

Administration of Veritas NetBackup 8.1.2

Veritas VCS-278

Version Demo

Total Demo Questions: 25

Total Premium Questions: 251

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, NetBackup Architecture	9
Topic 2, NetBackup Configuration	47
Topic 3, NetBackup Storage	76
Topic 4, NetBackup Backup	45
Topic 5, NetBackup Restore	27
Topic 6, NetBackup Monitoring and Troubleshooting	47
Total	251

QUESTION NO: 1

A backup job is showing the following error message:

```
Dec 5, 2018 4:11:02 PM - Info nbjm (pid=40455) starting backup job (jobid=369) for client
WIN-TN3QANTSQ1B.vrtslab.br, policy Oracle_SO_Dedup, schedule FULL
Dec 5, 2018 4:11:02 PM - Info nbjm (pid=40455) requesting STANDARD_RESOURCE resources from
RB for backup job (jobid=369, request id:{201EBB46-F8B9-11EB-B5BA-A118CF05FA8E})
Dec 5, 2018 4:11:02 PM - requesting resource __ANY__
Dec 5, 2018 4:11:02 PM - requesting resource nbumasterapp.vrtslab.br.NBU_CLIENT.MAXJOBS.WIN-
TN3QANTSQ1B.vrtslab.br
Dec 5, 2018 4:11:02 PM - Error nbjm (pid=40455) NBU status: 2111, EMM status: All storage
units are configured with On Demand Only and are not eligible for jobs requesting ANY storage unit
All storage units are configured with On Demand Only and are not eligible for jobs requesting
ANY storage unit (2111)
```

Which two actions can an administrator perform to ensure the backup completes successfully?

(Choose two.)

- A. ensure at least one storage unit is without the On Demand Only option selected.
- B. increase the Multiplexing value on the Storage Unit.
- C. increase the "Maximum concurrent jobs" parameter on the Storage Unit.
- D. assign a specific Storage Unit for that policy.
- E. increase the "Limit I/O streams" parameter on the disk volume.

ANSWER: A D

Explanation:

NetBackup must be able to select an eligible storage unit before it can start a scheduled backup. The setting represented by *On Demand Only* reserves a storage unit for jobs that explicitly request it, rather than allowing normal policy-driven scheduling to select it automatically. Therefore, ensuring that at least one storage unit is without the On Demand Only option selected provides NetBackup with a storage resource that is eligible for standard scheduled backup selection.

Assigning a specific Storage Unit for that policy is also an effective way to ensure successful allocation. A policy-level storage-unit selection directs the policy to use the intended eligible target instead of relying solely on automatic selection among available storage units. This is particularly useful when the administrator needs the job to use a designated storage resource or needs to avoid ambiguity in storage-unit selection. The selected storage unit must, of course, be configured and available for the backup workload. NetBackup documentation describes storage-unit selection and the use of the On Demand Only attribute as part of storage configuration and policy behavior. See the [Veritas NetBackup documentation portal](#) and the [NetBackup status code reference](#).

QUESTION NO: 2

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, 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 master 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:

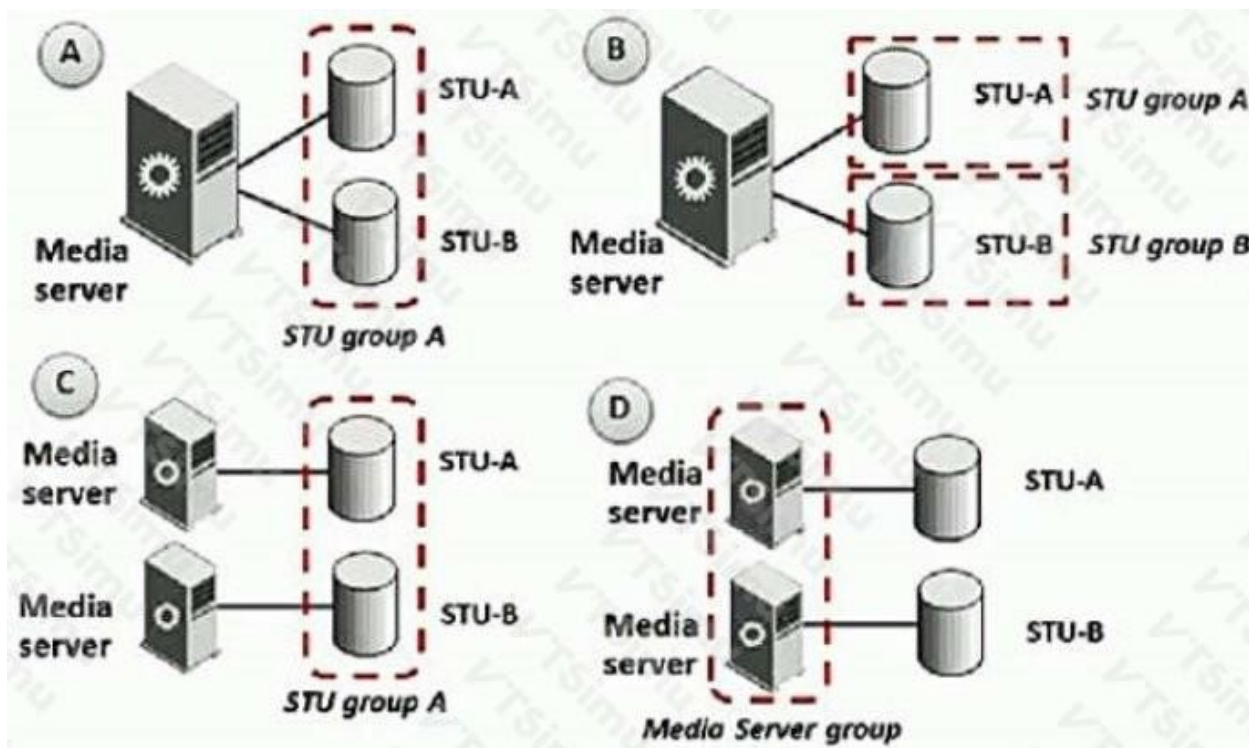
NetBackup retention selections are retention levels that are defined centrally on the master server. The schedule's Retention list displays the configured retention levels, rather than accepting an arbitrary duration directly in that schedule dialog. Therefore, the administrator should modify an existing retention level in the master server host properties, under Retention Periods, and set that level to a four-month duration. Once the master server's retention-period configuration is updated, that retention level becomes available for selection in the full-backup schedule for clientA.

This is appropriate even though the backups are written through a storage unit associated with media1. A media server supplies storage resources and performs media-related operations, but the master server owns the NetBackup catalog and policy configuration, including the retention-level definitions used by policies and schedules. The selected retention level controls how long backup images are retained before they are eligible for expiration and subsequent cleanup processing. Administrators should account for any existing policies or schedules using the retention level before changing it, because a retention-level definition can be shared across configured backup schedules. See Veritas NetBackup documentation at [NetBackup documentation](#) and the [Veritas knowledge base](#).

QUESTION NO: 3

Refer to the Exhibit.

Which diagram is supported for backups spanning BasicDisk storage?



- A. A
- B. B
- C. C
- D. D

ANSWER: C

Explanation:

The supported diagram is the one identified in the exhibit as **C**. In NetBackup, BasicDisk storage is configured as a storage unit containing one or more disk volumes that are accessible to the same media server. When a backup image outgrows the available capacity on the selected BasicDisk volume, NetBackup can continue the image on another eligible disk volume

within that BasicDisk storage unit. This is disk-volume spanning; it depends on the media server having access to each participating volume and on the volumes being configured together under the applicable BasicDisk storage-unit definition.

This design lets NetBackup use multiple locally accessible disk volumes as capacity for a single backup operation while retaining the normal BasicDisk storage-unit management model. The relevant topology therefore shows the backup data path through one media server to multiple disk volumes that belong to its BasicDisk storage. NetBackup documentation describes BasicDisk as storage based on disk volumes attached to a media server and explains its storage-unit configuration and behavior. See the [NetBackup Disk Storage Guide](#) and the [NetBackup Administrator's Guide](#).

QUESTION NO: 4

What is the purpose of the Logon and Password settings in the Disaster Recovery tab of a NetBackup catalog backup policy?

- A. to specify credentials required to access a network share
- B. to encrypt the NetBackup catalog backup data
- C. to require credentials to perform a catalog recovery
- D. to encrypt the disaster recovery file

ANSWER: A

Explanation:

The purpose of “to specify credentials required to access a network share” is to let NetBackup authenticate to the shared location configured for disaster-recovery information generated by the catalog backup policy. During a catalog backup, NetBackup can create disaster-recovery files that contain the information and instructions needed to begin recovering the NetBackup catalog after a major failure. If the disaster-recovery destination is a network share, the NetBackup services must have an account and password with sufficient permissions to connect to that share and write the required files. The Logon and Password fields on the Disaster Recovery tab supply those access credentials; they are operational connection settings for the destination, rather than a mechanism for protecting catalog backup contents. Correct share permissions are important because the disaster-recovery file must be available independently of the failed NetBackup environment when it is needed for recovery. Veritas documents catalog backup and disaster-recovery configuration in the NetBackup Administrator's Guide: [NetBackup core administration documentation](#). Additional NetBackup documentation is available through the [Veritas Documentation portal](#).

