DUMPSBOSS.

# Administration of Veritas Backup Exec 20.1

## Veritas VCS-325

### Version Demo

**Total Demo Questions: 10**

**Total Premium Questions: 104**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Configure Backup Exec 20.1 | 22 |
| Topic 2, Configure Storage Devices and Media | 25 |
| Topic 3, Configure Backup and Restore Jobs | 34 |
| Topic 4, Manage Backup Exec 20.1 | 14 |
| Topic 5, Troubleshoot Backup Exec 20.1 | 9 |
| Total | 104 |

QUESTION NO: 1

Backup Exec reports can be manually saved in any of the following five file formats; which two of these formats can the reports initially be displayed as? (Choose two.)

**A.** XML

**B.** CSV

**C.** HTML

**D.** PDF

**E.** XLS

**ANSWER: C D**

**Explanation:**

Backup Exec initially renders reports in **HTML** or **PDF** format. These are the two presentation-oriented formats used when an administrator opens or views a generated report from the Backup Exec console. HTML provides a browser-style, navigable report view, while PDF provides a fixed-layout report suitable for viewing, printing, and distribution without changing its layout. After a report has been generated and displayed, Backup Exec also supports manually saving or exporting report data in additional formats, including XML, CSV, and XLS. Those export formats are useful for data exchange, spreadsheet analysis, or processing by other tools, but the question specifically distinguishes initial report display from manual saving. Therefore, the correct selections are the formats intended for the report viewer: HTML and PDF. This behavior is documented in Veritas Backup Exec reporting documentation, which describes viewing reports in HTML or PDF and saving reports in the supported output formats. See the Veritas Backup Exec 20.1 documentation and the Backup Exec product support portal.

**QUESTION NO: 2**

What are two requirements for configuring Optimized Duplication between two or more Backup Exec servers? (Choose two.)

**A.** The Central Admin Server (CAS) and Managed Backup Exec Server (MBES) must be configured.

**B.** The NDMP option must be installed.

**C.** The OS must be similar on the Backup Exec servers where the Deduplication Folder needs to be shared.

**D.** The same Deduplication account must be used on all the Backup Exec servers.

**E.** The Deduplication storage on each Backup Exec server must be shared.

**ANSWER: A E**

**Explanation:**

Optimized Duplication in Backup Exec is designed for a Central Admin Server Option environment, in which a Central Admin Server coordinates operations involving its Managed Backup Exec Servers. Configuring the Central Admin Server and Managed Backup Exec Server relationship is therefore required so Backup Exec can manage the participating servers and initiate the optimized duplication workflow across them.

The deduplication storage used by the participating Backup Exec servers must also be shared. Shared deduplication storage provides the common storage configuration needed for the servers to work with the relevant Deduplication Folder as part of the optimized duplication design. This arrangement lets Backup Exec use deduplication-aware duplication processing rather than treating the operation as an ordinary independent copy workflow. These requirements apply to the Backup Exec server architecture and storage configuration, so they should be confirmed before creating or running the associated duplication jobs.

Veritas documents Central Admin Server and Managed Backup Exec Server administration, as well as deduplication storage configuration, in the Backup Exec documentation. Product documentation and release-specific administrative resources are also available through the Veritas Backup Exec support portal.

## QUESTION NO: 3

When is the Install Device Drivers Option unavailable in the Configure Storage wizard?

**A.** when Backup Exec detects hardware that is unsupported

**B.** when Backup Exec detects that device drivers are already installed

**C.** when Backup Exec is installed on a Windows 2008 or earlier operating system

**D.** when Backup Exec is installed on a Windows 2012 or later operating system

## ANSWER: D

**Explanation:**

The correct answer is **when Backup Exec is installed on a Windows 2012 or later operating system**. On Windows Server 2012 and newer Windows releases, Backup Exec does not present the *Install Device Drivers* choice in the Configure Storage wizard. Device-driver installation and management on these platforms is handled through the Windows driver framework and the operating system's device-management mechanisms rather than through this Backup Exec wizard option. Administrators should therefore confirm that the applicable storage hardware is recognized by Windows and that the vendor-supported Windows driver is installed before configuring the device for use in Backup Exec. Once Windows has made the device available, Backup Exec can detect and configure supported storage hardware and associated Backup Exec components as applicable. This behavior is platform-specific: the wizard's available controls are adjusted according to the Windows operating system on which Backup Exec runs. For Microsoft's description of driver installation and device management in modern Windows, see Windows driver installation documentation. Veritas Backup Exec product documentation and release-specific guidance are available through the Veritas Backup Exec documentation portal.

