DUMPSBOSS.

Administration of Veritas Enterprise Vault 12.x

Veritas VCS-322

Version Demo

Total Demo Questions: 20

Total Premium Questions: 207

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Enterprise Vault Architecture	30
Topic 2, Enterprise Vault Configuration	72
Topic 3, Enterprise Vault Administration	33
Topic 4, Enterprise Vault Archiving	33
Topic 5, Enterprise Vault Maintenance and Troubleshooting	39
Total	207

QUESTION NO: 1

What are the two supported Windows Server and Veritas Enterprise Vault 12.x server combinations? (Select two.)

A. Windows Server 2003

B. Windows Server 2008

C. Windows Server 2008 R2

D. Windows Server 2012

E. Windows Server 2012 R2

ANSWER: D E

Explanation:

For Veritas Enterprise Vault 12.x, the supported Windows Server operating systems for an Enterprise Vault server are **Windows Server 2012** and **Windows Server 2012 R2**. These operating systems are listed in the Enterprise Vault 12.x compatibility information as supported server platforms. This support designation is important because Enterprise Vault server components, including the Administration Console, Enterprise Vault services, storage services, and associated Microsoft SQL Server integrations, must be deployed on an operating system combination that Veritas has tested and approved for that Enterprise Vault release family.

Windows Server 2012 provides the base Windows Server 2012 platform supported by Enterprise Vault 12.x, while Windows Server 2012 R2 is separately identified as a supported revision of that platform. Selecting both reflects the supported operating-system choices available for an Enterprise Vault 12.x server installation. Administrators should also verify the precise Enterprise Vault 12.x maintenance release and any associated prerequisites before deployment, since compatibility can depend on installed service packs, cumulative updates, SQL Server version, and the feature set being used. Veritas publishes this information in its compatibility charts and documentation: Enterprise Vault compatibility charts and Veritas Enterprise Vault documentation.

QUESTION NO: 2

An organization is planning for a PST migration. Investigations reveal there are approximately 2TB of PST files to migrate. After the migration, the data stored to the Vault Store Partition is expected to be 50% or less compared with the original data size. The indexing level will be left at the default and the storage team is planning for the migration by adding additional storage for Indexes. How large are the indexes expected to grow?

A. up to 70 GB, because PST files are compacted during archiving

B. up to 103 GB, because the deduplication is estimated to be approximately 50% of the original size

C. up to 150 GB, because the deduplication is estimated to be approximately 50% of the original size and PST files contain additional MAPI attributes

D. up to 246 GB, because the index is based on a calculation of the original PST file size

ANSWER: D

Explanation:

up to 246 GB, because the index is based on a calculation of the original PST file size is correct. Enterprise Vault index-storage planning is calculated from the size of the source data being indexed, rather than from the post-collection Vault Store Partition capacity. Therefore, the expected 50% or greater reduction in vault-store data resulting from single-instance storage, compression, or other storage efficiencies does not reduce the index-sizing baseline.

For the default indexing configuration used in this planning scenario, allow up to approximately 12% of the original PST data volume for indexes. Two tebibytes is 2,048 GB; 12% of 2,048 GB is 245.76 GB. Rounded for storage planning, this is up to 246 GB of additional index storage. This capacity should be planned separately from the Vault Store Partition because Enterprise Vault maintains index data independently to support searching and retrieval. Veritas Enterprise Vault

documentation and product resources are available through the Enterprise Vault documentation portal and the Enterprise Vault support page.

QUESTION NO: 3

An administrator is reviewing the states of Vault Store partitions.

Which two statements are correct? (Select two.)

A. A Closed partition accepts new archived items

B. A Ready partition can become the next Open partition

C. A Closed partition does not accept normal new archived-item writes

D. An Offline partition is used for active archiving

E. An Open partition cannot be placed into backup mode

ANSWER: B C

Explanation:

A **Closed** partition does not accept normal new archived-item writes. Enterprise Vault closes a partition when it is no longer to be used for incoming archive data, although background operations such as expiry and collection processing can still modify its contents.

A **Ready** partition is available for Enterprise Vault to open when the current open partition is closed or reaches its configured capacity. This allows administrators to prepare partition storage in advance of a rollover event. See the Veritas Enterprise Vault documentation portal for Vault Store partition lifecycle guidance.

QUESTION NO: 4

Which status does the Indexing Summary tool display when there are orphaned index entries found in the index volume?