QUESTION NO: 5

Which two catalog components contain information on what has been backed up and its metadata in NetBackup? (Choose two.)

- A. Volume
- B. NBDB
- C. Image
- D. Class
- E. Media

ANSWER: B C

Explanation:

NetBackup's catalog is the collection of databases and related information that NetBackup uses to manage protected data and perform restores. **NBDB** is the relational NetBackup database. It stores catalog-related operational and configuration metadata, including information used by NetBackup to track resources and manage backup operations. This database is fundamental to maintaining a consistent view of the NetBackup environment.

The **Image** component, commonly called the image database, records the backup-image details needed to identify and restore protected content. Its records describe what was backed up, such as the client, backup time, policy context, files or objects represented by the backup image, and the media or storage location associated with that image. NetBackup consults this metadata when users browse for files or administrators initiate restores.

Together, NBDB and the image database provide the catalog information that supports backup tracking, image lookup, and recovery operations. Protecting the catalog is therefore essential: without its database and image metadata, NetBackup may be unable to locate backup data for restoration even when the backup storage itself remains available. See Veritas's [NetBackup documentation](#) and the [NetBackup catalog backup guidance](#).

QUESTION NO: 6

Which disk type is unsupported in a Media Server Load Balancing storage unit group?

- A. PureDisk
- B. BasicDisk
- C. AdvancedDisk
- D. Cloud Storage

ANSWER: B

Explanation:

BasicDisk is unsupported in a Media Server Load Balancing (MSLB) storage unit group. MSLB is designed to distribute backup work dynamically among eligible media servers that share access to the storage represented by the storage-unit group. This requires a storage configuration that NetBackup can manage consistently across the participating media servers, including awareness of the disk-pool and storage-server relationships used to select an available write target.

BasicDisk storage units represent directly configured disk paths on an individual NetBackup media server. Because this storage is tied to the local server and does not provide the shared disk-pool abstraction required for MSLB selection and load distribution, it cannot be included in an MSLB storage unit group. Administrators should use an MSLB-supported storage type when they need NetBackup to balance jobs between media servers rather than target a specific locally configured disk path.

Veritas documents storage-unit-group behavior and disk-storage configuration in the [NetBackup Administrator's Guide, Volume I](#). The applicable NetBackup release documentation is also available through the [Veritas NetBackup 8.1.2 documentation portal](#).

QUESTION NO: 7

How can an administrator check deduplication ratios in the NetBackup Administration Console, apart from the Activity Monitor?

- A. NetBackup Management > Storage > Storage Units
- B. Media and Device Management > Devices > Disk Pools
- C. NetBackup Management > Host Properties > Media Servers
- D. Media and Device Management > Credentials > Storage Servers

ANSWER: D

Explanation:

The correct location is **Media and Device Management > Credentials > Storage Servers**. In the NetBackup Administration Console, this view lists configured storage servers and provides access to their properties and operational information. For a

NetBackup deduplication storage server, the displayed information includes deduplication statistics, enabling an administrator to review the deduplication ratio without relying solely on job-specific details in Activity Monitor.

The deduplication ratio indicates the reduction obtained by storing unique data segments rather than repeatedly storing duplicate segments. Reviewing it at the storage-server level is useful for assessing overall deduplication-store efficiency across workloads, monitoring capacity savings, and validating that deduplication processing is producing the expected benefit. The value is associated with the deduplication storage server and its disk-pool environment, so the storage-server administration area is the appropriate console location for this broader operational view.

Veritas documents the Administration Console navigation and storage-server configuration functions in the [NetBackup documentation](#). Additional NetBackup product documentation is available through the [Veritas Documentation portal](#).

QUESTION NO: 8

Which two options are available to an administrator to bring the MSDP catalog back online in the case of a hardware problem that caused corruption? (Choose two.)

- A. restore the MSDP catalog from the NetBackup catalog backup.
- B. recover the MSDP catalog from a MSDP catalog backup.
- C. repair the MSDP catalog using the crchk tool.
- D. restore the MSDP catalog from a MSDP catalog shadow copy.
- E. repair the MSDP catalog using the recoverCR tool.

ANSWER: B D

Explanation:

MSDP maintains its own deduplication catalog, which contains the metadata required to locate and use deduplicated backup data. If hardware damage corrupts that catalog, NetBackup provides recovery paths intended to restore the catalog to a known consistent state and return the storage server to service. An administrator can **recover the MSDP catalog from a MSDP catalog backup**. This uses the catalog-protection data created for MSDP recovery, allowing the content-router catalog metadata to be reconstructed from a valid backup copy.

