DUMPSBOSS.

Creating HPE Data Protection Solutions

HP HPE0-V17

Version Demo

Total Demo Questions: 10

Total Premium Questions: 102

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Plan and Design HPE Data Protection Solutions	77
Topic 2, Install, Configure, and Setup HPE Data Protection Solutions	8
Topic 3, Manage, Monitor, and Optimize HPE Data Protection Solutions	8
Topic 4, Troubleshoot HPE Data Protection Solutions	9
Total	102

QUESTION NO: 1 - (SIMULATION)

Your customer currently uses an HPE Nimble storage array Data protection Is provided by Veeam connected to HPE StoreOnce Gen4 Catalyst stores

Your customer asks tor your advice regarding optimized data protection following the 3-2-1 rule with an additional copy outside the datacenter you ten them about the HPE StoreOnce feature called Cloud Bank storage.

Are these correct statements about enabling Cloud Bank storage in this environment?

Solution:Recovery Manager Central (RMC) must be deployed to handle the copy management from HPE Nimble to the HPE StoreOnce Catalyst store and from HPE StoreOnce lo the Cloud Bank store.

An RMC license for the Nimble array and a capacity-based license for Cloud Bank is required.

ANSWER: See the explanation for the answer

Explanation:

No. The proposed solution is not correct.

Recovery Manager Central (RMC) is **not required** for this environment. RMC is used to orchestrate application-consistent HPE Nimble snapshot backups to StoreOnce Catalyst stores; it is not required to move existing Veeam backups from a StoreOnce Catalyst store into Cloud Bank Storage.

Cloud Bank copy/tiering is configured and managed by the **HPE StoreOnce system** using its Cloud Bank configuration and policies. Veeam can continue to protect the Nimble-based workloads to the StoreOnce Catalyst store.

An RMC deployment and an RMC-for-Nimble license are therefore not required merely to enable Cloud Bank Storage.
A **capacity-based Cloud Bank Storage license** is required for the Cloud Bank capacity being used.

QUESTION NO: 2

The customer currently has one HPE 3PAR and two Nimble storage arrays connected via

Fibre Channel (FC) to 12 HPE OL380 servers running VMware

They make backups with Commvault to HPE StoreEver tape libraries. They also make snapshots inside the storage array, to lower RTO and RPO.

They store the snapshots on the array itself, and fear that they might be vulnerable to array failures They want to maintain their low RTO and RPO objectives whilestoring data outside the arrayis this a valid option for the customer?

Solution:Use HPE infoSight for autonomous data protection, storing data on multiple arrays based on predictive analytics defined policies

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because HPE InfoSight does not provide autonomous data-protection orchestration, snapshot placement, or policy-based replication of data across multiple storage arrays. InfoSight is HPE's AI-driven infrastructure-management and predictive-analytics platform. It analyzes telemetry from supported infrastructure to identify risks, forecast capacity needs, provide operational recommendations, and assist with support and troubleshooting. Those capabilities can help an administrator make informed data-protection and capacity decisions, but they do not cause snapshots to be copied to another array or create an independently recoverable copy outside the source array.

Meeting the stated requirement requires a storage replication or backup architecture that writes a separate copy to independent storage. The appropriate technology must be selected according to the platform and recovery requirements—for example, native array replication capabilities, application-aware backup software, or a secondary backup target—so that

recovery can continue if the source array fails while supporting the required recovery-point and recovery-time objectives. InfoSight may provide visibility into the health and capacity of that environment, but it is not the data-movement or data-protection mechanism. HPE describes InfoSight as an AI-driven platform for predictive analytics and infrastructure operations at HPE InfoSight and describes its storage data-services portfolio at HPE Data Services Cloud Console.

QUESTION NO: 3

Does this option describe a valid scenario for using the 3-2-1 data protection rule or the 3-2-1-1-0 data protection rule?

Solution: You intend to use at least 2 different media types

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct because using at least two different media types is a defining requirement of both the 3-2-1 and the enhanced 3-2-1-1-0 data-protection rules. The “three” represents maintaining at least three copies of important data: the production copy and two backup copies. The first “two” requires those copies to be stored on at least two distinct types of media or storage platforms. This diversity reduces the chance that one failure mode, such as a storage-array issue, media defect, software fault, or operational error affecting a particular platform, compromises every available copy. The “one” then requires at least one copy to be kept offsite. The expanded rule adds an additional offline or immutable copy and validation that backups can be restored without errors. Therefore, an intended design that uses two media types satisfies the media-diversity element and is a valid scenario for applying either rule. HPE data-protection solutions are designed around resilient backup, recovery, and cyber-resilience practices, including maintaining protected copies across appropriate storage locations and platforms. See HPE Data Protection and HPE: What is data protection?.

QUESTION NO: 4

You organize a workshop for your customers IT team to handover a newly deployed backup solution based on HPE StoreOnce backup targets with Veeam as the backup application

Is this an important best practice for this scenario?

