AM, 12 PM, 4 PM, and 10 PM daily. The backup copies must be read only using the Protection Copies feature provided by the XtremIO

6.x code.

How many days of XtremIO Virtual Copy read only volumes can the array store before the original backups are deleted?

A. 7

B. 5

C. 6

D. 8

ANSWER: D

Explanation:

8 is correct because XtremIO 6.x supports up to 32 Virtual Copies for a source volume. A Protection Copy is the read-only Virtual Copy implementation used to preserve a point-in-time image of the production data. The policy creates four Protection Copies per production volume each day: one at 8 AM, 12 PM, 4 PM, and 10 PM. Dividing the 32-copy limit by four copies created per day gives eight full days of retained read-only copies per volume. After the eighth day's four copies have been created, all 32 available Virtual Copy positions are occupied. Before the next scheduled copy is made on the ninth day, the oldest retained Protection Copy must be deleted to remain within the per-volume Virtual Copy limit. The fact that the policy applies to 500 volumes does not change this retention calculation, because the relevant limit is applied to each source volume's Virtual Copy lineage. Dell's XtremIO documentation and product documentation portal provide the operational guidance for Virtual Copies and Protection Copies: Dell XtremIO X2 documentation and Dell Technologies Info Hub.

QUESTION NO: 5

A systems administrator wants to double the throughput on an existing dual XtremIO X1 10 TB X-Brick cluster. All hosts performing I/O to the cluster are configured and tuned

according to Dell Technologies best practices.

To achieve the performance gain, what should be added?

A. A single 10 TB X-Brick Expansion Kit

B. A dual 20 TB X-Brick Expansion Kit

C. A single 20 TB X-Brick Expansion Kit

D. A dual 10 TB X-Brick Expansion Kit

ANSWER: D

Explanation:

A dual 10 TB X-Brick Expansion Kit is the appropriate addition because XtremIO performance scales out with the number of X-Bricks. The existing configuration contains two 10 TB X-Bricks. Adding another matched pair doubles the cluster from two to four X-Bricks, doubling the controller, CPU, cache, host-facing connectivity, and flash-resource contribution that collectively determine the system's available throughput. XtremIO distributes data and I/O across all X-Bricks in the cluster, so the added pair participates in servicing workloads rather than acting solely as capacity. Matching the 10 TB X-Brick type also maintains a balanced cluster configuration and is consistent with XtremIO expansion requirements for using compatible, like-sized X-Bricks. Since the hosts are already configured according to Dell Technologies best practices, the scale-out expansion directly addresses the need for additional array-side performance. Dell's XtremIO documentation describes the platform as a scale-out all-flash architecture in which X-Bricks are added in pairs to increase both performance and capacity. See the Dell XtremIO Support Matrix and the Dell XtremIO product information for XtremIO configuration and scale-out architecture information.

QUESTION NO: 6

An administrator has configured an SMTP server in the XtremIO WebUI and successfully sent a test email. Major-severity events are visible in the event list, but the storage administration team receives no email notifications.

What configuration should the administrator verify next?

A. Alert definitions

B. ESRS configuration

C. Private reports

D. Volume tags

ANSWER: A

Explanation:

Alert definitions is correct. SMTP configuration verifies that XtremIO can communicate with the email server, but alert definitions determine which events and severity levels generate notifications and identify the notification recipients. An enabled alert definition covering major-severity events is required before those events result in email messages.

QUESTION NO: 7

Which key components within XtremIO X1 provide an enterprise level of continuous availability?

A. Data Protection and Snapshots

B. Thin Provisioning and Snapshots

C. Thin Provisioning and Data Protection

D. Inline Data Deduplication and Inline Compression

ANSWER: A

Explanation:

Data Protection and Snapshots is correct because XtremIO X1 combines its distributed data-protection architecture with writable, space-efficient snapshots to support highly available enterprise operations. XtremIO Data Protection (XDP) distributes protected data across all available storage components rather than relying on conventional dedicated RAID groups. This design provides protection against drive failures while maintaining system availability and consistent performance. The array's active-active, scale-out architecture works with XDP so that data remains accessible through component-level failures and recovery activity.

XtremIO snapshots complement this protection by creating instantaneous, writable point-in-time copies without a full physical copy of the source volume. Their metadata-based implementation enables operational recovery, application testing, backup workflows, and rapid restoration while minimizing capacity and performance impact. Together, resilient distributed protection and efficient point-in-time copies address both hardware-failure resilience and data-recovery availability, which are essential aspects of continuous enterprise service. Dell's XtremIO X1 documentation is available through the Dell XtremIO X1 support documentation portal. Dell's Info Hub also provides Dell storage architecture and operational guidance.

QUESTION NO: 8

You are connecting a VMware cluster to an XtremIO array. The host will be connected to the array using QLogic Fibre Channel HBAs. Based on best practices, what is the

recommended value for the Execution Throttle?

A. 65535

B. 4096

C. 16384

D. 8192

ANSWER: B

Explanation:

The recommended Execution Throttle value is **4096**. Execution Throttle is a QLogic Fibre Channel HBA queue-control setting that limits the number of outstanding commands the adapter can issue. For VMware hosts attached to XtremIO, setting this value to 4096 is the XtremIO host-configuration best-practice value. It provides a suitably deep command queue for the highly parallel, low-latency XtremIO architecture while retaining controlled queue behavior across the host, HBA, SAN, and storage array. Correct queue-depth settings are important in an ESXi cluster because many virtual machines can issue I/O concurrently through the same physical adapters. A consistent 4096 setting on the applicable QLogic HBAs helps avoid unnecessarily restricting I/O concurrency and supports predictable performance as workload demand grows. This value should be applied as part of the overall validated host connectivity configuration, alongside the prescribed multipathing policy, HBA driver and firmware versions, and supported SAN design. Dell publishes XtremIO documentation and host-configuration material through its XtremIO product documentation page. VMware storage configuration guidance is available in the vSphere Storage documentation.