PassQueen
a.k.a dumpsqueen.com

Administration of Symantec Data Loss Prevention 15

Symantec 250-438

Version Demo

Total Demo Questions: 9

Total Premium Questions: 95

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, DLP Architecture	23
Topic 2, DLP Installation	7
Topic 3, DLP Configuration	18
Topic 4, DLP Policy Management	30
Topic 5, DLP Incident Management	9
Topic 6, DLP System Administration	8
Total	95

QUESTION NO: 1 - (SIMULATION)

What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

ANSWER: See the explanation for the answer

Explanation:

Correct installation order:

1. **Install and configure the database** (Oracle, when using an external Oracle database).
2. **Install the Symantec DLP Enforce Server.**
3. **Install the Detection Server components** (for example, Network Monitor, Network Prevent, Network Discover, or Network Protect, as applicable).
4. **Install/deploy Endpoint agents** (Endpoint Prevent/Endpoint Discover).

The Enforce Server is installed before Detection Servers because it supplies the central management console, policies, certificates, and configuration that Detection Servers use. Endpoint agents are deployed last, after Enforce Server is available to manage and register them.

If the simulation does not include a database item, begin with **Enforce Server**, then place all **Detection Servers**, followed by **Endpoint agents**.

QUESTION NO: 2

How do Cloud Detection Service and the Enforce server communicate with each other?

A. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 8100.

B. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 443.

C. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 1443.

D. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 443.

ANSWER: D

Explanation:

Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 443.

is correct because the Cloud Detection Service integration uses an outbound HTTPS connection from the Enforce Server to the cloud service. HTTPS provides the encrypted, authenticated channel used for service communication, and the standard destination port for this connection is TCP 443. This design is important for network planning: the Enforce Server must be able to establish outbound TCP sessions to the Cloud Detection Service endpoint through any intervening firewall or proxy, rather than requiring the cloud service to initiate an inbound connection to the customer's Enforce infrastructure. The connection direction supports deployments in which the Enforce Server is protected inside the organization's network perimeter while still being able to use cloud-hosted detection capabilities. Administrators should therefore ensure that outbound HTTPS traffic on port 443 is permitted from the Enforce Server and that any required proxy configuration, TLS inspection exceptions, and certificate trust settings are correctly implemented. Broadcom's Data Loss Prevention documentation is available through the Symantec Data Loss Prevention documentation portal; product-specific deployment and network guidance can also be accessed from the Broadcom Support portal.

QUESTION NO: 3

Which two actions can Network Protect perform on a file that Network Discover identifies as violating a policy? (Choose two.)

A. Move the file to a quarantine location

B. Replace the file with a marker file

C. Block the SMTP message containing the file

D. Disable the USB device that contains the file

E. Stop the endpoint operating system service

ANSWER: A B

Explanation:

Network Protect can **move the file to a quarantine location** and can **replace the file with a marker file**. These remediation actions are used with supported Network Discover file-system targets after a policy identifies sensitive content at rest.

A marker file can inform users that the original content was removed because it violated a data-protection policy. Network Protect does not block an SMTP message or control a USB device; those actions are associated with other DLP products and channels. See the Broadcom Symantec Data Loss Prevention documentation portal.

QUESTION NO: 4

Which two detection technology options ONLY run on a detection server? (Choose two.)

A. Form Recognition

B. Indexed Document matching (IDM)

C. Described Content Matching (DCM)

D. Exact data matching (EDM)

E. vector Machine Learning (VML)

ANSWER: B D

Explanation:

Indexed Document Matching (IDM) and Exact Data Matching (EDM) are the detection technologies that run only on a Symantec Data Loss Prevention detection server. Both technologies depend on centrally prepared and maintained data that is distributed to the applicable detection-server environment for policy evaluation. IDM uses indexed representations of protected source documents, enabling DLP to identify content that substantially matches material in the indexed document repository. EDM uses a structured database of protected records, such as customer or employee data, and detects occurrences of those records in monitored content.

Because these technologies require server-side indexing, database processing, and management of the associated matching data, their detection processing is performed by a detection server rather than locally by an endpoint agent. When configuring policies that use IDM or EDM, administrators must ensure that the relevant indexed documents or EDM data sources are configured and that the detection servers receive the required data updates. Symantec's detection-technology documentation identifies the supported detection locations and deployment requirements for these server-based matching methods. See Symantec DLP detection technology information and Broadcom Symantec Data Loss Prevention documentation.

