DUMPSBOSS.

# Veritas NetBackup 10.x and NetBackup Appliance 5.x Administrator

## Veritas VCS-285

## Version Demo

**Total Demo Questions: 23**

**Total Premium Questions: 230**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, NetBackup Architecture | 28 |
| Topic 2, NetBackup Installation and Configuration | 9 |
| Topic 3, NetBackup Administration | 138 |
| Topic 4, NetBackup Appliance Administration | 54 |
| Topic 5, Mix Questions | 1 |
| Total | 230 |

QUESTION NO: 1

What is the name of the feature that lets you configure immutability and indelibility of data in NetBackup?

**A.** Data Lock

**B.** Data Protection

**C.** Data Security

**D.** Data Integrity

**ANSWER: A**

**Explanation:**

**Data Lock** is the NetBackup feature used to configure protected retention for backup data through immutability and indelibility controls. It helps ensure that recovery points cannot be altered or deleted before their configured retention period expires, including in circumstances where an attacker obtains elevated credentials. This capability is a key ransomware-resilience control because it preserves a known-good, recoverable copy of data even if the production environment or backup administration accounts are compromised. In NetBackup, Data Lock is enabled at the storage lifecycle policy level and applies to supported storage targets and configurations. Its immutability controls prevent modification of protected backup images, while indelibility prevents deletion during the enforced retention period. Administrators should plan retention carefully before enabling Data Lock, since the purpose of the feature is to enforce that retention rather than allow routine administrative removal of backup data. Veritas documents Data Lock as part of its NetBackup ransomware protection capabilities and provides configuration details in the NetBackup documentation. See the NetBackup Data Lock documentation and the Veritas NetBackup product overview.

**QUESTION NO: 2**

Which interface can be accessed from the IPMI web interface or Veritas Remote Management (VRM) interface?

**A.** NetBackup Appliance Shell Menu (CLISH)

**B.** NetBackup Appliance Web Console

**C.** Appliance Management Console

**D.** NetBackup WebUI

**ANSWER: A**

**Explanation:**

NetBackup Appliance Shell Menu (CLISH) is the interface that can be accessed through the remote-console capability exposed by the IPMI web interface or Veritas Remote Management (VRM) interface. IPMI and VRM provide out-of-band hardware-management access, which is particularly useful when normal network access to the appliance is unavailable or when an administrator must work directly from the appliance console during initial configuration, troubleshooting, or recovery. After opening the remote console and authenticating to the appliance, the administrator is presented with the appliance's command-line environment, commonly called the NetBackup Appliance Shell Menu or CLISH. This menu-driven command interface supports appliance administration activities such as viewing status, configuring network settings, managing services, and performing maintenance operations. Because this access path is console based, it remains available independently of the normal browser-based appliance-management connection. Veritas documents the appliance command environment and its administrative commands in the NetBackup Appliance Commands Reference Guide. Veritas also provides current appliance documentation, including platform and remote-management guidance, through the NetBackup Appliance documentation portal.

**QUESTION NO: 3**

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 because replication requires reliable communication between the NetBackup source and target environments throughout image selection, catalog communication, and data transfer. If the participating hosts or domains cannot communicate, the replication operation may be unable to process any of the selected backup images, resulting in the reported message. There is insufficient storage space on the target storage server because replicated image data must be written to the target storage selected by the replication or storage lifecycle policy. When the target cannot allocate sufficient capacity for the incoming image data, each attempted image transfer can fail, leaving the job with no successfully processed images. Administrators should review the detailed job logs and Activity Monitor entries to identify the underlying transfer or storage allocation failure, verify network reachability between the involved NetBackup hosts, and confirm that the target disk pool or storage server has adequate available capacity. Veritas documents replication and duplication troubleshooting in the NetBackup Troubleshooting Guide; relevant job-status information is also available through the NetBackup documentation portal.

## QUESTION NO: 4

What are the two types of encryption that NetBackup supports for backup data?

