Administration of Veritas NetBackup 8.0

Veritas VCS-276

Version Demo

Total Demo Questions: 18

Total Premium Questions: 180

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	160
Total	180

QUESTION NO: 1

Which two restore types must be initiated from a client system rather than the Net Backup Administration Console on the master server? (Select two.)

A. Oracle:

B. MS-SharePoint

C. MS-Exchange

D. MS SQL-Server

E. VMware

ANSWER: A B

Explanation:

Oracle: restores are initiated on the Oracle client because NetBackup integrates with Oracle Recovery Manager (RMAN), which runs in the Oracle environment and directs the database restore and recovery workflow. RMAN communicates with the NetBackup media-management library on that client to request the required backup pieces, restore them, and apply Oracle recovery operations. This application-aware process therefore cannot be initiated solely through the master server's NetBackup Administration Console.

MS-SharePoint restores must be initiated from a SharePoint client, specifically a SharePoint front-end web server that has the NetBackup client software and SharePoint integration available. The restore process needs access to the SharePoint farm and its application-level interfaces so that recovered content is correctly restored into the SharePoint environment. Initiating recovery from the appropriate client also ensures that NetBackup can use the local SharePoint configuration and credentials required by the application-aware recovery workflow.

These requirements reflect the distinction between managing backup images on the master server and executing application-specific recovery operations in the protected application environment. See the Veritas NetBackup documentation and Oracle's RMAN restore and recovery documentation.

QUESTION NO: 2

The administrator of a large bank needs to preserve financial information for an extended period of time. The bank's NetBackup 8.0catalog is now over 800GB in size, causing the catalog backups to contend for resources with production system backups.

How can the administrator shorten the time needed to back up the catalog?

A. use the NetBackup 8.0Agent for Symantec Enterprise Vault to perform an online archive of the catalog

B. create a catalog archive policy and execute it from the command line using the bpcatarc command

C. use the NetBackup 8.0client-side deduplication feature to shorten the time it takes to perform a catalog backup

D. back up the catalog by scheduling an online Sybase database backup policy to allow the backup to run without contending for resources

ANSWER: B

Explanation:

The correct approach is to create a catalog archive policy and execute it from the command line using the bpcatarc command. NetBackup catalog archiving moves qualifying, older catalog images and associated information from the active catalog into an archive. This retains the information for long-term preservation while reducing the amount of data maintained in the active catalog database and image files. Because catalog backup operations protect the active catalog, reducing its size directly reduces the volume of catalog data that must be processed and written during each catalog backup. This is especially useful where retention or regulatory requirements require historical backup information to be kept, but operational recovery activity primarily relies on more recent catalog records. The administrator can define an archive policy that identifies

images eligible for archiving and use `bpcatarc` to perform the archive operation. The archived catalog data remains available for later recovery or access through the supported catalog-archive procedures, while routine catalog backups require fewer resources and complete more quickly. Veritas documents catalog archiving and the `bpcatarc` utility in the NetBackup Commands Reference: NetBackup Commands Reference. Additional catalog-management documentation is available from the Veritas NetBackup documentation portal.

QUESTION NO: 4

An administrator runs the following command on the Master Server to test connectivity to a client:

bptestbpcd -client clientA

The administrator receives the following message:

<16> bptestbpcd main: Function ConnectToBPCD (clientA) failed: 25 cannot connect on socket

Which two reasons may cause the error message? (Select two.)

A. an incorrect entry for the Master Server in the client's hosts file

B. the NetBackup processes on the client are stopped

C. the Master Server is unknown to the client

D. an incorrect entry for the client in the Master Server's hosts file

E. vnetd is stopped on the Master Server

ANSWER: B D

Explanation:

The correct causes are **the NetBackup processes on the client are stopped** and **an incorrect entry for the client in the Master Server's hosts file**. The `bptestbpcd -client clientA` command is run from the master server to test whether it can establish a NetBackup communications connection to the specified client. A status 25, “cannot connect on socket,” indicates that the initiating system could not establish the required network socket connection to the client-side NetBackup service.

If the client NetBackup processes are stopped, the client is not listening for the connection used by the test. Starting the applicable NetBackup Client Service or daemons restores the listener required for master-server-to-client communications. The command also depends on correct client name resolution at the master server. If the master server’s hosts file maps `clientA` to an incorrect address, NetBackup attempts to connect to the wrong host or an unreachable address and returns the socket-connect failure. Administrators should therefore verify that the client services are running and confirm that the client name resolves to its correct, reachable IP address from the master server. See Veritas documentation for the bptestbpcd command and the NetBackup status codes and troubleshooting documentation.

