DUMPSBOSS.

Administration of Veritas Backup Exec 16

Veritas VCS-323

Version Demo

Total Demo Questions: 11

Total Premium Questions: 115

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Installation and Configuration	23
Topic 2, Backup and Restore Operations	44
Topic 3, Storage Management	25
Topic 4, Managing and Monitoring Backup Exec	17
Topic 5, Troubleshooting	6
Total	115

QUESTION NO: 1

Which two Agent options support restores of individual items from Granular Recovery Technology (GRT) backup sets? (Select two.)

A. Agent for Application and Databases

B. Agent for Oracle on Windows

C. Agent for VMware and Hyper-V

D. Agent for Windows

E. Agent for Linux

ANSWER: A C

Explanation:

Granular Recovery Technology is designed to let Backup Exec recover individual objects from a protected application or virtual-machine backup without requiring restoration of the entire backup set first. **Agent for Application and Databases** supports GRT-enabled protection and recovery for supported Microsoft application workloads, allowing administrators to browse and select individual application objects during restore operations. This capability is particularly valuable when a specific mailbox item, directory object, or other application-level item must be recovered quickly while minimizing data movement and downtime.

Agent for VMware and Hyper-V supports GRT for supported virtual-machine backups. It enables Backup Exec to present the contents of a VM backup for granular selection, so administrators can restore individual files and supported application items from the virtualized workload rather than restoring the full virtual machine. GRT must be enabled and the protected workload must meet the relevant Backup Exec requirements, but these two agent options provide the applicable granular restore capabilities. Veritas documents Backup Exec product resources at Backup Exec documentation and provides product-specific support material at Veritas Backup Exec Support.

QUESTION NO: 2

Which backup method is invalid when performing a SharePoint farm backup using a SharePoint agent?

A. full â€“ back up databases

B. full copy â€“ back up databases (copy)

C. full (block-level)

D. differential (block-level)

E. incremental (block-level)

ANSWER: C

Explanation:

full (block-level) is invalid for a SharePoint farm backup performed through the Backup Exec SharePoint agent. A SharePoint farm is protected through the agent's SharePoint-aware backup workflow, which coordinates the farm's content and configuration databases and uses the applicable database-oriented or supported change-based backup methods. The generic full block-level method is not a valid selection for this type of SharePoint farm protection. Selecting a supported SharePoint method is important because Backup Exec must preserve the information required to recover farm components consistently, including the relationships among the protected SharePoint databases. Veritas documents the supported SharePoint backup methods and restrictions for Backup Exec in its knowledge-base guidance. For the product-specific details, see Veritas knowledge base article 000076109. Additional Backup Exec technical documentation is available through the Veritas Backup Exec support portal.

QUESTION NO: 3

What are two requirements for enabling the Backup Exec Management Command Line Interface (BEMCLI)? (Select two.)

A. Microsoft ReportViewer

B. Microsoft Visual C++ Redistributable

C. Microsoft Silverlight

D. Microsoft .NET 3.5

E. Microsoft Windows PowerShell V2

ANSWER: D E

Explanation:

Backup Exec Management Command Line Interface is implemented through Windows PowerShell cmdlets, so **Microsoft Windows PowerShell V2** is required to provide the command shell and cmdlet framework used to load and run BEMCLI commands. Backup Exec 16 documentation identifies PowerShell 2.0 as the required PowerShell version for this component. **Microsoft .NET 3.5** is also required because the Backup Exec command-line components depend on the .NET Framework runtime and associated libraries when BEMCLI is enabled or installed. These prerequisites should be present on the Backup Exec server before enabling the interface, ensuring that its PowerShell snap-in and Backup Exec management commands can be registered and executed successfully. In environments where later Windows versions include newer PowerShell releases, the documented Backup Exec 16 prerequisite remains relevant because the product's BEMCLI integration was designed and validated with the Windows PowerShell 2.0 framework. Review the Backup Exec documentation set for the release-specific installation prerequisites and BEMCLI procedures at Veritas Backup Exec Documentation. Microsoft's .NET Framework deployment guidance is available at .NET Framework installation guide.

QUESTION NO: 4

Which option should an administrator select to add a tape with a barcode to the library?

A. Initialize now

B. Scan

C. Inventory and Catalog now

D. Inventory

ANSWER: D

Explanation:

Inventory is the appropriate operation after a barcoded tape has been physically loaded into a robotic library. During an inventory, Backup Exec examines the library slots and updates its media database with the media that is present. For libraries equipped with a barcode reader, Backup Exec obtains the barcode labels as part of this process, allowing it to identify and track the tape without requiring the tape contents to be read. This makes inventory the normal administrative action for bringing newly inserted barcoded media under Backup Exec management and ensuring that the displayed library-slot and media information is current.