## QUESTION NO: 4

In which scenario should an administrator choose to use the faster processing method for Hyper-V backups?

**A.** The administrator wants to use full and incremental backup methods.

**B.** The administrator wants to use full and differential backup methods.

**C.** The administrator wants to use client-side deduplication for backups.

**D.** The Hyper-V host has limited space for checkpoints.

## ANSWER: A

**Explanation:**

The administrator wants to use full and incremental backup methods. In Backup Exec Hyper-V protection, the Faster processing method is designed for environments where reducing the time and resources required to process backup jobs is the priority. This method uses a full backup as the baseline and then uses incremental backups to capture only the changes made since the preceding backup. Because subsequent jobs handle a smaller changed-data set rather than repeatedly processing all changes since the full backup, daily backup processing is typically quicker and requires less backup storage than repeatedly creating larger changed-data sets.

Administrators should choose this method when the backup window, host workload, and efficient day-to-day job processing are more important operational considerations. The full backup establishes the recoverable base, while each incremental backup contributes the changes needed to bring a protected virtual machine forward to a selected recovery point. Backup Exec documents the Hyper-V processing-method behavior and the full/incremental backup-chain model in its product documentation. See the Veritas Backup Exec documentation and the Backup Exec product support page for current administration guidance.

## QUESTION NO: 5

An administrator has a backup job that protects three SQL instances on the server. The third instance hosts a very important application database, so the administrator wants to ensure that instance is the first one backed up.

What is the most efficient way to ensure the application database instance is the first to be backed up?

**A.** drag the application database instance to the top of the backup selections tree

**B.** create a new backup job that backs up only the application database instance, and run that backup job first

**C.** use the reordering controls on the Selection Details page to make the application database instance the first one selected

**D.** select the specific SQL instance in the backup selection list and use the Tag as business-critical option

**ANSWER: C**

**Explanation:**

Use the reordering controls on the Selection Details page to make the application database instance the first one selected. Backup Exec lets an administrator control the order of selections within a job through the Selection Details view. Moving the important SQL instance to the first position causes Backup Exec to process that selection before the other SQL-instance selections in the same backup job. This directly meets the requirement without introducing a separate job, separate schedule, or additional job-management overhead.

Keeping the instances in one job also retains the existing job's storage, schedule, retention, notification, and operational settings. The selection-order controls are intended for cases in which a particular protected resource needs priority within an otherwise shared job. For SQL protection, Backup Exec identifies SQL instances and databases through the SQL Agent and processes the job's configured selections accordingly; placing the application instance first provides the requested priority while preserving the existing backup design.

Refer to the official Veritas Backup Exec documentation portal for the Administration Guide and SQL Agent configuration guidance. Veritas also provides Backup Exec product documentation and support resources at Veritas Backup Exec Support.

**QUESTION NO: 6**

An administrator runs a server backup to the Tape Library and has two backups created for the same server. The first backup contains the drive backup [C, D], and the second backup has the system state selected. When a virtual conversion of the server is attempted, the Convert to virtual option is greyed out.

What could be the reason for the Convert to virtual option being greyed out?

**A.** Catalogs operation needs to be performed on the backup sets.

**B.** The Convert to virtual option is unsupported on tape backups.

**C.** Simplified Disaster Recovery (SDR) is disabled.

**D.** The VMware and Hyper-V Agent needs to be installed.

**ANSWER: C**

**Explanation:**

Simplified Disaster Recovery (SDR) is disabled is the applicable reason because Backup Exec uses SDR capabilities as part of its physical-to-virtual conversion workflow. SDR provides the recovery framework and machine configuration information needed to reconstruct a protected Windows computer in a virtual environment. When SDR is disabled, Backup Exec does not make the Convert to virtual workflow available, so the command can appear greyed out even when backup data for the computer is present.