An administrator can also **restore the MSDP catalog from a MSDP catalog shadow copy**. The shadow-copy mechanism provides an additional recovery source for the MSDP catalog. It is specifically useful when the active catalog has been damaged and a locally maintained shadow copy is available and usable. Both methods address catalog-level recovery rather than simply checking the catalog or attempting a general repair operation. After recovery, standard NetBackup validation and storage-service checks should be completed before resuming normal backup or restore activity. Veritas documents MSDP configuration, catalog protection, and recovery concepts in the [NetBackup documentation](#) and provides related operational guidance through the [Veritas Knowledge Base](#).

QUESTION NO: 9

An administrator is configuring a new device and receives the following error message:

Unable to determine robot type

What are two possible solutions? (Choose two.)

- A. download a new device_mapping file from the Veritas Support website.
- B. ensure the tape drive is closed and ready for use.
- C. perform a rescan of the available tape drives.
- D. verify compatibility for the library with NetBackup.
- E. select the correct device type for the drives.

ANSWER: A D

Explanation:

NetBackup determines a robot type by comparing the device inquiry information that the operating system reports with its device-mapping definitions. Downloading and installing a current `device_mapping` file from Veritas Support can add recognition data for newer or previously unmapped robotic libraries. After the mapping update is installed, the administrator can rerun device discovery or the configuration wizard so NetBackup evaluates the library again using the updated definitions. Veritas distributes product updates and related files through its official Support Downloads area: [Veritas Support Downloads](#).

Verifying compatibility for the library with NetBackup is also essential. A robot must be supported for the applicable NetBackup release, operating system, connection method, and library firmware configuration. The NetBackup Hardware Compatibility List identifies supported robotic-library configurations and helps confirm whether the reported library can be automatically identified and configured by that NetBackup version. If a library is not listed for the required environment, a mapping-file update alone does not establish product support. Consult the current compatibility information before completing the device configuration: [Veritas NetBackup Hardware Compatibility List](#).

QUESTION NO: 10

Which two storage unit types can be configured in NetBackup? (Choose two.)

- A. Deduplication
- B. NDMP
- C. Robot
- D. Media Manager
- E. Tape

ANSWER: B D

Explanation:

NetBackup can configure an **NDMP** storage unit and a **Media Manager** storage unit. An NDMP storage unit is used when NetBackup protects data on NDMP hosts, such as supported NAS filers, through the Network Data Management Protocol. The storage-unit definition identifies the NDMP host and enables NetBackup to direct backup and restore operations appropriately for NDMP-managed storage.

A Media Manager storage unit is used for storage managed through NetBackup Media Manager, most commonly tape devices and tape libraries. It provides the configuration through which NetBackup selects media and drives for jobs targeting the associated robotic or standalone tape environment. In other words, the storage unit is the logical NetBackup destination, while the underlying tape hardware and media resources are administered by Media Manager.

These are distinct selectable storage-unit types in the NetBackup storage-unit configuration workflow for the relevant NetBackup release. Veritas describes the available storage-unit types and their configuration roles in its NetBackup documentation and support material. See [Veritas support article 000117525](#) and the [Veritas NetBackup documentation portal](#).

QUESTION NO: 11

A policy uses a frequency-based automatic backup schedule.

Which two schedule settings control when NetBackup can start the backup? (Choose two.)

- A. Frequency
- B. Backup window

- C. Retention period
- D. Exclude dates
- E. Media multiplexing level

ANSWER: A B

Explanation:

The **frequency** determines how much time must elapse after a successful backup before the schedule is again due to run. The **backup window** defines the period during which NetBackup is allowed to start the backup. For a frequency-based schedule, both conditions affect backup eligibility: the frequency must be satisfied and an appropriate backup window must be open.

Calendar dates and excluded dates apply to calendar-based scheduling rather than frequency-based scheduling. The retention period controls how long the resulting image is retained, not when the backup can start. See the [Veritas NetBackup documentation](#) for policy schedule configuration information.

QUESTION NO: 12

Which two conditions must be met before a NetBackup client can perform a successful backup to a media server? (Choose two.)

- A. The client must be able to resolve and communicate with the NetBackup primary server and media server.
- B. The client must be included in an applicable NetBackup policy.
- C. The client must be configured as a NetBackup primary server.
- D. The client must own the target storage unit.
- E. The client must be configured as a robotic library host.

ANSWER: A B

Explanation:

The client must be able to resolve and communicate with the NetBackup primary server and the selected media server. NetBackup relies on correct host-name resolution and network connectivity for control and data communication between the participating hosts.

