PassQueen
a.k.a dumpsqueen.com

Administration of Veritas Enterprise Vault 12.3

Veritas VCS-324

Version Demo

Total Demo Questions: 21

Total Premium Questions: 218

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Enterprise Vault Overview	17
Topic 2, Enterprise Vault Server Configuration	45
Topic 3, Enterprise Vault Configuration	56
Topic 4, Enterprise Vault Administration	9
Topic 5, Managing Archives	18
Topic 6, Managing Storage	33
Topic 7, Monitoring and Troubleshooting	40
Total	218

QUESTION NO: 1

Which function is controlled by the Enterprise Vault Admin Service?

A. managing access to databases for other Enterprise Vault components

B. defining the Enterprise Vault configuration

C. warning if virtual memory is running low

D. managing the mail and five servers from which data is archived

ANSWER: A

Explanation:

The Enterprise Vault Admin Service controls **managing access to databases for other Enterprise Vault components**. It is a core Enterprise Vault service that acts as the controlled interface to Enterprise Vault's configuration data, particularly the Directory database. Other Enterprise Vault services and administrative tools use the Admin Service when they need configuration information or need to perform configuration-related database operations. This centralizes database access rather than allowing each component to connect and manage configuration data independently.

This role is important to the platform's service architecture: Enterprise Vault components depend on configuration information such as site, server, archive, task, and policy settings, and the Admin Service makes that information available in a managed manner. The service therefore must be running for normal administration and for components that require access to the Enterprise Vault Directory database configuration. Veritas documents the Enterprise Vault services and their responsibilities in its Enterprise Vault administration documentation; see the Enterprise Vault documentation set and the Veritas Enterprise Vault support knowledge base.

QUESTION NO: 2

Which two options must be enabled on the client side browser to enable the use of

Enterprise Vault Search? (Select two.)

A. JavaScript

B. ActiveX

C. TLS 1.2

D. Cookies

E. Check for server certificate revocation

ANSWER: A D

Explanation:

Enterprise Vault Search requires **JavaScript** and **Cookies** to be enabled in the client browser. JavaScript supplies the browser-side behavior used by the Search interface, including interactive controls, query submission, navigation, and the dynamic presentation of search results. Without browser scripting, the web-based Search application cannot provide its required functionality.

Cookies are also required because Enterprise Vault Search uses them to maintain the user's authenticated web session and associated request state while the user moves between search pages, opens result items, refines a query, or performs related actions. The browser must therefore permit cookies for the Enterprise Vault Search site; organizational browser policy should allow the Enterprise Vault site as a trusted or permitted site where necessary.

These requirements apply to the browser client accessing the Enterprise Vault Search web application and should be checked alongside the supported-browser and deployment prerequisites for the installed Enterprise Vault release. Veritas documentation for Enterprise Vault is available through the Enterprise Vault 12.3 documentation portal; current product documentation can also be accessed from Veritas Documentation.

QUESTION NO: 3

Which two statements apply to Enterprise Vault index volumes? (Select two.)

A. they contain searchable information for archived items

B. they can be placed in Backup mode while they are backed up

C. they contain the original archived item data for a Vault Store partition

D. they are stored only in the EnterpriseVaultDirectory database

E. they can be deleted without affecting archive search results

ANSWER: A B

Explanation:

An Enterprise Vault index volume contains searchable information for archived items, so it is used to support searches of archive content. Index volumes are separate from Vault Store partitions, which contain the archived item data itself. This distinction is important for capacity planning, backup, and recovery.

Index volumes can also be placed in Backup mode while they are being backed up. Backup mode protects the index volume during the backup process and helps ensure that the backup captures a consistent index state. After the backup completes successfully, the administrator can return the index volume to normal processing.

See the Veritas Enterprise Vault documentation portal for index administration and backup guidance.

QUESTION NO: 4

Which two environments should be configured with multiple Enterprise Vault directories?

(Select two.)

A. separate active directory domain 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 Enterprise Vault servers in different data centers

ANSWER: B E

Explanation:

Multiple Enterprise Vault directories are appropriate where the deployment must be separated at an organizational security or administration boundary. The configuration data held by an Enterprise Vault Directory defines and manages the Enterprise Vault sites, servers, services, and related configuration in that directory. Using distinct directories for groups that require independent administration or security separation prevents a single shared directory from becoming a common administrative boundary. This design also permits each separated group to manage its Enterprise Vault environment according to its own operational controls.