A. Missing items

B. Failed items

C. Deleted items

D. Extra items

ANSWER: D

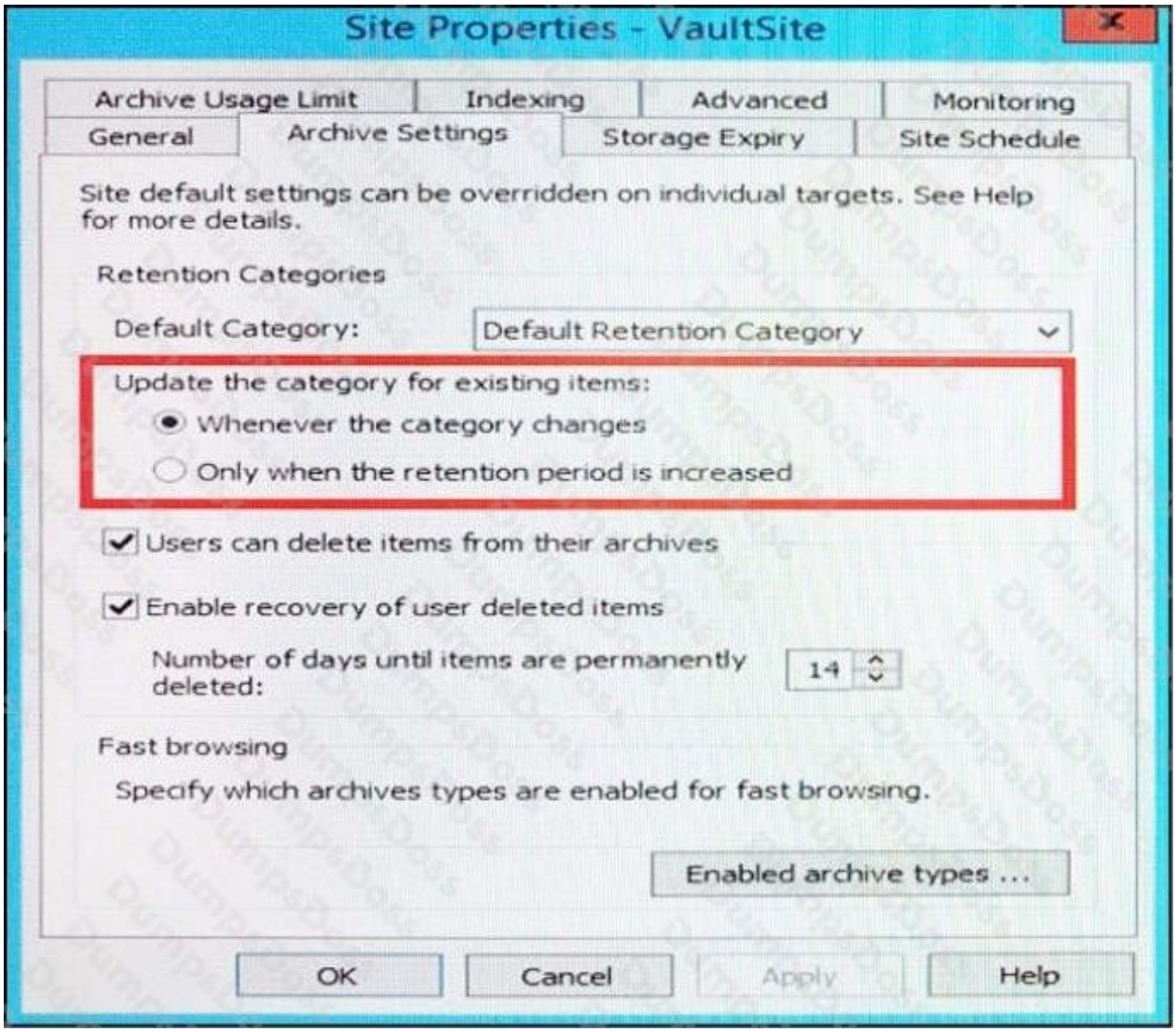
Explanation:

The correct status is **Extra items**. The Indexing Summary tool compares the items represented in an Enterprise Vault archive with the entries held in the corresponding index volume. An orphaned index entry is an entry that remains in the index but no longer has a matching archived item. Because the index contains a record in excess of what exists in the archive, Enterprise Vault reports that condition as an extra item.

This distinction is useful when investigating index consistency. The summary identifies the direction of the discrepancy: an archived item without a corresponding searchable index entry is treated as a missing index-side record, whereas an index-side entry without its associated archive item is an extra record. Administrators can use this result to determine whether index maintenance or a repair workflow is needed, while preserving the relationship between archived content and its searchable metadata. Enterprise Vault documentation and product resources are available through the Enterprise Vault documentation portal and the Enterprise Vault support page.

QUESTION NO: 5

Refer to the Exhibit.



What does the Site Setting shown in the red box apply to?