The client must also be configured as a client in an applicable policy. The policy identifies the client, specifies the data selections, and supplies the schedules and storage configuration that NetBackup uses for the backup. Connectivity alone is not sufficient when no policy includes the client. See the [Veritas NetBackup documentation portal](#) for client connectivity and policy administration information.

QUESTION NO: 13

To reduce network use by limiting the number of parallel backup streams, which cloud setting should be modified under the Scalable Storage host property?

- A. Metering > Metering interval
- B. Network Connections > Maximum concurrent jobs
- C. Throttling > Total available bandwidth
- D. Throttling > Sampling interval

ANSWER: B

Explanation:

Network Connections > Maximum concurrent jobs is the applicable Scalable Storage host property because it controls how many cloud-storage jobs NetBackup can run simultaneously for that host. A cloud backup stream consumes network connections and transfer capacity while it sends backup data to the cloud provider. Reducing this value limits the number of streams that can be active at the same time, directly reducing aggregate network consumption and preventing the cloud connection from being saturated by parallel work.

This setting is particularly useful when the available WAN bandwidth is shared with production applications, when a cloud provider imposes practical connection limits, or when backup activity must be intentionally paced. The limit applies at the cloud-host connection level, so NetBackup queues additional eligible work until a concurrent job slot becomes available. Consequently, it provides a predictable way to trade backup throughput for lower simultaneous network demand without changing the backup selection or retention configuration. Veritas documents cloud-storage configuration and host properties in its NetBackup documentation resources; see the [Veritas Documentation portal](#) and the [NetBackup product support page](#).

QUESTION NO: 14

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? (Choose two.)

- A. vnetd is stopped on the master server.
- B. The master server is unknown to the client.
- C. The NetBackup processes on the client are stopped.
- D. Nbdiscovery needs to be running on the client.
- E. There is an incorrect entry for the client in the master server's hosts file.

ANSWER: C E

Explanation:

The correct causes are that the NetBackup processes on the client are stopped and that there is an incorrect entry for the client in the master server's hosts file. The `bptestbpcd -client clientA` command tests whether the master server can resolve and establish a NetBackup connection to the specified client's NetBackup Client Service (bpcd). If the client-side NetBackup processes are not running, the client cannot accept the requested NetBackup connection, so the connectivity test fails. Starting the NetBackup Client Service and confirming that its associated NetBackup services are operational restores the endpoint required by the test.

Correct client name resolution on the master server is equally essential. A stale, misspelled, or otherwise incorrect hosts-file mapping can cause `clientA` to resolve to an invalid IP address. In that case, `bptestbpcd` attempts to contact the wrong system rather than the intended NetBackup client and reports a connection failure. Administrators should verify that the client hostname resolves to the client's current, reachable address using the configured name-resolution order, then correct the hosts entry if it overrides valid DNS information. Veritas documents `bptestbpcd` as a utility for testing connectivity to the NetBackup client service; see the [NetBackup Commands Reference Guide](#) and the [NetBackup documentation portal](#).

QUESTION NO: 15

An administrator is attempting to protect 500TB of Windows file system data in a 4-hour backup window, when the file servers are idle. The daily change rate for the data is below 1%, and an Initial full backup has been performed to a high performance disk array configured as an Advanced Disk storage unit.

What can the administrator do to ensure subsequent backups complete within the backup window?

- A. configure NetBackup Accelerator
- B. configure multiplexing
- C. configure client-side deduplication
- D. configure Synthetic backups

ANSWER: A

Explanation:

Configure NetBackup Accelerator. Accelerator is designed for environments in which a conventional full backup would require reading and transferring a very large amount of unchanged client data. After the initial full backup establishes the baseline, Accelerator uses change tracking to identify the data that changed since the prior backup. For subsequent accelerated full backups, the client sends only the changed data while NetBackup combines that data with information from the previous backup image to maintain a complete, full-backup recovery image.

In this scenario, the initial full image already exists on an AdvancedDisk storage unit and the daily change rate is below one percent. Rather than attempting to process and transmit the entire 500 TB data set during every four-hour window, Accelerator limits client-side scanning and network transfer primarily to the relatively small changed portion. This substantially reduces the amount of work required during each subsequent full backup while retaining the restore advantages associated with a full backup image. Accelerator support and configuration requirements, including supported policies and storage considerations, are documented in the NetBackup Administrator's Guide and the NetBackup Accelerator documentation: [Veritas NetBackup documentation](#) and [Veritas NetBackup Accelerator information](#).

QUESTION NO: 16

An administrator needs to back up Windows and Linux file servers to an Advanced Disk storage unit targeting a high speed disk array. Backup traffic shares a busy network with mission critical application traffic.

