DUMPSBOSS.

Administration of Veritas eDiscovery Platform 8.2 for Administrators

Veritas VCS-413

Version Demo

Total Demo Questions: 11

Total Premium Questions: 111

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

How should an administrator identify withheld or problematic documents during a production job?

A. Use an Exceptions Report

B. Use a Reconciliation Report

C. Use a Slipsheet Report

D. Use a DocumentConverter.log

ANSWER: C

Explanation:

Use a Slipsheet Report. In Veritas eDiscovery Platform productions, a slipsheet is used to represent a document that is not produced in its native form or in the normal production output. This commonly occurs when content is withheld, such as for privilege or confidentiality, or when a document cannot be processed or converted successfully for the requested production format. The Slipsheet Report provides administrators with a production-focused record of these substituted or exceptional documents, allowing them to identify the affected items and review the reason associated with each slipsheet. This information supports quality control before delivery and helps production teams account for documents that require special treatment, follow-up, or disclosure tracking. Reviewing the report as part of the production workflow helps ensure that the delivered set and any withheld or problematic items are documented consistently. Veritas identifies eDiscovery Platform as a solution for collecting, processing, reviewing, and producing electronically stored information; production reporting is an important control within that process. See the Veritas eDiscovery Platform product information and the Veritas eDiscovery Platform support documentation portal for product documentation and administration resources.

QUESTION NO: 2

What is the default setting and purpose for the esa.icp. employee.skipEmployeeSync property?

A. The default is False, and it causes automatic synchronization with Active Directory.

B. The default is False, and it causes automatic synchronization with Exchange mailboxes.

C. The default is False, and it causes automatic synchronization with Domino servers.

D. The default is True, and it prevents automatic synchronization with Domino servers.

ANSWER: A

Explanation:

The default is False, and it causes automatic synchronization with Active Directory. The `esa.icp.employee.skipEmployeeSync` setting controls whether the eDiscovery Platform skips its scheduled employee synchronization process. With the default value of `False`, the process is not skipped, so the platform automatically synchronizes employee information from the configured Active Directory source. This synchronization keeps employee-related data used by the platform current, including directory identities and associated employee attributes needed for processing and administration. The property name is phrased as a skip control: setting it to `False` leaves the normal synchronization behavior enabled, whereas changing it is an administrative exception intended to suppress that automatic operation when necessary. Administrators should treat this as a configuration-level control and ensure that any change is aligned with the organization's directory-management and maintenance procedures. Veritas product documentation and support resources for eDiscovery Platform configuration can be accessed through the Veritas Support search for this property and the Veritas eDiscovery Platform documentation portal.

QUESTION NO: 3

Which LDAP property is no longer applicable in Veritas eDiscovery Platform 8.2?

A. esa.ldap.connectionPassword.enc

B. esa. Ldap.connectionURL

C. esa.ldap.connectionPassword

D. esa.ldap.connectionName

ANSWER: A

Explanation:

`esa.ldap.connectionPassword.enc` is the LDAP property that is no longer applicable in Veritas eDiscovery Platform 8.2. This property belonged to the earlier LDAP password-handling configuration model, in which an encrypted-password-specific property could be present in the platform configuration. In version 8.2, administrators should not rely on this legacy `.enc` property when reviewing, migrating, or troubleshooting LDAP settings. Configuration reviews after an upgrade should therefore identify and remove any dependency on `esa.ldap.connectionPassword.enc`, while ensuring that the active LDAP connection configuration and credentials are maintained through the supported version-appropriate settings and administrative procedures. This distinction is particularly important during upgrades: retaining obsolete custom properties can create confusion about which value the platform actually uses, complicate support investigations, and lead to unnecessary manual changes. Consult the product documentation delivered for the installed release and the Veritas documentation portal for the current LDAP configuration and upgrade guidance. Veritas maintains product documentation and release-specific materials through its Documentation portal; product resources are also available from the Veritas eDiscovery Platform support page.

QUESTION NO: 4

What is the purpose of the Veritas eDiscovery Platform 8.2 Automation Rules feature?

A. To automate data processing after collection

B. To automate manual review tasks

C. To automate data collection tasks

D. To automate data export for outside counsel

ANSWER: B

Explanation:

The purpose of the Automation Rules feature is **to automate manual review tasks**. In eDiscovery Platform review workflows, reviewers commonly perform repetitive actions as documents are reviewed, such as applying tags or updating coding decisions when specified conditions are met. Automation Rules enable an administrator or authorized user to define those conditions and the corresponding review action so that the platform can apply the action consistently without requiring a reviewer to repeat the same manual step for every matching item. This improves review efficiency, helps make coding more consistent across a case, and reduces the likelihood that routine actions are missed during high-volume document review. The feature is therefore part of the platform's review and analysis workflow rather than a mechanism primarily intended to run collection, processing, or external-counsel export operations. Veritas describes eDiscovery Platform as a solution for managing the eDiscovery lifecycle, including analysis and review activities; see the Veritas eDiscovery Platform product page. Product documentation and release-specific administration materials are available through the Veritas Documentation portal.