A. restored and re-archived mailbox items

B. mailbox shortcuts

C. archives moved using the Move Archive wizard

D. Storage Queue items

ANSWER: B

Explanation:

The setting applies to mailbox shortcuts. In Enterprise Vault, a shortcut is the item that Enterprise Vault creates in an Exchange mailbox to represent content that has been archived. It lets a user continue to see and open archived content from Outlook while the original item is stored in the Enterprise Vault archive. Site-level shortcut settings govern the way these mailbox shortcut items are handled across the Enterprise Vault site, including behaviors associated with creating, maintaining, updating, or deleting shortcuts according to the configured policy and site controls. This scope is distinct from archive relocation operations and storage-queue processing: the setting concerns the mailbox-facing shortcut objects that users encounter in their folders. Enterprise Vault documentation describes shortcuts as mailbox items that provide access to archived items and explains that shortcut behavior is managed through Enterprise Vault policy and configuration settings. See the Veritas Enterprise Vault documentation and the Veritas Enterprise Vault knowledge base for administration guidance on mailbox archiving and shortcut management.

QUESTION NO: 6

Which two customer scenarios are likely to result in multiple Enterprise Vault (EV) directories?

(Select two.)

A. separate active directory domains with bi-directional trusts

B. security or administrative boundaries between different groups of the organization

C. different retention policy requirements between different departments in the business

D. different single instance requirements for different departments in the business

E. very slow connectivity between archiving targets and EV servers in different data centers

ANSWER: B E

Explanation:

Security or administrative boundaries between different groups of the organization are a strong reason to deploy multiple Enterprise Vault directories. An Enterprise Vault directory represents an independently administered Enterprise Vault environment, with its own Directory database and directory service configuration. Where groups require separation of administration, configuration ownership, operational control, or security governance, separate directories provide the appropriate isolation.

Very slow connectivity between archiving targets and EV servers in different data centers can also justify multiple Enterprise Vault directories. Enterprise Vault services depend on reliable, responsive communication with the Enterprise Vault Directory and related SQL databases. A geographically distributed design with persistently poor WAN performance can impair normal operations and administration. Deploying an independently managed directory in each affected location can keep directory-dependent activity local, reduce WAN dependency, and support more reliable service operation.

These scenarios are architectural decisions made during Enterprise Vault planning, balancing operational autonomy, infrastructure connectivity, and the ability to manage each environment independently. Veritas describes Enterprise Vault product capabilities at Veritas Enterprise Vault and provides product documentation through the Enterprise Vault documentation portal.

QUESTION NO: 7

A Veritas Enterprise Vault 12.x for Exchange (EV) administrator activated Auditing at the Directory level. During this process, the administrator created the audit database and can log on the SQL server without errors. The administrator checks the content of the audit database and notices that nothing is being audited.

How should the administrator resolve this issue?

A. after enabling auditing on the EV Directory, restart the EV Admin Service level

B. enable Auditing in the Exchange Server properties in the VAC and select the auditing options

C. enable Auditing in the EV Server properties in the VAC and select the auditing options

D. enable Auditing in the EV Site properties in the VAC and select the auditing options

ANSWER: C

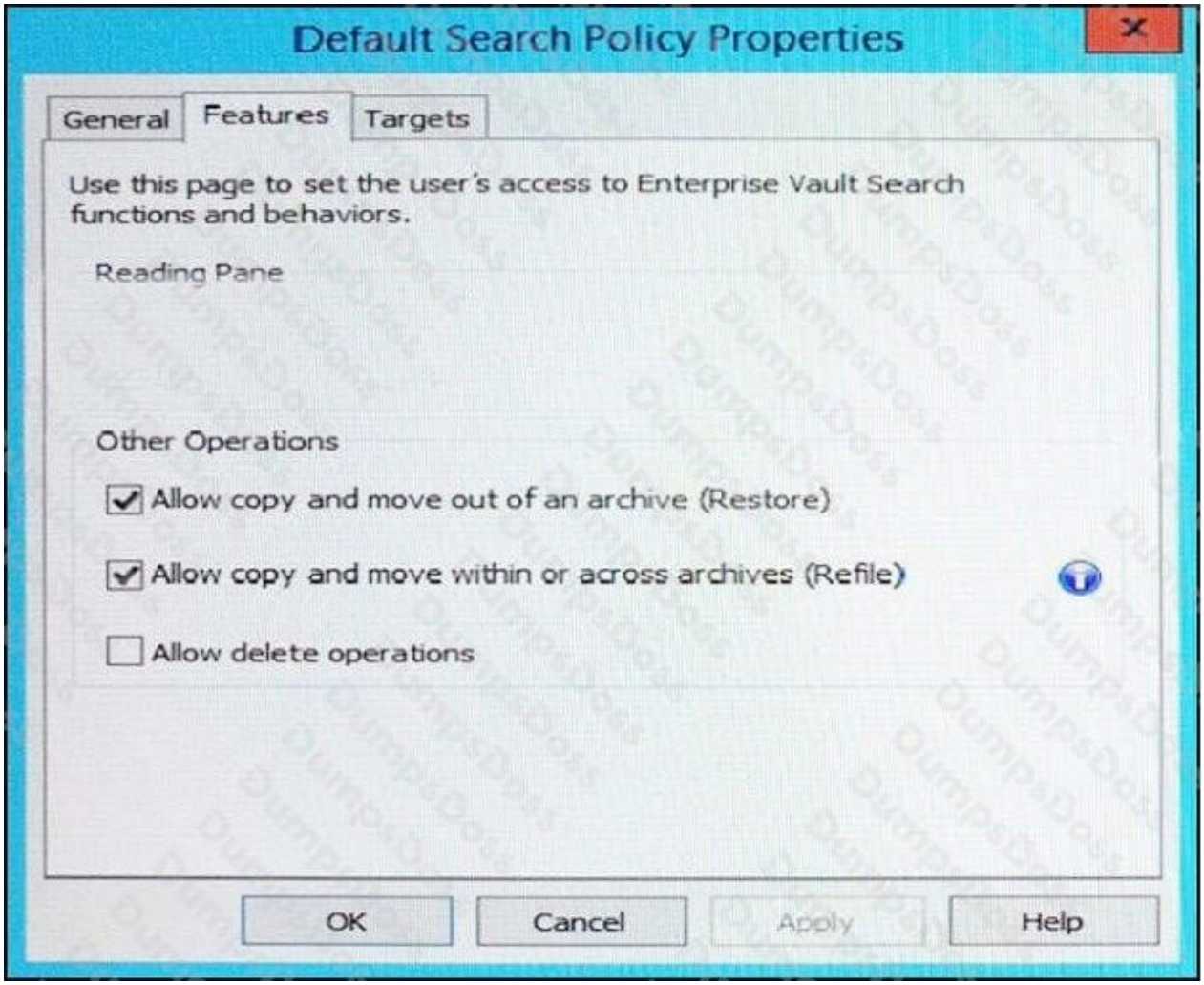
Explanation:

Enable Auditing in the EV Server properties in the VAC and select the auditing options. Activating auditing at the Directory level establishes the audit infrastructure, including the SQL Server audit database and the connection information Enterprise Vault needs to use it. It does not, by itself, cause Enterprise Vault servers to generate audit records. Auditing must also be enabled on each applicable Enterprise Vault server, with the required audit categories selected in that server's properties. Once those settings are applied, the Enterprise Vault server can write the selected administrative and operational audit events to the configured audit database. This separation lets an organization create one centrally managed audit database

while controlling, per Enterprise Vault server, both whether auditing is active and which actions are recorded. The administrator should therefore open the relevant Enterprise Vault server's properties in the Vault Administration Console, enable auditing, select the required event types, apply the configuration, and then perform an auditable action to verify that records are being added. Veritas Enterprise Vault documentation is available through the Enterprise Vault documentation portal; product documentation and administration resources can also be located through Veritas Support.

QUESTION NO: 8

A user's Search Policy is configured as shown:



Which two actions will the Search Policy allow the user to perform if the user has Full Control permissions to all relevant archives in Enterprise Vault Search? (Select two.)

A. move an item from one File System Archive to another File System Archive

B. move an item from an SMTP Archive to an Exchange Journal Archive

C. copy an item from an Exchange Journal Archive to an Exchange Mailbox Archive

D. copy an item from a File System Archive to the original file server

E. move an item from one Exchange Mailbox Archive to another Exchange Mailbox Archive

ANSWER: A E

Explanation:

Enterprise Vault Search policies control the archive-search operations that users can perform, independently of the archive permissions that determine whether the user can access the source and target archives. With Full Control on every archive

involved, the configured policy permits moving an item between File System Archives and moving an item between Exchange Mailbox Archives. These are archive-to-archive move operations within the archive types enabled by the policy, so the user has both the required Search Policy entitlement and the permissions needed to remove the item from its source and place it in its destination.

The ability to move is significant because Enterprise Vault applies the operation to the archived item and its archive location; Full Control alone does not grant a Search action that the policy has not enabled. Likewise, the policy's enabled archive-type combinations determine the permitted source and destination scope. Therefore, the permitted actions are *move an item from one File System Archive to another File System Archive* and *move an item from one Exchange Mailbox Archive to another Exchange Mailbox Archive*. Veritas Enterprise Vault documentation and product resources are available through the Enterprise Vault support page and the Veritas documentation portal.

QUESTION NO: 9

Users are being prompted for a username and password when trying to access archived items. Which setting can the administrator change to prevent the prompt?