Solution:Use HW snapshot integration in the Job advanced properties it is much raster and has lighter impact on the production VMs to be hacked up.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Hardware-snapshot integration is not a universal handover best practice merely because the backup repository is an HPE StoreOnce system and Veeam is the backup application. StoreOnce provides deduplicated backup-target services, including integration options such as Catalyst, while Veeam hardware-storage snapshot workflows depend on a separately supported source-storage platform, its configuration, and the organization’s recovery requirements. The choice to use storage snapshots must therefore be designed, tested, and documented specifically for the protected virtual-machine environment; it cannot be assumed from the presence of a StoreOnce target.

For this handover, the IT team should instead receive and validate the implemented backup and recovery operating procedures: job schedules, retention settings, StoreOnce repository or Catalyst configuration, access credentials, monitoring and alert response, capacity management, and—most importantly—tested restore procedures. If hardware snapshot integration was intentionally deployed for compatible production storage, its requirements and recovery behavior should be covered as an environment-specific operational procedure rather than presented as a general requirement. HPE describes

StoreOnce as a purpose-built backup and recovery platform at HPE StoreOnce; Veeam documents storage-snapshot integration prerequisites and workflows in its Storage Systems documentation.

QUESTION NO: 5

Your customer runs a hyperconverged solution based on HPE SimpliVity. with a built-in data protection mechanism from HPE SimpliVity They try to recover objects from a

Microsoft Exchange server but cannot find the option in the user interface

Is this valid response regarding their problem?

Solution:Since HPE SimpliVity does not support Granular ObjectRestore (GRE). you must use an additional data protection application like Veeam

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. HPE SimpliVity's built-in data protection is VM-centric: it creates efficient, policy-driven backups of virtual machines and supports VM recovery and file-level recovery. Although application-consistent backup behavior can be used for supported Windows workloads through VSS, this does not provide an Exchange-aware browser for restoring individual mailbox objects such as messages, contacts, calendar items, or mailboxes. Consequently, an administrator will not find an Exchange granular-object recovery function in the SimpliVity user interface.

Recovering individual Exchange objects requires a data-protection product that can interpret Exchange data and present the protected content for item-level recovery. Veeam is an appropriate example because its Veeam Explorer for Microsoft Exchange provides granular recovery capabilities for Exchange items from protected backups. The customer can therefore continue to use SimpliVity for its integrated VM backup and recovery capabilities while using an application-aware backup solution when Exchange object-level restore requirements apply. HPE describes SimpliVity as a hyperconverged platform with integrated data protection at HPE SimpliVity. Veeam documents Exchange item-level recovery in its Veeam Explorer for Microsoft Exchange documentation.

QUESTION NO: 6

Is this a valid statement regarding Commvaultcomponents?

Solution:For larger environments where highavailability Is critical, the CommServe server can be clustered

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. The CommServe server is Commvault's central management component: it hosts the CommServe database and coordinates configuration, policy, job-control, and reporting functions across the CommCell environment. Because this role is critical to management operations, Commvault supports high-availability designs for environments that require continued service when the primary CommServe host experiences a failure. A clustered CommServe deployment provides a protected CommServe service that can fail over to another cluster node, helping maintain access to the CommServe functions and database services.

Clustering is particularly appropriate for larger deployments in which an extended interruption to central management could affect backup scheduling, restores, monitoring, or administrative access. It should be planned with compatible operating-system clustering, shared or otherwise protected database storage, network naming, and the Commvault-supported

configuration requirements for the selected release. Commvault also documents CommServe high-availability approaches, including LiveSync, which can be selected where its architecture is a better fit for the organization's recovery objectives. See the CommServe high availability documentation and the CommServe LiveSync documentation.

QUESTION NO: 7

A customer wants to replace an aging tape-based backup platform using a Grandfather-Father-Son (GFS) rotation scheme. They are considering replacing the entire solution with public cloud storage as a backup target is this a valid recommendation for this customer?

Solution: Cloud storage is ideal for the Grandfather copies of backup data for long-term data retention Keep an on-premises solution for the 'Son' copies to guarantee lower RTO and RPO numbers.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct because the proposed design applies a practical hybrid approach to GFS retention rather than treating every backup copy identically. Grandfather copies are typically retained for long periods and are accessed infrequently. Public cloud object storage can therefore be an appropriate target for these copies, providing scalable off-site retention without requiring the customer to continually expand local backup capacity. Cloud-based retention can also strengthen resilience by maintaining a copy away from the production location.

Keeping the most recent Son copies on premises supports the operational recovery objectives that matter most after a routine restore request or outage. Local backup storage generally offers predictable throughput and lower access latency for restoring recently protected workloads. This helps the customer meet more aggressive recovery time objectives while maintaining frequent backup schedules that support recovery point objectives. The resulting architecture retains the GFS concept: rapidly recoverable short-term copies remain local, while long-term copies are moved to a cost-efficient off-site cloud tier. HPE positions its data-protection portfolio around combining on-premises protection with cloud-integrated backup, recovery, and retention capabilities. See HPE StoreOnce and HPE Data Protection Solutions.

