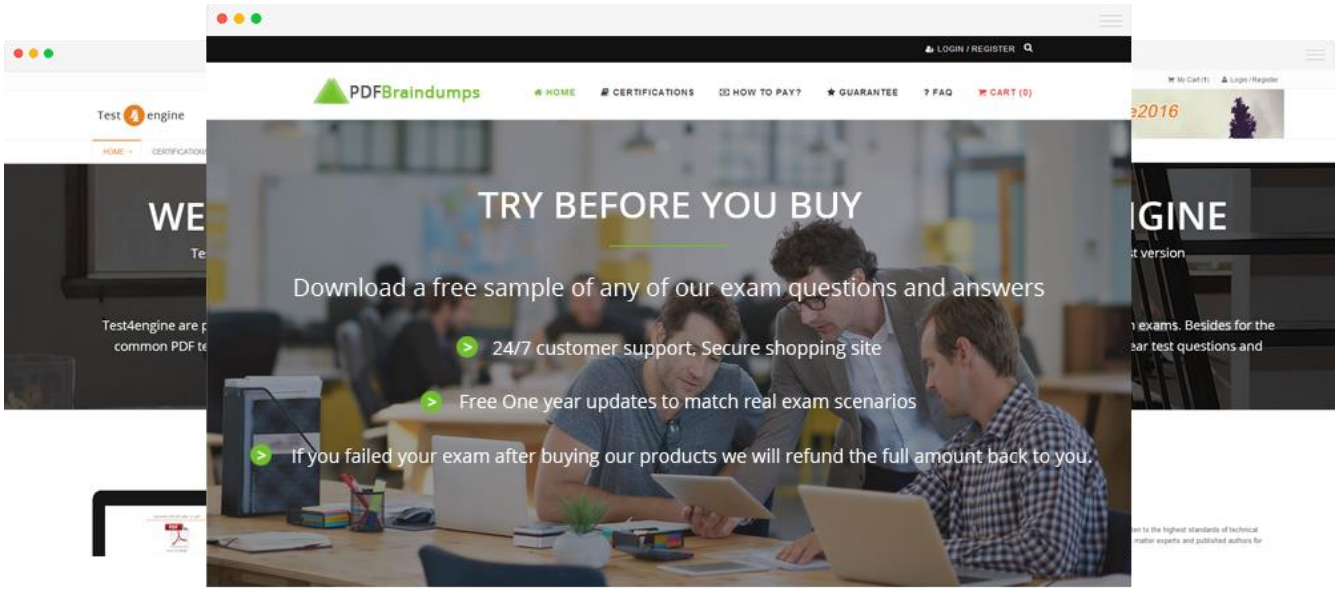
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

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 forLiveUpdate Administrators (LUAs) or Group Update Providers (GUPs)in theManage phase, checking theContent Delivery configurationis 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 Documentationhighlights 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 theSymantec 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)andOption 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 theSymantec LiveUpdate server for pre-release content, theLiveUpdate Policyis 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:
TheCloud Enrollment Screenwithin the SEP Manager is where administrators can validate theCloud 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 Documentationnotes 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:
TheExecutive Summarysection of theSES Complete Solution Designprovides asummary 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 Documentationhighlights 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:
TheDesign phasein theSESC Implementation Frameworkincludes thecreation 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 Curriculumoutlines 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:

TheSymantec Communities platformprovidesaccess 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 Documentationdescribes 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 againstRansomware attacks, an administrator should enableIntrusion Prevention System (IPS), SONAR(Symantec Online Network for Advanced Response), andDownload 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 Documentationemphasizes 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 theSymantec SES Complete Implementation FrameworkareAssess, Design, Implement,andManage. 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 Curriculumoutlines these phases as core components for a successful deployment and management lifecycle of the SES Complete solution.