A. Desktop Policy > Web Applications tab > Add all Enterprise Vault servers to intranet zone and Bypass local proxy server

B. Desktop Policy > Advanced tab > Outlook > modify the Add server to Intranet Zone option to include all Exchange CAS servers

C. Mailbox Policy > Advanced tab > Archiving General > change the Inherited Permissions setting to On

D. Mailbox Policy > Advanced tab > Archiving General > change the Include default and anonymous permissions setting to On

ANSWER: A

Explanation:

Desktop Policy > Web Applications tab > Add all Enterprise Vault servers to intranet zone and Bypass local proxy server is correct because it configures client browsers to treat the Enterprise Vault web servers as trusted intranet resources and to connect to them directly rather than through a proxy. This permits the browser to use Integrated Windows Authentication automatically when it opens archived content through Enterprise Vault web applications. As a result, the user's current Windows credentials can be supplied transparently to Enterprise Vault, avoiding an additional username-and-password prompt.

The setting must include every Enterprise Vault server that users can be directed to, including servers used for archive access and, where applicable, load-balanced server names. Policy changes are distributed to clients through the Enterprise Vault Desktop/Outlook client policy update process, so administrators should allow time for policy refresh or ensure clients receive the updated policy. The intranet-zone and proxy-bypass configuration is specifically intended to support seamless authenticated access to Enterprise Vault web components from managed client computers. See the Veritas product documentation portal and the Veritas Support site for Enterprise Vault documentation and configuration guidance.

QUESTION NO: 10

An administrator has Site Properties set to allow user deletion.

Which steps must the administrator perform to make the Delete operation available to users in Enterprise Vault Search?

A. configure a Search Policy > define a Search Provisioning Group > run the Client Access Provisioning Task

B. configure a Desktop Policy > define an Exchange Provisioning Group > run the Exchange Provisioning Task

C. configure a Search Policy > define an Exchange Provisioning Group > run the Exchange Provisioning Task

D. configure a Desktop Policy > define a Search Provisioning Group > run the Client Access Provisioning Task

ANSWER: A D

Explanation:

To expose the Delete command in Enterprise Vault Search, the user must be provisioned for Client Access and be assigned a policy that permits deletion. The required workflow is to configure the applicable policy, place the intended users in a Search Provisioning Group, and run the Client Access Provisioning Task so that Enterprise Vault creates or updates the users' Client Access settings. A Search Policy is the policy type specifically used to control Enterprise Vault Search functionality, including whether users can perform deletion operations. A Desktop Policy can also supply the applicable client-access deletion setting for users provisioned through a Search Provisioning Group. In both cases, the Site Properties setting is the site-wide prerequisite, while the provisioning group and Client Access Provisioning Task apply the permitted functionality to the individual users. The task should be run after policy or group membership changes, and it can also run on its configured schedule. Veritas documentation describes Search provisioning and Client Access Provisioning Task configuration in the Enterprise Vault administration documentation: Enterprise Vault Administration Guide. Product documentation and version-specific guides are available from the Veritas Enterprise Vault documentation portal.

QUESTION NO: 11

Which two reports require monitoring to be enabled? (Select two.)

A. Single Instance Storage Reduction Summary

B. Enterprise Vault Server Seven Day Health Status

C. Exchange Server Journal Mailbox Archiving Health

D. Archive Item Access

E. Archive item Access Trends

ANSWER: B C

Explanation:

The reports that require Enterprise Vault monitoring to be enabled are **Enterprise Vault Server Seven Day Health Status** and **Exchange Server Journal Mailbox Archiving Health**. Enterprise Vault Monitoring collects operational and health data from Enterprise Vault servers and their associated services, then stores the monitored results for reporting. The seven-day health report depends on this collected monitoring data to present a recent view of server health, including service and operational status over the reporting period. Similarly, the journal mailbox archiving health report uses monitoring data to assess the health and processing status of Exchange journal mailbox archiving, helping administrators identify whether journal archiving is operating normally and whether issues require attention.

Monitoring must therefore be configured and active before these health-oriented reports can contain the required data. In practice, administrators should allow monitoring to run long enough to gather data across the selected reporting range, particularly for a seven-day status report. Veritas Enterprise Vault documentation describes Monitoring as the mechanism for collecting Enterprise Vault operational information used to assess system health and availability. See the Veritas Enterprise Vault documentation portal and the Enterprise Vault product support page.

QUESTION NO: 12

An administrator has configured a volume on a Windows file server for File System Archiving (FSA).

Which Enterprise Vault task archives eligible files from the configured volume?

A. FSA Archiving Task

B. Storage Expiry Task

C. File Blocking Task

D. Index Administration Task

ANSWER: A

Explanation:

The **FSA Archiving Task** processes files on configured file server volumes according to the selected FSA policy. The task evaluates eligible files, archives them to Enterprise Vault, and can create placeholders when the applicable policy settings permit it.

The FSA Agent provides the file-server integration required for FSA features, but it does not perform scheduled archival processing independently. The FSA Archiving Task is the Enterprise Vault task responsible for this processing. See the Veritas Enterprise Vault documentation portal for File System Archiving administration guidance.

QUESTION NO: 13

Which tool can an administrator use to view Veritas Enterprise Vault 12.x (EV) Audited data?

