

DUMPS ARENA

Cohesity Certified Protection Professional – NetBackup Appliances

Cohesity COH-285

Version Demo

Total Demo Questions: 28

Total Premium Questions: 282

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, NetBackup Appliance Architecture	56
Topic 2, NetBackup Appliance Installation and Configuration	9
Topic 3, NetBackup Appliance Administration and Maintenance	156
Topic 4, NetBackup Appliance Troubleshooting	61
Total	282

QUESTION NO: 1

What is the name of the plug-in that performs deduplication on the NetBackup client or media server?

- A. NetBackup Deduplication Engine
- B. NetBackup Deduplication Manager
- C. NetBackup Deduplication Plug-in
- D. NetBackup Deduplication Service

ANSWER: C

Explanation:

NetBackup Deduplication Plug-in is the correct term for the NetBackup component that enables deduplication processing at the client or at a media server. In NetBackup deduplication architecture, this plug-in identifies duplicate data segments and avoids sending or storing redundant copies, depending on the configured deduplication workflow. When client-side deduplication is used, the client performs the deduplication work before transmitting unique data to the deduplication storage server. With media-server deduplication, the media server performs this function after receiving the backup data. This capability reduces network traffic for client-side processing and reduces the disk capacity required for retained backup data in either deployment model. The plug-in works with NetBackup's Media Server Deduplication Pool architecture and is installed as part of the relevant NetBackup client or media-server software components, according to the deployment design. Veritas documentation describes client-side and media-server deduplication as NetBackup Deduplication Plug-in functions and explains how the processing location affects data flow and resource usage. See the [NetBackup Deduplication Guide](#) and the [NetBackup deduplication architecture documentation](#).

QUESTION NO: 2

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

Which step must the administrator perform to ensure a successful backup?

- A. enable the NTFS or ReFS change journal for the file systems in the virtual machine
- B. ensure the third-party OST is supported by the Accelerator with VMware-type policies feature in the Hardware Compatibility List
- 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: B

Explanation:

ensure the third-party OST is supported by the Accelerator with VMware-type policies feature in the Hardware Compatibility List is required because NetBackup Accelerator for VMware image backups depends on both VMware Changed Block Tracking and compatible target-storage functionality. For this workload, NetBackup identifies changed virtual-machine disk blocks through VMware CBT; the Windows guest operating system's file-system change journal is not the mechanism used to accelerate the image-level backup. The target OST device must also be explicitly qualified to accept Accelerator backups for VMware-type policies. Generic OpenStorage support alone does not establish that a vendor's appliance, plug-in, and relevant software version can support the optimized VMware Accelerator data path. Before configuring production policies, the administrator should consult the NetBackup Hardware Compatibility List for the exact OST vendor and device combination and confirm the listed Accelerator capability for VMware policies. This validation ensures that the storage unit can process the backup correctly and avoids failures caused by an unsupported Accelerator operation. NetBackup's VMware Accelerator guidance describes the VMware CBT-based design and storage requirements, while the compatibility resources provide the authoritative support matrix for certified OST integrations. See [NetBackup compatibility lists](#) and [NetBackup VMware documentation resources](#).

QUESTION NO: 3

An administrator has a NetBackup Appliance that failed to CALL HOME during an unexpected hard drive failure.

Which two reasons may have prevented CALL HOME from working? (Choose two.)

- A. Call Home is set to disabled.
- B. The MyCohesity Credentials are incorrect.
- C. TELEMETRY_UPLOAD is disabled (Set to ' NO ').
- D. The Call Home Proxy settings are incorrect.
- E. The factory installed license key is expired.

ANSWER: A C

Explanation:

Call Home is set to disabled and TELEMETRY_UPLOAD is disabled (Set to ' NO ') are the relevant settings because both control whether the appliance can generate and transmit proactive support information. NetBackup Appliance Call Home is designed to notify support of certain hardware and appliance events, including disk failures, so that a case or service workflow can be initiated without waiting for manual intervention. The Call Home feature must be explicitly enabled for this automated notification path to operate. In addition, the appliance must be permitted to upload telemetry. Setting TELEMETRY_UPLOAD to NO prevents the appliance from sending the telemetry and diagnostic information that supports Call Home reporting. These settings should be verified as part of appliance health checks, especially after deployment, upgrades, security-hardening changes, or configuration restores. Administrators should also validate outbound connectivity according to their organization's approved network design after enabling the feature. Veritas documents appliance administration and support-related configuration in the [NetBackup Appliance documentation](#) and provides current product documentation through the [Veritas Documentation portal](#).

