156-215.81 Q&As

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/156-215-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain Why does it not detect the windows domain?

A. SmartConsole machine is not part of the domain

B. Security Gateway is not part of the Domain

C. Identity Awareness is not enabled on Global properties

D. Security Management Server is not part of the domain

Correct Answer: A

While enabling the Identity Awareness blade, the Identity Awareness wizard does not automatically detect the Windows domain because the SmartConsole machine is not part of the domain. The SmartConsole machine needs to be a member of the Windows domain or have access to a domain controller in order to detect the domain automatically.

References: Check Point R81 Identity Awareness Administration Guide, page 10.

QUESTION 2

What is the default shell for the command line interface?

A. Clish

B. Admin

C. Normal

D. Expert

Correct Answer: A

Clish is the default shell for the command line interface. It is a user-friendly shell that provides a menu-based and a command-line mode. Admin, Normal, and Expert are not valid shell names.

QUESTION 3

The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways.

Which statement best describes this Secure Internal Communication (SIC)?

A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.

B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.

C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.

D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.

Correct Answer: A

The statement that best describes Secure Internal Communication (SIC) is:

After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA. SIC is a mechanism that ensures secure communication between Check Point components by

using certificates that are issued by an Internal Certificate Authority (ICA). The other statements are not accurate descriptions of SIC.

QUESTION 4

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

A. Security Management Server\\'s /home/.fgpt file and is available for future SmartConsole authentications.

B. Windows registry is available for future Security Management Server authentications.

C. There is no memory used for saving a fingerprint anyway.

D. SmartConsole cache is available for future Security Management Server authentications.

Correct Answer: D

When logging in for the first time to a Security Management Server through SmartConsole, a fingerprint is saved to the SmartConsole cache and is available for future Security Management Server authentications. The fingerprint is a unique identifier of the Security Management Server that is used to verify its identity and prevent man-in-the- middle attacks. The SmartConsole cache is a local folder on the client machine that stores temporary files and settings. References: Check Point Security Management Administration Guide R81, p. 25-26

QUESTION 5

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services

B. Load Sharing Mode Services

C. Threat Agent Solution

D. Public Cloud Services

Correct Answer: A

Smart Cloud Services is an option for deployment of Check Point SandBlast Zero-Day Protection. It is a cloud-based

service that provides advanced threat prevention for files and URLs, without requiring any on-premise infrastructure or appliances . References:

[Check Point SandBlast Zero-Day Protection], [Smart Cloud Services]