Multiple directories are also appropriate when the archiving targets and Enterprise Vault servers are in data centers connected by very slow links. Enterprise Vault components depend on directory information for normal operation and configuration access. Keeping the relevant directory infrastructure local to each environment reduces reliance on a constrained WAN connection, avoids making directory communication a performance or availability dependency across the data centers, and supports a more resilient distributed deployment. Veritas documentation describes the Directory as the central configuration component and provides planning guidance for Enterprise Vault deployment architecture. See the Enterprise Vault 12.3 documentation and the Veritas Support documentation portal.

QUESTION NO: 5

Which administrative role allows viewing of Veritas Enterprise Vault 12.3 reports?

A. Search Administrator

B. Storage Administrator

C. Power Administrator

D. Report Administrator

ANSWER: C

Explanation:

Power Administrator is correct because this Enterprise Vault administrative role has unrestricted administrative access across the Enterprise Vault environment, including access to reporting functions and the ability to view Enterprise Vault reports. The Power Administrator role is intended for senior or central Enterprise Vault administrators who require broad control of directory, storage, provisioning, retention, monitoring, and reporting-related administration. Consequently, a user assigned this role can open and review reports without needing their permissions limited to a particular administrative area.

Enterprise Vault uses role-based administration to grant permissions appropriate to operational responsibilities. A Power Administrator's permissions span the product rather than being scoped only to a particular service or subsystem. This broad access makes the role suitable when viewing reports is one of several required administrative tasks. Veritas documentation for Enterprise Vault administration and reporting is available through the Enterprise Vault documentation portal and the Enterprise Vault product support page.

QUESTION NO: 6

Which pre-requisite is necessary for installing Enterprise Vault Reporting?

A. the Active Directory account used for reporting requires an Exchange Mailbox

B. log in as the ReportingUser account, and run the Enterprise Vault Management Shell utility once

C. add the Active Directory reporting account to the Exchange Administrators group

D. Microsoft SQL Server Reporting Services

ANSWER: D

Explanation:

Microsoft SQL Server Reporting Services is necessary because Enterprise Vault Reporting uses SQL Server Reporting Services (SSRS) as its reporting platform. The Enterprise Vault Reporting installation deploys and configures report content for SSRS, while SSRS provides the reporting web service and report-management infrastructure used to process, render, and present the Enterprise Vault reports. Therefore, an appropriate, configured SSRS installation must be available before Enterprise Vault Reporting can be installed and configured. The SQL Server Reporting Services instance also needs to be reachable by the Enterprise Vault environment and configured in a supported mode and version for the Enterprise Vault release. This prerequisite is distinct from ordinary SQL Server database functionality: the reporting feature specifically depends on the SSRS reporting service, not merely on a SQL Server Database Engine instance. Refer to the Enterprise Vault documentation for the version-specific reporting installation requirements at Veritas Enterprise Vault documentation and to Microsoft's SSRS installation guidance at Install SQL Server Reporting Services.

QUESTION NO: 7

An administrator has configured Exchange journal archiving and Exchange mailbox archiving in the same Vault Store Group. The administrator wants to take advantage of optimized single instance storage in Veritas Enterprise Vault 12.3 for Exchange. Where must the administrator configure the sharing level to achieve this?

A. on the Vault Store properties

B. on the Vault Store partition properties

C. on the Vault Store group properties

D. on the Enterprise Vault server properties

ANSWER: C

Explanation:

Configure the sharing level on the Vault Store group properties. In Enterprise Vault, a Vault Store Group is the administrative boundary that controls whether single-instance storage sharing is permitted across the vault stores that belong to that group. Setting the appropriate sharing level there enables Enterprise Vault to recognize matching Exchange items that are archived by different processes, such as journal archiving and mailbox archiving, and to retain shared content efficiently rather than storing duplicate copies where the configured sharing scope allows it.

This setting is especially relevant when journal and mailbox data are directed to vault stores in the same Vault Store Group. The group-level sharing configuration determines the intended deduplication scope for those stores, while the individual vault store and partition configurations provide storage-related settings rather than defining the cross-store sharing scope. The Enterprise Vault documentation describes Vault Store Groups as the location for managing sharing behavior and related vault-store grouping configuration. For product documentation and administration guidance, see the Veritas Enterprise Vault documentation portal and the Enterprise Vault documentation resources.

QUESTION NO: 8

Which component can be placed on a non-clustered resource?

