DUMPSBOSS.

Administration of Veritas NetBackup 8.1.2 and NetBackup Appliances 3.1.2

Veritas VCS-279

Version Demo

Total Demo Questions: 11

Total Premium Questions: 118

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An administrator has resolved the condition that caused a tape volume to be frozen and wants to return the volume to an active state.

Which command should the administrator use?

A. bpmedia -unfreeze

B. vmphyinv -unfreeze

C. bpverify -activate

D. bpduplicate -resume

ANSWER: A

Explanation:

bpmedia -unfreeze is the correct command. NetBackup freezes media when it detects conditions that may affect media reliability or backup integrity. After the administrator has investigated and corrected the underlying problem, the `bpmedia -unfreeze` operation can return the volume to an active state for NetBackup use.

The cause of the frozen state should be reviewed before the volume is unfrozen. For example, media write errors, drive problems, or robotic-library issues can cause NetBackup to freeze a tape. Unfreezing the volume without correcting the underlying fault can result in repeated backup failures or additional media errors. The `vmphyinv` command inventories a robot, while `bpverify` validates backup images. See the Veritas NetBackup Commands Reference Guide for media administration command syntax.

QUESTION NO: 2

An administrator suspects that a media server cannot establish a NetBackup connection to a client.

Which command should the administrator run from the media server to test communication with the client NetBackup Client Service?

A. bptestbpcd

B. bpverify

C. bpimmedia

D. nbdevquery

ANSWER: A

Explanation:

bptestbpcd is the correct command. It tests the connection from a NetBackup server to the `bpcd` service on a client. The command helps verify that the media server can resolve the client name, reach the client across the network, and communicate with the NetBackup Client Service.

This test is useful when backup jobs fail before data transfer begins or when the administrator needs to distinguish a NetBackup client-service connectivity issue from a storage or policy issue. If the command fails, the administrator should investigate name resolution, firewall rules, routing, and the status of NetBackup services on the client. See the NetBackup 8.1.2 documentation for NetBackup command and troubleshooting guidance.

QUESTION NO: 3

A file system on a server that has different files changing daily becomes corrupt, and a restore is required. The system is being backed up using True Image Restore with move detection enabled.

The most recent backups of this file system are displayed below:

☞ Monday: A full backup

☞ Tuesday: A differential incremental backup

☞ Wednesday: A cumulative incremental backup

☞ Thursday: A differential incremental backup

☞ Friday: A differential incremental backup

What is the minimum number of backup images that will be used to fully restore the server to its most current state?

A. one

B. two

C. three

D. four

E. five

ANSWER: D

Explanation:

four is correct. Restoring the file system to its Friday state requires the Monday full backup image, the Wednesday cumulative incremental image, and the Thursday and Friday differential incremental images. The Wednesday cumulative incremental contains every file that changed since the last full backup, which was Monday. It therefore includes the changes captured in Tuesday's differential incremental and makes the separate Tuesday image unnecessary for this restore.

After Wednesday, each differential incremental contains changes made since the immediately preceding successful backup. Consequently, the Thursday image supplies changes made after the Wednesday cumulative backup, and the Friday image supplies changes made after Thursday. Combining the Monday full image with Wednesday's cumulative image and the two subsequent differential images reconstructs the most current version of every file.

True Image Restore maintains information about the backed-up file-system state so that restore processing can select the appropriate image versions for the requested point in time. Move detection helps preserve the correct handling of files that were moved or renamed, but it does not eliminate the need to use the backup images containing changes made after the cumulative incremental. See the NetBackup 8.1 documentation and Veritas's NetBackup incremental-backup guidance.

QUESTION NO: 4

A master server has failed and must be recovered after replacement hardware has been configured.

Which two items are required to recover the NetBackup catalog? (Choose two.)

