

Administration of Veritas NetBackup 8.0 and NetBackup Appliances 3.0

Veritas VCS-277

Version Demo

Total Demo Questions: 26

Total Premium Questions: 261

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Configure NetBackup	116
Topic 2, Configure a NetBackup Appliance	10
Topic 3, Use NetBackup	35
Topic 4, Maintain NetBackup	29
Topic 5, Troubleshoot NetBackup	53
Topic 6, Perform NetBackup Appliance Administration	18
Total	261

QUESTION NO: 1

Which two performance scenarios benefit from seeding the MSDP pool? (Select two.)

- A. new client backups over WAN
- B. new application backups over SAN
- C. new VADP VMware backups using media server as the backup host
- D. new replication to a new DR site
- E. new clients with large file systems containing small files

ANSWER: A E

Explanation:

Seeding an MSDP pool is beneficial for *new client backups over WAN* because it establishes the deduplication information needed to identify duplicate content before large amounts of data must traverse a constrained or high-latency connection. With an effective seed, subsequent backups can send only the unique data segments that are not already represented in the deduplication pool, reducing WAN traffic and improving backup throughput.

Seeding also benefits *new clients with large file systems containing small files*. Processing many small files can create substantial metadata, fingerprinting, and comparison work. A seeded pool gives the deduplication process an established basis for recognizing data that is already known, helping reduce the amount of data that must be transferred and stored while making the initial protection of this type of client more efficient. These use cases align with Veritas guidance for MSDP pool seeding, which is intended to improve initial backup performance when network capacity or the characteristics of a new client's data set would otherwise make deduplication processing more costly. See the Veritas MSDP documentation at [MSDP web deliverable](#) and the [NetBackup Deduplication Guide](#).

QUESTION NO: 2

Veritas recommends that TLS (Transport Layer Security) be enabled for security purposes when using appliance syslog forwarding.

Which step must the administrator perform first to upload the certificate files which are required for TLS Anonymous Authentication configuration?

- A. copy the certificate and private key files:ca-server.pem, nba-rsyslog.pem and nba-rsyslog.key to a non-appliance location
- B. run Settings > LogForwarding ShareOpen to open NFS and CIFS shares on the appliance
- C. mount an NFS or a CIFS share to `appliance_name/inst/logforwarding` on the server where the certificates reside
- D. upload the certificate and private key files to `inst/logforwarding`

ANSWER: B

Explanation:

The required first step is to run **Settings > LogForwarding ShareOpen** to open NFS and CIFS shares on the appliance. This appliance command makes the Log Forwarding share available to an administrator over the network, providing the controlled location used to transfer the certificate authority certificate, appliance certificate, and private-key files needed for TLS anonymous authentication. After the share has been opened, the administrator can mount the appropriate NFS or CIFS export from the system holding the certificate files and place the files in the appliance's Log Forwarding directory. Opening the share first is essential because it establishes the transfer path before any remote host can access that location to upload the required TLS material. Veritas documents this certificate-upload workflow as part of configuring secure syslog forwarding on NetBackup appliances. The share should be used only for the required transfer and administered according to the organization's security procedures. See Veritas guidance in [NetBackup Appliance syslog forwarding TLS configuration](#) and the [NetBackup Appliances Commands Reference Guide](#).

QUESTION NO: 3

Which two actions should an administrator take to allow NetBackup to manage the allocation of volumes to volume pools? (Select two.)

- A. define a scratch pool and add all of the volumes to it so NetBackup will move volumes to the other pools as volumes are needed
- B. assign volumes to all volume pools as required in the environment
- C. define a scratch pool with assigned volumes so NetBackup will move the assigned volumes to other pools as volumes are needed
- D. create volume pools as required, but refrain from adding volumes to the pools
- E. assign volumes to NetBackup and DataStore volume pools so NetBackup will move the assigned volumes to other pools as volumes are needed

ANSWER: A D

Explanation:

To let NetBackup manage media allocation dynamically, the administrator should define a scratch pool and add all of the volumes to it so NetBackup will move volumes to the other pools as volumes are needed, and create volume pools as required, but refrain from adding volumes to the pools. A scratch pool is a special volume pool that supplies unassigned media to other eligible volume pools. When a backup requires media and a target volume pool has no suitable available volume, NetBackup can select a volume from the scratch pool and assign it to the requesting pool. This assignment is controlled by NetBackup according to the storage unit, volume pool, media type, and availability requirements of the job. Keeping the operational volume pools empty initially is important to this workflow because it leaves the media in the scratch pool, where it remains available for automatic assignment to whichever pool needs it. After NetBackup assigns a volume from scratch, that volume is no longer a scratch volume and is associated with the destination volume pool. This approach centralizes spare-media management and avoids manually preallocating media among pools. See Veritas guidance on [scratch pools and media management](#) and the [NetBackup Administrator's Guide](#).