A. MSMQ data

B. Vault Store Partitions

C. Enterprise Vault application binaries

D. Index locations

ANSWER: C

Explanation:

Enterprise Vault application binaries can be placed on a non-clustered resource because they are installed locally on every node that can host the Enterprise Vault virtual server. Each cluster node requires its own local installation of the Enterprise Vault software so that, after a cluster failover, the node assuming ownership already has the executables, services, and supporting program files needed to run the virtual server. These binaries are not data that must move with the clustered service; they are consistent software installations maintained on each participating node. This design lets the clustered Enterprise Vault resources fail over independently of the local program installation while preserving service availability. During installation and maintenance, administrators should ensure that the same Enterprise Vault version, updates, and configuration-compatible binaries are installed on all nodes. Veritas documents the supported Enterprise Vault deployment and clustering requirements in its Enterprise Vault documentation portal: Veritas Enterprise Vault documentation. Following these requirements ensures that every possible owner node is prepared to host the Enterprise Vault service when cluster ownership changes.

QUESTION NO: 9

An administrator is preparing to move the Veritas Enterprise Vault 12.3 for Exchange (EV) server to new hardware. The EV indexes and vault stores have been backed up. Which two customized components of EV should be backed up and available for the move? (Select two.)

A. the License File

B. Vault Cache Location

C. Configuration.exe.config

D. Mailbox .msg files in \Program Files (x86)\Enterprise Vault

E. Server Cache Location

ANSWER: A D

Explanation:

the License File and **Mailbox .msg files in \Program Files (x86)\Enterprise Vault** should be retained when moving an Enterprise Vault server to replacement hardware. The license file is required to restore the server's licensed Enterprise Vault functionality after the new server has been installed and configured. Keeping the existing license available also avoids an unnecessary delay in bringing Enterprise Vault services back online while entitlement details are recovered or a replacement license file is obtained.

The mailbox `.msg` files in the Enterprise Vault installation folder can contain customized message templates used by Enterprise Vault. These templates preserve organization-specific text and presentation for Enterprise Vault-generated mailbox messages. A standard installation on the replacement server can install default versions, so retaining the customized files is necessary to ensure that the established messaging experience is carried forward with the server move. These items should be copied safely before the old server is decommissioned and restored only as appropriate after the Enterprise Vault software installation on the replacement host.

Veritas Enterprise Vault product and documentation resources are available from Veritas Enterprise Vault and the Enterprise Vault documentation portal.

QUESTION NO: 10

What is the Veritas recommended minimum amount of memory required for Veritas

Enterprise Vault 12.3 ?

A. 8 GB

B. 16 GB

C. 32 GB

D. 4 GB

ANSWER: B

Explanation:

16 GB is the Veritas-recommended minimum memory allocation for an Enterprise Vault 12.3 server. This baseline provides sufficient RAM for the Enterprise Vault services, indexing-related activity, storage processing, and the operating system to run reliably under the supported configuration. Memory is particularly important because Enterprise Vault can perform several resource-intensive operations concurrently, such as archiving, retrieval, indexing, and background maintenance tasks. Allocating the documented minimum helps avoid unnecessary paging and performance contention that can affect vault operations and end-user access. This value is a minimum platform requirement rather than a sizing recommendation for every deployment. Environments with high item volumes, multiple provisioning tasks, extensive indexing, large numbers of users, or several Enterprise Vault roles hosted together may require additional memory following capacity planning and performance monitoring. Consult the Enterprise Vault 12.3 documentation set for the release-specific installation and hardware requirements, and use Veritas documentation and support resources when designing the server configuration. See the Veritas Enterprise Vault 12.3 documentation and the Veritas Support portal.

QUESTION NO: 11

What does an Administrator need to do first to enable Journal Archiving?

A. manually create the Journal archive

B. run the Exchange Journaling Task

C. run the Enable Journal Mailbox wizard

D. set up a separate Vault Store for journaling

ANSWER: A

Explanation:

Before a journal mailbox can be enabled for Enterprise Vault processing, an appropriate Journal archive must exist to receive and retain the journaled messages. Therefore, the first required action is to manually create the Journal archive. Creating it establishes the archive destination and lets the administrator apply the required archive configuration, including its vault store location, retention category, and other archive properties appropriate for compliance data. The archive can then be selected or associated when the journal mailbox is enabled and the Journal task is configured to collect messages from that mailbox. This sequence ensures that Enterprise Vault has a defined, policy-controlled target for every item that Exchange journals, rather than beginning journal processing without an established archive destination. Journal archiving is normally deployed for regulatory and legal retention, so defining the archive up front is an important administrative control. Veritas Enterprise Vault documentation and product resources are available from the Enterprise Vault 12.3 documentation portal. For the Exchange-side journaling concepts that provide the source messages Enterprise Vault captures, see Microsoft's journaling procedures documentation.