A. the disaster recovery file

B. the catalog backup media

C. the original client backup policy

D. a current NetBackup client package

E. the media server bp.conf file

ANSWER: A B

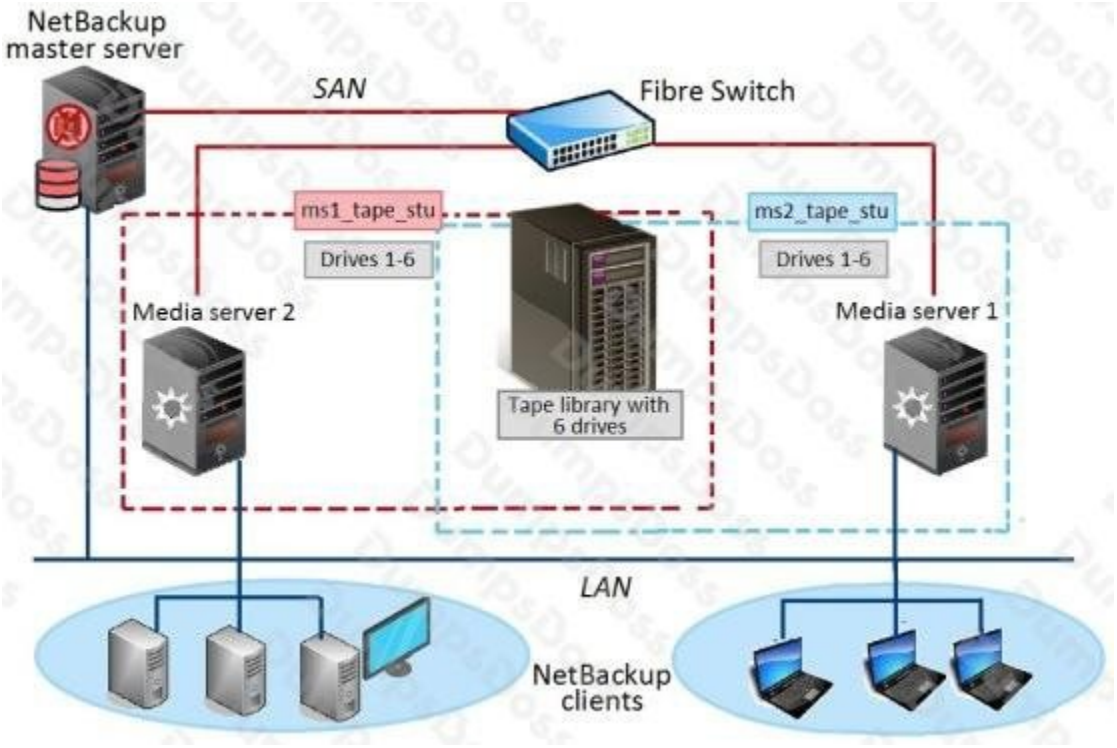
Explanation:

The disaster recovery file and the catalog backup media are required for catalog recovery. The disaster recovery file contains the information that identifies the catalog backup and provides the recovery details that NetBackup needs to begin the catalog recovery procedure. The catalog backup media contains the actual catalog backup images that must be restored.

NetBackup catalog recovery restores the configuration and image information that was protected by the NBU-Catalog policy. A current disaster recovery file should always be stored separately from the master server and its catalog volumes. The original policy configuration alone does not contain the catalog backup data, and a normal client backup cannot be substituted for a catalog backup. Veritas documents catalog backup and recovery procedures in the NetBackup Administrator's Guide, Volume I.

QUESTION NO: 5

Refer to the exhibit.



Two media servers, sharing a library with 6 tape drives, exist in the NetBackup environment displayed in the exhibit. Both weekly Full and daily Differential Incremental backups need to run for the clients and each schedule has a different retention period. Because of network topology, some clients back up to Media server 1 and some back up to Media server 2. The environment suffers from multiple status 96 failures during the backup window.

How can the administrator minimize the number of failures?

A. increase the “Media unmount delay”

B. configure media multiplexing

C. enable backups to span tape media

D. enable media sharing

ANSWER: D

Explanation:

Enable media sharing. NetBackup status 96 indicates that a backup job could not obtain the media or tape-drive resources required to proceed. In this environment, both media servers need concurrent access to the same physical tape library, but backup demand can vary significantly between the servers during the backup window. Enabling media sharing allows NetBackup to coordinate use of the shared library resources across the media servers rather than leaving drive availability

effectively constrained by the server that initially owns or reserves a resource. This improves the likelihood that an available tape drive can be used by the media server with active jobs waiting for resources.