QUESTION NO: 7

Which status code applies only to disk storage units?

A. 129

B. 86

C. 219

D. 2805

ANSWER: A

Explanation:

Status code 129 is the disk-storage-specific status code. In NetBackup, this status indicates that NetBackup could not obtain disk-volume information needed for a disk storage unit. Disk storage units depend on NetBackup being able to identify and query the underlying disk volume or mount point, including its availability and capacity, before it can select the storage for a job. Consequently, this code is associated specifically with disk-based storage configuration and access rather than the general media-management or job-processing conditions that can arise across multiple storage types.

When status 129 is reported, an administrator should validate the disk storage unit path, ensure that the relevant disk volume is mounted and accessible to the NetBackup services, and verify that the storage server can retrieve volume details. Checks should also include operating-system permissions, the health and free space of the target filesystem, and whether any associated disk pool or storage lifecycle configuration remains available. Veritas documents status-code meanings and recommended administrative troubleshooting in the NetBackup status-code reference and the NetBackup documentation portal: NetBackup Status Codes Reference and Veritas NetBackup support knowledge base.

QUESTION NO: 8

What is the purpose of the Login and Password settings in the Disaster Recovery tab of a Net Backup catalog backup policy?

A. to specify credentials required to access a network share

B. to encrypt the Net Backup catalog backup data

C. to require credentials to perform a catalog recovery

D. to encrypt the disaster recovery file

ANSWER: A

Explanation:

The purpose is **to specify credentials required to access a network share**. A NetBackup catalog backup policy can be configured to create a disaster recovery package and copy that package to a remote shared location. The Login and Password fields on the Disaster Recovery tab provide the account credentials NetBackup uses when it connects to that specified network share. This permits the disaster recovery information to be stored separately from the primary NetBackup server, where it can be available if the original master server or its local disk is lost. The configured account must have the necessary permissions to connect to the share and create or update the disaster recovery package there. These settings therefore support access to the external destination for the package; they are not settings for catalog-data encryption or for controlling authorization during a later catalog recovery. Veritas documents catalog backup and disaster-recovery-package configuration as part of catalog protection in the NetBackup Administrator's Guide. See the NetBackup 8.0 Administrator's Guide, Volume I and the Veritas NetBackup catalog backup documentation.

QUESTION NO: 9

Which two NetBackup features are available to protect the Media Server Deduplication Pool (MSDP) catalog? (Select two.)

A. NetBackup catalog backups

B. MSDP catalog policy

C. Optimized Catalog Duplication

D. MSDP shadow copies

E. Checkpoints

ANSWER: A D

Explanation:

NetBackup catalog backups and MSDP shadow copies are the NetBackup features used to protect an MSDP catalog. A NetBackup catalog backup captures the NetBackup configuration and catalog information needed to reconstruct the

environment during disaster recovery. For an MSDP deployment, this protection includes the MSDP-specific catalog information that NetBackup requires to recognize and recover the deduplication pool correctly after a loss or rebuild of the media server.

MSDP shadow copies provide an additional, MSDP-specific protection mechanism for deduplication metadata. NetBackup maintains shadow copies of the MSDP catalog so that a usable copy of the metadata is available for recovery operations. This protection is important because MSDP catalog metadata maps NetBackup images to the deduplicated data stored in the pool; preserving that metadata is necessary to make the stored backup data usable after recovery.

These mechanisms should be incorporated into the site's normal disaster-recovery procedures. Catalog backups must be run successfully and retained on recoverable storage, while MSDP shadow-copy protection supplements that catalog-protection workflow for the deduplication pool. Veritas documents MSDP catalog protection and recovery procedures in the NetBackup Deduplication Guide and the associated catalog recovery guidance in the NetBackup documentation library.

QUESTION NO: 10

Which two prerequisites must an administrator perform to enable restoration of individual objects and attributes in Active Directory? (Select two.)

A. install the NetBackup File System daemon (nbfsd) on the client

B. choose the "Enable granular recovery" option in the policy

C. choose the "Use Accelerator" option in the policy

D. choose Active Directory policy type

E. enable the Network File System (NFS) on the client

ANSWER: B E

Explanation:

To restore individual Active Directory objects and attributes, NetBackup must create a backup that supports Granular Recovery Technology (GRT). Therefore, selecting the *"Enable granular recovery"* setting in the policy is required. This setting instructs NetBackup to preserve the information needed to browse and recover individual directory objects from a Windows System State/Active Directory backup rather than limiting recovery to the full backup image.