QUESTION NO: 12

Which two statements correctly describe the Enterprise Vault PST Locator Task and PST Collector Task? (Select two.)

A. the PST Locator Task identifies PST files on target computers

B. the PST Collector Task copies located PST files to a central holding location

C. the PST Locator Task archives PST contents directly to a Vault Store

D. the PST Collector Task creates new Exchange mailboxes for PST owners

E. the PST Locator Task rebuilds index volumes for migrated PST items

ANSWER: A B

Explanation:

The **PST Locator Task identifies PST files on target computers**, while the **PST Collector Task copies located PST files to a central holding location**. These tasks support centrally managed PST migration by first discovering PST files and then collecting the identified files for subsequent processing and import into Enterprise Vault archives.

The PST Locator Task does not itself archive the content of the PST files, and the PST Collector Task does not create Exchange mailboxes. After PST files have been located and collected, the administrator can use the appropriate Enterprise Vault PST migration method to import their contents. See the Veritas Enterprise Vault documentation for PST migration and collection-task guidance.

QUESTION NO: 13

Enterprise Vault servers EVSERVER1 and EVSERVER2 need to be installed as primary and failover node in a cluster configuration.

Where must the Veritas Enterprise Vault 12.3 application binaries be installed?

A. the installation path must be the same for either node

B. the installation path must be different for either node

C. the installation path must be on the cluster quorum

D. the installation path must be on the system drive

ANSWER: A

Explanation:

the installation path must be the same for either node is correct. In an Enterprise Vault cluster, the Enterprise Vault program files and application binaries are installed locally on every physical cluster node, rather than on shared cluster storage. Veritas requires the local installation location to be identical across the nodes that can host the clustered Enterprise Vault service. Using a consistent path ensures that, after a failover, the active node can locate the same executable files, supporting components, registry configuration, and service definitions in the expected location. The Enterprise Vault data and configuration that must move with the clustered service are handled through the appropriate shared resources and clustered configuration; the application binaries themselves remain local to each node. Before configuring the clustered server, install the same Enterprise Vault version, patches, and hotfixes on each node, using the same local installation path. This produces equivalent application environments and supports reliable ownership changes between EVSERVER1 and EVSERVER2. Veritas documentation for Enterprise Vault 12.3 is available through the Enterprise Vault documentation portal; the clustered-server installation guidance is also indexed in the Enterprise Vault support and documentation page.

QUESTION NO: 14

Which two ways can an administrator access the Exchange mailbox archiving report for the purpose of verifying the last time a user mailbox was archived? (Select two.)

A. use the Get-ExchMBXArchRep PowerShell cmdlet

B. Administration Console > open the Exchange Server Properties: Reporting tab

C. Administration Console > open the Exchange Mailbox Task Properties: Reporting tab

D. SQL Reporting Services > Open the "Hourly rate" report

E. Exchange mailbox archiving reports site summary page at the following URL:http://evserver/EnterpriseVault/ExchangeArchivingReports.aspx

ANSWER: C E

Explanation:

The Exchange Mailbox Task Properties: Reporting tab provides an Administration Console route to the Exchange mailbox archiving report for the selected mailbox task. This report contains mailbox-level archiving activity information, including the most recent time that Enterprise Vault archived a mailbox. It is therefore useful when an administrator is validating that scheduled archiving is processing user mailboxes as expected.

The Exchange mailbox archiving reports site summary page at `http://evserver/EnterpriseVault/ExchangeArchivingReports.aspx` is the corresponding web-based reporting entry point. From this Enterprise Vault reporting site, an administrator can open Exchange mailbox archiving report data and identify the reported last-archived time for a particular user mailbox. Access requires that the Enterprise Vault reporting components and the relevant reporting configuration are available on the Enterprise Vault server. These two methods are complementary: one starts from the configured Exchange mailbox task in the Administration Console, while the other starts directly at the Exchange Archiving Reports web page. Veritas documents reporting and Exchange mailbox archiving administration in the Enterprise Vault Administration Guide; see Veritas Enterprise Vault documentation and Enterprise Vault 12.3 documentation index.

QUESTION NO: 15

A Veritas Enterprise Vault 12.3 administrator wants to view how many items are archived on a monthly basis.

Which report should the administrator schedule and run?