**A.** Client-side encryption and media server encryption

**B.** Software encryption and hardware encryption

**C.** Symmetric encryption and asymmetric encryption

**D.** All of the above

**ANSWER: B**

**Explanation:**

NetBackup supports **software encryption and hardware encryption** for protecting backup data. Software encryption is performed by NetBackup components before the data is written to the backup storage target. Depending on the selected configuration, NetBackup can perform this encryption at the client or at the media server, while NetBackup manages the encryption settings and the keys needed to recover the protected backup images.

Hardware encryption uses encryption capabilities built into supported storage hardware, particularly tape drives. In this model, the drive encrypts the data as it is written to media. NetBackup can integrate with the hardware-encryption workflow and its key-management configuration so that encrypted backup media remains recoverable through properly configured NetBackup operations. The applicable method is selected based on factors such as the storage device, performance requirements, compliance controls, and the organization’s key-management design.

Veritas documents these as the two overall encryption approaches for NetBackup backup data: software-based encryption performed by NetBackup and hardware-based encryption performed by supported storage devices. See the Veritas

NetBackup Security and Encryption Guide and the NetBackup documentation portal for the current encryption configuration and operational guidance.

## QUESTION NO: 5

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

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

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

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

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

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

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

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

## ANSWER: B D

**Explanation:**

The correct actions are to ensure the DR file is created on a volume other than the NetBackup volume and to configure a valid email address of the administrator in the “Send email” option. A catalog backup creates a disaster recovery (DR) file containing the information needed to begin recovery of the NetBackup catalog. That file must remain accessible even if the disk or partition containing the NetBackup catalog is lost. Writing it to a separate volume provides isolation from a failure affecting the catalog volume and allows the administrator to retrieve the recovery information during a disaster-recovery procedure.

NetBackup can also send the DR file by email after the catalog backup completes. Configuring a valid recipient address creates an additional off-host copy that can be accessed independently of the affected NetBackup server storage. This is particularly useful when a local storage failure makes locally written files unavailable. In practice, administrators should use a separate protected location for the generated DR file and verify that email delivery succeeds, so recovery instructions are available when they are needed. Veritas documents catalog backup and disaster-recovery-file handling in the NetBackup Administrator's Guide, Volume I and its catalog recovery documentation.

## QUESTION NO: 6

A newly installed NetBackup client cannot complete backups. The administrator must verify both the client configuration and communication with the client backup service before changing policy settings.

Which two commands are appropriate for this initial investigation? (Choose two.)

**A.** bpclntcmd -pn

**B.** bptestbpcd

**C.** bpverify

**D.** bpexpdate

**E.** bpmedia

## ANSWER: A B

**Explanation:**

**bpclntcmd -pn** verifies the client-side NetBackup configuration and communication with the configured primary server. It is useful for identifying an incorrect server association or name-resolution issue.

**bptestbpcd** tests communication with the NetBackup Client Service daemon, bpcd, on the client. This helps verify that the server can reach the client service required for backup processing. **bpverify** validates existing backup images, while **bpexpdate** changes image expiration and **bpmedia** manages media information.

## QUESTION NO: 7

A NetBackup appliance is reporting an error with the message "Media error: 0x00000002". What does this error mean?

**A.** The media is full. B. The media is damaged.

**B.** The media is not supported by NetBackup.

**C.** The media is not inserted in the device correctly.

## ANSWER: C

**Explanation:**

“The media is not inserted in the device correctly.” is the appropriate interpretation of this appliance media error. The message indicates that the appliance or its associated device cannot access the expected media. In practical terms, the media is absent, incompletely loaded, or not properly seated in the device, preventing NetBackup from establishing the required media access. The first corrective action is therefore to check the physical media and device condition: verify that the correct cartridge or removable medium is present, fully inserted, and recognized by the drive or library. If the device is robotic, confirm that the media was successfully moved to the intended location and that the device inventory reflects its actual location. After reseating or correctly loading the media, rescan or inventory the device as appropriate and retry the operation. Veritas recommends using the NetBackup Appliance and NetBackup administrative documentation when investigating appliance alerts and device/media operations, including checks of appliance monitoring information and storage-device status. See the Veritas NetBackup Appliance documentation and the NetBackup documentation for operational guidance.

## QUESTION NO: 8

What are the security risks associated with NetBackup appliances?