QUESTION NO: 4

What is the name of the feature that allows NetBackup to migrate data from Cloud Catalyst to MSDP direct cloud tiering?

- A. Cloud Migration
- B. Cloud Conversion
- C. Cloud Transition
- D. Cloud Transformation

ANSWER: B

Explanation:

Cloud Conversion is the NetBackup feature designed to move existing CloudCatalyst cloud data into an MSDP direct cloud tier configuration. It provides a supported migration path for customers modernizing their cloud-storage architecture while retaining the protection data already written through CloudCatalyst. The conversion process transfers the relevant CloudCatalyst-managed backup images and metadata into the target MSDP disk pool and its configured cloud tier, so NetBackup can continue to manage restores, retention, and image lifecycle operations through the MSDP direct-to-cloud framework. This is particularly valuable when transitioning away from the CloudCatalyst deployment model without requiring protected workloads to be backed up again solely to populate the new cloud-tier target. Before performing the conversion, administrators should ensure that the NetBackup version, target MSDP configuration, cloud provider configuration, and capacity planning meet the documented prerequisites. Cohesity NetBackup documentation describes MSDP cloud-tier administration and the supported workflows for managing cloud-resident backup data. See the [NetBackup documentation portal](#) and the [Cohesity NetBackup product documentation and resources](#) for current product guidance.

QUESTION NO: 5

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

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

- A. bpimage
- B. bpimmedia
- C. bpimagelist
- D. bpmedia
- E. bpimport

ANSWER: B D

Explanation:

`bpimmedia` and `bpmedia` are the required commands because a recovery from media written by an unavailable media server requires both the image-catalog association and the Enterprise Media Manager media ownership to be reassigned to the available server. The `bpimmedia -newserver` operation updates the media-server association held in NetBackup image records. This lets NetBackup identify the replacement server as the server that can access the backup image's media during restore processing. The `bpmedia -newserver` operation updates the media ownership information maintained by Enterprise Media Manager. This makes the replacement server the recognized owner of the applicable tape media and enables it to use the shared library resources for the restore. The administrator should use the appropriate old-server and new-server values and limit the operation to the affected media as required by the environment. Together, these changes align catalog image metadata with media-management ownership, allowing the available server connected to the same library to mount and read the needed media. Consult the NetBackup Commands Reference for the supported syntax and operational safeguards for `bpimmedia` and `bpmedia`: [NetBackup documentation](#) and [NetBackup Commands Reference](#).

QUESTION NO: 6

What is the name of the feature that lets you update NetBackup software and appliance firmware from a centralized location?

- A. VxUpdate
- B. VxUpgrade
- C. VxPatch
- D. VxInstall

ANSWER: A

Explanation:

VxUpdate is the centralized update capability for NetBackup appliances. It is designed to coordinate distribution and installation of supported NetBackup software releases, appliance software updates, and firmware updates across appliance infrastructure from one management point. This approach standardizes maintenance activity, helps administrators apply approved update versions consistently, and reduces the operational effort of performing separate updates directly on every appliance. VxUpdate uses downloaded and staged update packages, allowing an administrator to plan the update process and then deploy applicable content to the managed appliance targets. In an appliance environment, this centralized workflow is particularly useful for maintaining compatible appliance and firmware versions while reducing update-management complexity. NetBackup documentation describes appliance upgrade and firmware-update processes and the centralized management functions available for appliance administration. See the [NetBackup Appliance Commands Reference Guide](#)

and the [NetBackup Appliance documentation library](#) for product documentation and current release-specific update procedures.

QUESTION NO: 7

An administrator has backups for a Linux client that are failing with the following error message:

“Status 58: can’t connect to client”

Which command should the administrator use to identify why the media server is unable to connect to the client?