The client also must have Network File System (NFS) enabled. NetBackup uses NFS-based access during the granular-recovery workflow to mount and present the backed-up Active Directory data for object-level browsing and recovery. Once these prerequisites are in place, an administrator can use the NetBackup recovery interface to locate Active Directory containers, objects, and supported attributes and restore the required items.

These requirements are part of the NetBackup Windows granular recovery configuration and Active Directory recovery procedures. See the NetBackup 8.0 Windows Administrator's Guide and the Veritas NetBackup granular recovery documentation.

QUESTION NO: 11

Using the default values in the activity monitor, a failed job is discovered among hundreds of jobs that ran during the evening. The administrator would like to view all related jobs to verify they completed successfully.

Where in the activity monitor can the administrator find all related jobs?

A. right-click the failed job and select View Job hierarchy

B. right-click the failed job and select Troubleshooter

C. double-click the failed job and select the Detailed Status tab

D. right-click the failed job and select Details

ANSWER: A

Explanation:

The correct selection is *right-click the failed job and select View Job hierarchy*. In the NetBackup Administration Console Activity Monitor, Job Hierarchy displays the relationship between a selected job and its associated jobs. This is particularly useful after locating a failed job in a large activity list, because the administrator can view the parent, child, and related jobs together rather than manually searching through hundreds of job records. The hierarchy helps establish whether the overall operation included multiple coordinated jobs and lets the administrator inspect their completion states in context. For example, policies and storage workflows can create related job activity that is easier to interpret as a hierarchy than as separate rows in the monitor. Veritas documents Job Hierarchy as an Activity Monitor function for viewing related jobs and their relationships. This capability supports efficient validation of the broader backup operation after an individual job failure is found. See the NetBackup Administration Console guidance in the Veritas NetBackup Administrator's Guide, Volume I and the Activity Monitor documentation.

QUESTION NO: 13

An administrator wishes to modify the Override default job priority option for on MS Windows type restore job before the restore job begins.

Where in the Microsoft Windows Backup, Archive, and Restore console can the administrator configure this option?

A. after clicking the Restore button, in the Restore Marked Files dialog box

B. at the bottom of the options listed in File > NetBackup Client Properties > Network

C. in the Backup, Archive, and Restore window, under the Restore Files tab

D. within File > Specify NetBackup Machines and Policy Type

ANSWER: A

Explanation:

The correct location is *after clicking the Restore button, in the Restore Marked Files dialog box*. In the NetBackup Windows Backup, Archive, and Restore interface, an administrator first selects the required items on the Restore Files tab and then initiates the restore by clicking **Restore**. NetBackup displays the Restore Marked Files dialog before submitting the restore job. This dialog is where the restore request is finalized, including the destination and restore behavior settings, and it provides the job-priority control. Selecting **Override default job priority** enables the administrator to assign a priority for that specific restore request rather than using the configured default priority. The priority is therefore set before the restore is submitted to the NetBackup job scheduler, allowing the requested restore to receive the intended scheduling preference. This per-job setting is particularly useful when an urgent recovery must be scheduled ahead of routine restore activity without changing the general client or policy defaults. Veritas documents the Windows Backup, Archive, and Restore procedures and restore-request settings in its NetBackup documentation: NetBackup 8.0 documentation and Veritas NetBackup support knowledge base.

QUESTION NO: 14

An administrator is comparing the NetBackup Accelerator and Net Back up FlashBackup features to determine which feature should be used for backup of a very large file system with millions of files.

Which consideration is irrelevant when determining whether to use NetBackup Accelerator or Net Back up FlashUackup in the situation?

A. the file system change rate

B. the file system storage capacity

C. the type of file system being used

D. the file system folder depth

ANSWER: D

Explanation:

the file system folder depth is the irrelevant consideration. NetBackup Accelerator and FlashBackup are evaluated according to factors that affect backup method eligibility, scanning behavior, change tracking, and the amount of data that must be protected or restored. A directory tree's nesting depth does not itself determine whether either technology is supported or appropriate. Although a deeply nested hierarchy can be an operational characteristic of a workload, folder depth is not a selection criterion for choosing Accelerator rather than FlashBackup.