**A.** Data loss

**B.** Data corruption

**C.** Denial of service attacks

**D.** All of the above

## ANSWER: D

**Explanation:**

All of the above is correct because protecting a NetBackup appliance involves preserving the availability, integrity, and recoverability of the backup environment. A security incident that compromises appliance access, configuration, storage, or network communications can make protected backup images unavailable or destroy them, resulting in data loss. Unauthorized changes to backup images, catalogs, configuration data, or recovery-related components can also undermine the integrity of data and create data-corruption risk. In addition, an attacker or other disruptive event can exhaust appliance, network, or service resources and prevent administrators, clients, or media servers from using backup and restore services, which is a denial-of-service condition. These risks are especially important because NetBackup appliances commonly hold backup data and provide critical recovery services during an outage or ransomware incident. Veritas recommends securing administrative access, applying supported updates, using appropriate network controls, and monitoring the environment to help protect appliance services and backup assets. See the Veritas NetBackup Security and Encryption Guide and the NetBackup Appliance documentation for security guidance and appliance administration information.

## QUESTION NO: 9

Which guide should be consulted to learn about the configuration and administration of NetBackup deduplication options?

**A.** Veritas NetBackup AdvancedDisk Storage Solutions Guide

**B.** NetBackup Web UI Administrator's Guide

**C.** Veritas NetBackup Deduplication Guide

**D.** Veritas NetBackup OpenStorage Solutions Guide for Disk

## ANSWER: C

**Explanation:**

The **Veritas NetBackup Deduplication Guide** is the appropriate reference because it is specifically dedicated to planning, configuring, managing, monitoring, and troubleshooting NetBackup deduplication. It covers the deduplication technologies and choices available in NetBackup, including Media Server Deduplication Pool deployments, client-side deduplication, storage-server considerations, disk-pool configuration, deduplication policies, replication, and operational maintenance. An administrator needs this focused guidance when determining how data is deduplicated, where deduplication occurs, how the deduplication storage is configured, and how deduplicated backups are administered throughout their lifecycle. Veritas publishes the guide as part of its NetBackup documentation set and updates it by product release, so the edition matching the installed NetBackup version should be used. The NetBackup documentation portal provides access to the current and earlier product documentation, including the Deduplication Guide: Veritas NetBackup documentation. Veritas also provides a dedicated documentation landing page for NetBackup resources and release-specific manuals: NetBackup documentation resources. Consulting the dedicated guide ensures that deduplication settings and administration procedures are applied according to the supported architecture and documented best practices.

## QUESTION NO: 10

A client is protected by a weekly full backup and daily cumulative incremental backups. The full backup completed on Sunday, and cumulative incremental backups completed successfully from Monday through Thursday.

Which two images are required to restore the client to its state at the end of Thursday? (Choose two.)

**A.** the Sunday full backup

**B.** the Thursday cumulative incremental backup

**C.** the Monday cumulative incremental backup

**D.** the Tuesday cumulative incremental backup

**E.** the Wednesday cumulative incremental backup

## ANSWER: A B

**Explanation:**

The Sunday full backup establishes the baseline and is required for the restore. The Thursday cumulative incremental backup is also required because a cumulative incremental backup includes all changes since the most recent successful full backup. Therefore, it includes the changes captured by the Monday, Tuesday, and Wednesday cumulative backups as well as Thursday's changes.

The earlier cumulative incremental images are not required when the latest cumulative incremental image is available. This is the key operational difference between cumulative and differential incremental backups.

## QUESTION NO: 11

An administrator is designing a storage lifecycle policy for a workload that requires an initial backup copy on local disk followed by a managed duplicate copy on another storage target.

Which two statements are true about this configuration? (Choose two.)

**A.** The first operation should be a Backup operation.

**B.** The policy schedule must select the storage lifecycle policy.

**C.** The policy schedule must select a disk pool directly.

**D.** The first operation should be a Duplication operation.

**E.** Each storage unit must be configured as On Demand Only.

**ANSWER: A B**

**Explanation:**

A storage lifecycle policy that creates an initial backup and then a duplicate copy must begin with a **Backup** operation. The subsequent **Duplication** operation can process the image after the initial backup copy has been created.