Media sharing is particularly appropriate where multiple media servers service different client groups because of network topology while using one common robotic library. It lets tape-drive capacity be used more efficiently as Full and Differential Incremental schedules overlap, reducing job queueing and the resulting allocation failures. The administrator should also ensure that the shared-library configuration, drive paths, robot control, storage units, and media-server permissions are correctly configured before relying on this capability. Veritas documentation for NetBackup administration and status-code troubleshooting is available from the NetBackup documentation portal and the Veritas support search for NetBackup status 96.

QUESTION NO: 6

An administrator has a MS-Windows type policy that has failed for a Microsoft Windows NetBackup client. The policy uses the ALL_LOCAL_DRIVES backup selection. See the extract from the end of the job details below:

Which two logs will provide the most relevant information for troubleshooting and resolving the error? (Choose two.)

A. Operating system logs on the client

B. NetBackup bpfis logs on the media server

C. NetBackup bptm logs on the media server

D. Operating system logs on the media server

E. NetBackup bpfis logs on the client

ANSWER: A E

Explanation:

Operating system logs on the client and **NetBackup bpfis logs on the client** are the most relevant sources for a Windows client backup failure involving `ALL_LOCAL_DRIVES`. NetBackup uses the client-side snapshot framework to obtain a consistent view of the volumes selected for backup. On Windows, this commonly involves the Volume Shadow Copy Service (VSS), associated writers, providers, and volume-level operations. The Windows Application and System event logs can therefore identify the underlying Windows or VSS condition, including writer failures, provider errors, service issues, or storage and filesystem events occurring when the snapshot is requested.

The client-side `bpfis` log records NetBackup FlashBackup/snapshot processing details. It is the key NetBackup diagnostic log for seeing the snapshot request, the volumes being processed, the snapshot method used, and detailed error information returned during snapshot creation or cleanup. Reviewing its timestamps alongside client Windows event logs correlates the NetBackup job failure with the originating operating-system event and supports a targeted resolution. Veritas documents NetBackup logging and diagnostic log locations in the NetBackup Troubleshooting Guide; Microsoft documents VSS troubleshooting and writer diagnostics at Volume Shadow Copy Service.

QUESTION NO: 7

An administrator needs to review the state of backup images that are being processed by Storage Lifecycle Policies.

Which NetBackup utility should the administrator use?

A. nbstlutil

B. bpstulist

C. bpimmedia

D. nbdevquery

ANSWER: A

Explanation:

nbstlutil is the correct utility. The `nbstlutil` utility provides information about Storage Lifecycle Policy processing, including image state and the operations that NetBackup must complete for images that are managed by an SLP.

This utility is useful when investigating pending duplication, replication, or expiration processing and when determining why images remain in an incomplete or pending state. The information can help an administrator distinguish between images waiting for storage resources and images that have encountered processing failures. `bpstulist` lists storage units, `bpimmedia` reports image-media relationships, and `nbdevquery` reports disk-storage objects. Veritas documents SLP monitoring utilities in the NetBackup Commands Reference Guide.

QUESTION NO: 8

An administrator is creating a Storage Lifecycle Policy (SLP) that backs up client data to disk and then duplicates the backup images to tape.

Which two statements are correct about the SLP configuration? (Choose two.)

A. The first operation in the SLP must be a backup operation.

B. A duplication operation can create a tape copy after the backup operation completes.

C. A duplication operation must be configured before the backup operation.

D. An SLP can create its initial backup image with a replication operation.

E. The backup and duplication operations must use the same storage unit.

ANSWER: A B

Explanation:

An SLP must begin with a backup operation because the backup operation creates the initial image copy that later SLP operations use. A duplication operation requires an existing source image, so it cannot be the first operation in a policy that protects new client data.

The duplication operation can follow the backup operation and create a copy on tape. In this configuration, NetBackup first writes the client backup to the disk destination defined by the backup operation. The SLP then manages the duplication of that disk copy to the tape destination according to the operation's schedule and resource availability. See the NetBackup 8.1.2 documentation for Storage Lifecycle Policy configuration guidance.

