DUMPSBOSS.

Riverbed Certified Solutions Professional - Storage Delivery Exam

Riverbed 599-01

Version Demo

Total Demo Questions: 10

Total Premium Questions: 109

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which Granite appliance feature would be used to implement disconnected operations? (Select 2)

A. Pinning

B. Offlining

C. High availability

D. MPIO

E. Prepopulation

ANSWER: A E

Explanation:

Pinning and prepopulation are the Granite features used together to prepare and sustain disconnected operations at a branch site. Prepopulation proactively transfers the required storage blocks from the data-center-resident Granite Core to the Granite Edge while connectivity is available. This allows the branch to have the necessary data locally before a planned WAN outage or disconnection occurs, rather than needing to retrieve blocks on demand after the link is unavailable.

Pinning designates selected data as locally retained on the Granite Edge. Pinned blocks are protected from normal cache eviction, ensuring that the branch retains the working set needed by its servers throughout the disconnected period. In practical use, administrators prepopulate the relevant volumes or data set and pin the required blocks so applications can continue accessing local storage while the WAN connection to the Core is unavailable. These capabilities are fundamental to Granite's branch-office continuity model, in which local access is maintained and changes are later reconciled after connectivity returns. Riverbed's SteelFusion/Granite product information and documentation resources are available through Riverbed Support: SteelFusion software and Riverbed SteelFusion product information.

QUESTION NO: 2

A branch server issues a read to a projected LUN. The requested block is not resident in the Granite Edge blockstore, but the Edge-to-Core connection is available. What occurs?

A. The Granite Edge retrieves the block from the Granite Core.

B. The Granite Edge permanently offlines the LUN.

C. The host reads the block directly from the storage array.

D. The Granite Edge discards the read request.

ANSWER: A

Explanation:

The Granite Edge retrieves the required block from the Granite Core and then services the host read. The Edge blockstore is a local cache, so a cache miss does not prevent normal access when the Core is reachable. After the block is obtained, it can be retained in blockstore according to the applicable cache and pinning policies. This allows the branch host to access centrally hosted storage through the local Granite Edge iSCSI presentation while Granite handles the remote block retrieval.

Release-specific Granite and SteelFusion administration guidance is available through the Riverbed Documentation portal and the Riverbed Support portal.

QUESTION NO: 3

A WAN outage occurs while a Granite Edge is serving a projected LUN. A branch host requests a block that is not present in the local blockstore. What is the expected result?

A. The read is satisfied from the Granite Core.

B. An I/O error occurs.

C. The branch host is redirected to the storage array.

D. The missing block is generated by the Granite Edge.

ANSWER: B

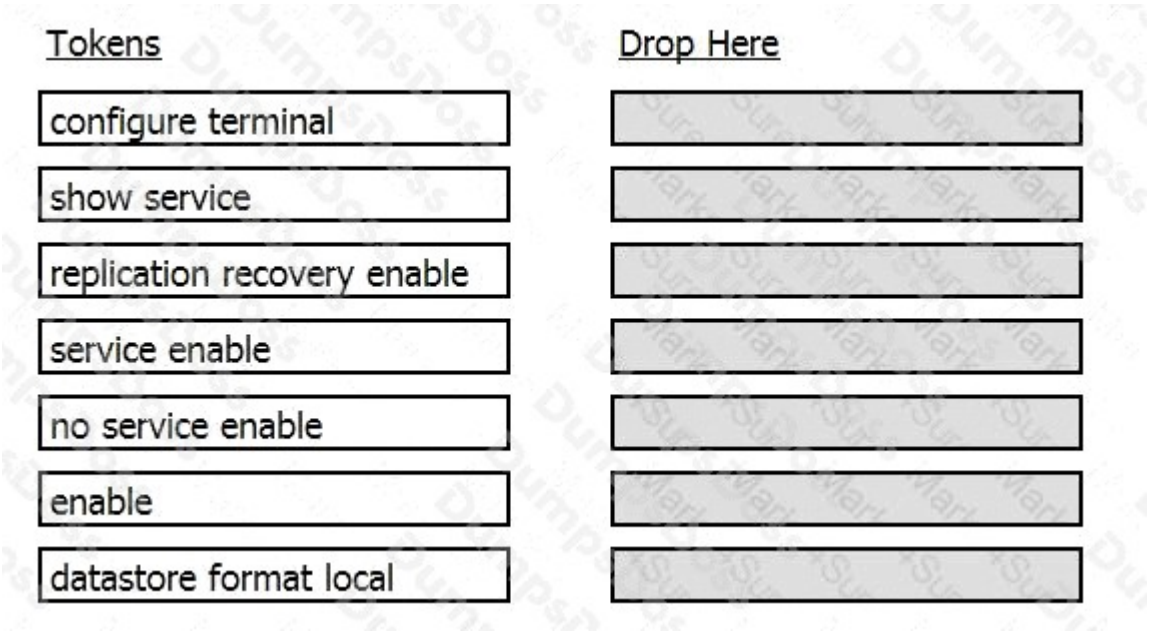
Explanation:

An I/O error occurs. During a WAN outage, the Granite Edge can continue to satisfy reads only for blocks that are already resident in its blockstore. If the requested block is absent, the Edge cannot retrieve it from the Granite Core while connectivity is unavailable. The host request therefore cannot be completed as a normal read operation.

This is why workloads requiring disconnected operation must have their required data prepopulated and pinned before the planned disconnection. Pinning protects the selected blocks from normal cache eviction, while prepopulation transfers the required blocks to the Edge in advance. See the Riverbed Documentation portal for release-specific Granite disconnected-operation guidance.

QUESTION NO: 4 - (SIMULATION)

If performing a disaster recovery (DR), what commands and in what order do they need to be run?



ANSWER: Check the explanation for the answer

Explanation:

Run the DR recovery commands in this order:

```
enable
configure terminal
no service enable
datastore format local
replication recovery enable
service enable
show service
```

This disables the service before formatting the local datastore, enables replication recovery mode, re-enables the service so recovery can proceed, and finally verifies service status.

QUESTION NO: 5

If the following system log messages occur during cloud storage provider configuration on Whitewater appliance, select the actions below that can be taken to diagnose the causE. (Select 5)

Riverbed rfsd[29622]: [retry.ERR] (29625) failed request 0 of get_buckets after receiving 1032: "1032: There was a mismatch between the signature in the request and the signature computed by the server.", status=access denied Riverbed rfsd[29622]: [replicator.ERR] (29625) Failed to list buckets : access denied Riverbed rfsd[29622]: [rfsd.ERR] (29625) Cloud test faileD. access denied Riverbed rfsd[29622]: [rfsd.ERR] (29625) Cloud test failed

A. Reboot the Whitewater appliance and see if the error resolves itself.

B. Restart the Whitewater appliance storage optimization service and see if the error resolves itself.

C. Verify the cloud storage provider credentials within Whitewater appliance.

D. Verify the cloud storage provider credentials outside of Whitewater appliance.

E. Take a TCP trace.

F. Check the Whitewater appliance system date/time.

ANSWER: B C D E F

Explanation:

The appropriate diagnostic actions are restarting the Whitewater appliance storage optimization service, verifying the cloud-storage credentials both within and outside the appliance, taking a TCP trace, and checking the appliance system date and time. The log shows that Whitewater can submit a bucket-list request but that the cloud provider rejects its calculated request signature. Signature-based cloud APIs derive request authentication from credential material and request details, and the request timestamp is commonly part of that calculation. Consequently, confirming that the configured access credentials are complete and accurate, then independently testing those credentials with the provider, distinguishes an appliance configuration issue from an account, permission, or provider-side issue.

Checking the Whitewater clock is especially important because material time drift can cause a provider to calculate a different valid-time signature than the client. A TCP trace provides request/response evidence for support analysis, including connectivity, endpoint selection, TLS negotiation, and the returned provider error. Restarting the storage optimization service is a focused diagnostic step that reinitializes the cloud connector and permits a clean retest without requiring a full appliance reboot. AWS's signature documentation describes how credentials, canonical request data, and timestamps participate in request signing: AWS Signature Version 4 signing process. Riverbed's product documentation portal provides the applicable Whitewater administration and troubleshooting documentation: Riverbed Documentation.

