

Reliable exam torrent & valid VCE PDF materials & dumps torrent files

Input your exam code ...



Our high-quality valid VCE PDF materials & dumps torrent files guarantee you pass exam 100% for sure. Our reliable exam torrent will be the best help for your exams and will give you a new start, a new life.

All Products

Contact now



Quality and Value

VCETorrent Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.



Easy to Pass

If you prepare for the exams using our VCETorrent testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.



Try Before Buy

VCETorrent offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

19728

CUSTOMERS

32727

DOWNLOADS

21728

TEAM MEMBERS

26394

SHARES

<http://www.vcetorrent.com>

Reliable exam torrent & valid VCE PDF materials & dumps torrent files

Exam : **250-586**

Title : Endpoint Security Complete
Implementation - Technical
Specialist

Vendor : Symantec

Version : DEMO

NO.1 What should be checked to ensure proper distribution and mapping for LUAs or GUPs in the Manage phase?

- A. Content Delivery configuration
- B. Replication between sites
- C. Security Roles
- D. Default or custom Device/Policy Groups

Answer: A

Explanation:

To ensure proper distribution and mapping for LiveUpdate Administrators (LUAs) or Group Update Providers (GUPs) in the Manage phase, checking the Content Delivery configuration is essential. This configuration ensures that updates are correctly distributed to all endpoints and that LUAs or GUPs are properly positioned to reduce bandwidth usage and improve update efficiency across the network.

Symantec Endpoint Protection Documentation highlights the importance of verifying Content Delivery configuration to maintain effective update distribution and optimal performance, particularly in large or distributed environments.

NO.2 Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?

- A. The System Policy
- B. The LiveUpdate Policy
- C. The System Schedule Policy
- D. The Firewall Policy

Answer: B

Explanation:

To use the Symantec LiveUpdate server for pre-release content, the administrator should edit the LiveUpdate Policy. This policy controls how endpoints receive updates from Symantec, including options for pre-release content.

* Purpose of the LiveUpdate Policy: The LiveUpdate Policy is specifically designed to manage update settings, including source servers, scheduling, and content types. By adjusting this policy, administrators can configure endpoints to access pre-release content from Symantec's servers.

* Pre-Release Content Access: Enabling pre-release content within the LiveUpdate Policy allows endpoints to test new security definitions and updates before they are generally available. This can be beneficial for organizations that want to evaluate updates in advance.

* Policy Configuration for Symantec Server Access: The LiveUpdate Policy can be set to point to the Symantec LiveUpdate server, allowing endpoints to fetch content directly from Symantec, including any available beta or pre-release updates.

Explanation of Why Other Options Are Less Likely:

* Option A (System Policy) and Option C (System Schedule Policy) do not govern update settings.

* Option D (Firewall Policy) controls network access rules and would not manage LiveUpdate configurations.

Therefore, to configure access to the Symantec LiveUpdate server for pre-release content, the LiveUpdate Policy is the correct policy to edit.

NO.3 Where can you validate the Cloud Enrollment configuration in the SEP manager?

- A. Advanced Security page
- B. Cloud Enrollment Screen
- C. Heat map
- D. Settings

Answer: B

Explanation:

The Cloud Enrollment Screen within the SEP Manager is where administrators can validate the Cloud Enrollment configuration. This screen provides details about the current cloud enrollment status and any associated settings, allowing administrators to verify that the enrollment aligns with organizational policies and to troubleshoot any connectivity or setup issues.

Symantec Endpoint Protection Documentation notes that accessing the Cloud Enrollment Screen provides essential information to ensure proper integration between the SEP Manager and the cloud, facilitating a smooth transition to a cloud-managed environment.

NO.4 Which section of the SES Complete Solution Design provides a summary of the features and functions to be implemented?