QUESTION NO: 4

An administrator needs to identify the backup IDs for all backup images of client1.example.com that were created during the previous day.

Which command should the administrator use?

- A. bpimagelist
- B. bpmedialist
- C. bpdjobs
- D. bppllist

ANSWER: A

Explanation:

The `bpimagelist` command is used to list NetBackup backup images from the catalog. It supports options to filter images by client name and time range, allowing the administrator to locate the backup IDs that were created for a particular client during a specified period. The backup ID can then be used with other NetBackup commands, such as `bpexpdate`, `bpduplicate`, or `nbrestorevm`, where applicable.

The `bpmedialist` command displays media information, `bpdjobs` reports job information, and `bppllist` displays policy configuration. See the [Veritas NetBackup documentation portal](#) for NetBackup command reference information.

QUESTION NO: 5

A policy is created using the Standard policy type. The default settings are used. Linux hosts s1 and s2 are added in the client list and ALL_LOCAL_DRIVES is specified in the Backup Selection.

Host s1 has the mount points listed below:

/

/opt

/usr

/usr/home

Host s2 has the mount points listed below:

/

/proc

/tmp

/usr

How many streams will be created when the policy runs for both clients?

- A. two
- B. four
- C. five
- D. eight

ANSWER: A

Explanation:

two is correct. In a Standard policy using the default settings, NetBackup does not enable the policy's multiple-data-stream capability. Consequently, each client is backed up as one stream (one client backup job), even when the ALL_LOCAL_DRIVES directive expands to identify multiple local file systems on that client. The mount-point layout therefore does not cause separate streams for /, /opt, /usr, and the other listed file systems under the default policy configuration.

Because the policy contains two clients, s1 and s2, NetBackup creates one stream for s1 and one stream for s2, for a total of two streams. To produce separate streams for eligible file systems, an administrator would need to explicitly configure the policy to allow multiple data streams; that is not part of the stated default configuration. NetBackup documentation describes policy configuration and the multiple-stream setting in the [NetBackup Administrator's Guide, Volume I](#). Veritas also documents NetBackup product documentation access through its [NetBackup documentation portal](#).

QUESTION NO: 6

Which two NetBackup server roles can be configured on a NetBackup appliance? (Select two.)

- A. master server
- B. media server
- C. client
- D. robot controller
- E. OpsCenter server

ANSWER: A B

Explanation:

A NetBackup appliance can be configured as a **master server** or as a **media server**. When configured as a master server, the appliance hosts the NetBackup catalog and performs centralized policy, scheduling, and job-management functions. When configured as a media server, the appliance provides the backup and restore data path and can host storage such as an MSDP pool.

A NetBackup client is a protected host rather than an appliance server role. A robot controller and an OpsCenter server are not NetBackup appliance roles. See the [Veritas NetBackup Appliance documentation](#) for appliance role and deployment information.

QUESTION NO: 7

Weekly full backups run for clientA on master1 using a storage unit that belongs to media1. The administrator is required to retain clientA's full backups for a period of four months. When the administrator modifies the Full schedule, four months is missing from the selection list.

Where should the administrator add the four-month retention period under Host Properties?

- A. Master Servers > master1 > Retention Periods
- B. Clients > clientA > Global Attributes
- C. Media Servers > media1 > Retention Periods
- D. Master Servers > master1 > Global Attributes

ANSWER: A

Explanation:

Master Servers > master1 > Retention Periods is the correct location because retention periods are configured as master-server settings in NetBackup. A schedule's retention setting selects from the retention levels that have been defined for the master server managing the policy. Therefore, when the required four-month value is absent while editing the Full schedule, the administrator must first add or adjust a retention level under the Retention Periods host-property node for master1. After that retention period is defined, it becomes available for selection in the policy schedule.

Retention is applied to backup images and governs how long NetBackup keeps the image and its associated catalog information available for restore. The configured duration is represented by a retention level; policies and schedules use that level rather than creating an arbitrary duration directly in every schedule. Because master1 owns the NetBackup catalog and policy configuration for clientA, its retention-period configuration controls the values available to this backup policy. The storage unit's association with media1 affects where backup data is written, but the policy's available retention values originate from the master server. Veritas documents retention configuration in the NetBackup Administration Guide: [NetBackup Documentation](#) and its product documentation portal: [NetBackup 8.0 Documentation](#).