- A. bpcIntcmd
- B. nbemmcmd
- C. bpplclients
- D. bpclient
- E. bptestbpcd

ANSWER: E

Explanation:

`bptestbpcd` is the appropriate NetBackup diagnostic utility because it tests the actual connection path from a media server to the NetBackup Client Service (`bpcd`) on the target client. Running it on the media server with the client name, such as `bptestbpcd -client <client_name> -verbose`, produces detailed connection output that helps isolate the cause of status 58. Its results can reveal issues such as client-name resolution inconsistencies, inability to reach the client over the network, blocked required NetBackup ports, or failure of the client service to accept the connection. This directly reproduces and diagnoses the communication operation that must succeed before a media server can perform a backup or restore with that Linux client. The verbose output is especially useful for determining the stage at which the connection fails and for collecting evidence for further network or client-service troubleshooting. Veritas documents NetBackup command-line utilities in the [NetBackup Commands Reference Guide](#); status-code troubleshooting guidance is also available through the [Veritas Support knowledge base](#).

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? (Select two.)

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

ANSWER: A B

Explanation:

The supported methods for returning a corrupted Media Server Deduplication Pool (MSDP) catalog to service are to recover it from an MSDP catalog backup and to restore it from an MSDP catalog shadow copy. NetBackup Deduplication Manager maintains catalog shadow copies, along with transaction logs, as a local recovery mechanism. When an appropriate shadow copy is available, restoration uses that copy and transaction-log replay to return the catalog to a current, usable state. Administrators should also configure a dedicated MSDP catalog backup policy. This backup is an essential additional recovery layer, particularly for a serious hardware failure in which the active catalog and its local shadow-copy area are

unavailable or damaged. The MSDP catalog requires this dedicated protection because it is managed separately from the regular NetBackup catalog backup process. In practice, the shadow-copy recovery path provides fast recovery for catalog corruption when local recovery data remains intact, while recovery from an MSDP catalog backup provides the durable recovery path for broader loss scenarios. See Veritas guidance on [MSDP catalog backup and recovery](#) and the [NetBackup Deduplication Guide](#).

QUESTION NO: 9

What are the two types of reports that NetBackup provides to verify and monitor backup activities?

- A. Activity Monitor and OpsCenter Analytics
- B. Job Monitor and Report Manager
- C. Backup Monitor and Dashboard Analytics
- D. Activity Monitor and Report Manager

ANSWER: A

Explanation:

Activity Monitor and OpsCenter Analytics is correct because these facilities address complementary operational-monitoring and reporting needs in a NetBackup environment. Activity Monitor provides the immediate, job-level operational view needed to verify backup activity as it happens or after completion. Administrators use it to review job status, progress, start and end times, policy and client details, throughput, and job messages. This makes it the primary interface for quickly confirming whether protection jobs completed successfully and for investigating an individual job's execution history.

OpsCenter Analytics extends this visibility into centralized historical reporting and analysis. It collects and presents information across NetBackup domains, allowing administrators to evaluate backup trends, capacity consumption, compliance, success rates, and service-level outcomes over time. Its analytics and report capabilities are particularly valuable where teams need summarized evidence of protection performance rather than only the status of a single running or completed job. Together, Activity Monitor supplies detailed operational verification, while OpsCenter Analytics supplies broader reporting and trend analysis for ongoing monitoring. NetBackup documentation describes job monitoring through the Activity Monitor and centralized reporting capabilities through OpsCenter. See the [NetBackup documentation portal](#) and the [OpsCenter documentation](#).

QUESTION NO: 10

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

- A. choose the "Collect Disaster Recovery information" option in the policy
- B. choose the FlashBackup-Windows policy type
- C. install the NetBackup File System daemon (nbfscd) on the client
- D. choose the "Enable granular recovery" option in the policy
- E. enable the Network File System (NFS) on the client

ANSWER: D E

Explanation:

To restore individual Active Directory objects and attributes, the backup policy must have granular recovery enabled. In NetBackup, this setting directs the backup process to collect the information required for Granular Recovery Technology to browse and restore Active Directory data at the object and attribute level. It must be configured before the backup that will be used as the source for granular recovery is created.