A. EV Application Event Log

B. auditviewer.exe

C. EV Operations Management webapp

D. the auditing tab in the properties of the EV server

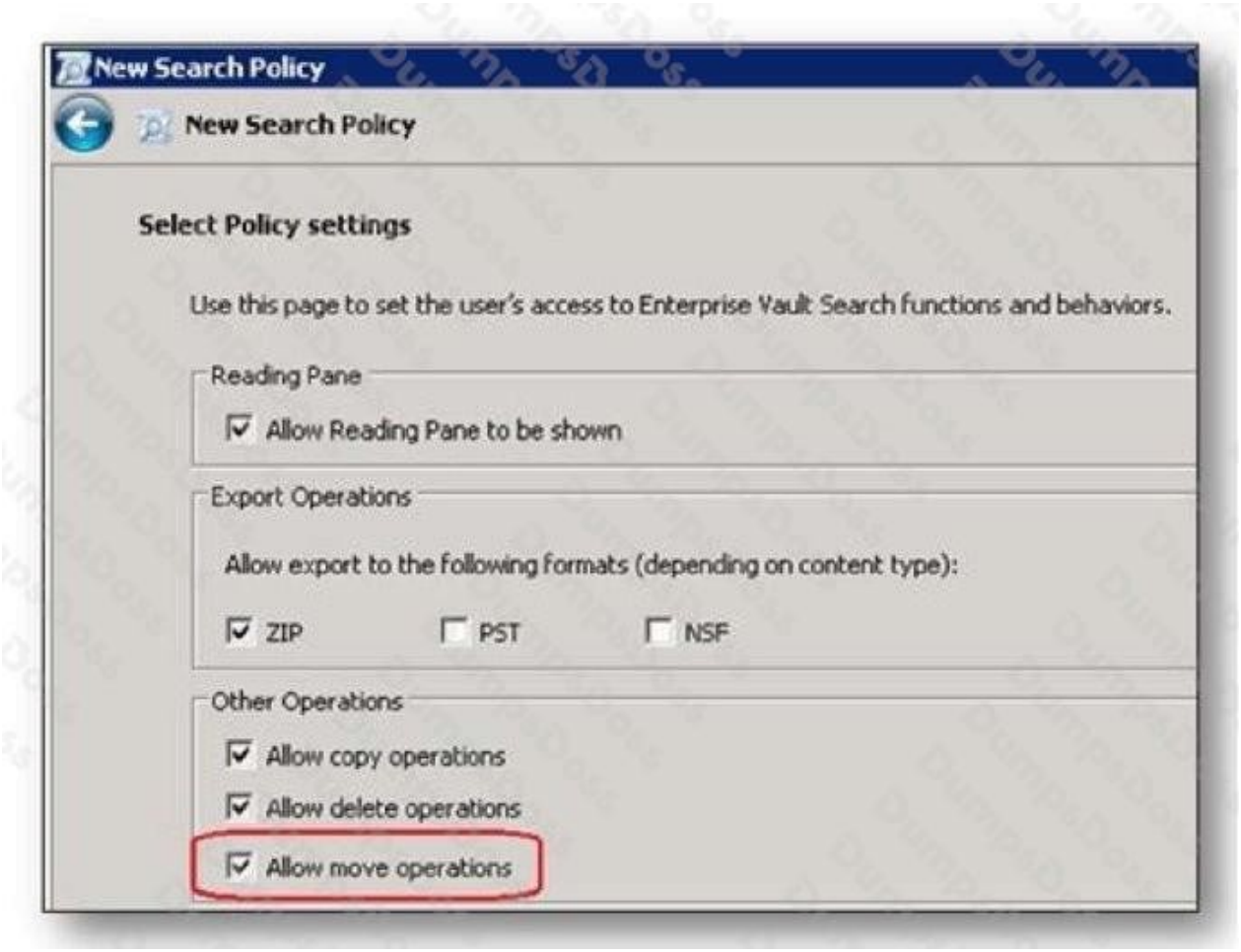
ANSWER: B

Explanation:

auditviewer.exe is the Enterprise Vault Auditing Viewer executable used to examine the audit records that Enterprise Vault creates when auditing is enabled. Auditing records significant administrative and operational activity, providing an accountability trail that administrators can review when investigating configuration changes, access activity, or other audited events. The viewer presents the stored audit information in a form intended for audit review and supports locating relevant records through its available filtering and viewing functions. It is therefore the appropriate Enterprise Vault tool for directly viewing audited data, rather than merely reviewing general server status or standard event messages. Enterprise Vault auditing must first be configured and enabled for the relevant actions, and the administrator needs suitable permissions to access the audit data. Veritas documentation for Enterprise Vault provides product documentation and administration resources, including the auditing feature and its management requirements. See the Veritas Enterprise Vault 12.5 documentation portal and the Enterprise Vault support page for official documentation and support resources.