The administrator should first make the tape available to the library, such as by placing it in an import/export slot and moving it into a storage slot if required by the library workflow. Running Inventory then synchronizes Backup Exec's view of the robotic library with the actual media loaded in it. Veritas describes inventory as the operation used to update Backup Exec information about media in a storage device; barcode-capable libraries provide barcode-based media identification. See the Veritas Backup Exec Administration Guide and the Backup Exec product documentation portal for storage-device and media-management guidance.

QUESTION NO: 5

Which two alternate destinations are available when using the restore wizard to restore from file and folder backups? (Select two.)

A. Zip file

B. Drive and Path

C. Microsoft Virtual Hard Disk

D. PST file

E. VMDK file

ANSWER: A E

Explanation:

Zip file and **VMDK file** are supported alternate-destination formats for file and folder restores in Backup Exec. Restoring to a Zip file packages the selected restored content into a portable archive, which is useful when the files need to be delivered, retained, or moved without immediately placing them back into a production file-system location. Restoring to a VMDK file writes the restored content to a VMware virtual-disk format, enabling the data to be mounted or used in a VMware-oriented recovery or migration workflow. These choices are presented as alternate restore targets in the Restore wizard for file and folder backup data, allowing administrators to direct recovered data into a portable archive or virtual-disk container rather than simply restoring it in place. Veritas documents restore operations and destination selection through the Backup Exec administration documentation; see the Backup Exec Administrator's Guide and the Veritas Backup Exec support knowledge base for restore-related guidance.

QUESTION NO: 6

When does Backup Exec Data Lifecycle Management (DLM) delete all the backup sets on which the backup set expiry date is reached?

A. when the backup sets contain multiple unexpired incremental backup sets, but the full backup has expired

B. when the backup sets contain expired backup sets created by different backup definitions

C. when the Allow Backup Exec to delete all expired backup sets option is checked

D. when the backup sets are available on a deduplication disk storage device

ANSWER: C

Explanation:

Backup Exec Data Lifecycle Management deletes every backup set whose retention period has expired when the *Allow Backup Exec to delete all expired backup sets* option is enabled. This setting instructs Backup Exec to process expiration based on each backup set's configured expiry date, rather than retaining an otherwise expired set because of backup-set relationships within a backup chain. It is useful when an organization needs retention processing to consistently reclaim storage as soon as the defined retention period ends.

DLM evaluates expiration during its scheduled maintenance and cleanup processing. A backup set is eligible only after its configured retention period has elapsed; enabling this setting does not cause unexpired data to be deleted. Administrators should therefore ensure that the retention periods assigned in backup definitions meet recovery, operational, and compliance requirements before selecting the setting. Veritas documents Backup Exec administration and storage/retention management in its Backup Exec documentation and provides related product documentation through the Backup Exec support portal.

QUESTION NO: 7

Which action must an administrator take to properly restore System State on a live Windows Web server?

A. restore System State in Safe mode

B. restore System State in Directory Services Restore mode

C. restore System State and reboot the server

D. restore System State with the option toMark this server as the primary arbitrator

ANSWER: C

Explanation:

The required action is to restore System State and reboot the server. A Windows System State recovery replaces protected operating-system configuration and components, which can include the registry, boot files, the COM+ class registration database, system files protected by Windows Resource Protection, and—in the case of a web server—relevant IIS configuration held in the system configuration. Because key components are in use while Windows is running, the restored state cannot be fully loaded and applied until the machine restarts. The reboot is therefore an essential completion step for a System State restore to the original, live server, rather than merely an optional operational precaution. Administrators should also plan the recovery during an approved maintenance window, because restarting a web server interrupts hosted applications and network services. Microsoft documents System State recovery as a recovery operation that requires restart processing so that Windows can apply the recovered system configuration; see wbadmin start systemstaterecovery. Veritas Backup Exec similarly treats System State recovery as a Windows system recovery workflow; Backup Exec documentation and product resources are available through the Veritas Backup Exec Support portal.

QUESTION NO: 8

In which two circumstances will the overwrite protection period for a tape begin? (Select two.)

A. at the start time of an overwrite job (if there are no appends)

B. at the end time of an overwrite job (if there are no appends)

C. at the start time of the last append operation on a media

D. at the end time of the first append operation on a media

E. at the end time of the last append operation on a media

ANSWER: B E

Explanation:

Overwrite protection in Backup Exec is calculated from the completion of the operation that most recently writes the relevant backup data to the tape. Therefore, when a tape is used by an overwrite job and no subsequent append occurs, the overwrite protection period begins at the end time of that overwrite job. This ensures that the configured protection duration is measured only after the backup has finished writing successfully.