The backup policy or schedule must select the storage lifecycle policy for NetBackup to use the defined operations. A disk pool provides managed disk capacity, but it does not itself define the ordered backup and duplication workflow. Setting a storage unit to On Demand Only is unrelated to the required operation order.

## QUESTION NO: 12

An administrator is preparing a cloud storage target for use by NetBackup backup policies. The cloud provider account is supported and network access to the provider has been verified.

Which two NetBackup storage objects must be configured before a policy can select the cloud target as a storage destination? (Choose two.)

**A.** a cloud storage server

**B.** a cloud disk pool

**C.** a cloud client policy type

**D.** a catalog backup policy

**E.** a tape volume pool

**ANSWER: A B**

**Explanation:**

A cloud storage server must be configured to define NetBackup connectivity and authentication for the cloud provider. A cloud disk pool must then be created from that cloud storage server to represent the available cloud storage capacity.

After these objects exist, the administrator creates a storage unit that references the disk pool and selects that storage unit, or an applicable storage lifecycle policy, in the backup policy. A cloud account alone is not a NetBackup storage destination, and a catalog backup policy is unrelated to configuring cloud capacity.

## QUESTION NO: 13

A primary server has suffered a catastrophic disk failure, including loss of the NetBackup catalog. The administrator must begin a catalog recovery.

Which two items are required to perform the recovery? (Choose two.)

**A.** the disaster recovery file created by the catalog backup

**B.** the catalog backup image or catalog backup media

**C.** the most recent client full backup image

**D.** the storage lifecycle policy used by production backups

**E.** the NetBackup client installation package

**ANSWER: A B**

**Explanation:**

A catalog backup image is required because it contains the catalog data that must be restored. The disaster recovery (DR) file is also required because it contains the information needed to identify the catalog backup and begin the catalog recovery process.

Regular client backup images do not contain the NetBackup catalog, and a storage lifecycle policy does not replace the DR information needed to locate and recover the catalog backup. The DR file should be retained separately from the primary server and catalog volumes.

## QUESTION NO: 14

How is the expiration date of an imported image determined during an import?

**A.** by using the original backup date plus infinity

**B.** by using the original backup date plus the original retention

**C.** by using the import date plus seven years

**D.** by using the import date plus the original retention

**ANSWER: D**

**Explanation:**

NetBackup determines an imported image's expiration by adding the image's original retention period to the date on which the image is imported. Therefore, the appropriate answer is *by using the import date plus the original retention*. Importing reconstructs the image records in the NetBackup catalog from the backup media; it does not reinstate an already elapsed expiration timeline based on the date the backup was first created. The resulting cataloged image receives an expiration calculation beginning at import time, while retaining the retention period associated with the imported backup. This behavior is important when recovering catalog information or importing backups written by another NetBackup environment, because an image that was created long ago can still be available after it is imported if its retention interval is applied from the import date. Administrators should confirm that the intended retention level is associated with the import operation and should account for the resulting expiration when planning media preservation and subsequent restores. Veritas documents the import operation and its retention-related controls in the NetBackup Commands Reference Guide; broader image and media-management behavior is covered in the NetBackup documentation portal.

## QUESTION NO: 15

A policy protects five clients and has four backup selections. The administrator has enabled Allow multiple data streams, and the policy creates excessive concurrent work during the backup window.

Which two policy changes can reduce the number of concurrent child backup jobs generated by this policy? (Choose two.)

**A.** Clear Allow multiple data streams.

**B.** Set a lower Limit jobs per policy value.

**C.** Increase the storage unit multiplexing value.

**D.** Expand the backup window.

**E.** Increase the maximum concurrent jobs setting on the storage unit.

**ANSWER: A B**

**Explanation:**

Clearing **Allow multiple data streams** prevents NetBackup from creating separate child jobs for multiple backup selections on a client. Setting **Limit jobs per policy** establishes a maximum number of jobs from that policy that may run concurrently.

Increasing multiplexing can allow more data streams to share a storage device and does not reduce the number of jobs generated by the policy. Expanding the backup window changes when jobs can run, but it does not directly limit policy concurrency. Increasing storage-unit job limits can allow additional jobs to run rather than constraining them.