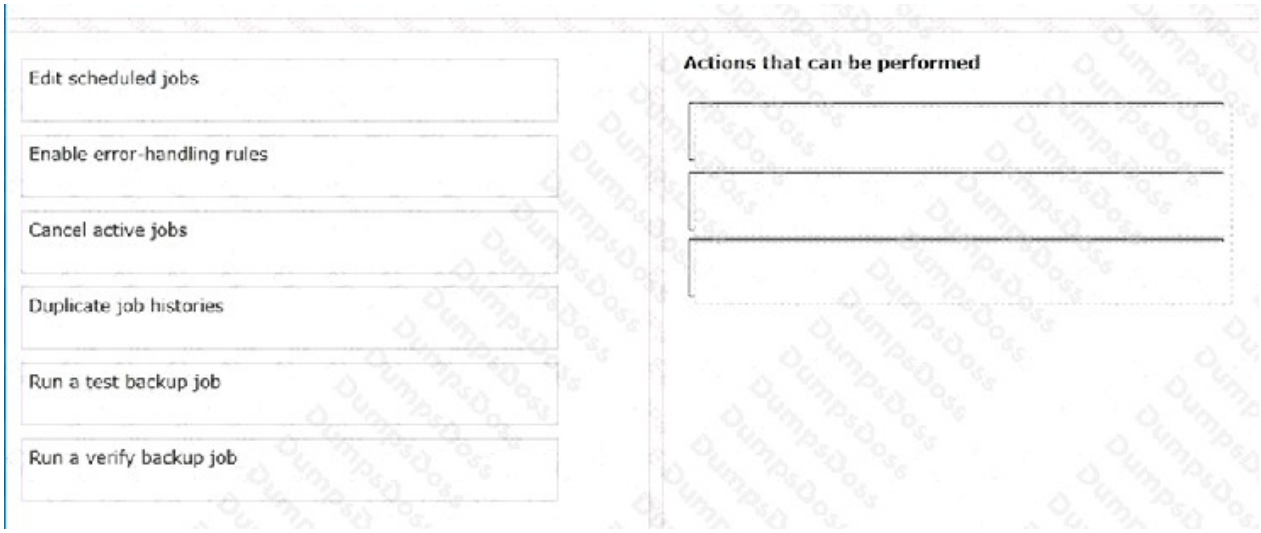
For a successful conversion, the selected recovery data must also provide the information necessary to recover the operating system and required volumes. Backup Exec evaluates the backup content and the availability of the SDR-based recovery functionality before allowing a conversion to proceed. Administrators should verify that SDR is enabled in Backup Exec settings and that the computer's backups include the required system and volume data for recovery. Veritas

documents SDR as a Backup Exec recovery feature and documents conversion to virtual machines as a recovery workflow in the Backup Exec Administrator's Guide. See the Veritas Backup Exec documentation and the Veritas Backup Exec knowledge base for product guidance.

## QUESTION NO: 7 - (SIMULATION)

Which actions can an administrator perform on an active or scheduled job in the Job Monitor pane?

Drag the three (3) actions that an administrator can perform in the Jobs pane on the Job Monitor from the left column to the right column.




## ANSWER: See the explanation for the answer

**Explanation:**

Select these three actions in the **Jobs** pane of Job Monitor:

Editing and test-running apply to scheduled jobs, while cancellation applies to currently active jobs. Duplicating job histories and running a verify operation are associated with job-history/completed-job activities rather than active or scheduled jobs in the Jobs pane. Error-handling rules are configured elsewhere.