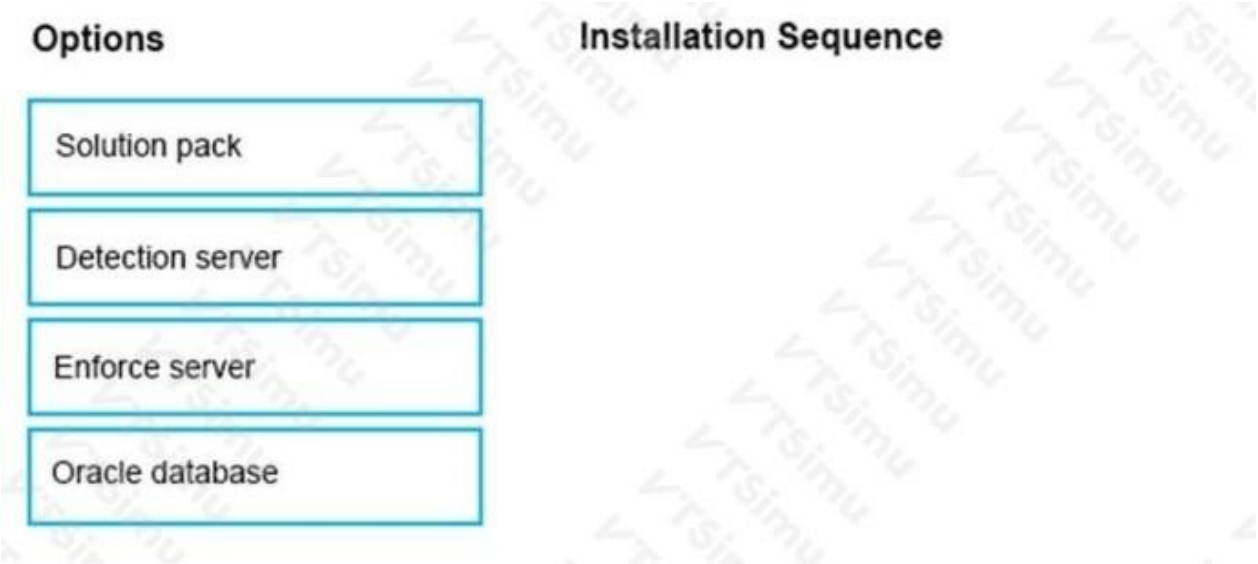
QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

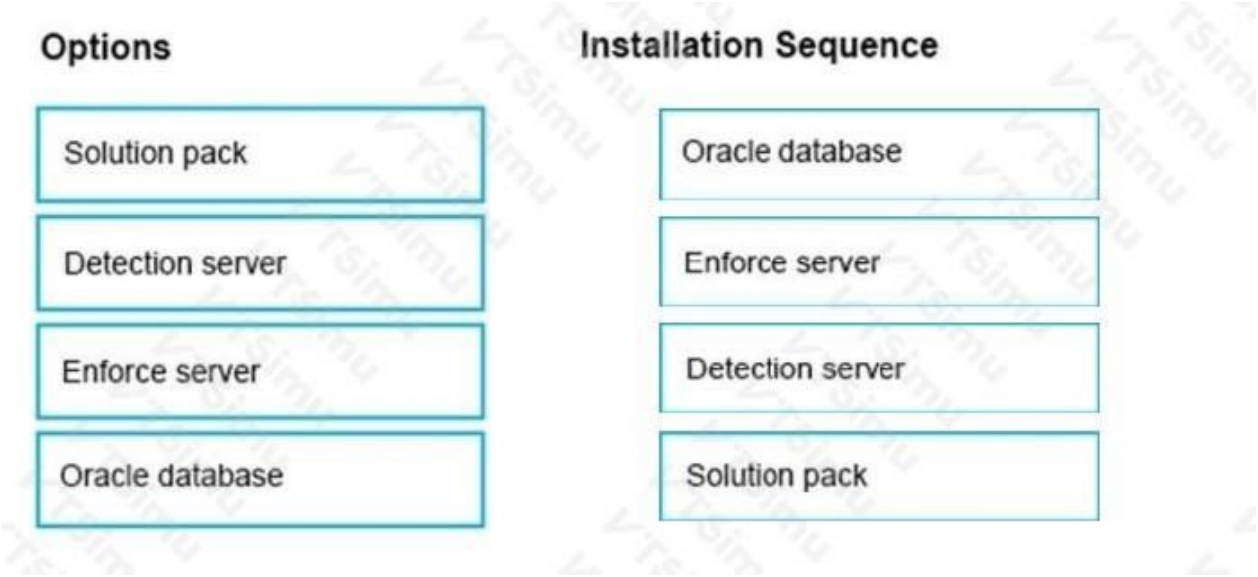
What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

Select and Place:



ANSWER:



Explanation:

The correct installation sequence is Oracle database, Enforce server, Detection server, and Solution pack. This order establishes the Symantec Data Loss Prevention environment in the dependency order used by the installation process. The Oracle database comes first because it hosts the DLP data repository used by the Enforce Server, including configuration, incident, policy, and operational data. A functioning database is therefore required before the central management application can be deployed and initialized.

The Enforce Server is installed next because it is the management and administration layer of the DLP deployment. It connects to the Oracle database during installation and creates or uses the required repository structures. Once the Enforce Server is available, it supplies the console and the central services through which the environment is configured and managed.

A Detection server follows the Enforce Server. Detection servers are managed through, and communicate with, the Enforce Server, so the central server must already be operational when a Detection server is installed and enrolled. This lets the Detection server obtain its configuration and report detection activity to the established DLP environment.