A. Items Archival Rate

B. Storage Summary

C. Archived Item Access Trends

D. Content Provider Ingest History

ANSWER: A

Explanation:

The **Items Archival Rate** report is the appropriate report because it presents the volume of items that Enterprise Vault archives over time. Its purpose is to let an administrator measure archival activity and identify the number of items archived during each reporting interval, including monthly intervals when the report is scheduled or filtered for that period. This makes it useful for trend analysis, capacity planning, and confirming that archiving activity is occurring at the expected rate across the Enterprise Vault environment.

Enterprise Vault Reporting provides reports specifically intended to monitor operational archive activity. By scheduling the Items Archival Rate report to run monthly, the administrator receives recurring historical data that can be compared month to month. The resulting figures provide the requested count of archived items rather than merely showing storage consumption or user access activity. Report scheduling also allows the output to be generated and delivered automatically, avoiding the need to manually run the report at the end of every month.

See the Enterprise Vault documentation library at Veritas Enterprise Vault documentation and the product support portal at Veritas Enterprise Vault support for reporting and report-scheduling guidance.

QUESTION NO: 16

Which action must an administrator take to view the clustered message queues for an Enterprise Vault clustered server?

A. the " Component Services " snap-in located in the Microsoft MMC console

B. the ClusterCompMgmt command located in the Enterprise Vault installation folder (typicallyC:\Program Files (x86)\Enterprise Vault)

C. the " Computer Management " snap-in located in the Microsoft MMC console

D. the ClusterPerfMon command located in the Enterprise Vault installation folder (typicallyC:\Program Files (x86)\Enterprise Vault)

ANSWER: B

Explanation:

The required action is to run the `ClusterCompMgmt` command from the Enterprise Vault installation folder, normally `C:\Program Files (x86)\Enterprise Vault`. In a clustered Enterprise Vault deployment, Microsoft Message Queuing resources are associated with the clustered virtual server rather than simply with the physical node currently being administered. `ClusterCompMgmt.exe` opens Computer Management in the appropriate clustered context, allowing the administrator to view the message queues that belong to the Enterprise Vault virtual server. This is important when checking queue status, reviewing pending messages, or carrying out troubleshooting, because the relevant queues must be viewed through the clustered server context. The utility is supplied as part of Enterprise Vault specifically to make the clustered Computer Management view available; it should be run on an Enterprise Vault cluster node with suitable administrative permissions. Veritas documentation for Enterprise Vault administration and clustering is available through the Veritas Enterprise Vault documentation portal. Additional product documentation and technical guidance can be accessed from Veritas Enterprise Vault Support.

QUESTION NO: 17

An email system is configured to journal a copy of all messages for all users to a single SMTP email address, 'Journal@evsmtp.local". An SMTP target email address is set for journal@evsmtp.local and additional SMTP target email addresses are configured for three users.

Which two steps must the administrator perform to ensure only messages belonging to the three user SMTP target email addresses are archived? (Select two.)

A. Enterprise Vault Site Properties > Advanced > SMTP > Selective Journal Archiving

B. Enterprise Vault Server Properties > Advanced > SMTP > Selective Journal Archiving

C. enable archiving for SMTP target email address journal@evsmtp.local and all three user SMTP target email addresses

D. disable archiving for SMTP target email address journal@evsmtp.local and all three user SMTP target email addresses

E. disable archiving for SMTP target email address journal@evsmtp.local and enable it for all three user SMTP target email addresses

ANSWER: B E

Explanation:

Selective journal archiving is configured at the Enterprise Vault server level, through the SMTP settings in the server's Advanced properties. Enabling this setting instructs Enterprise Vault to make an archiving decision based on the SMTP target addresses identified in the journaled message, rather than simply archiving every item delivered to the common journal recipient. This is essential when the messaging system journals all users' mail to one address such as journal@evsmtp.local.

The common journal address must have archiving disabled, because it is only the transport destination receiving the complete journal stream. Each of the three individual user SMTP target email addresses must have archiving enabled. With selective journal archiving active, Enterprise Vault processes the journal stream but archives only those messages that match an enabled individual target address. This lets the organization journal broadly at the mail-system level while applying a narrower Enterprise Vault archive scope to the intended users.

For Enterprise Vault product documentation and SMTP archiving configuration guidance, see the Veritas Enterprise Vault 12.3 documentation and the Veritas support documentation search.

QUESTION NO: 18

An administrator needs to remove an Index Server from an Index Server Group and place it in another group.

When can this process be completed?