QUESTION NO: 8

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 an administrator to ensure the DR file is available for future use? (Select 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 C

Explanation:

The correct safeguards are to **ensure the DR file is created on a volume other than the NetBackup volume** and to **ensure the NetBackup catalog is on a non-root volume**. A catalog backup produces a disaster-recovery file containing essential information needed to recover the NetBackup environment. That file must remain accessible even if the volume containing the NetBackup installation is lost, damaged, or must be rebuilt during disaster recovery. Storing it on a separate volume isolates the recovery instructions from the software volume that may be affected by the same failure.

Locating the NetBackup catalog on a non-root volume is also an available protection measure. It separates critical catalog data from the operating system root filesystem and supports recovery planning when the root volume is unavailable or requires reinstallation. Together, these measures reduce the risk that a single volume failure removes both the NetBackup environment and the information required to restore it. Veritas documents catalog backup and disaster-recovery procedures in the [NetBackup Administrator's Guide, Volume I](#) and provides NetBackup documentation resources at [Veritas NetBackup Documentation](#).

QUESTION NO: 9

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 parent and child jobs?

- A. right-click the failed job and select **Sort** , and sort by **Job PID**
- B. double-click the failed job and select the **Detailed Status** tab
- C. right-click the failed job and select **View Job Hierarchy**
- D. right-click the failed job and select **Troubleshooter**

ANSWER: C

Explanation:

right-click the failed job and select View Job Hierarchy is correct because NetBackup represents operations that generate multiple jobs as a parent-and-child job structure. For example, a policy execution can create a parent job that coordinates one or more child jobs that perform the actual backup, duplication, or other work. Viewing the hierarchy from the failed job provides the administrator with the associated job tree, allowing them to identify the parent job and all related child jobs together and review their completion states. This is especially useful when the Activity Monitor contains a large number of jobs and the administrator needs to assess the outcome of the complete operation rather than only the individual failed job. The hierarchy view is designed specifically for tracing related jobs and their relationships from a selected job record. Veritas documents Activity Monitor job monitoring and job-related administrative tasks in the NetBackup Administrator's Guide, Volume I: [NetBackup documentation](#). Additional NetBackup product documentation and version-specific guides are available through the [Veritas Documentation portal](#).

QUESTION NO: 10

An administrator is adding a new media server appliance to an existing NetBackup appliance master server.

What is the correct sequence to configure the new appliance in the NetBackup domain?

- A. configure the new media server, the configuration process automatically adds the new server to the master server

- B. configure the new media server, then manually add the new media server to the master server's bp.conf
- C. configure the new media server, then add the new media server to the master server in the Web console under Manage > Additional Servers
- D. add the new media server to the master server in the Web console under Manage > Additional Servers, then configure the new media server

ANSWER: D

Explanation:

The correct sequence is to add the new media server to the master server in the Web console under Manage > Additional Servers, then configure the new media server. This establishes the appliance as an authorized and known host in the existing NetBackup domain before its media-server role is configured. The master appliance supplies the domain relationship and the information needed for the new appliance to join the correct NetBackup environment during its initial configuration.

Adding the appliance first is especially important in appliance deployments because the configuration workflow relies on the master server recognizing the media server and allowing the secure trust and host configuration process to proceed. After the appliance has been listed as an additional server on the master appliance, the media-server appliance can be configured with the master server details and complete its role-specific setup. This ordering avoids attempting to configure a media server before the master server has registered it as part of the domain. Veritas documents this process in its NetBackup Appliance guidance; see [Veritas knowledge base article 000115103](#) and the [NetBackup Appliance documentation](#).

QUESTION NO: 11

Some NetBackup jobs are affected by the failure of a disk in an Advanced Disk pool, but the jobs are unavailable to view in the Activity Monitor.

In which two places can the administrator view Net Backup jobs affected by the disk failure? (Select two.)