QUESTION NO: 6

Which VIF configurations does the Whitewater appliance support? (Select 3)

A. Round robin

B. 801a.d

C. 802.3ad

D. Transmit/receive load balance

E. Transmit load balance

F. Receive load balance

ANSWER: C D E

Explanation:

Whitewater supports the VIF bonding configurations **802.3ad**, **Transmit/receive load balance**, and **Transmit load balance**. These modes provide supported ways to aggregate or balance appliance network connectivity across multiple physical interfaces. 802.3ad is the standards-based link-aggregation mode, commonly deployed with switch-side LACP configuration, allowing the appliance and switch to negotiate an aggregated link. Transmit load balance distributes outbound traffic among member links while retaining a straightforward receive path. Transmit/receive load balance extends balancing behavior so that both traffic directions can benefit from the bonded interface arrangement, subject to the network design and switch behavior. Selecting a VIF mode that matches the connected switch configuration is essential: 802.3ad specifically requires compatible switch aggregation settings, whereas the load-balancing modes are selected when their operational model suits the deployment. Riverbed's Whitewater documentation and support resources provide the appliance-specific networking guidance, while the Linux bonding documentation describes the underlying 802.3ad, transmit-load-balancing, and adaptive load-balancing mode behavior: Riverbed Support and Linux Ethernet Bonding Driver documentation.

QUESTION NO: 7

Which of the following is an iSCSI-compliant SAN technology with snapshot integration that has been qualified with Granite appliance?

A. EMC VMAX 5876

B. Dell FAS270

C. NetApp FAS270

D. Hitachi PS4000

E. IBM XIV 3000

ANSWER: C

Explanation:

NetApp FAS270 is the qualified platform in this question. Riverbed Granite appliances use block storage presented over iSCSI for Granite Core storage, and their array qualification requirements include support for the storage operations needed to create and manage snapshots. NetApp FAS systems using ONTAP provide iSCSI LUN service and integrated Snapshot technology, allowing Granite to coordinate point-in-time copies as part of its edge data-management and recovery workflow. The FAS270 designation appears in the legacy Granite-qualified storage-array lists associated with the product generation covered by this exam. Qualification is specific to the storage platform, supported ONTAP release, iSCSI configuration, and applicable Riverbed Granite software release; it is not merely a general statement that a vendor offers iSCSI. This makes NetApp FAS270 the appropriate answer because it combines the required iSCSI SAN connectivity with the snapshot integration recognized by Granite. For NetApp background on iSCSI SAN LUNs and Snapshot copies, see NetApp ONTAP SAN host documentation and NetApp ONTAP Snapshot copy documentation.

QUESTION NO: 8

-- Exhibit –

-- Exhibit --

Refer to the exhibit. What should be used for the recommended cables between the Clustered Granite Cores on eth0_2 and eth0_3?