When a tape remains appendable and additional backup data is appended, the protection timing is based on the end time of the last append operation. The last append is the most recent write to the media, so its completion establishes the point from which Backup Exec protects the tape against being overwritten. This behavior prevents a tape from becoming overwriteable before the retention interval for its newest appended backup data has elapsed.

These rules align with Backup Exec's media-management model: overwrite protection applies to the media set and is updated by completed write operations. Veritas documentation on media sets and retention settings is available in the Backup Exec Administrator's Guide and the Backup Exec documentation portal.

QUESTION NO: 9

What is a capability of the Backup Exec Agent for VMware and Hyper-V?

A. It integrates directly with the Simplified Disaster Recovery (SDR) process to provide complete recovery.

B. It enables image-level protection of virtual machines with physical Raw Device Mapping volumes.

C. It shuts down and restarts virtual machines to consistently backup the content.

D. It supports agentless virtual machine backup and complete recovery of guest virtual machines.

ANSWER: B D

Explanation:

The Backup Exec Agent for VMware and Hyper-V supports host-based, image-level protection of virtual machines, including VMware environments that use physical Raw Device Mapping volumes. This capability is important in enterprise VMware deployments because RDMs may be used to present storage directly to a guest while retaining a virtual-machine-based protection workflow. Backup Exec can use the virtualization platform integration to coordinate protection at the virtual-machine level rather than requiring a traditional full backup agent deployment solely to obtain the VM image.

It also supports agentless virtual-machine backup and complete recovery of guest virtual machines. Agentless protection uses the VMware or Hyper-V host and its virtualization APIs to capture the VM image. The resulting backup can be used for full VM recovery, allowing the protected guest to be recreated as a virtual machine, including its operating system, configuration, and protected virtual disks. This makes the feature suitable for rapid recovery of an entire virtual workload while reducing guest-level backup administration for image protection. Veritas describes Backup Exec virtualization protection and recovery capabilities on its Backup Exec product page; product documentation is available through the Veritas Backup Exec documentation portal.

QUESTION NO: 10

Where should an administrator set the option to make all new jobs choose a particular disk storage as the target device?

A. change the storage options inBackup Exec Settings

B. change the storage options in each new job

C. change the storage options in theJob Defaults

D. change the storage options in the properties of the storage

ANSWER: C

Explanation:

Administrators should change the storage options in the Job Defaults because Job Defaults supplies the initial configuration values used whenever a new job is created. Setting the preferred disk storage target there causes new backup jobs to inherit that device selection automatically, which provides consistent job creation and avoids having to select the same storage target repeatedly. Job Defaults are intended for settings that should apply broadly to newly created jobs, while still allowing an administrator to alter the inherited setting for an individual job when a particular workload has different protection or storage requirements. In Backup Exec, the storage section of Job Defaults is therefore the appropriate centralized location for establishing the default destination device used by new jobs. This behavior aligns with Veritas documentation describing Job Defaults as the source of default job settings and with the product documentation for configuring storage used by backup jobs. See the Veritas Backup Exec documentation and the Veritas knowledge base for Backup Exec configuration guidance.

QUESTION NO: 11

Backup Exec allows an administrator to make duplicate copies of deduplicated backup sets and transfer them to a different Backup Exec server. The transfer process is optimized, meaning only unique blocks (those not already contained in the deduplication storage of the destination server) are copied.

What is this functionality called?

A. optimized deduplication

B. optimized replication

C. optimized duplication

D. optimized synchronization

ANSWER: C

Explanation:

optimized duplication is the Backup Exec functionality that creates a duplicate copy of a deduplicated backup set at another Backup Exec server while minimizing data sent across the network. Backup Exec evaluates the data blocks in the source deduplication storage against blocks already held by the destination server's deduplication storage. It transfers only blocks that are not already present at the destination, rather than retransmitting the entire backup set. This provides an efficient method for moving protected data to another Backup Exec environment for offsite retention, disaster recovery planning, or centralized copy management, especially where available bandwidth is limited. The destination receives a usable duplicate backup set, while the deduplication technology reduces the volume of data that must traverse the connection. Veritas describes this capability as optimized duplication in Backup Exec's deduplication and duplication-copy documentation. For additional product documentation, see the Veritas Backup Exec Administrator's Guide and the Backup Exec documentation portal.