Network File System (NFS) must also be enabled on the Active Directory client, meaning the domain controller or AD LDS/ADAM host being protected. NetBackup uses NFS as part of the granular recovery workflow to expose backup contents for item-level browsing and recovery. NetBackup documentation identifies NFS as a requirement on the media server and on Active Directory domain controllers or AD LDS/ADAM hosts participating in Active Directory granular backup and restore operations. Together, enabling granular recovery in the policy and enabling NFS on the client provide the policy configuration and host-level capability needed to restore individual directory objects and attributes. See [NetBackup Active Directory granular recovery documentation](#) and [NetBackup Granular Recovery Technology requirements](#).

QUESTION NO: 11

Which two tasks should an administrator perform prior to upgrading NetBackup Appliances to version 3.1.2? (Choose two.)

- A. obtain necessary third-party plug-ins
- B. decrease the size of the configuration volume
- C. reset the appliance user password to the default value
- D. delete previously downloaded release updates, client packages, and client add-ons
- E. use the Migration Utility to capture pre-upgrade settings within a NetBackup Catalog Backup

ANSWER: A D

Explanation:

Before starting the upgrade to NetBackup Appliance 3.1.2, the administrator should obtain necessary third-party plug-ins. Appliance software upgrades do not necessarily include every add-on required for integrations that use third-party components. Obtaining the applicable plug-ins in advance ensures that required functionality can be restored or maintained after the appliance software is upgraded, without delaying the upgrade workflow while additional packages are located and downloaded.

The administrator should also delete previously downloaded release updates, client packages, and client add-ons. These files consume space in appliance storage areas and may no longer be applicable after the target release is installed. Removing obsolete downloaded packages is an important pre-upgrade housekeeping step because it helps ensure adequate available space for the upgrade payload, temporary installation files, and upgrade processing. It also reduces the risk of retaining outdated package content that can create operational confusion after the appliance is moved to version 3.1.2.

These preparations align with the NetBackup Appliance upgrade guidance, which emphasizes reviewing package requirements and preparing appliance storage before installing an appliance release update. See the [NetBackup Appliance documentation](#) and the [NetBackup Appliance upgrade best-practices guidance](#).

QUESTION NO: 12

What is the purpose of NetBackup Compatibility Lists?

- A. To provide a comprehensive list of supported operating systems, applications, and hardware for NetBackup.
- B. To list the prices of NetBackup licenses.
- C. To offer troubleshooting advice for NetBackup users.
- D. To provide free training courses on how to use NetBackup.

ANSWER: A

Explanation:

NetBackup Compatibility Lists provide the authoritative support matrix for a NetBackup deployment. They identify supported operating systems, platform versions, applications and databases, hardware, cloud integrations, and related product

combinations. Administrators use these lists during planning, installation, upgrades, and troubleshooting to verify that the NetBackup version and features they intend to use are supported with the protected workload and environment. This validation is important because support can vary by NetBackup release, client operating system, agent type, database version, appliance model, and integration method. Reviewing the appropriate compatibility list before making a change helps ensure that a configuration is eligible for vendor support and operates within the tested interoperability requirements. Veritas publishes the compatibility resources through its NetBackup compatibility portal, where users can select the relevant NetBackup version and technology area, such as operating systems, applications, cloud, or hardware. For current matrices and compatibility guidance, consult the [NetBackup Compatibility List and Documentation resources](#) and the [NetBackup Software Compatibility List](#).

QUESTION NO: 13

A restore has failed with the following job details:

Error bptm ... error requesting media, TpErrno = Robot operation failed

awaiting resource ... Pending Action: All drives down

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

- A. the operating system logs
- B. the logs from the NetBackup bpbkar process
- C. the nbdevconfig command
- D. the bpmedia command
- E. the robtest command

ANSWER: A E

Explanation:

The operating system logs and the robtest command are the appropriate resources because the reported failure is in the tape-media and robotic-device path. The `bptm` process is requesting media, but the robotic operation cannot complete, while the pending action reports that all tape drives are unavailable. This points to a condition affecting the media server's ability to communicate with, control, or use the tape library and its drives. Relevant causes can include device-driver or operating-system errors, SAN connectivity or zoning conditions, SCSI communication failures, a library hardware state, or drives that are offline or otherwise unavailable to NetBackup.