For a file system containing millions of files, the important evaluation centers on the backup method's support for the specific file system and platform, the scale of the protected data, and the workload's data-change characteristics. Accelerator is designed to reduce subsequent backup processing by using changed-block tracking information together with the prior backup image, while FlashBackup is intended for efficient backup of file-system data at the raw-device level in supported configurations. Those architectural and workload factors govern the practical decision; the number of directory levels does not. Veritas documents FlashBackup and Accelerator behavior, requirements, and supported configurations in its NetBackup documentation: NetBackup 8.0 documentation and Veritas NetBackup Accelerator overview.

QUESTION NO: 16

Weekly full backups run for client A on maeter1 using a storage unit that belongs to medial. The administrator is required to retain client A's full backups for a period of four months. When the administrator modifies the full schedule, an option for 4 months is missing from the Retention drop down list.

How can the administrator add a four month retention?

A. modify an existing retention level in the server host properties, under Retention Periods

B. ignore the selection list and type in the desired retention period directly

C. add a new retention period in the media server host properties, under Retention Periods

D. increase the Image cleanup Interval in the master server host properties, under Clean-up

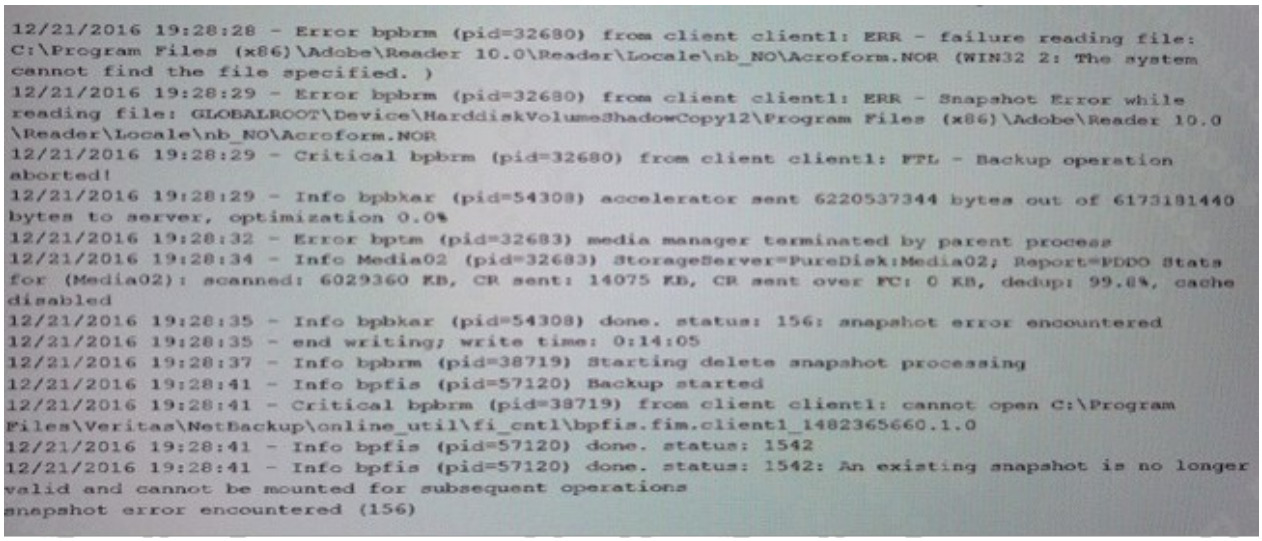
ANSWER: A

Explanation:

The correct action is to modify an existing retention level in the server host properties, under Retention Periods. NetBackup policies and schedules select retention by using predefined retention levels rather than by accepting an arbitrary duration directly in the schedule's Retention list. The available values in that list are determined by the retention-period configuration maintained on the master server. An administrator can therefore select an unused retention level and change its duration to four months in the master server's Host Properties, under Retention Periods. Once saved, that retention level becomes available for selection in the policy schedule and applies to images created under that schedule after the change. Retention settings control how long backup images remain protected before they become eligible for expiration; they are independent of the storage unit's media server and the image-cleanup interval. Before repurposing a retention level, the administrator should confirm that it is not already assigned to other policies, because changing a level affects every policy and image using that level. Veritas documents retention levels and their configuration in the NetBackup Administrator's Guide: NetBackup documentation and the related Veritas knowledge base guidance on retention periods.