A. GigE straight-through cables

B. GigE crossover cables

C. This is not a valid design, for clustered Granite Cores

D. Fiber cables only

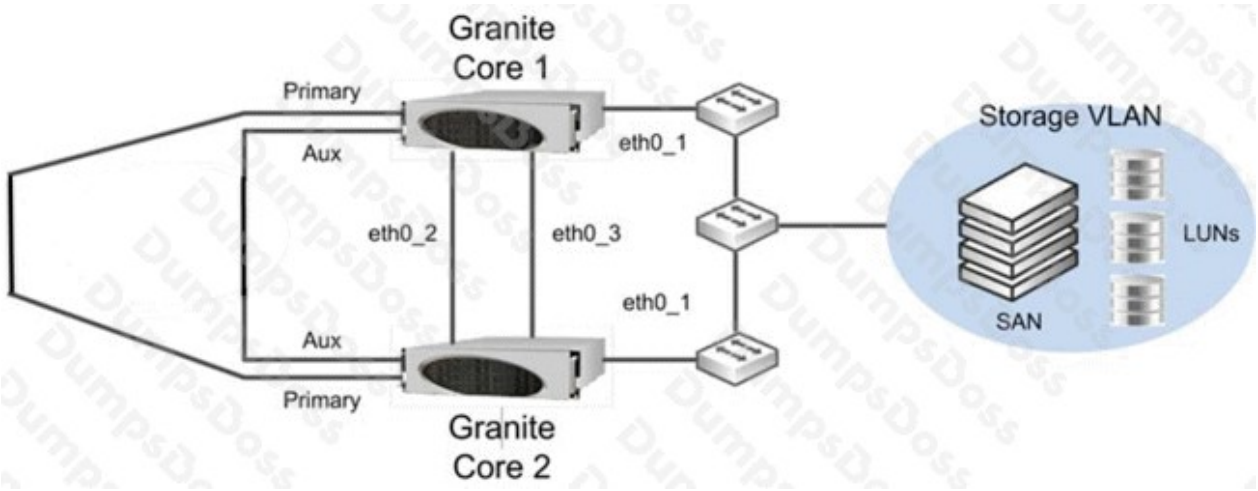
ANSWER: B

Explanation:

GigE crossover cables are the recommended connection for the dedicated eth0_2 and eth0_3 links between two clustered Granite Cores. These interfaces are used as direct, peer-to-peer cluster connections rather than as ordinary LAN-facing interfaces connected through an Ethernet switch. A crossover cable provides the required transmit/receive pair mapping for a direct connection between like Ethernet ports, allowing each Core to communicate with its cluster peer over the dedicated paths. Using two dedicated physical links also supports the resilient cluster design expected for the Core pair: the cluster can maintain its internal communications across separate links and can detect link or peer failures appropriately. This recommendation applies to the Granite/SteelFusion Core clustered deployment design and should be followed when the selected Ethernet adapters do not provide automatic MDI/MDIX crossover capability. Riverbed documentation and software resources for SteelFusion/Granite products are available through the Riverbed Support portal; current Riverbed product documentation can also be accessed at Riverbed Documentation.

QUESTION NO: 9

-- Exhibit –



-- Exhibit --

Refer to the exhibit. Which interface should be used for the Granite Edge connection?

A. Aux Port

B. Eth0_1

C. Eth0_2

D. Primary Port

E. Eth0_3

ANSWER: D

Explanation:

The **Primary Port** should be used for the Granite Edge connection. On a Granite Edge appliance, the primary interface is the designated network-facing interface for the appliance's normal operational connectivity, including communication required for the Edge deployment. It is the interface intended to place the Edge on the production network so that it can reach the relevant SteelFusion/Granite infrastructure and participate in the configured topology. The primary interface is also the appropriate port to use during initial network configuration when establishing the appliance's main network identity and routing. Selecting the Primary Port ensures that the Edge connection follows the appliance's supported interface role design and uses the network path intended for operational traffic. Riverbed's SteelFusion documentation and product resources describe the Edge appliance architecture and its role in connecting remote-site services with centralized storage and core infrastructure. See the Riverbed SteelFusion product overview and the Riverbed documentation portal for appliance deployment and interface-configuration guidance.

QUESTION NO: 10

Which statements correctly describe the use of MPIO with Granite high availability deployments? (Select 2)

A. MPIO provides a host with more than one path to presented storage.

B. MPIO protects a different failure domain than redundant WAN links.

C. MPIO converts a Granite Edge into an iSCSI initiator.

D. MPIO removes the need for Granite Edge high availability.

E. MPIO replicates Local LUN data to the Granite Core.

ANSWER: A B

Explanation:

MPIO provides a host with more than one path to presented storage. In a Granite high-availability design, supported host multipathing can maintain access when an individual storage path, interface, or related component fails. The host recognizes multiple paths to the same storage device and can use an available alternate path.

MPIO protects a different failure domain than redundant WAN links. MPIO provides storage-path resilience between the host and presented storage. Redundant WAN links protect connectivity between the branch and data-center Granite infrastructure. A resilient Granite design can use both because they address separate parts of the end-to-end service path.

MPIO does not eliminate the need for correctly configured Granite Edge high availability, redundant WAN design, or supported host configuration. See the Microsoft MPIO overview and the Riverbed Support portal for deployment guidance.