Which feature can the administrator implement to optimize this backup environment?

- A. network resiliency
- B. client-side deduplication
- C. NetBackup Accelerator
- D. Synthetic backups

ANSWER: D

Explanation:

Synthetic backups are correct because they use existing backup images already stored on disk to construct a new full backup image, rather than requiring the client to resend all protected data across the network for every full backup. After an initial full backup, the file servers can send incremental changes; NetBackup then synthesizes a full backup on the media server using the prior full image and the incremental images. This is particularly useful where the clients share a congested network with business-critical applications, because it substantially reduces the amount of data that must traverse that network during recurring full-backup cycles.

An AdvancedDisk storage unit backed by a high-speed disk array is an appropriate target for this workflow because the storage system must efficiently read the existing backup images and write the synthesized full image. The result is a current full backup image available for restore and retention requirements while minimizing client processing and network utilization compared with repeatedly performing conventional full backups. NetBackup documentation describes synthetic backups as a

disk-based capability that creates a full backup from previous full and incremental backups. See the [NetBackup Administrator's Guide, Volume I](#) and the [NetBackup documentation portal](#).

QUESTION NO: 17

An administrator has a backup policy with the following policy attributes:

3 paths listed in the Backup Selections list

5 clients listed in the Clients list

"Allow multiple data streams" is selected

"Limit jobs per policy" is set to 4

How many jobs go Active when the job is started, excluding parent jobs, assuming there are enough storage resources to handle the expected jobs?

- A. 3
- B. 4
- C. 12
- D. 15

ANSWER: B

Explanation:

4 is correct. When *Allow multiple data streams* is enabled, NetBackup can split the backup work into separate child jobs based on the policy's backup selections and clients. In this case, the policy can potentially create work for three backup-selection paths across five clients, yielding up to fifteen child jobs over the life of the policy run. However, the *Limit jobs per policy* attribute controls the maximum number of jobs from that policy that NetBackup may run concurrently. Because that setting is four, only four child backup jobs transition to the Active state at the start, even though sufficient storage resources are available and additional child jobs are eligible to run. Remaining child jobs stay queued until one of the active jobs completes and frees a policy-job slot. Parent jobs are excluded because they coordinate policy execution rather than represent the individual data-stream backup jobs being counted. This behavior lets an administrator use multiple streams for parallelism while preventing one policy from consuming too many concurrent job resources. Veritas documents policy job limits and multiplexed or multiple-stream backup behavior in the [NetBackup Administrator's Guide](#) and the [NetBackup policy configuration documentation](#).

QUESTION NO: 18

An MSDP media server is experiencing performance issues when running multiple deduplication backup jobs concurrently over 10 GbE. When switched to AdvancedDisk on the same media server, the backups perform well.

Which step can be utilized to mitigate the performance issues?

- A. increase the "Maximum concurrent jobs" for the MSDP storage unit
- B. increase the size of the MSDP disk pool on the storage server
- C. add load balancing media servers for the storage server
- D. increase the "Job priority" on the MSDP backup policy

ANSWER: C

Explanation:

Adding load balancing media servers for the storage server can mitigate the MSDP performance bottleneck by distributing deduplication backup processing across multiple eligible media servers. MSDP performs more work than AdvancedDisk for each backup stream: in addition to receiving data, it fingerprints data, performs deduplication processing, and writes deduplicated segments and metadata. Therefore, a single MSDP media server can become constrained by CPU, memory, disk I/O, or deduplication-processing capacity even when the network is capable of 10 GbE throughput. The fact that AdvancedDisk performs well on the same host and network helps isolate the issue to the additional MSDP processing workload rather than basic network connectivity.

With media-server load balancing configured appropriately, NetBackup can select from multiple media servers that can service the storage target. This spreads concurrent backup jobs and their associated deduplication workload instead of concentrating all streams on one MSDP server. The design should ensure that each participating server has sufficient CPU, memory, network bandwidth, and storage performance, and that the configuration follows the supported MSDP and storage-server design rules. See Veritas documentation for [NetBackup deduplication guidance](#) and the [NetBackup 8.1.2 documentation set](#).

QUESTION NO: 19

What is the maximum age of the host's Certificate Revocation List (CRL) before communication with the host is prevented?

- A. 48 hours
- B. 5 days
- C. 7 days
- D. 30 days

ANSWER: C

Explanation:

7 days is correct. In NetBackup's host-certificate security framework, the Certificate Revocation List is used to identify certificates that must no longer be trusted before their normal expiration date. NetBackup requires hosts to have sufficiently current revocation information so that certificate validation remains meaningful. If a host's locally available CRL becomes older than seven days, NetBackup treats the revocation data as too stale and prevents certificate-based communication with that host.