Operating-system logs provide the low-level driver, device, path, and hardware events needed to establish whether the host can see and communicate with the robot and drives. The `robtest` utility is specifically designed to test robotic-device operations from the media server. It can inspect robot, drive, and slot status and perform controlled inventory or media-movement tests, helping isolate whether the problem is at the robot or drive layer before retrying the restore. NetBackup documentation for tape-device administration and commands is available through the [NetBackup documentation portal](#); the [Broadcom NetBackup certification resources](#) also cover tape and device-management concepts.

QUESTION NO: 14

An administrator is performing a backup and receives the following error message:

129 Message: Disk storage unit is full

Which NetBackup command should the administrator use to report the potential free space of AdvancedDisk storage units?

- A. nbdevquery
- B. nbdiscover
- C. nbemmcmd

ANSWER: A**Explanation:**

`nbdevquery` is the appropriate NetBackup command because it queries disk-pool and storage-unit capacity and status information managed through NetBackup Enterprise Media Manager. For AdvancedDisk storage, its status output can report capacity-related values, including the potential free space that NetBackup can make available for new backup images. This is particularly relevant when a job reports status 129, because the usable capacity seen by NetBackup can be affected by existing images, disk-pool allocation, and space that may be reclaimed under configured image-expiration and cleanup policies. An administrator can use `nbdevquery` with the applicable storage type and status-listing arguments to review this information and determine whether the reported condition reflects genuinely exhausted storage capacity or capacity that NetBackup may reclaim. The command is therefore a key diagnostic tool for AdvancedDisk disk-pool capacity investigation and storage lifecycle management. Veritas documents `nbdevquery` in the NetBackup Commands Reference and describes AdvancedDisk capacity management in its NetBackup administration documentation. See the [NetBackup documentation portal](#) and the [Veritas NetBackup knowledge base](#) for product documentation and operational guidance.

QUESTION NO: 15

A media server is scheduled for maintenance. Another media server is available and can access the same appliance disk storage. The administrator wants restores of images written by the unavailable media server to continue without changing image ownership.

Which two conditions are required for Restore Failover to work? (Select two.)

- A. Configure the original and replacement media servers in the Restore Failover section of the primary server Host Properties.
- B. Ensure that the replacement media server can access the storage that contains the backup images.
- C. Use `bpmedia` to change ownership of every affected image to the replacement media server.
- D. Add the replacement media server to each affected client backup policy.
- E. Configure the replacement media server as the primary server.

ANSWER: A B**Explanation:**

The replacement media server must be able to access the storage that contains the backup images, because it must read the selected image during the restore. The original and replacement media servers must also be configured in the primary server Host Properties under Restore Failover. This mapping authorizes NetBackup to redirect restores when the original media server is unavailable.

Changing media ownership with `bpmedia` is not required for Restore Failover. Likewise, placing the replacement server in the client backup policy does not establish a restore-failover relationship.

QUESTION NO: 16

Which two statements correctly describe a NetBackup storage lifecycle policy? (Select two.)

- A. It can define a backup operation followed by a duplication operation.
- B. It can be selected as the storage destination in a backup policy.
- C. It replaces the need to configure storage units.
- D. It is used to create client backup selections.

E. It assigns NetBackup client software versions to protected hosts.

ANSWER: A B

Explanation:

A storage lifecycle policy defines the sequence of operations that NetBackup applies to backup images, such as creating a backup copy and then duplicating or replicating that copy to another storage target. A backup policy can select a storage lifecycle policy as its storage destination, allowing NetBackup to apply that defined lifecycle automatically.

A storage lifecycle policy does not itself represent a physical storage target. Storage units and disk pools provide the actual storage resources used by the operations in the lifecycle policy.

QUESTION NO: 17

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 are valid causes because image replication depends on both successful communication to the target environment and sufficient capacity for the replicated image data. A replication job processes one or more eligible backup images; if communication between the participating domains is unavailable or interrupted, none of the selected images may complete transfer. When this occurs across the images considered by the job, NetBackup reports that no images were successfully processed.