- A. Media and Device Management > Device Monitor > Disk Pool
- B. NetBackup Management > Reports > Disk Reports > Disk Logs
- C. NetBackup Management > Reports > Disk Reports > Disk Pool Status
- D. NetBackup Management > Reports > Disk Reports > Disk Storage Unit Status
- E. NetBackup Management > Reports > Media Logs

ANSWER: B E

Explanation:

NetBackup Management > Reports > Disk Reports > Disk Logs and **NetBackup Management > Reports > Media Logs** provide historical reporting data that remains available when an affected job is no longer displayed in Activity Monitor. Disk Logs records activity and errors associated with disk-based storage, including events relevant to an AdvancedDisk pool and its constituent disks. An administrator can use this report to identify disk-related failures and correlate the reported activity with the affected backup processing.

Media Logs provides the media-oriented record of NetBackup job activity. It can be used to locate the job information associated with the affected backup data and to review the job's recorded media operations and status after the job has left the normal Activity Monitor view. Together, these reports provide the disk-storage event perspective and the job/media history needed to investigate the impact of a failed disk in an AdvancedDisk pool. Veritas documents the available NetBackup reporting capabilities in the [NetBackup Administrator's Guide](#) and provides NetBackup product documentation through the [Veritas Documentation portal](#).

QUESTION NO: 12

What is the default length of time that true image restore (TIR) information is retained in the NetBackup catalog?

- A. 1 day
- B. 3 days
- C. 28 days
- D. 30 days

ANSWER: A

Explanation:

NetBackup retains true image restore (TIR) information in the catalog for **1 day** by default. TIR data is file-level metadata that NetBackup collects for an image, allowing users to browse and select individual files and directories during restore operations without needing to scan the entire backup image. Because this metadata can consume catalog space, its retention is managed separately from the backup image's normal retention period. The default one-day setting provides short-term file-level restore browsing capability while limiting ongoing catalog growth. Administrators can alter the TIR-information retention behavior when operational requirements call for longer availability of granular restore information, but such changes should account for catalog sizing and processing overhead. The setting applies to the TIR metadata maintained by the NetBackup catalog; it does not change the retention period of the underlying backup image itself. Veritas documents TIR as catalog information used to support file and directory restore selection and describes its management in the NetBackup Administrator's Guide. See the [NetBackup documentation portal](#) and the [Veritas knowledge base](#) for NetBackup catalog and true image restore information.

QUESTION NO: 13

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? (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 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** provide the most useful evidence because processing an ALL_LOCAL_DRIVES selection occurs at the Windows client and depends on that client's local volumes, file-system services, and snapshot-related components. The Windows Application and System event logs can identify underlying volume, VSS, storage-driver, file-system, or service failures that NetBackup reports only as a backup failure. These events often supply the Windows error code and component name needed to correct the condition.

The client-side `bpfis` log records NetBackup file-system processing associated with identifying and accessing the local drive selections. It can show the point at which NetBackup encounters a problem while resolving the requested local drives or interacting with the client file system. Correlating the timestamps and error messages in this log with Windows Event Viewer entries establishes whether the failure originates in NetBackup's file-system processing or in the Windows host environment. Veritas documentation on NetBackup diagnostic logging and Windows-client troubleshooting is available in the [NetBackup Troubleshooting Guide](#) and through the [Veritas support documentation search](#).

QUESTION NO: 14

An administrator needs to back up 100 clients using 10 LTO5 tape drives.

Which policy setting will perform the backup fastest?

- A. Allow multiple data streams
- B. Limit jobs per policy
- C. Media multiplexing
- D. Use Accelerator

ANSWER: C

Explanation:

Media multiplexing is the appropriate setting because it lets NetBackup write data from multiple backup jobs concurrently to a single tape drive. With a large number of clients relative to the available tape drives, multiplexing enables NetBackup to keep the LTO5 drives supplied with data while many client jobs are active. This is especially valuable when an individual client or stream cannot continuously provide data fast enough to maintain the native streaming rate of an LTO drive. Keeping drives streaming reduces start-and-stop tape motion, commonly called shoe-shining, and improves aggregate backup throughput.

NetBackup controls this behavior through the policy's multiplexing setting, which determines the number of jobs that can share a drive concurrently. The setting should be selected with awareness of the recovery requirement: data from multiplexed jobs is interleaved on the tape, so restores can require the tape to traverse data belonging to other jobs. For a backup-window objective involving 100 clients and only 10 tape drives, however, using media multiplexing is the policy-level choice that best maximizes concurrent use of the available tape hardware. Veritas documents multiplexing and its tape-drive behavior in the [NetBackup documentation portal](#) and the [Veritas NetBackup knowledge base](#).

QUESTION NO: 15

Backups are failing with status code 96 because tapes have NOT returned to the scratch volume pool after all the images on the tapes have expired.

What may be preventing the media from returning to the scratch pool?