QUESTION NO: 5

Which two backup methods are available in Veritas eDiscovery Platform 8.2? (Choose two.)

A. Snapshot

B. Incremental

C. MySQL

D. Case

E. Scheduled

ANSWER: D E

Explanation:

Veritas eDiscovery Platform 8.2 provides both **Case** and **Scheduled** backup methods. A case backup is intended to protect the information associated with an individual case. This enables case-specific data to be backed up and subsequently restored when that particular case must be recovered, moved, or otherwise protected independently of other cases. It supports focused administration because the backup scope is the selected case rather than the entire appliance environment.

A scheduled backup provides recurring protection through a configured backup schedule. Administrators use this method to automate routine backup operations, helping ensure that platform data is protected consistently without requiring a separate manual action for every backup cycle. Scheduling is particularly important for operational continuity because it establishes a repeatable backup process and allows administrators to align backup frequency with the organization's recovery and retention requirements.

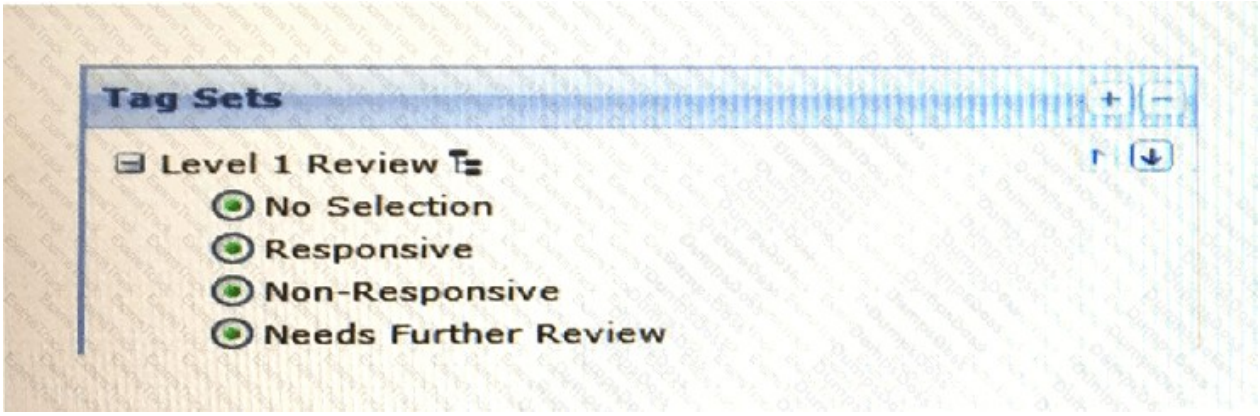
Together, these methods address both targeted, case-level recovery needs and ongoing administrative protection needs. Consult the Veritas eDiscovery Platform documentation portal for the applicable Administration Guide and release-specific backup procedures: Veritas product documentation. Additional product support resources are available from Veritas Support.

QUESTION NO: 6

Refer to the exhibit.

A reviewer accidentally tagged all items discovered in a search as "Responsive".

How can the tagging be reversed?



A. Re-run the search> on the batch web page, check No Selection> run the batch operation

B. Re-run the search> on the batch web page, select Remove Tag>check Responsive> run the batch operation

C. Re-run the search> in the Tag dialog box, check No Selection> run the bulk tagging operation

D. Re-run the search> in the Tag dialog box, select Remove Tag> check Responsive> run the bulk tagging operation

ANSWER: D

Explanation:

Re-run the search in the Tag dialog box, select Remove Tag, check Responsive, and run the bulk tagging operation. The Responsive designation is an applied tag, so reversing the accidental bulk action requires a bulk tag-removal operation that

explicitly targets that same tag. After re-running the search to return the affected items, the Tag dialog provides the bulk-tagging controls. Selecting *Remove Tag* changes the operation from applying a tag to removing an existing one; selecting *Responsive* identifies precisely which applied tag is to be removed. Running the bulk tagging operation then removes Responsive from all items in the current search result set, restoring them to their prior untagged state with respect to that tag. This is the appropriate remediation because it operates on the same item population identified by the search and makes a targeted metadata change rather than altering the search itself. Veritas eDiscovery Platform documentation describes using search results and bulk operations to manage review-item tags and related review metadata. See the Veritas eDiscovery Platform documentation and the Veritas eDiscovery Platform knowledge base for product guidance.

QUESTION NO: 7

Data has been prepared for a case, however it was broadly gathered without any restrictions.

Which two options are available in Veritas eDiscovery Platform 8.2 to restrict data processing via the pre-processing options? (Choose two.)