Likewise, the target storage server must be able to accept the incoming replicated data and any associated metadata. If the target disk pool, deduplication storage, or underlying target storage lacks usable capacity, image processing cannot finish successfully. If every image selected for that replication operation encounters this condition, the job produces the same aggregate result. Administrators should therefore validate end-to-end connectivity and name resolution between the source and target domains, then review target storage capacity, disk-pool availability, and storage-server health before rerunning the affected replication jobs. NetBackup's status-code and troubleshooting documentation provides the framework for interpreting job results and reviewing detailed job logs: [NetBackup documentation](#) and [NetBackup technical support knowledge base](#).

QUESTION NO: 18

Which command is used by VxUpdate to upgrade clients?

- A. vmupdate
- B. nbrepo
- C. nbinstallcmd

ANSWER: C

Explanation:

nbinstallcmd is the command-line utility used with NetBackup VxUpdate to deploy NetBackup software packages to managed hosts, including performing client upgrades. VxUpdate centrally orchestrates the lifecycle of NetBackup client software: administrators first make the appropriate client package available in the NetBackup repository, then use VxUpdate policies and deployment operations to target eligible clients. The **nbinstallcmd** utility provides the command-line interface for initiating and managing those package deployment activities rather than requiring an interactive console workflow. This supports consistent upgrades across many clients while allowing deployment selection to be based on host characteristics, installed versions, and policy configuration. The account running the command must have the required NetBackup authorization, and the target clients must meet the VxUpdate prerequisites for remote deployment. For the official VxUpdate workflow and client software deployment guidance, see the [NetBackup Web UI Administrator's Guide](#) and the [NetBackup Commands Reference Guide](#).

QUESTION NO: 19

How can you manually duplicate a backup image?

- A. Use the NetBackup administration console to duplicate the image.
- B. Restore the image to a test system and then duplicate it.
- C. Use the NetBackup command line to duplicate the image.

ANSWER: A

Explanation:

Use the NetBackup administration console to duplicate the image. In the Administration Console, an administrator can locate the relevant backup image in the Catalog view and initiate a duplication operation for that selected image. This is the standard interactive workflow for manually creating another copy of an existing backup image, rather than relying on an automated storage lifecycle policy or scheduled duplication process. During the duplication workflow, the administrator selects the destination storage and can review the image details before submitting the operation. NetBackup then creates the additional copy while retaining the original image and its catalog information, allowing the new copy to be used for recovery according to its configured retention and availability. This console-based process is especially useful when an administrator needs to make an on-demand copy for operational, retention, or offsite-protection purposes. Veritas documents image duplication as a NetBackup operation and provides the associated command reference in the [NetBackup Commands Reference Guide](#). Additional NetBackup administration documentation is available through the [Veritas NetBackup documentation portal](#).

QUESTION NO: 20

What are the different types of images that can be managed by NetBackup?

- A. Full images
- B. Differential images
- C. Incremental images
- D. Clone images

ANSWER: A B C

Explanation:

NetBackup manages backup images created by different backup methods, including full and incremental processing. **Full images** contain all selected data at the time of the backup and provide the baseline from which subsequent recovery chains can be built. **Differential images** capture data that changed since the most recent backup of any relevant type; during a restore, NetBackup uses the full image together with the required differential image set to reconstruct the selected recovery point. **Incremental images** represent backups that capture changed data rather than all protected data. In NetBackup terminology, incremental processing can be configured as differential incremental or cumulative incremental, according to the policy schedule and recovery requirements. NetBackup catalogs these backup images and their associated metadata so that administrators can browse, select, duplicate, retain, expire, and restore protected data. Image management is therefore based on the backup images generated by these full and incremental backup operations, with the catalog maintaining the information needed to locate the applicable media or storage copies for recovery. See the [NetBackup Administrator's Guide](#) and the [Veritas NetBackup documentation](#) for backup-type and image-catalog concepts.

QUESTION NO: 21

A NetBackup backup job is taking longer than expected. What steps can be taken to troubleshoot the problem?