QUESTION NO: 17

An administrator has a MS-Windows type policy that has fatted 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:



```
12/21/2016 19:28:28 - Error bpbrm (pid=32680) from client client1: ERR - failure reading file:
C:\Program Files (x86)\Adobe\Reader 10.0\Reader\Locale\nb_NO\Acroform.NOR (WIN32 2: The system
cannot find the file specified. )
12/21/2016 19:28:29 - Error bpbrm (pid=32680) from client client1: ERR - Snapshot Error while
reading file: GLOBALROOT\Device\HarddiskVolumeShadowCopy12\Program Files (x86)\Adobe\Reader 10.0
\Reader\Locale\nb_NO\Acroform.NOR
12/21/2016 19:28:29 - Critical bpbrm (pid=32680) from client client1: FTL - Backup operation
aborted!
12/21/2016 19:28:29 - Info bpbkar (pid=54308) accelerator sent 6220537344 bytes out of 6173181440
bytes to server, optimization 0.0%
12/21/2016 19:28:32 - Error bptm (pid=32683) media manager terminated by parent process
12/21/2016 19:28:34 - Info Media02 (pid=32683) StorageServer=PureDisk:Media02; Report=PDDO Stats
for (Media02): scanned: 6029360 KB, CR sent: 14075 KB, CR sent over FC: 0 KB, dedup: 99.8%, cache
disabled
12/21/2016 19:28:35 - Info bpbkar (pid=54308) done. status: 156: snapshot error encountered
12/21/2016 19:28:35 - end writing; write time: 0:14:05
12/21/2016 19:28:37 - Info bpbrm (pid=38719) Starting delete snapshot processing
12/21/2016 19:28:41 - Info bpfis (pid=57120) Backup started
12/21/2016 19:28:41 - Critical bpbrm (pid=38719) from client client1: cannot open C:\Program
Files\Veritas\NetBackup\online_util\fi_cntl\bpfis.fim.client1_1482365660.1.0
12/21/2016 19:28:41 - Info bpfis (pid=57120) done. status: 1542
12/21/2016 19:28:41 - Info bpfis (pid=57120) done. status: 1542: An existing snapshot is no longer
valid and cannot be mounted for subsequent operations
snapshot error encountered (156)
```

Which two logs will provide the most relevant information for troubleshooting and resolving the error? (Select 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 togs 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 because processing of the `ALL_LOCAL_DRIVES` selection occurs on the Windows client. NetBackup must enumerate the local volumes and, where applicable, interact with Windows snapshot components before it can read the selected data. The client Windows Event Viewer logs, particularly the Application and System logs, can identify operating-system, volume, file-system, VSS, or provider conditions that prevent that client-side processing from completing. The client `bpfis` log records NetBackup File System Interface activity and supplies the detailed NetBackup-side context for volume discovery and snapshot/file-system operations. Together, these two sources correlate the underlying Windows condition with the precise NetBackup operation that encountered it. Veritas documents that NetBackup logging is component-specific and that the relevant client process log should be collected when diagnosing client backup failures. See the NetBackup documentation and Veritas guidance on NetBackup logging and troubleshooting.

QUESTION NO: 18

In which two places can an administrator view the amount of space used in the Media Server Deduplication Pool? (Select two.)

A. Reports > Disk Reports > Disk Storage Unit Status

B. Device Monitor > Disk Pools

C. Reports > Disk Reports > Disk Logs

D. Devices > Disk Pools

E. Reports > Disk Reports > Disk Pool Status

ANSWER: D E

Explanation:

The administrator can view MSDP capacity usage from **Devices > Disk Pools** and from **Reports > Disk Reports > Disk Pool Status**. The Disk Pools view is the operational console location for inspecting configured disk pools, including an MSDP disk pool's capacity-related values. It provides the pool-level information needed to determine how much of the pool is occupied, based on its reported total and available capacity. This makes it useful when checking the current condition of a specific deduplication pool while administering storage.

The Disk Pool Status report provides the reporting view of disk-pool capacity and status. It can be used to review the amount of storage consumed and remaining for disk pools, including Media Server Deduplication Pool storage, in a report-oriented format. Using these two locations gives an administrator both an immediate administration-console view and a disk-storage status report for monitoring MSDP space utilization. Veritas documents disk-pool administration and monitoring in the NetBackup Administrator's Guide and maintains NetBackup product documentation through its documentation portal: NetBackup Administrator's Guide and Veritas product documentation.