A. Filter by Date

B. Filter by File Type

C. Filter by Keyword

D. Filter by Location

E. Filter by Author

ANSWER: A B

Explanation:

Filter by Date and **Filter by File Type** are the available pre-processing restrictions for narrowing a broadly collected data set before it is processed for a case. A date filter limits the submitted content according to date criteria, helping administrators focus processing on the relevant time period and avoid expending processing capacity on material outside the case scope. A file-type filter restricts processing to selected categories or extensions of files, which is useful when the matter requires particular document, archive, email, or other supported content types.

These filters are applied as part of the processing workflow, before the platform performs the downstream extraction, indexing, and analysis work required to make data available for review. Using them at this stage is especially valuable after an unrestricted collection because it reduces the volume that enters the case-processing pipeline while retaining a defensible, defined scope based on objective metadata and file classification criteria. Veritas documentation for eDiscovery Platform administration and processing workflows is available through the Veritas Documentation portal; product support resources are also available at Veritas Support.

QUESTION NO: 8

Which two statements are true about locking a production folder? (Choose two.)

A. Locking helps preserve the integrity of the production set.

B. Unlocking a production folder requires an appropriate access right.

C. Locking automatically deletes native files from the case.

D. Locking grants every Case User permission to export the production.

E. Locking changes all documents to TIFF format.

ANSWER: A B

Explanation:

Locking helps preserve the integrity of the production set and **unlocking a production folder requires an appropriate access right** are correct. A locked production folder protects the selected material from ordinary changes after the production set has been finalized. This supports a controlled and defensible production workflow.

The ability to unlock a production folder is a sensitive permission and is not available to every case user by default. Administrators should grant it only when operational procedures require a user to make controlled changes after a folder has been locked. See the Veritas Documentation portal for eDiscovery Platform production administration guidance.

QUESTION NO: 9

A Collection Admin is able to log in to Veritas eDiscovery Platform 8.2, but unable to access Collections data. After a period of time, access to the Collections data is acquired.

What is the reason for the intermittent access?

A. The MySQL service has restarted.

B. A Data Map refresh finally completed.

C. An EV Collection Task finally completed.

D. A Collections backup is in progress.

ANSWER: D

Explanation:

A Collections backup is in progress. Veritas eDiscovery Platform protects collection data while a Collections backup operation is running so that the backup represents a consistent, recoverable state. During this processing window, a Collection Admin can still authenticate to the appliance because login and role authorization are functioning normally, but access to the affected Collections data can be temporarily unavailable. Once the backup processing completes and the temporary protection on the collection data is released, the administrator can access the data again without requiring a change to the account, role, or collection permissions.

This behavior is therefore time-dependent: the access issue appears during the backup activity and clears when that activity finishes. Administrators should confirm whether a scheduled or manually initiated Collections backup overlaps with the reported period before investigating user authorization or collection configuration. Veritas documentation for eDiscovery Platform, including administration and backup-related guidance, is available from the Veritas eDiscovery Platform documentation portal. Product documentation and compatibility resources can also be accessed through Veritas SORT.

QUESTION NO: 10

An administrator is planning an upgrade to Veritas eDiscovery Platform 8.2.

Which two actions should be completed before starting the upgrade? (Choose two.)

A. Verify that all cases are online and processing is complete.

B. Perform the applicable platform backups.

C. Delete all completed processing batches.

D. Disable indexing for every case.

E. Unlock all production folders.

ANSWER: A B

Explanation:

Verify that all cases are online and processing is complete and **perform the applicable platform backups** are required pre-upgrade activities. Verifying case status and processing completion ensures that the upgrade begins from a stable operational state and avoids interrupting active processing work. Completing the applicable backups provides a recovery point for platform configuration, case information, and Legal Hold or Collections data as required by the deployment.

Administrators should also follow the release-specific compatibility and upgrade instructions for the installed environment. See the Veritas SORT eDiscovery Platform 8.2 documentation portal and the Veritas Documentation portal.

QUESTION NO: 11

Which two options are available when analyzing documents using Find Similar? (Choose two.)

A. Across all cases

B. Across all folders

C. Across Entire Case

D. Within saved searchers

E. Within Search results

ANSWER: C E

Explanation:

Find Similar supports two scopes that let reviewers control the population used to identify documents with comparable content to the selected document. **Across Entire Case** runs the similarity analysis against the full document population in the current case. This is useful when the reviewer needs to discover potentially related material regardless of the folder, search, or result set from which the original document was opened. **Within Search results** limits the comparison to the documents returned by the active search. This gives reviewers a focused way to assess related documents within a defined responsive, custodial, date-based, or otherwise filtered set of results. These scopes allow the reviewer to choose between broad case-wide discovery and targeted analysis of the current result population without leaving the review workflow. Veritas product documentation is accessed through the Veritas Documentation portal; use the portal's eDiscovery Platform 8.2 documentation and search for "Find Similar" to review the feature's workflow and scope behavior. Additional official product resources are available from the Veritas Support search for eDiscovery Platform 8.2.