- A. Check the backup job 's settings.
- B. Check the backup device 's health.
- C. Check the network bandwidth.
- D. Contact Cohesity Support for assistance.
- E. Review the backup job configuration, backup device health, and network bandwidth; if the issue persists, collect job details and contact Cohesity Support.

ANSWER: E

Explanation:

Review the backup job configuration, the health and performance of the backup device, and available network bandwidth; if the issue persists, collect the relevant job details and contact Cohesity Support. Slow backup performance can result from an interaction of several components rather than a single setting. Start by using NetBackup job details and status information to identify the point at which throughput declines, then verify that policy settings, schedules, streams, and storage-target selections align with the protection design. Confirm that the appliance and its storage targets are healthy and are not constrained by active workloads, resource contention, or hardware alerts. Network connectivity and throughput between the protected client, media services, and the appliance should also be validated, particularly when backups traverse remote links. Capturing this evidence creates a clear performance baseline and provides the diagnostic information needed for an effective support case if local checks do not resolve the delay. Cohesity documentation is available through the [Cohesity Documentation portal](#), and NetBackup product documentation and support resources are available from the [Veritas Documentation portal](#).

QUESTION NO: 22

What are the different reports that are available to verify and monitor NetBackup?

- A. Backup job status reports
- B. Storage utilization reports
- C. Image integrity reports
- D. All of the above

ANSWER: A B C D

Explanation:

Backup job status reports, storage utilization reports, and image integrity reports are all valuable report categories for verifying protection activity and monitoring the operational condition of a NetBackup environment. Backup job status reporting provides visibility into the outcome and progress of protection jobs, enabling administrators to confirm that scheduled backups complete as expected and to identify jobs requiring attention. Storage utilization reporting helps teams monitor capacity consumption and trends, supporting planning for backup storage and preventing capacity-related operational issues. Image integrity reporting supports confidence that protected backup images remain usable and recoverable by reporting on image validation and integrity-related activity. Taken together, these report categories provide coverage of job execution, storage health and consumption, and recoverability assurance. Therefore, "All of the above" is also correct because it accurately includes each of these available monitoring and verification report types. NetBackup's administration documentation describes monitoring job activity and managing storage as core operational tasks; see the [NetBackup Web UI Administrator's Guide](#) and the [NetBackup reporting documentation](#).

QUESTION NO: 23

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 > Host properties > Media Servers > Configure Media Server
- 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. Adding the appliance from the master appliance first establishes the intended NetBackup domain relationship and supplies the master-server information required by the media-server appliance during its configuration. The master server is the authoritative control point for the domain, so it must recognize and authorize the additional appliance before that appliance is configured to operate as a media server. After the additional-server entry is created, configuring the new appliance completes its setup with the appropriate role and connectivity to the existing master server. This workflow also ensures that the appliance is incorporated through the supported NetBackup Appliance management process rather than relying on manual configuration-file changes. Cohesity's NetBackup offering continues to use the established NetBackup architecture in which the primary/master server centrally manages media servers and protection operations. See the [Cohesity NetBackup product information](#) and the [NetBackup Appliances documentation portal](#) for appliance administration and configuration guidance.

QUESTION NO: 24

A Linux client has a root file system and a separate file system mounted at /data. An administrator must protect both file systems but must not include any other mounted file systems that might later be mounted beneath the root file system.

Which two policy settings should the administrator use? (Select two.)

- A. Include / in the Backup Selections list.
- B. Include /data in the Backup Selections list.
- C. Enable the Cross mount points policy attribute.
- D. Use ALL_LOCAL_DRIVES as the only backup selection.
- E. Enable granular recovery for the policy.

ANSWER: A B

Explanation:

The administrator should include both `/` and `/data` as explicit backup selections. The explicit `/data` selection ensures that the separate file system is protected.

The Cross mount points option should remain disabled. With that option disabled, NetBackup does not automatically cross from the root file system into other mounted file systems encountered during processing. Explicitly selecting `/data` protects that intended mount point without causing NetBackup to include unrelated mounts.