## QUESTION NO: 16

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 produced by its supported backup methods, including full and incremental backup processing. A full image contains all selected data for the backup selection and establishes the baseline from which subsequent incremental protection can be restored. Differential images represent the data that changed since the most recent successful full or incremental backup; NetBackup commonly describes this method as a differential incremental backup. Incremental images are also managed in NetBackup's catalog and are used with the relevant full image to restore protected data efficiently. In NetBackup terminology, incremental protection can be configured as differential incremental or cumulative incremental, depending on the policy schedule and the required recovery behavior. The NetBackup catalog tracks these images and their associated copies, retention, storage location, and relationships so that the appropriate backup sequence can be selected during a restore. Veritas documentation describes full and incremental backup methods and their restore requirements in the NetBackup Administrator's Guide. See the Veritas NetBackup documentation portal and the NetBackup backup types documentation.

## QUESTION NO: 17

A NetBackup appliance is not backing up data from a specific client. What steps can be taken to troubleshoot the problem?

**A.** Check the client's backup policies.

**B.** Check the client's connectivity to the appliance.

**C.** Check the appliance's logs for errors.

**D.** Contact Veritas Support for assistance.

**ANSWER: A**

**Explanation:**

Checking the client's backup policies is the most appropriate initial troubleshooting action because NetBackup policy configuration determines whether the client is selected for protection at all. Review the policy's client list to confirm that the client name resolves to and matches the name configured in NetBackup. Then verify that the policy is active, has an applicable schedule, and includes valid backup selections for the client. The schedule window, calendar, backup type, and policy attributes must permit the intended job to run. For a policy that uses a query or client-selection rule, confirm that the client still meets the rule's criteria. Also review the policy's storage and retention settings to ensure they support the intended protection workflow. A policy can appear correctly configured at a high level while a client is omitted, assigned an incorrect hostname, excluded by a selection rule, or not covered by an enabled schedule. NetBackup administrators use policy configuration as the authoritative definition of which clients and data are protected, so validating this configuration directly addresses why one specific client is not being backed up. Veritas documents policy management and client configuration in the NetBackup Administrator's Guide and provides product documentation through the NetBackup documentation portal.

## QUESTION NO: 18

Which guide should be referred to for configuring deduplication options in NetBackup 10.1?

**A.** Veritas NetBackup Deduplication Guide: v10.1

**B.** Veritas NetBackup Appliance Administrator's Guide: v5.0

**C.** Veritas NetBackup 10.1 Administrator's Guide, Volume I

**D.** Veritas NetBackup Appliance Commands Reference Guide: v5.0

## ANSWER: A

**Explanation:**

**Veritas NetBackup Deduplication Guide: v10.1** is the appropriate reference because it is the product-specific documentation dedicated to NetBackup deduplication technology and its configuration. It describes how to plan, enable, and administer deduplication, including configuration of Media Server Deduplication Pool storage, client-side and media-server-side deduplication behavior, storage-server settings, disk-pool considerations, and operational requirements. These details are essential when selecting and configuring deduplication options, since the applicable settings can depend on the deduplication architecture, supported storage, client or media-server role, and the backup workflow being used.

Using the guide that matches the NetBackup 10.1 release is important because supported features, configuration procedures, requirements, and terminology can change between versions. Veritas publishes versioned product documentation so administrators can validate settings against the exact NetBackup release deployed in their environment. The NetBackup 10.1 documentation set is available through the Veritas NetBackup 10.1 Documentation portal. For broader product documentation access and release-specific guides, use the Veritas NetBackup Support and Documentation page.

## QUESTION NO: 19

Which two tasks can be performed from the Appliance Web Console? (Select two.)

**A.** run a manual backup

**B.** create a backup policy

**C.** add or delete additional servers

**D.** create a storage lifecycle policy

**E.** resize the MSDP partition

## ANSWER: C E

**Explanation:**

The Appliance Web Console provides appliance-level administration functions, including management of the systems that are authorized to use the appliance as a media server. Therefore, administrators can use it to add or delete additional

servers. This capability is used to maintain the list of approved additional NetBackup media servers that can access and use the appliance storage resources, without requiring a separate appliance-shell workflow.

