PassQueen
a.k.a dumpsqueen.com

RSA Certified SE Professional in Data Loss Prevention Exam

RSA 050-SEPRODLP-01

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What are the two data detection methods used by RSA DLP?

A. Describing and auditing content

B. Fingerprinting and Marking content

C. Fingerprinting and auditing content

D. Describing and fingerprinting content

ANSWER: D

Explanation:

RSA DLP uses content description and content fingerprinting as its two principal data-detection approaches. Therefore, **Describing and fingerprinting content** is correct. Content description identifies data by evaluating characteristics that can be expressed as rules or classifiers, such as keywords, regular expressions, file properties, document metadata, and patterns associated with regulated or sensitive information. This approach is useful when the organization can define the identifying traits of the data it wants to protect.

Content fingerprinting protects known sensitive content by creating a compact representation of source material, such as selected documents or records. RSA DLP can then compare monitored content against those fingerprints to detect complete copies as well as relevant partial reproductions, even when normal document attributes or formatting differ. Using both methods lets policy designers protect data that is identifiable by a defined description and data that must be recognized by its relationship to an authoritative source. RSA describes its data-loss-prevention capabilities and content-aware protection approach at RSA Data Loss Prevention. Additional RSA product and documentation resources are available through the RSA Community.

QUESTION NO: 2

What are the three ways to install permanent RSA DLP Datacenter agents on a machine?

A. Generate a pre-configured installer, use the agent.msi installer, set up a scan group and run a scan

B. Use the agent-installer.exe program, use the agent.msi installer, set up a scan group and run a scan

C. Generate a pre-configured installer, use the agent.msi installer, and use the agentinstaller.exe program

D. Generate a pre-configured installer, set up a scan group and run a scan, use the agentinstaller.exe program

ANSWER: C

Explanation:

Generate a pre-configured installer, use the agent.msi installer, and use the agentinstaller.exe program is correct because RSA DLP Datacenter supports permanent-agent deployment through each of these installation paths. A pre-configured installer packages the agent with the required deployment and communication settings, allowing administrators to distribute an installation package that requires little or no interactive configuration on the target machine. The `agent.msi` package supports managed software-distribution approaches, such as deployment through enterprise endpoint-management tools or Windows Installer–based mechanisms. The `agentinstaller.exe` utility provides the executable-based installation path and can be used where an administrator installs or scripts the permanent agent directly.

A permanent agent remains installed after deployment and is available for ongoing discovery and scheduled scanning activity according to its configured policies and scan settings. These three methods therefore address common deployment models: packaged installation, MSI-based centralized distribution, and executable or scripted installation. This distinction is important when planning a scalable DLP rollout across servers and endpoints. RSA product documentation and support

resources are available through the RSA Community, and RSA's data-protection product information is available at NetWitness Data Loss Prevention.

QUESTION NO: 3

What is the default selection for components to include when installing the Enterprise

Manager software?

A. Enterprise Manager only

B. Enterprise Coordinator only

C. Enterprise Manager and Enterprise Coordinator

D. No components are selected by default

ANSWER: C

Explanation:

The default selection is **Enterprise Manager and Enterprise Coordinator**. The Enterprise Manager installation package presents both server-side components as selected by default so that a standard deployment can provide the central management interface as well as the coordination services needed by the RSA Data Loss Prevention environment. Enterprise Manager is the administrative console and policy-management component, while Enterprise Coordinator supports communication and coordination among DLP system components. Selecting both during the initial installation is therefore the expected default for a typical deployment, rather than requiring an administrator to manually choose each component.

An administrator can change the component selection when a design calls for separated roles, such as placing services on different hosts for scale, resiliency, or an established distributed architecture. That deployment decision does not alter the installer's initial default selection. This question concerns the preselected components displayed by the Enterprise Manager installer, which includes both components. RSA product documentation and support resources for DLP installation and deployment materials are available through the RSA DLP documentation portal and the RSA Community.

QUESTION NO: 4

Which RSA DLP product is focused on protecting Data at Rest?