QUESTION NO: 25 - (SIMULATION)

What is the name of the log file that records all activities related to NetBackup appliance security? A. `security.log`

B. `audit.log`

C. `secure.log`

D. `auth.log`

ANSWER: See the explanation for the answer

Explanation:

Correct answer: B. `audit.log`

On a NetBackup appliance, security-related activities are recorded in the `audit.log` file. This audit log captures security events and administrative activity for review and compliance purposes.

QUESTION NO: 26

Which of the following is NOT a way to obtain NetBackup Appliance updates and EEBs?

A. Appliance Shell Menu (CLISH)

B. Appliance Management Server (AMS)

C. Appliance Web Console

D. Cohesity Support website

ANSWER: A

Explanation:

Appliance Shell Menu (CLISH) is the correct answer because it is the appliance's local command-line administration interface, rather than an update and EEB acquisition channel. Administrators use the shell menu to perform appliance-side operational tasks and to manage software packages after they have been made available to the appliance. Obtaining a NetBackup Appliance software update or an engineering emergency binary requires access to an authorized distribution mechanism, where the required package can be downloaded, entitled, and, when applicable, selected for the relevant appliance software version. This distinction matters operationally: the package must be sourced and validated first, then staged and installed through the appropriate appliance management workflow. Cohesity's support resources provide entitled customers with access to product support and software-related downloads, while the NetBackup Appliance documentation describes the supported lifecycle procedures for appliance software and hotfix maintenance. See the [Cohesity Support portal](#) and the [NetBackup Appliance documentation](#) for the supported maintenance and update procedures.

QUESTION NO: 27

A NetBackup appliance is reporting a high network usage. What steps can be taken to troubleshoot the problem?

- A. Check the appliance 's logs for errors.
- B. Check the appliance 's backup policies.
- C. Reduce the amount of data being backed up.
- D. Contact Cohesity Support for assistance.

ANSWER: B

Explanation:

Checking the appliance's backup policies is the appropriate first troubleshooting step because policies define the backup workloads that generate network traffic. Review the policy schedules, client selections, backup windows, frequency, and any simultaneous job activity to identify whether multiple large or overlapping backups are running during the period of elevated utilization. Policy configuration can also reveal recently added clients, expanded selection criteria, or schedule changes that have increased the volume of protected data or the number of concurrent data streams. This establishes whether the observed network consumption corresponds to expected backup activity and provides a focused basis for adjusting scheduling or workload distribution if needed. NetBackup documentation describes policies as the configuration that determines what is backed up, which clients are included, and when backup operations run. The appliance administration guidance should be used alongside policy review to correlate the reported network usage with active jobs and appliance activity. See the [Veritas NetBackup documentation portal](#) and the [Cohesity documentation portal](#) for current product administration and monitoring guidance.

QUESTION NO: 28

Refer to the Exhibit.

An administrator is trying to access client properties on the NetBackup Administration Console and receives the following message:

When checking the services on the master server, the administrator sees that the PBX service is down.

Which two commands can the administrator use to increase the PBX log level to determine the reason for the message above? (Choose two.)

- A. vxlogcfg
- B. pbxcfg
- C. vxpbx_exchanged
- D. pbx_exchange
- E. vxlogmgr

ANSWER: A E

Explanation:

`vxlogcfg` and `vxlogmgr` are the NetBackup unified-logging utilities used when collecting additional diagnostic information for NetBackup components, including PBX. PBX is a shared communication service used by NetBackup processes, so a PBX startup or communication failure can prevent the Administration Console from retrieving client properties. Increasing the PBX diagnostic and debug logging makes the service's initialization, listener, authentication, and interprocess communication activity available for review.

`vxlogcfg` is used to configure the logging settings for a unified-logging product and organization ID, including the debug and diagnostic levels used by PBX. After the required logging configuration is in place, `vxlogmgr` is used to manage the unified-log environment and its generated log records. Together, these utilities allow an administrator to collect and maintain the detailed PBX evidence needed to identify why the service is not running. Logging should be returned to its normal level after troubleshooting, because elevated diagnostic levels can generate substantial log volume.

See the official [Veritas NetBackup documentation portal](#) for NetBackup command references and the [Veritas Support portal](#) for PBX troubleshooting guidance.