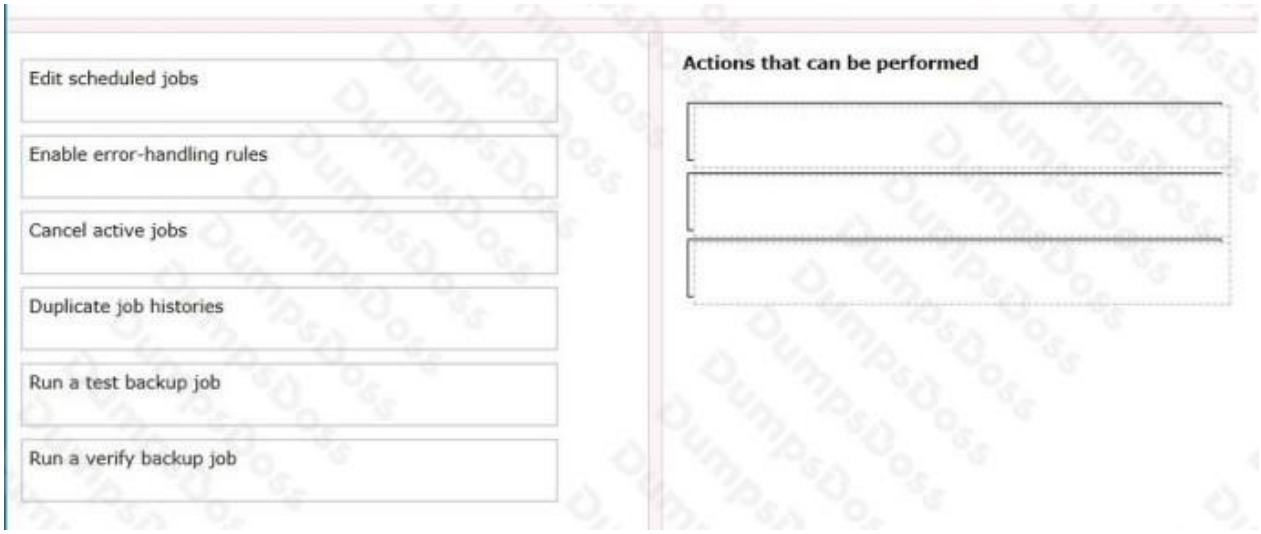
## QUESTION NO: 8 - (DRAG DROP)

DRAG DROP

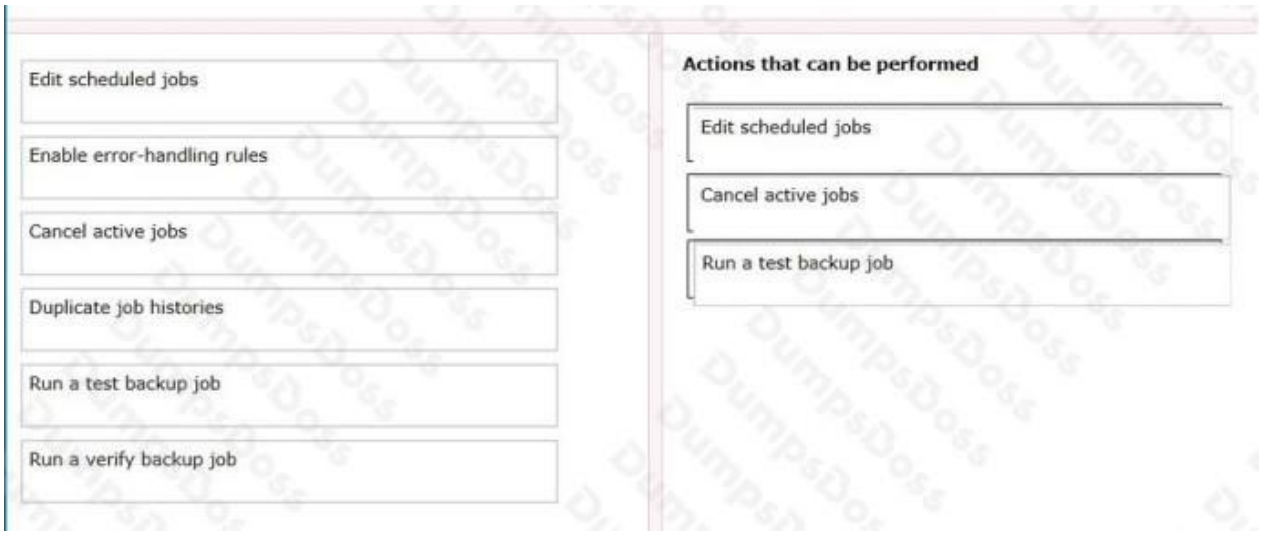
Which actions can an administrator perform on an active or scheduled job in the Job Monitor pane?