- A. Infrastructure Design
- B. Configuration Design
- C. Initial Test Plan
- D. Executive Summary

Answer: D

Explanation:

The Executive Summary section of the SES Complete Solution Design provides a summary of the features and functions to be implemented. This summary is tailored for stakeholders and decision-makers, offering a high-level overview of the solution's capabilities, key features, and intended outcomes without going into technical specifics. It helps to convey the value and strategic benefits of the SES Complete solution to the organization.

SES Complete Implementation Documentation highlights the Executive Summary as a crucial section for communicating the solution's scope and anticipated impact to executives and non-technical stakeholders.

NO.5 What does the Design phase of the SESC Implementation Framework include?

- A. Creation of a SES Complete Solution Design
- B. Creation of a SES Complete Solution Proposal
- C. Assessing the base architecture and infrastructure requirements
- D. Implementation of the pilot deployment of the Solution

Answer: A

Explanation:

The Design phase in the SESC Implementation Framework includes the creation of a SES Complete Solution Design. This design document details the architectural plan for deploying SES Complete, including component layout, communication flows, security policies, and configurations. The Solution Design serves as a blueprint that guides the subsequent phases of implementation, ensuring that the deployment aligns with both technical requirements and business objectives.

SES Complete Implementation Curriculum outlines the Solution Design as a critical deliverable of the Design phase, providing a comprehensive, structured plan that directs the implementation and

ensures all security and operational needs are met.

NO.6 What does the Symantec Communities platform provide?

- A. Access to professionals, experts, and enthusiasts to discuss, collaborate, and share knowledge
- B. Access to the latest product documentation, downloads, and support information
- C. Access to the My Entitlements list
- D. Access to customer support incidents

Answer: A

Explanation:

The Symantec Communities platform provides access to professionals, experts, and enthusiasts to discuss, collaborate, and share knowledge. This platform allows users to connect with others in the cybersecurity field to exchange insights, best practices, and solutions related to Symantec products. It fosters a collaborative environment where users can gain assistance, share experiences, and stay informed about the latest developments.

Symantec Endpoint Security Documentation describes the Symantec Communities as a collaborative forum beneficial for troubleshooting, networking, and expanding knowledge on cybersecurity topics and Symantec tools.

NO.7 What protection technologies should an administrator enable to protect against Ransomware attacks?

- A. Firewall, Host Integrity, System Lockdown
- B. IPS, SONAR, and Download Insight
- C. IPS, Firewall, System Lockdown
- D. SONAR, Firewall, Download Insight

Answer: B

Explanation:

To protect against Ransomware attacks, an administrator should enable Intrusion Prevention System (IPS), SONAR (Symantec Online Network for Advanced Response), and Download Insight. These technologies collectively provide layered security against ransomware by blocking known exploits (IPS), detecting suspicious behaviors (SONAR), and analyzing downloaded files for potential threats (Download Insight), significantly reducing the risk of ransomware infections.

Symantec Endpoint Protection Documentation emphasizes the combination of IPS, SONAR, and Download Insight as essential components for ransomware protection due to their proactive and reactive threat detection capabilities.

NO.8 What are the main phases within the Symantec SES Complete implementation Framework?

- A. Assess, Design, Implement, Manage
- B. Plan, Execute, Review, Improve
- C. Gather, Analyze, Implement, Evaluate
- D. Assess, Plan, Deploy, Monitor

Answer: A

Explanation:

The main phases within the Symantec SES Complete Implementation Framework are Assess, Design, Implement, and Manage. Each phase represents a critical step in the SES Complete deployment process.

- * Assess: Understand the current environment, gather requirements, and identify security needs.
- * Design: Develop the Solution Design and Configuration to address the identified needs.
- * Implement: Deploy and configure the solution based on the designed plan.
- * Manage: Ongoing management, monitoring, and optimization of the deployed solution.

These phases provide a structured methodology for implementing SES Complete effectively, ensuring that each step aligns with organizational objectives and security requirements.

SES Complete Implementation Curriculum outlines these phases as core components for a successful deployment and management lifecycle of the SES Complete solution.