- A. The media was created in volume pools other than the scratch pool.
- B. The media is in an off-site location.
- C. The media was written with multiplexed images.
- D. The media is in a **Suspended** state.

ANSWER: A

Explanation:

The media was created in volume pools other than the scratch pool. NetBackup's scratch-pool handling is intended to manage unallocated media that is supplied from a scratch pool for use by another eligible volume pool. When the final NetBackup image on such media expires, NetBackup can make the media available again through the scratch-pool process, subject to the pool configuration and media state. Media that was created or introduced directly in a non-scratch volume pool does not have that scratch-pool allocation relationship. Consequently, expiration of all images alone does not cause it to be reassigned automatically to the scratch pool. An administrator must manage the volume's pool assignment as appropriate before it can contribute to the scratch inventory used for future backups. Maintaining sufficient eligible scratch media is important because NetBackup status code 96 indicates that no media is available for the requested backup operation. The NetBackup Administrator's Guide describes volume pools, scratch media, and media allocation behavior; see the [NetBackup Administrator's Guide documentation](#). For the status-code definition and operational guidance, consult [Veritas NetBackup status code 96 information](#).

QUESTION NO: 16

An administrator plans to use NetBackup-managed tape encryption for long-term backup copies.

Which two requirements must be met for hardware encryption of the tape media? (Select two.)

- A. encryption-capable tape drives
- B. a configured Key Management Service environment
- C. a scratch volume pool
- D. multiplexing enabled on the storage unit
- E. a disk staging storage unit

ANSWER: A B

Explanation:

Hardware encryption requires **encryption-capable tape drives** because the tape drive performs encryption as data is written to the media. NetBackup must also have a configured **Key Management Service (KMS)** environment to create, manage, and retrieve the encryption keys that are required to write and restore encrypted backup images.

A scratch pool supplies unassigned tapes and does not provide encryption. Multiplexing affects tape-drive stream usage, while a disk staging storage unit is unrelated to tape hardware encryption. See the [Veritas NetBackup documentation portal](#) for NetBackup encryption and key-management guidance.

QUESTION NO: 17

After creating a NBU-Catalog 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 an administrator to ensure the DR file is available for future use? (Select 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. specify a user that has credentials to the volume that contains NetBackup binaries
- D. configure a valid email address of the administrator in the Send email option
- E. specify the NBU-Catalog backup policy as a critical policy

ANSWER: B D

Explanation:

“ensure the DR file is created on a volume other than the NetBackup volume” is correct because the disaster recovery file must be stored independently of the disk or partition that holds the NetBackup catalog. A catalog backup creates the disaster recovery information needed to rebuild the NetBackup master server configuration and catalog after a catastrophic failure. Placing that file on separate storage preserves access to the recovery instructions when the catalog volume itself is unavailable. NetBackup provides configuration for the disaster recovery file location as part of catalog-backup configuration, and administrators should select a location protected from the same storage failure domain.

“configure a valid email address of the administrator in the Send email option” is also correct because NetBackup can email the disaster recovery file after the catalog backup completes. This creates an additional off-host copy that can be retrieved during recovery, provided the email system is accessible and the recipient retains the message securely. Using both a separate volume and email delivery provides independent availability paths for the recovery information. Veritas describes catalog backup and disaster recovery file handling in the [NetBackup Administrator's Guide](#) and the [Veritas knowledge base guidance for catalog disaster recovery](#).

QUESTION NO: 18

What happens if the Maximum data streams property is enabled for a particular client?

- A. NetBackup ignores Maximum jobs per client and uses either Limit jobs per policy or Maximum indexing jobs per indexing server, whichever is lowest
- B. NetBackup ignores Maximum jobs per client and uses either Maximum data streams or Limit jobs per policy, whichever is lowest
- C. NetBackup ignores Maximum indexing jobs per indexing server and uses Maximum jobs per client or the Limit jobs per policy, whichever is lowest
- D. NetBackup ignores Limit jobs per policy and uses either Maximum data streams or Maximum jobs per client, whichever is lowest

ANSWER: B

Explanation:

When the *Maximum data streams* property is enabled for a client, NetBackup uses that client-specific setting to control concurrent backup streams instead of the global *Maximum jobs per client* host-property setting. This lets an administrator tune concurrency for a particular client according to its available CPU, memory, network bandwidth, storage performance, and ability to process simultaneous backup operations. The effective number of streams is still constrained by the policy's *Limit jobs per policy* value: NetBackup uses whichever of the client's Maximum data streams value and the policy limit is lower. For example, a client configured for six maximum data streams in a policy limited to four jobs can run no more than four concurrent jobs under that policy. This behavior is useful where most clients should follow a common global concurrency limit but a specific client requires a different limit. It prevents the global per-client limit from overriding the explicit Maximum data streams value while retaining the policy-level safeguard against excessive simultaneous activity. See Veritas documentation for the client host properties and job-concurrency controls in the [NetBackup Administrator's Guide, Volume I](#) and the [NetBackup documentation portal](#).