QUESTION NO: 14

Refer to the exhibit.



Which capability does the "Allow move operations" setting provide?

A. users can move items within the archive

B. users can restore items to the original location and simultaneously delete the archived versions

C. users can restore items as a ZIP file and simultaneously delete the archived versions

D. users can move items into a ZIP file

ANSWER: B

Explanation:

The setting allows users to move an archived item back to its original mailbox location while removing the corresponding item from Enterprise Vault. In this context, a move is not merely a retrieval or a copy operation: Enterprise Vault restores the selected archived item to the location from which it was originally archived and then deletes the archived version, subject to the user's permissions and the archive's retention configuration. This capability is useful when an item needs to be returned permanently to the mailbox rather than remain retained as an archived copy after restoration. The setting therefore controls whether users can perform this restore-and-delete workflow through the Enterprise Vault client interfaces. Administrators should apply it with care because moving an item changes the content retained in the archive; policies such as retention categories and legal holds can still limit whether deletion of the archived copy is permitted. Veritas Enterprise Vault documentation and product resources are available through the Enterprise Vault documentation portal and the Enterprise Vault product support page.

QUESTION NO: 15

An administrator is running a pilot installation of Veritas Enterprise Vault 12.x and wants to copy everything that has been archived back to the original mailboxes before enabling archiving for everyone.

What is the best tool for this task according to Veritas documentation?

A. Move Archive Utility

B. EVSVR

C. Export Archive Wizard

D. Policy Manager (EVPM)

ANSWER: A

Explanation:

Move Archive Utility is the appropriate Enterprise Vault tool when an administrator needs to return the complete contents of an archive to its associated, original mailbox. It is designed for archive-move scenarios and can move all archived items back into the target Exchange mailbox, making it suitable for ending or reversing a pilot deployment before broadening the archiving rollout. The utility processes the archive content directly and preserves the practical objective of repopulating users' mailboxes with the data that Enterprise Vault had archived.

For a pilot, this approach lets the administrator return users to a mailbox-based working state before changing the scope of the Enterprise Vault deployment. The administrator should plan capacity carefully: restored data consumes Exchange mailbox and database storage, and the move should be scheduled and monitored so that mailbox quotas, throughput, and operational impact are controlled. Veritas documents its Enterprise Vault administration utilities and archive-management procedures in the Enterprise Vault product documentation portal: Veritas Enterprise Vault documentation. Product support resources, including technical guidance and documentation access, are also available through Veritas Enterprise Vault Support.

QUESTION NO: 16

The CIO of a company has asked for a report of the archiving performance for all users. In which two file formats does Veritas Enterprise Vault 12.x produce reports? (Select two.)

A. HTML

B. CSV

C. TXT

D. XLS

E. XML

ANSWER: A B

Explanation:

Enterprise Vault Reporting supports report output in **HTML** and **CSV** formats. HTML provides a formatted, browser-viewable presentation of the report, suitable for reviewing the archiving-performance results directly and sharing a readable report with stakeholders. CSV provides the report data in a delimited format that can be opened in spreadsheet and analysis tools, enabling the CIO or an administrator to sort, filter, aggregate, and further analyze archiving statistics for all users.

For an all-users archiving-performance request, these two formats serve complementary purposes: HTML is appropriate for the polished operational report, while CSV is appropriate when the underlying result data needs additional analysis or incorporation into a broader management report. Enterprise Vault reporting documentation describes the available report formats and the use of reports to monitor Enterprise Vault operations and activity. See the Veritas Enterprise Vault documentation portal at Enterprise Vault documentation and the Veritas support knowledge base at Veritas Support.

QUESTION NO: 17

A Veritas Enterprise Vault 12.x environment contains two Enterprise Vault servers named EV1 and EV2. VaultStore1 is associated with EV1 and VaultStore2 is associated with EV2. An Enterprise Vault Indexing Service is installed on EV1, but Enterprise Vault Indexing Service is NOT installed on EV2. The administrator notices that items in VaultStore1 are being indexed, but items in VaultStore2 are NOT.

Which two complete solutions ensure both VaultStore1 and VaultStore2 are indexed? (Select two.)

A. install the Enterprise Vault Indexing Service on EV2

B. create an Index Administration Task on EV2

C. Change the Site's Indexing Level from Brief to Full

D. change the location of the index volumes from EV1 to EV2

E. create an Index Server Group that includes EV1 and assign VaultStore2

ANSWER: A E

Explanation:

Installing the Enterprise Vault Indexing Service on EV2 provides a local indexing server for VaultStore2. The Indexing Service performs the content extraction and index creation required for archived items to become searchable. With an indexing service available on the server that hosts VaultStore2, Enterprise Vault can process the vault store's indexing workload locally, while EV1 continues to process VaultStore1.