Drag the three (3) actions that an administrator can perform in the Jobs pane on the Job Monitor from the left column to the right column.

**Select and Place:**




**ANSWER:**




**Explanation:**

Backup Exec Job Monitor is the central workspace for supervising jobs and taking operational action against the selected job. A scheduled job remains an editable configuration object, so an administrator can select it and edit the scheduled job when its job settings, selections, storage, schedule, or other configuration needs to be updated. This lets administration changes be made without recreating the job.

For a job that is currently processing, Job Monitor provides control of the running operation. Cancelling an active job is therefore an available action. This is useful when processing must be stopped because of a maintenance window, an incorrect configuration, an unexpected impact on a protected resource, or a need to free Backup Exec resources for a higher-priority task.

Job Monitor also supports starting a test backup job. A test run validates the job's setup and reports what Backup Exec expects to do, while allowing the administrator to check job configuration and anticipated results before relying on the job for normal protection processing. It is a practical operational check after changing a job or before putting a new protection workflow into production.

Thus, the correct set of actions is editing scheduled jobs, cancelling active jobs, and running a test backup job. Veritas documents Job Monitor job-management functions in the Backup Exec administration documentation. The broader Backup Exec documentation library is also available from the Veritas Backup Exec documentation portal.

## QUESTION NO: 9

Which two methods can an administrator use to find more information on Backup Exec job error messages? (Choose two.)

**A.** review the job log and click the UMI link

**B.** use the Backup Exec Diagnostic utility Bediag.exe

**C.** in the Administrative Console, open the Help pages and search for the error

**D.** use the Veritas Quick Assist tool

**E.** search the Veritas Technical Support Knowledge base for common errors

**ANSWER: A E**

**Explanation:**

Backup Exec job logs provide the most direct starting point for researching a failed job. When an error includes a UMI (Unique Message Identifier), selecting the UMI link in the job log opens the associated Veritas support information. That information typically supplies the message description, likely causes, recommended corrective actions, and related technical articles. This makes *review the job log and click the UMI link* an effective built-in method for obtaining details that are specific to the reported error.

*Search the Veritas Technical Support Knowledge base for common errors* is also appropriate because Veritas publishes knowledge-base articles for Backup Exec error codes, job failures, configuration conditions, and known issues. Searching by the exact error text, UMI, error number, or relevant job component helps an administrator locate current troubleshooting guidance and any applicable updates or hotfix information. Veritas specifically documents using error-message and UMI information to locate support content. See Veritas support article 100021291 and the Veritas Backup Exec Support portal.

**QUESTION NO: 10**

Which two requirements must be met to use T10 hardware encryption for a Backup Exec tape backup? (Choose two.)

**A.** The tape drive must support T10 hardware encryption.

**B.** A hardware-encryption passphrase must be configured in Backup Exec.

**C.** The tape media must belong to the Scratch Media set.

**D.** The Deduplication Feature must be installed.

**E.** Software compression must be enabled for the backup job.

**ANSWER: A B**

**Explanation:**

The tape drive must support hardware encryption that conforms to the T10 encryption standard. T10 hardware encryption is performed by the compatible tape device, rather than by Backup Exec software encryption, so an unsupported drive cannot provide this capability.

An administrator must also configure the hardware-encryption credentials, including the required passphrase, in Backup Exec. Backup Exec uses this information to manage the encryption keys needed to write and later restore encrypted tape data. The passphrase and associated key information must be retained securely because encrypted backup sets cannot be restored without the applicable encryption credentials.

See the Veritas Backup Exec documentation portal for tape-device and hardware-encryption configuration guidance.