QUESTION NO: 19

An administrator has a backup policy with the following attributes:

5 paths listed in the Backup Selections list

3 clients listed in the Clients list

Allow multiple data streams is selected

Max Jobs per Client value set to 4

How many jobs go Active when the job is started, excluding parent jobs?

- A. 8
- B. 9
- C. 12
- D. 15

ANSWER: C

Explanation:

12 is correct. With *Allow multiple data streams* enabled, NetBackup can divide a client backup into separate child jobs based on the backup selections, allowing multiple streams to process concurrently. The five listed paths provide up to five potential streams for each client. However, the policy's *Max Jobs per Client* setting limits concurrent active child jobs for any one client to four. Therefore, each of the three clients can start four active child jobs, rather than all five potential path-based streams at once. The active-job calculation is consequently three clients multiplied by four concurrent jobs per client, for a total of 12

active child jobs. Parent jobs are excluded because they coordinate the policy execution; the question specifically requests the jobs that become Active for the actual backup streams. NetBackup may queue any remaining stream for a client until an active stream completes and a per-client job slot becomes available. Veritas documents multiple data streams and the per-client job limit in the NetBackup Administrator's Guide, Volume I: [NetBackup 8.0 documentation](#). The relevant operational behavior is also covered in Veritas NetBackup product documentation: [Veritas NetBackup documentation portal](#).

QUESTION NO: 20

Some NetBackup jobs are affected by the failure of a disk in an AdvancedDisk pool, but the jobs are unavailable to view in the Activity Monitor.

In which two places can the administrator view NetBackup jobs be affected by the disk failure? (Select two.)

- A. Media and Device Management > Device Monitor > Disk Pool
- B. NetBackup Management > Reports > Disk Reports > Disk Logs
- C. NetBackup Management > Reports > Disk Reports > Disk Pool Status
- D. NetBackup Management > Reports > Disk Reports > Disk Storage Unit Status
- E. NetBackup Management > Reports > Media Logs

ANSWER: B E

Explanation:

NetBackup Management > Reports > Disk Reports > Disk Logs is a suitable place to investigate the impact because Disk Logs report disk-related operations and errors. When an AdvancedDisk pool member fails, this report provides the disk-level event information needed to identify operations that encountered the failed disk and to correlate those events with the affected job activity.

NetBackup Management > Reports > Media Logs also provides visibility for jobs whose processing was affected but which are no longer displayed in Activity Monitor. Media Logs retain media-management activity, including job-related entries associated with storage operations. Reviewing this report lets an administrator locate historical job information and relevant status details around the time of the disk failure.

Together, the disk-focused log and the media-management log provide the appropriate reporting paths for determining which jobs were affected after a disk failure in an AdvancedDisk pool, particularly when the active-job display no longer contains those jobs. Veritas documents this troubleshooting approach in its support guidance: [Veritas support article 000119038](#).