Creating an Index Server Group that includes EV1 and assigning VaultStore2 to that group is an alternative complete design. Index Server Groups allow a vault store to use an Indexing Service on a different Enterprise Vault server. In this configuration, EV1's existing Indexing Service can process indexing requests for VaultStore2 as well as VaultStore1. This supports centralized or shared indexing capacity without requiring an Indexing Service installation on every Enterprise Vault server. The selected group must contain an available indexing server, and VaultStore2 must be assigned to that group so Enterprise Vault knows where to send its indexing work.

Veritas describes Index Server Groups and the assignment of vault stores to indexing servers in the Enterprise Vault administration documentation: Enterprise Vault documentation. Additional product documentation and version-specific administration resources are available from the Veritas Enterprise Vault support portal.

QUESTION NO: 18

A user has mistakenly deleted several items from the mailbox archive. The default site setting "Enable recovery of user deleted items" is selected and set to 14 days. The Enterprise Vault administrator recover the items.

What is the result of this action?

A. specified deleted items newer than 14 days will be recovered to the mailbox

B. all deleted items newer than 14 days will be recovered to the mailbox

C. all deleted items newer than 14 days will be recovered to the archive

D. specified deleted items newer than 14 days will be recovered to the archive

ANSWER: C

Explanation:

When an Enterprise Vault administrator performs deleted-item recovery, Enterprise Vault recovers all eligible deleted archive items that remain within the configured recovery period. In this case, the site setting enables recovery for 14 days, so every item deleted during that recovery window is restored to its original archive location. The recovery operation is not limited to only the particular items that prompted the administrator's action, and it does not place the recovered content back into the user's Exchange mailbox. The recovered items reappear in the Enterprise Vault archive, where the user can access them through the normal archive client or search interfaces. The 14-day value is measured from the time each item was deleted; in the option wording, "newer than 14 days" should be understood as items deleted within the preceding 14 days. After the

configured recovery period has elapsed, deleted archive items are no longer eligible for this recovery process. This behavior lets administrators restore accidentally deleted archive content while maintaining the archive as the authoritative storage location. See the Enterprise Vault documentation library at Veritas Enterprise Vault documentation and the product support portal at Veritas Enterprise Vault Support.

QUESTION NO: 19

Which two configurations are valid options for Microsoft Clustering in an Enterprise Vault environment? (Select two.)

A. Active/Active

B. Active/Passive

C. N+1 (Hot Standby)

D. Failover with replica

E. Failover with fault tolerance

ANSWER: B C

Explanation:

Enterprise Vault supports Microsoft Cluster Service configurations that provide high availability for the Enterprise Vault server role and its associated services. **Active/Passive** is a supported arrangement in which the Enterprise Vault virtual server and clustered resources normally run on one node and move to a passive node when a planned or unplanned failover occurs. This approach maintains a single active Enterprise Vault instance while allowing service recovery through the cluster.

N+1 (Hot Standby) is also a valid Microsoft clustering design for Enterprise Vault. In this model, multiple active nodes can host separate Enterprise Vault virtual servers or workloads, and an additional standby node has sufficient capacity to take over the workload of a failed node. This design can improve hardware utilization while retaining failover capability, provided that resource ownership, shared storage, and Enterprise Vault service dependencies are configured correctly. Enterprise Vault clustering guidance emphasizes configuring clustered Enterprise Vault resources and using supported Microsoft failover-clustering architecture so that the virtual server identity and services transfer cleanly during failover. See the Veritas Enterprise Vault documentation and Microsoft Failover Clustering overview.

QUESTION NO: 20

Which two Exchange server roles require installation of Veritas Enterprise Vault 12.x for Exchange extensions to provide users access to their archived content via Outlook Web Access (OWA) in a mixed Microsoft Exchange 2003 and 2007 environment? (Select two.)

A. Hub Transport Server

B. Front-end Server

C. Back-end Server

D. Mailbox Server

E. Client Access Server

ANSWER: B E

Explanation:

In a mixed Exchange 2003 and Exchange 2007 organization, the Enterprise Vault OWA extensions must be deployed on the servers that process the respective OWA client requests. The **Front-end Server** is the Exchange 2003 role that presents OWA to users and proxies their web requests to the appropriate mailbox infrastructure. Installing the Enterprise Vault

extensions there enables archived-item access and Enterprise Vault OWA functionality for users connecting through Exchange 2003 OWA.

For Exchange 2007, OWA is provided through the **Client Access Server** role. This role hosts the OWA virtual directories and handles the web session in which Enterprise Vault must expose archived content, links, and retrieval functions. Therefore, the Enterprise Vault Exchange extensions are required on the Client Access Server for Exchange 2007 OWA access. In a mixed environment, both web-facing role types must be covered so that users of either OWA version can work with their archived items. Veritas Enterprise Vault documentation is available through the Enterprise Vault documentation portal; Veritas also maintains product-specific technical guidance in its Enterprise Vault support portal.