The web console also provides storage administration for the appliance, including the ability to resize the MSDP partition when the appliance configuration and available disk capacity support that operation. Resizing lets an administrator adjust the space allocated to the appliance's Media Server Deduplication Pool so that storage capacity remains aligned with operational requirements. These are appliance-management tasks exposed through the dedicated Appliance Web Console. Veritas documents the available appliance administration interfaces and storage-management procedures in the NetBackup Appliance 5.0 documentation and the Appliance Web Console documentation.

## QUESTION NO: 20

A new storage shelf is added to an existing appliance.

Which command under Manage > Storage must the administrator perform first after a new shelf is connected to the appliance and the appliance is powered on?

**A.** Add

**B.** Scan

**C.** Resize

**D.** Edit

## ANSWER: B

**Explanation:**

**Scan** is the first required operation because the appliance must discover the newly connected physical storage shelf before that shelf can be incorporated into appliance-managed storage. The Scan operation queries the storage hardware and refreshes the appliance's inventory of available shelves and disks. This discovery step confirms that the shelf is visible through the expected cabling and controllers and makes its capacity available for subsequent storage configuration tasks. After discovery has completed successfully, the administrator can use the appropriate follow-on storage action to integrate the detected capacity into the appliance's storage configuration. Performing discovery first is important because management operations depend on the appliance having an up-to-date view of the connected hardware. Veritas documents appliance storage expansion and disk-shelf procedures in the NetBackup Appliance documentation, including the required detection and configuration workflow. See the Veritas NetBackup Appliance documentation and the Veritas NetBackup Appliance hardware and storage expansion guidance.

## QUESTION NO: 21

What is the minimum size of a file that can be deduplicated by NetBackup?

**A.** 1 KB

**B.** 8 KB

**C.** 64 KB

**D.** 128 KB

## ANSWER: B

**Explanation:**

**8 KB** is the minimum file size that NetBackup can deduplicate. NetBackup deduplication processes backup data by identifying duplicate data segments and retaining a unique segment only once in the deduplication storage pool, while subsequent matching segments are represented by references. Files smaller than 8 KB do not meet the minimum threshold for this processing and therefore are stored without deduplication. This threshold is important when estimating deduplication effectiveness: backup sets containing large numbers of very small files may show a lower overall deduplication ratio, even

when much of the remaining data is highly repetitive. The value applies to NetBackup deduplication behavior rather than to a general operating-system file-size limit. Administrators should consider file-size distribution, change rate, backup policy selection, and the applicable deduplication storage configuration when evaluating expected savings. Veritas documents NetBackup deduplication concepts, configuration, and operational behavior in its NetBackup Deduplication Guide, available through the NetBackup documentation portal. Product documentation and version-specific administrator guidance can also be accessed from the Veritas NetBackup support page.

## QUESTION NO: 22 - (SIMULATION)

What are the two types of log files that record all activities related to NetBackup appliance security? A. security.log and audit.log

B. secure.log and auth.log

C. security.log and auth.log

D. secure.log and audit.log

## ANSWER: See the explanation for the answer

**Explanation:**

**Correct answer: A. `security.log` and `audit.log`**

NetBackup Appliance security-related activity is recorded in the `security.log` and `audit.log` files. These logs support reviewing security events and auditing appliance activity.

## QUESTION NO: 23

An administrator must create a second copy of each successful backup on another storage target after the initial backup completes. The copy operation must be managed automatically by NetBackup.

Which two configuration actions are required? (Choose two.)

**A.** create a storage lifecycle policy with a backup operation and a duplication operation

**B.** select the storage lifecycle policy in the backup policy schedule

**C.** configure the initial storage unit as On Demand Only

**D.** set the backup schedule retention period to zero

**E.** enable multiplexing on every storage unit used by the policy

## ANSWER: A B

**Explanation:**

A storage lifecycle policy must contain a backup operation followed by a duplication operation. The backup operation creates the initial image, and the subsequent duplication operation directs NetBackup to create the additional copy on the configured destination storage.

The policy schedule must then select the storage lifecycle policy as its storage destination. Selecting only a storage unit writes a single backup copy and does not invoke the storage lifecycle operations. A storage lifecycle policy coordinates the required copy workflow and tracks whether the configured operations have completed.