QUESTION NO: 8

A customer is currently using HPE StoreEver MSL2Q24 tape libraries with LT06 tape drives. They contact you about the need for more capacity on the tapes with the ever-lasting growth of data within their company.

Does this recommendation offer a viable option Tor upgrading the storage capacity of the tape libraries?

Solution: Upgrade to LTO8 drives giving the highest capacity or tapes at this moment

The customer stilt needs a dedicated LT06 drive for future restores from their current LT06 tapes.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. An HPE StoreEver MSL2024 library provides two drive bays, so it can be configured with an LTO-8 drive to write higher-capacity media while retaining an LTO-6 drive for access to the customer's existing LTO-6 cartridges. This is important because LTO drive compatibility is generation-specific: an LTO-8 drive does not provide a restore path for LTO-6 cartridges. Keeping the dedicated LTO-6 drive therefore preserves the ability to perform future restores from the existing backup set without preventing the organization from adopting the newer drive technology for new backup jobs.

LTO-8 cartridges provide 12 TB native capacity per cartridge, compared with 2.5 TB native for LTO-6, substantially increasing capacity per tape and reducing the number of cartridges needed for new data. The library's multiple-drive architecture supports this mixed-drive approach, subject to using the appropriate drive interface and firmware supported by the installed library configuration. This recommendation satisfies both requirements: greater capacity for ongoing data growth and continued recoverability of data retained on LTO-6 media. See the LTO-8 technology overview and HPE's StoreEver tape storage portfolio.

QUESTION NO: 9

Does this option describe a valid scenario for using the 3-2-1 data protection rule or the 3-

2-1-1-0 data protection rule?

Solution:You intend to use atleast 2 different media types

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. Using at least two different media types directly satisfies the "2" component of both the 3-2-1 and 3-2-1-1-0 data-protection rules. These rules establish a layered recovery strategy: maintain three copies of data, store those copies on two distinct types of storage media, and keep one copy offsite. The extended 3-2-1-1-0 approach further calls for an additional copy that is offline, air-gapped, or immutable, along with zero backup-recovery errors verified through testing. Media diversity reduces the risk that one technology-specific failure, operational error, or security event affects every recoverable copy. For example, production data might reside on primary disk storage while a backup copy is retained on a separate backup appliance or removable/cloud-based storage tier. The two media types should be genuinely distinct in failure characteristics and management domain, rather than simply being two volumes on the same storage system. HPE data-protection solutions, including StoreOnce, are designed to support resilient backup architectures and recovery workflows as part of a broader cyber-resilience strategy. See HPE's data protection overview and HPE StoreOnce information.

QUESTION NO: 10

You are optimizing the design of an existing data protection solution. The customer Is using the following systems In their environment

• HPE DL380 GenS/9/10 servers

• HPE Nimble AF60

• HPE StoreEver MSL6030 tape library with LT04 drives

• HPE FlexFabflc 5900 switches for LAN and SAN connectivity (ISCSI based)

• VMware ESXI 6.5

• Windows 2016

• Veeam9.5U2

You want to replace the aging tape library with a new HPE StoreOnce 5650 solution with

VTL virtual tape library and Catalyst targets with HPE Nimble snapshot Integration

Is this what you should use to assess current backup deployment?

Solution:Use HPE Info Sight lovalidate that the current HPE Nimble storage array is

running the correctNimble OS version tosupport storage integration withthe used VMware

ESXI

A. Yes

B. No

ANSWER: A

Explanation:

Yes. Verifying the installed NimbleOS version and the array's VMware interoperability status is an appropriate part of assessing the existing backup deployment before introducing StoreOnce Catalyst targets and Nimble snapshot-based protection. HPE InfoSight provides operational visibility for connected HPE Alletra 6000/Nimble Storage arrays, including software and system-health information, recommendations, and analytics that help identify whether the current platform is at an appropriate supported software level. This establishes an accurate baseline for the storage component on which VMware-integrated snapshot workflows depend.

In this environment, VMware ESXi 6.5 and the installed NimbleOS release must be considered together, because snapshot orchestration relies on supported VMware and storage integration behavior. Confirming that baseline early helps ensure that the planned Veeam and HPE Nimble snapshot integration can be designed on a supported configuration, rather than treating the replacement of the physical tape library as an isolated change. It also provides useful current-state data for planning upgrades or remediation before the StoreOnce 5650 deployment. HPE describes InfoSight's infrastructure monitoring, predictive analytics, and recommendation capabilities at HPE InfoSight. HPE's storage portfolio and associated support resources for Nimble-based systems are available through HPE Alletra Storage.