A. during the processing time of the Index Administration task

B. before archived items have been indexed

C. when the Indexing Service is stopped

D. after indexes have been put into Backup mode

ANSWER: B

Explanation:

The process can be completed **before archived items have been indexed**. In Enterprise Vault, an Index Server Group defines the Index Servers that are available to process and maintain index data for the archives assigned to that group. Before an Index Server has processed archived content, it has no established index-data association that would need to remain aligned with its original group. The administrator can therefore remove the unused server from its current Index Server Group and add it to the required destination group.

Once an Index Server has indexed archive items, its relationship to the index data and the group configuration is established. Enterprise Vault protects that configuration to preserve the integrity, availability, and management of existing indexes. Administrators should therefore plan Index Server Group membership before enabling indexing workloads or assigning archives that will generate indexed content. This is particularly important when designing capacity, high availability, and archive distribution, because moving a server after it begins processing data is not the supported method for redistributing indexed archives.

For Enterprise Vault product documentation and administration guidance, see the Veritas Enterprise Vault documentation portal.

QUESTION NO: 19

Which two key benefits are provided by Veritas Enterprise Vault 12.3 ? (Select two.)

A. it natively archives all structured data

B. it archives unstructured data

C. it allows administrators to import PST files into the archive

D. it eliminates the need for backups

E. it eliminates the need for centralized information management

ANSWER: B C

Explanation:

Veritas Enterprise Vault provides archiving for unstructured information, including commonly deployed content sources such as email and file-system data. Its archiving model moves or copies eligible content from production repositories into a managed archive while retaining appropriate access mechanisms, helping organizations control primary-storage growth and apply retention and information-governance policies. This is a core Enterprise Vault capability rather than a feature limited to a particular structured application or database platform.

Enterprise Vault also supports importing PST files into an Enterprise Vault archive. PST migration is valuable because it brings data that users may have retained locally or outside centrally managed mail storage under the organization's archive, retention, search, and compliance controls. Administrators can use Enterprise Vault's PST-related facilities to locate, process, and import PST content, reducing dependence on unmanaged personal archive files and making that historical mail available through the archive. These capabilities align with Enterprise Vault's purpose of centrally managing, retaining, and discovering business information. Veritas describes Enterprise Vault archiving and governance capabilities at Veritas Enterprise Vault and provides product documentation through the Veritas Documentation portal.

QUESTION NO: 20

A Veritas Enterprise Vault 12.3 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 on EV1 and assign VaultStore2 to it

ANSWER: A E

Explanation:

Installing the Enterprise Vault Indexing Service on EV2 provides VaultStore2 with a local indexing service. Enterprise Vault can then submit indexing work for the vault store hosted by EV2, while the existing Indexing Service on EV1 continues to process indexing work for VaultStore1. This is a complete solution because each Enterprise Vault server that hosts a vault store has access to a local Indexing Service.

Creating an Index Server Group on EV1 and assigning VaultStore2 to it is also a complete solution. Index Server Groups allow Enterprise Vault to separate the location of a vault store from the server that performs its indexing. By associating VaultStore2 with a group that contains EV1's existing Indexing Service, Enterprise Vault sends VaultStore2 indexing requests to EV1. This provides centralized or remote indexing without requiring an Indexing Service installation on EV2. The group assignment is the essential configuration that directs the vault store's indexing workload to an available indexing server.

These approaches reflect Enterprise Vault's supported indexing architecture, in which Indexing Services can process local vault-store data or serve vault stores assigned through Index Server Groups. See the Enterprise Vault 12.3 documentation and the Veritas Enterprise Vault indexing guidance.

QUESTION NO: 21

Which three components should be included in an Enterprise Vault backup strategy to support recovery of archived data and search functionality? (Select three.)

A. Enterprise Vault SQL databases

B. Vault Store partitions

C. Index locations

D. Users' Outlook profiles

E. Internet Information Services log files

ANSWER: A B C

Explanation:

Enterprise Vault SQL databases, **Vault Store partitions**, and **index locations** are key components of an Enterprise Vault backup strategy. The SQL databases contain Enterprise Vault configuration and vault-store metadata. Vault Store partitions contain the archived item data, and index locations contain the searchable index data for archived content.

Backing up these components enables the administrator to recover both the archived content and the information Enterprise Vault requires to locate and search that content. The backup process should follow the documented Enterprise Vault procedures, including the correct use of Backup Mode where applicable. See the Veritas Enterprise Vault documentation for backup and recovery requirements.