The Solution pack is applied after the core platform components are in place. At that stage, the deployed DLP environment can accept the packaged solution content and configuration in the context of an operational Enforce Server, repository, and Detection-server infrastructure. This sequence avoids attempting to configure solution content before the services and

database it relies on have been established. Broadcom's Symantec Data Loss Prevention documentation provides the product installation and deployment guidance for these components.

QUESTION NO: 6

Which action should a DLP administrator take to secure communications between an on-premises Enforce server and detection servers hosted in the Cloud?

A. Use the built-in Symantec DLP certificate for the Enforce Server, and use the "sslkeytool" utility to create certificates for the detection servers.

B. Use the built-in Symantec DLP certificate for both the Enforce server and the hosted detection servers.

C. Set up a Virtual Private Network (VPN) for the Enforce server and the hosted detection servers.

D. Use the "sslkeytool" utility to create certificates for the Enforce server and the hosted detection servers.

ANSWER: A

Explanation:

Use the built-in Symantec DLP certificate for the Enforce Server, and use the "sslkeytool" utility to create certificates for the detection servers. This follows the Symantec DLP SSL trust model for communication between the Enforce Server and its detection servers. The Enforce Server installation includes its DLP server certificate, which is used to establish the Enforce Server identity. Detection servers require their own SSL certificates so that their connections to Enforce can be authenticated and encrypted, including when those systems are deployed in a cloud environment.

The `sslkeytool` utility is the DLP-supported mechanism for creating and managing the certificates and keystores used by detection servers. After the detection-server certificates are generated and installed, the Enforce Server and detection servers can validate the configured trust relationship and protect management and incident-related traffic with SSL/TLS. This certificate-based configuration is especially important when the communication path crosses network boundaries between on-premises infrastructure and cloud-hosted servers. Symantec DLP documentation is available from the Broadcom Symantec Data Loss Prevention documentation portal; Broadcom also provides product support resources through the Broadcom Knowledge Base.

QUESTION NO: 7

Which option correctly describes the two-tier installation type for Symantec DLP?

A. Install the Oracle database on the host, and install the Enforce server and a detection server on a second host.

B. Install the Oracle database on a local physical host, and install the Enforce server and detection servers on virtual hosts in the Cloud.

C. Install the Oracle database and a detection server in the same host, and install the Enforce server on a second host.

D. Install the Oracle database and Enforce server on the same host, and install detection servers on separate hosts.

ANSWER: D

Explanation:

Install the Oracle database and Enforce server on the same host, and install detection servers on separate hosts. This is the standard two-tier Symantec Data Loss Prevention deployment model: the first tier contains the Enforce Server and its Oracle database together, while the second tier contains one or more Detection Servers on different machines. Enforce Server provides the central management interface, stores configuration and incident data in the database, distributes policies, and receives incident information. Detection Servers perform the monitoring, discovery, or endpoint-related detection work assigned to them and communicate their results to Enforce.

This topology separates the resource-intensive detection workload from the management and database workload, allowing Detection Servers to be placed and scaled according to the monitored channels, network locations, and organizational capacity requirements. It also lets administrators add Detection Servers without moving the Enforce Server database. Broadcom's Data Loss Prevention documentation describes the Enforce Server, database, and Detection Server roles and deployment planning considerations in its Symantec Data Loss Prevention documentation. Additional product deployment and administration resources are available through the Broadcom Support portal.

QUESTION NO: 8

Which two response-rule types can apply actions automatically when a DLP policy generates an incident? (Choose two.)

A. Automated Response Rules

B. Smart Response Rules

C. Detection Rules

D. Endpoint Locations

E. Incident Status Attributes

ANSWER: A B

Explanation:

Automated Response Rules and **Smart Response Rules** are the correct answers. Automated Response Rules apply configured actions automatically when an incident meets the policy conditions. Smart Response Rules use incident context and configured conditions to determine the applicable action dynamically. Both response-rule types can automate incident handling and enforcement behavior, depending on the detection channel and supported response action.

See the Broadcom Symantec Data Loss Prevention documentation portal for policy and response-rule administration.

QUESTION NO: 9

Which server target uses the "Automated Incident Remediation Tracking" feature in Symantec DLP?

A. Exchange

B. File System

C. Lotus Notes

D. SharePoint

ANSWER: B

Explanation:

File System is the server target associated with Automated Incident Remediation Tracking in Symantec Data Loss Prevention. During a Discover scan of a file-system target, DLP can perform configured automated remediation actions on files that generate incidents, such as moving, deleting, or otherwise handling the discovered content according to the applicable policy and remediation configuration. Automated Incident Remediation Tracking provides visibility into the outcome of those remediation operations, allowing administrators to determine whether the requested action was completed and to investigate remediation issues when necessary.

This tracking is important because incident detection and remediation are separate operational steps: an incident can be created when sensitive data is found, while the remediation status records the subsequent action taken against the file. Administrators can therefore use the incident's remediation details to monitor operational results and troubleshoot failures. Symantec's DLP documentation specifically addresses troubleshooting this feature in the context of Discover remediation workflows. See the Symantec DLP documentation on troubleshooting automated incident remediation tracking and the Broadcom Data Loss Prevention documentation portal.