QUESTION NO: 21

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:

```

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: GLOBALROT\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.fm.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 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 because ALL_LOCAL_DRIVES backups on a Windows client require NetBackup to enumerate and protect local volumes, often using the Windows snapshot framework. The bpfis process is the client-side NetBackup component that coordinates snapshot activity and records detailed diagnostic information about snapshot creation, provider interaction, and file-system-related failures. Its client log can therefore identify the specific operation and underlying Windows error that caused the backup to fail.

The Windows client's operating-system event logs, especially the Application and System logs, provide the corresponding operating-system evidence. They can report VSS writer or provider failures, volume and file-system conditions, service errors, and other Windows events occurring at the same time as the NetBackup job. Correlating timestamps and error messages between these logs and bpfis output is the appropriate way to isolate whether the condition is caused by the Windows snapshot subsystem, a local volume, or a related client service.

Veritas documents bpfis as part of the snapshot-processing workflow and describes gathering client-side NetBackup logs for troubleshooting. See the [NetBackup Troubleshooting Guide](#) and the [NetBackup Logging Guide](#).

QUESTION NO: 22

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 or attributes, the backup must be created with granular recovery enabled. Selecting *choose the "Enable granular recovery" option in the policy* causes NetBackup to prepare the Active Directory backup for Granular Recovery Technology (GRT). GRT is what allows the administrator to browse backed-up Active Directory content and select specific directory objects or attributes for recovery instead of performing only a full system-state or directory-services restore.

The Active Directory client must also provide the Network File System service, represented by *enable the Network File System (NFS) on the client*. During a granular restore, NetBackup accesses the backup contents through its granular-recovery mounting workflow. The NFS capability on the Windows domain controller is required to support that access and enables NetBackup to present the required recovery view for object-level selection. These prerequisites apply before the administrator performs the restore from the NetBackup console.

Veritas documents granular recovery configuration and the required client-side components in the [NetBackup Administrator's Guide, Volume I](#). Additional NetBackup documentation and version-specific guidance are available from the [Veritas NetBackup Support portal](#).

QUESTION NO: 23

A Netbackup environment suffers from intermittent network outages between the Media Server Drduplication Pool (MSOP) media server and clients during the backup window. This results in multiple backup failures.

How should an administrator overcome the backup failure issue?

- A. enable Network Resiliency
- B. configure client-side deduplication
- C. increase the client connect timeout
- D. increase the CR_STATS_TIMLR interval

ANSWER: A

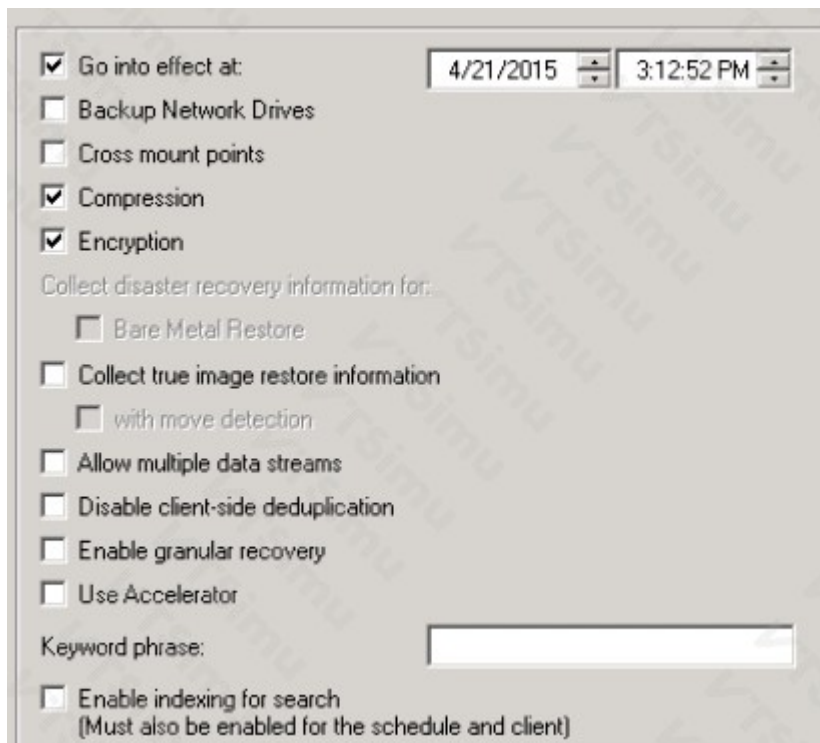
Explanation:

enable Network Resiliency is correct because NetBackup Network Resiliency is specifically designed to let a backup job survive temporary loss of connectivity between a client and the media server that is receiving its backup data. When the connection is interrupted, NetBackup retains the job state and waits for communication to be restored rather than immediately treating the interruption as an unrecoverable backup failure. After the client and media server reconnect within the configured resiliency period, data transfer can continue, allowing the backup to complete without requiring the administrator to restart the entire job.

This capability is particularly relevant when the affected path is between protected clients and a media server used with a media server deduplication pool. It addresses transient network instability during the backup window while preserving the intended client-to-media-server data path and deduplication workflow. The administrator should enable and configure Network Resiliency according to the expected duration of the outages and the organization's backup-window requirements. Veritas documents Network Resiliency as a NetBackup feature for handling temporary client/media-server connection failures in the [NetBackup Administrator's Guide](#). Additional NetBackup documentation is available through the [Veritas Documentation portal](#).

QUESTION NO: 24

Refer to the exhibit.