This limit protects the NetBackup environment from continuing to trust a host certificate that may have been revoked after the host last obtained revocation information. Administrators should therefore ensure that certificate and CRL distribution components remain available and that hosts can refresh their CRL within the permitted interval. Reviewing NetBackup certificate-management status and resolving connectivity or trust issues promptly helps prevent interruptions when the seven-day CRL-age threshold is reached. Veritas documents certificate-based authentication, host identity, and certificate revocation handling in the [NetBackup Security and Encryption Guide](#). Additional certificate-management information is available in the [NetBackup documentation portal](#).

QUESTION NO: 20

Upon arriving at work on a Monday, an administrator sees several replication jobs that have failed with the following error message:

no images were successfully processed

Which two reasons may be the cause for the error code? (Choose two.)

- A. The checkpoint restart is disabled for the replication jobs.
- B. There are network connectivity issues between the source and target domains.
- C. The NetBackup host ID-based certificate was revoked.
- D. There is insufficient storage space on the target storage server.

E. There are insufficient tapes in the replication volume pool.

ANSWER: B D

Explanation:

There are network connectivity issues between the source and target domains, and there is insufficient storage space on the target storage server. NetBackup replication requires reliable communication between the source and target environments for the target to receive image metadata, establish the required control connections, and transfer backup data. A connectivity interruption or an unavailable remote service can prevent every image selected by a replication operation from being processed, resulting in the reported message.

Replication also depends on usable target-side storage resources. The target storage server must be able to accept the incoming replicated image data and its associated catalog or storage metadata. If the destination does not have adequate available capacity, NetBackup cannot successfully complete processing for the selected images. Administrators should validate network reachability and relevant NetBackup services between domains, then review target storage capacity, disk-pool status, and storage-server alerts before retrying affected replication work. NetBackup documentation and status-code guidance are available through the [NetBackup documentation portal](#) and Veritas's [technical support portal](#).

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: 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? (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:

For a Windows backup using the ALL_LOCAL_DRIVES directive, NetBackup must discover the local volumes and, when appropriate, create and use a snapshot so that files can be backed up consistently while they may be in use. The *NetBackup bpfis logs on the client* are therefore directly relevant because the bpfis process performs snapshot-related operations and

records detailed information about the snapshot method, volume processing, VSS interaction, and any failure returned during those operations. Enable and inspect the client bpfis debug log to identify the precise snapshot or filesystem condition associated with the job failure.

Operating system logs on the client are equally important because Windows records VSS, VolSnap, disk, filesystem, and provider events in Event Viewer. These events can identify a failed VSS writer, an unavailable provider, insufficient shadow-copy storage, or a volume-level issue at the same time as the NetBackup failure. Correlating the client Event Viewer timestamps with the bpfis log provides the most useful path to determine the underlying Windows-side cause and apply the appropriate remediation. Veritas describes NetBackup logging in its [NetBackup Logging Guide](#); Microsoft documents VSS troubleshooting and event collection in its [Volume Shadow Copy Service overview](#).

QUESTION NO: 22

To create a load balancing media server, you must first configure it as a storage server.

- A. True
- B. False

ANSWER: B

Explanation:

False is correct. In NetBackup, a media server and a storage server are distinct concepts. A media server performs backup and restore data movement and can be selected through NetBackup storage-unit configuration and media-server selection logic. Load balancing distributes work among eligible media servers according to the configured storage units, storage-unit groups, policies, available resources, and device availability. The media server does not need to be configured as a storage server merely to participate in that selection and load-balancing behavior.

A storage server is specifically associated with disk-based storage managed through NetBackup disk pools, such as OpenStorage or other supported disk-storage technologies. Configuring a media server as a storage server is required only when that host must manage or present the relevant disk storage to NetBackup. That disk-storage role is separate from the general role of a media server that writes backup data and can be used in media-server load balancing. NetBackup administrators therefore configure the required media servers and storage-unit or storage-unit-group settings for the workload; storage-server configuration is applied when the selected disk-storage architecture requires it. See the [NetBackup Administrator's Guide, Volume I](#) and the [NetBackup documentation portal](#) for storage-unit, disk-pool, and storage-server configuration guidance.