A. RSA DLP Network

B. RSA DLP Navigator

C. RSA DLP Interceptor

D. RSA DLP Datacenter

ANSWER: D

Explanation:

RSA DLP Datacenter is the component designed to protect data at rest. It discovers and assesses sensitive information stored within enterprise repositories, allowing an organization to locate data such as personal information, payment-card data, or intellectual property in file shares, content repositories, and supported databases. After identifying that content, administrators can apply policies and remediation workflows to reduce exposure, such as notifying data owners, quarantining data, or applying appropriate access controls. This stored-data discovery and remediation role is what distinguishes the Datacenter product in the RSA DLP architecture. RSA DLP's product documentation and support resources describe the Datacenter deployment and its supported data-source integrations, while the broader product documentation provides the architecture and administration context for discovery policies and incident handling. See the RSA Data Loss Prevention documentation portal and the RSA Data Loss Prevention support knowledge base.

QUESTION NO: 5

An analyst expects to see DLP incidents in Enterprise Manager but the incident list is empty. Which checks are appropriate initial troubleshooting steps? Select all that apply.

A. Verify that the applicable policy is enabled

B. Confirm that the relevant data path reaches the inspection component

C. Review incident filters and assignment scope

D. Immediately run resetdevice on all Network appliances

ANSWER: A B C

Explanation:

First verify that the expected policy is enabled for the relevant DLP product. Next, confirm that the monitored traffic or repository activity is actually reaching the applicable inspection component. The analyst should also review search filters and assignment scope, because the default incident view can be limited to records assigned to the logged-in user. If these checks do not identify the problem, service and component connectivity can then be investigated.

Resetting a Network appliance is disruptive and is not an appropriate first action for an incident-display issue.

QUESTION NO: 6

An RSA DLP Network appliance is being repurposed for a different deployment. Which statements correctly describe the expected use of the `resetdevice` command? Select all that apply.

A. It resets appliance configuration and pairing information

B. It retains network settings

C. It retains time settings

D. It permanently removes the appliance operating system

E. It is equivalent to a normal reboot command

ANSWER: A B C

Explanation:

The `resetdevice` command resets the appliance's DLP configuration and pairing information, which is useful before configuring it for another deployment. It preserves the appliance's network and time settings, avoiding the need to rebuild basic connectivity before re-enrollment. After the reset, the appliance must be configured and paired again through the applicable DLP management workflow. The command is not equivalent to a routine reboot.

QUESTION NO: 7

Which RSA DLP product is designed to discover and scan sensitive data stored in repositories such as file shares and databases?

A. RSA DLP Endpoint

B. RSA DLP Network

C. RSA DLP Datacenter

D. RSA DLP ICAP Server

ANSWER: C

Explanation:

RSA DLP Datacenter is used to locate and assess sensitive information at rest in enterprise repositories. It supports discovery-oriented scanning of configured storage locations, including file systems and databases, so administrators can identify policy violations in stored content. Endpoint DLP focuses on user activity at the endpoint, while Network DLP addresses data moving through monitored network channels.

QUESTION NO: 8

Which actions help validate that an RSA DLP Network Sensor is receiving complete traffic for inspection? Select all that apply.

A. Use a TAP feed for the Sensor monitoring connection

B. Use tcpflowx to confirm packet visibility

C. Verify that both directions of sessions reach the Sensor

D. Use tcpdump to capture from the Napatech analysis card

ANSWER: A B C

Explanation:

A Sensor must receive the relevant traffic, including both directions of applicable TCP sessions, before it can reliably reconstruct and inspect content. A TAP feed is the preferred monitoring connection, and `tcpflowx` is the appliance utility used to verify that traffic reaches the analysis card. Confirming bidirectional visibility also helps identify asymmetric routing or incomplete SPAN/TAP feeds.

`tcpdump` is not the appropriate validation tool for the appliance Napatech capture path; `tcpflowx` is designed for that purpose.

QUESTION NO: 9

An administrator is preparing a policy for RSA DLP Endpoint enforcement. Which tasks are required or appropriate before the policy can protect endpoint activity? Select all that apply.

A. Associate applicable content blades

B. Configure Endpoint settings in the policy's Endpoint tab

C. Enable the policy for RSA DLP Endpoint

D. Restart Enterprise Manager services

ANSWER: A B C

Explanation:

The policy requires content-detection logic, so appropriate content blades must be associated with it. Endpoint-specific behavior is configured on the policy's **Endpoint** tab, where the administrator selects the relevant remediation and related Endpoint settings. The policy must also be enabled for RSA DLP Endpoint before it becomes active for that product.

Restarting Enterprise Manager services is not a normal policy-authoring or activation step.

For product documentation, see the RSA Community.