The screenshot shows the 'Policy Configuration' window for a Veritas NetBackup policy. The 'Go into effect at' field is set to 4/21/2015 at 3:12:52 PM. The 'Backup Network Drives' checkbox is unchecked. The 'Cross mount points' checkbox is unchecked. The 'Compression' checkbox is checked. The 'Encryption' checkbox is checked. The 'Collect disaster recovery information for:' section has 'Bare Metal Restore' unchecked and 'Collect true image restore information' unchecked, with 'with move detection' also unchecked. The 'Allow multiple data streams' checkbox is unchecked. The 'Disable client-side deduplication' checkbox is unchecked. The 'Enable granular recovery' checkbox is unchecked. The 'Use Accelerator' checkbox is unchecked. The 'Keyword phrase' field is empty. The 'Enable indexing for search' checkbox is unchecked, with a note below it stating '(Must also be enabled for the schedule and client)'.

What is the outcome of the policy shown in the exhibit?

- A. The client encrypts then compresses the data before sending it to the Media Server.
- B. The client compresses and the Media Server encrypts the data before sending it to the tape drive.
- C. The client compresses then encrypts the data before sending it to the Media Server.
- D. The client sends the data to the Media Server, which compresses and then encrypts the data.

ANSWER: C

Explanation:

The client compresses then encrypts the data before sending it to the Media Server. The policy settings shown enable client-side compression and client-side encryption, so both operations occur on the NetBackup client before the backup stream leaves the client host. NetBackup first compresses the backup data, reducing the amount of data that must be transmitted and stored. It then encrypts that compressed stream to protect its confidentiality while it travels to the media server and is ultimately written to storage. This sequence is significant because compression is effective only on unencrypted, patterned data; encryption transforms data into an intentionally non-patterned form that should not be compressed afterward. The media server therefore receives an already compressed and encrypted backup stream and manages its movement to the selected storage destination. NetBackup policy attributes determine whether compression is performed by the client or media server, while encryption configuration controls where the backup data is encrypted. For additional details on policy configuration and encryption behavior, see the [Veritas NetBackup documentation](#) and the [Veritas NetBackup encryption guidance](#).

QUESTION NO: 25

An administrator configures a VMware backup host to use SAN transport for virtual-machine backups.

Which two conditions are required for the backup host to use SAN transport? (Select two.)

- A. the backup host has physical SAN access to the datastore LUNs

- B. the datastore LUNs are visible to the backup host
- C. VMware Tools is installed on the backup host
- D. the virtual machines are powered off before the backup begins
- E. the backup host is configured as the vCenter Server

ANSWER: A B

Explanation:

The backup host must have physical Fibre Channel or iSCSI access to the datastore LUNs, and the datastore LUNs must be visible to the backup host. SAN transport reads virtual-machine disks directly from the SAN rather than transferring the backup data through the ESXi management network. Zoning, LUN masking, and operating-system configuration must allow the backup host to discover and read the required datastore devices.

The backup host should not mount or modify the datastore file systems. NetBackup accesses the underlying datastore devices for backup processing while VMware continues to manage the virtual-machine files. See the [Veritas NetBackup documentation portal](#) for VMware transport-mode requirements.

QUESTION NO: 26

Which two appliance performance scenarios benefit from seeding the MSDP pool? (Select two.)

- A. new client backups over WAN
- B. new application backups over SAN
- C. new VADP VMWare backups using Media Server as the backup host
- D. new replication to a new DR site
- E. new clients with large file systems containing small files

ANSWER: A D

Explanation:

Seeding an MSDP pool is particularly valuable for *new client backups over WAN* and for *new replication to a new DR site*. In both cases, the initial full dataset would otherwise require a substantial transfer across a bandwidth-constrained or high-latency network. Pool seeding establishes the initial data set locally on the target MSDP storage, allowing subsequent NetBackup deduplication processing and optimized duplication to transfer only the changed or unique segments. This sharply reduces WAN utilization and shortens the time needed to establish protection for remote clients or a disaster-recovery copy. For a new DR site, seeding avoids sending the entire initial protected data set over the network before regular optimized duplication can operate efficiently. After the seed is in place, replication can continue with the smaller deduplicated deltas that are typical of MSDP optimized duplication. Veritas describes MSDP as its deduplication storage technology and documents optimized duplication as a mechanism for efficiently moving deduplicated backup images between storage locations. See the [NetBackup Appliance documentation](#) and the [NetBackup Deduplication Guide](#) for MSDP and optimized-duplication guidance.