QUESTION NO: 23

A restore has failed with the following jobs details:

```
1/7/2017 4:02:23 PM - Info tar32(pid=48292) Restore started.
1/7/2017 4:02:23 PM - connected; connect time: 00:00:08
1/7/2017 4:17:33 PM - Error bptm(pid=5112) error requesting media, TpErrno = Robot operation failed
1/7/2017 4:17:35 PM - current media A12345 complete, requesting next resource IBM.ULTRIUM-
TD4.019:NetBackup:A12345
1/7/2017 4:17:41 PM - awaiting resource IBM.ULTRIUM-TD4.019:NetBackup:A12345 A pending request has
been generated for this resource request.
Operator action may be required. Pending Action: All drives down.,
Media ID: A12345, Barcode: A12345L4, Density: hcart, Access Mode: Read,
Action Drive Name: N/A, Action media server: Media-02, Robot Number: 1, Robot Type: TLD,
Volume Group: 000_00001 TLD, Action Acs: N/A, Action Lsm: N/A
```

Which two resources should the administrator use to troubleshoot this issue? (Choose two.)

- A. the bpfmedia command
- B. the robtest command
- C. the operating system logs

- D. the logs from the NetBackup "bpbkar" process
- E. the nbdevconfig command

ANSWER: D E

Explanation:

The logs from the NetBackup "bpbkar" process are a primary restore-troubleshooting resource because bpbkar is the NetBackup client process that performs backup, archive, and restore work. Its debug log records restore-side processing details, including file-system operations, stream handling, communication events, and the underlying error returned while data is being recovered. Reviewing this log at the affected client provides the detailed context that is not available from the high-level job status alone.

The nbdevconfig command is also appropriate because it reports and helps validate NetBackup device configuration information. A restore that requires media access depends on NetBackup being able to identify and use the configured storage devices correctly. The command can be used to inspect configured robots, drives, and device-related information, allowing the administrator to correlate the restore failure with the storage-device configuration used by NetBackup. Together, bpbkar logging and device-configuration verification cover both the restore execution path and the storage resources needed to satisfy the restore request. Veritas documents NetBackup command usage in its [NetBackup Commands Reference Guide](#) and troubleshooting guidance in the [NetBackup documentation portal](#).

QUESTION NO: 24

Which two media status destinations are excluded in the count against maximum number of partially full media? (Choose two.)

- A. Imported
- B. Active
- C. MPX
- D. Multi-Retlev
- E. Frozen

ANSWER: A E

Explanation:

Imported and **Frozen** media are excluded when NetBackup evaluates a volume pool's configured maximum number of partially full media. The setting is intended to control the number of usable, appendable partially filled volumes that NetBackup keeps available in the pool. Imported media is handled through the import workflow and is not treated as an ordinary candidate in this partially full-media limit. Frozen media has been intentionally made unavailable for further NetBackup use, commonly because of media errors, suspected integrity issues, or an administrative decision, so it is also excluded from the count.

This exclusion prevents non-appendable or specially managed media from consuming the pool's allowance for partially full media and affecting NetBackup's normal media-selection behavior. Administrators can therefore use the maximum partially full media setting to manage the available writable-media population without needing to account for imported or frozen volumes. Veritas documents volume-pool media management and partially full-media behavior in the [NetBackup Administrator's Guide, Volume I](#). Additional NetBackup documentation resources are available through the [Veritas NetBackup Support](#) portal.

QUESTION NO: 25

An administrator wishes to configure a backup for VMware clients using NetBackup Accelerator using third-party OST storage. The clients are running Windows as the guest OS.

Which step must the administrator perform to ensure the backup completes successfully?

- A. ensure the hardware shows Accel_VMware as a supported feature in the Hardware Compatibility List
- B. enable the NTFS or ReFS change journal for the file systems in the virtual machine
- C. create at least one backup policy schedule with the Accelerator forced rescan option
- D. create the client track log by restarting the NetBackup Client Service after saving the policy

ANSWER: A

Explanation:

Ensure the hardware shows Accel_VMware as a supported feature in the Hardware Compatibility List. NetBackup Accelerator for VMware requires that the selected storage and its OST plug-in explicitly support the VMware Accelerator capability. With third-party OST storage, this is not assumed merely because the device is supported for ordinary NetBackup backups or because it supports other accelerator workflows. The storage vendor's plug-in must advertise the *Accel_VMware* capability to NetBackup so that NetBackup can use the required optimized VMware Accelerator operations correctly. The Hardware Compatibility List is the authoritative source for confirming the storage platform, plug-in version, and feature support combination before the policy is configured and run. This requirement concerns the storage integration; the guest operating system being Windows does not remove the need to validate the OST Accelerator capability. Confirming this support avoids configuring an Accelerator-enabled VMware policy against a target that cannot perform the required operations. See the Veritas NetBackup documentation at [NetBackup documentation](#) and the Veritas compatibility resources at [NetBackup compatibility list information](#).