QUESTION NO: 9

Prior to initiating a restore, an administrator realizes that media needed for the restore was written by a server that is unavailable. The administrator does have another server that can perform the restore and that is connected to the same library.

Which two commands can the administrator perform to change the server ownership, so the restore can be performed? (Choose two.)

A. bpimage

B. bpimmedia

C. bpimagelist

D. bpmedia

E. bpimport

ANSWER: A D

Explanation:

The correct commands are `bpimage` and `bpmedia`, used with their `-movedb` operations to transfer NetBackup catalog ownership from the unavailable media server to the replacement server. The ownership change must cover both the image records and the media records: image ownership enables NetBackup to locate and use the backup-image metadata required for restore selection, while media ownership allows the available server to manage and mount the physical backup media in the shared library.

For this situation, the administrator uses `bpimage -movedb` to move image database ownership from the unavailable server to the server that will perform the restore. The administrator also uses `bpmedia -movedb` to move the associated media database ownership. After these catalog updates, the replacement server can access the relevant image and media information and use the library-connected media to perform the restore. This approach is intended for a media-server replacement or unavailability scenario and should be performed carefully with the correct old-server and new-server values.

Veritas documents these commands and their ownership-transfer syntax in the NetBackup Commands Reference Guide. Additional NetBackup product documentation is available from the Veritas NetBackup documentation portal.

QUESTION NO: 10

An administrator has an audible appliance alarm detected in the data center.

Which command should the administrator use to troubleshoot the reason for the alarm?

A. Settings > NetBackup Misc Show

B. Appliance > Status

C. Monitor > Hardware > ShowHealth

D. Support > Test > Software

ANSWER: C

Explanation:

`Monitor > Hardware > ShowHealth` is the appropriate NetBackup Appliance CLI command because an audible alarm is typically associated with a hardware health event that requires immediate investigation. The ShowHealth command displays the appliance's current hardware-health state and identifies issues reported by monitored components, such as power supplies, fans, temperature sensors, disk hardware, and other platform elements. This information lets the administrator correlate the physical alarm with the component or sensor condition that generated it and determine the appropriate corrective action, such as replacing a failed field-replaceable unit or addressing an environmental condition.

The command is located under the Monitor appliance-shell menu because it is intended for operational health monitoring rather than NetBackup configuration or software diagnostic testing. Administrators should review the reported health details promptly, especially where a component is in a degraded or critical state, and then follow the applicable appliance hardware-service procedures. Veritas documents appliance monitoring and hardware-status commands in its NetBackup Appliance documentation. See the NetBackup Appliance documentation and the Veritas NetBackup Appliance support portal.

QUESTION NO: 11

After creating a NBU-Catalog type backup policy, an administrator receives the following message:

DR file is on the same partition as your catalog and will be unusable in an actual disaster or disk failure.

Which two options are available to the administrator to ensure the DR file is available for future use? (Choose two.)

A. ensure the folder DR file is on a non-root volume

B. ensure the DR file is created on a volume other than the NetBackup volume

C. ensure the NetBackup catalog is on a non-root volume

D. configure a valid email address of the administrator in the “Send email” option

E. configure Auto Image Replication to send the DR file to a remote master server

ANSWER: B D

Explanation:

The administrator should ensure the DR file is created on a volume other than the NetBackup volume and configure a valid email address of the administrator in the “Send email” option. A catalog backup produces disaster-recovery information that is needed to recover the NetBackup catalog after loss of the master server or its catalog storage. This information must be retained independently of the catalog itself. Placing the DR file on a different volume protects it from a failure of the partition that contains the catalog and provides a locally accessible recovery copy.

The catalog backup policy can also email the disaster-recovery information to the configured recipient. Sending it to a valid administrator mailbox creates an additional off-host copy that remains available even when the master server’s local catalog partition cannot be accessed. The recipient should preserve the email and its DR information in accordance with the organization’s recovery procedures. Using both an independent storage volume and email delivery provides separate recovery paths for the catalog recovery data. Veritas documents catalog backup and disaster-recovery procedures in the NetBackup Administrator’s Guide, Volume I and the related NetBackup disaster recovery documentation.