Free Questions for 156-315.81 by dumpssheet

Shared by Walsh on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have used the SmartEvent GUI to create a custom Event policy. What is the best way to display the correlated Events generated by SmartEvent Policies?

Options:

A- Open SmartView Monitor and select the SmartEvent Window from the main menu.

B- In the SmartConsole / Logs & Monitor --> open the Logs View and use type:Correlated as query filter.

C- In the SmartConsole / Logs & Monitor -> open a new Tab and select External Apps / SmartEvent.

D- Select the Events tab in the SmartEvent GUI or use the Events tab in the SmartView web interface.

Answer:

C

Explanation:

The best way to display the correlated events generated by SmartEvent policies is to open a new tab in the SmartConsole / Logs & Monitor and select External Apps / SmartEvent. This will launch the SmartEvent GUI, which provides a comprehensive view of the network security events, including charts, reports, and timelines.The SmartEvent GUI can also be accessed from a web browser using the SmartView web interface1. Reference:Check Point R81 SmartEvent Administration Guide

Question 2

Question Type: MultipleChoice

Which two Identity Awareness daemons are used to support identity sharing?

Options:

A- Policy Activation Point (PAP) and Policy Decision Point (PDP)

B- Policy Manipulation Point (PMP) and Policy Activation Point (PAP)

C- Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)

D- Policy Decision Point (PDP) and Policy Enforcement Point (PEP)

Answer:

D

Explanation:

The two Identity Awareness daemons that are used to support identity sharing are Policy Decision Point (PDP) and Policy Enforcement Point (PEP). PDP is a daemon that runs on Security Gateways that acquire identities from various sources, such as AD Query, Identity Agent, Captive Portal, etc. PEP is a daemon that runs on Security Gateways that enforce the security policy based on identities received from PDPs. Identity sharing is a feature that allows PDPs to share identities with other PDPs or PEPs in different gateways or domains.

Reference: [Check Point R81 Identity Awareness Administration Guide]

Question 3

Question Type: **MultipleChoice**

What are the correct steps upgrading a HA cluster (M1 is active, M2 is passive) using Multi-Version Cluster(MVC)Upgrade?

Options:

A- 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on

2) Upgrade the passive node M2 to R81.20

3) In SmartConsole, change the version of the cluster object

4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails

5) After examine the cluster states upgrade node M1 to R81.20

6) On each Cluster Member, disable the MVC mechanism

B- 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on
2) Upgrade the passive node M2 to R81.20
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy

C- 1) In SmartConsole, change the version of the cluster object
2) Upgrade the passive node M2 to R81.20
3) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 #cphaconf mvc on
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsole, change the version of the cluster object

D- 1) Upgrade the passive node M2 to R81.20
2) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 #cphaconf mvc on
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.20

Answer:

C

Explanation:

The correct steps upgrading a HA cluster (M1 is active, M2 is passive) using Multi-Version Cluster (MVC) Upgrade are:

In SmartConsole, change the version of the cluster object to R81.20.

Upgrade the passive node M2 to R81.20 using CPUSE or CLI.

Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 using the commandcphaconf mvc on.

Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails by selectingContinue installing on other Gatewaysin thePolicy Installation Settingsdialog box.

After examining the cluster states usingcphaprob statand verifying that both members are synchronized, upgrade node M1 to R81.20 using CPUSE or CLI.

On each Cluster Member, disable the MVC mechanism using the commandcphaconf mvc offand Install the Access Control Policy3.

Question 4

Question Type: **MultipleChoice**

What is the main objective when using Application Control?

Options:

A- To filter out specific content.

B- To assist the firewall blade with handling traffic.

C- To see what users are doing.

D- Ensure security and privacy of information.

Answer:

D

Explanation:

The main objective when using Application Control is to ensure security and privacy of information. Application Control is a blade that enables administrators to control access to web applications and web sites based on categories, users, groups, machines, and time.Application Control can also block or limit usage of applications that pose security risks or consume excessive bandwidth2. Reference:Check Point R81 Application Control Administration Guide

Question 5

Question Type: MultipleChoice

What is the command switch to specify the Gaia API context?

Options:

A- You have to specify it in the YAML file api.yml which is located underneath the /etc. directory of the security management server

B- You have to change to the zsh-Shell which defaults to the Gaia API context.

C- No need to specify a context, since it defaults to the Gaia API context.

D- mgmt_cli --context gaia_api <Command>

Answer:

D

Explanation:

The command switch to specify the Gaia API context ismgmt_cli --context gaia_api <Command>. This switch allows the user to execute Gaia OS commands through the management API.The Gaia API context is different from the default management API context, which is used to execute commands related to the security policy and objects1. Reference:Check Point R81 Management API Reference Guide

Question 6

Question Type: MultipleChoice

What is the biggest benefit of policy layers?

Options:

A- To break one policy into several virtual policies

B- Policy Layers and Sub-Policies enable flexible control over the security policy

C- They improve the performance on OS kernel version 3.0

D- To include Threat Prevention as a sub policy for the firewall policy

Answer:

B

Explanation:

The biggest benefit of policy layers is that they enable flexible control over the security policy. Policy layers and sub-policies allow administrators to break one policy into several virtual policies, each with its own set of rules and actions. Policy layers can be ordered, shared, and reused across different policies. Policy layers can also include Threat Prevention as a sub-policy for the firewall policy.

Reference: [Check Point R81 Security Management Guide]

Question 7

Question Type: MultipleChoice

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

Options:

A- Centos Linux

B- Gaia embedded.

C- Gaia

D- Red Hat Enterprise Linux version 5

Answer:

B

Explanation:

Rugged appliances are small appliances with ruggedized hardware that are designed for harsh environments. Like Quantum Spark appliances, they use Gaia embedded as their operating system. Gaia embedded is a lightweight version of Gaia that supports a subset of features and commands. Reference: [Check Point R81 Gaia Embedded Administration Guide]

Question 8

Question Type: MultipleChoice

The Check Point installation history feature in provides the following:

Options:

A- View install changes and install specific version

B- Policy Installation Date only

C- Policy Installation Date, view install changes and install specific version

D- View install changes

Answer:

C

Explanation:

The Check Point installation history feature provides the following:

Policy Installation Date: The date and time when the policy was installed on the Security Gateway.

View install changes: The ability to view the differences between two policy versions that were installed on the Security Gateway.

Install specific version: The ability to install a specific policy version from the installation history on the Security Gateway3.
Reference:Check Point R81 SmartConsole Guide

Question 9

Question Type: MultipleChoice

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

Options:

A- Publish changes

B- Save changes

C- Install policy

D- Install database

Answer:

C

Explanation:

In order for changes made to policy to be enforced by a Security Gateway, an administrator must perform the action of installing policy. Installing policy is the process of transferring the policy package from the Security Management Server to the Security Gateway. Publishing changes is the process of saving changes to the database and making them available to other administrators.Saving changes is the process of saving changes to a session without publishing them2. Reference:Check Point R81 Security Management Guide

Question 10

Question Type: MultipleChoice

Alice & Bob are going to deploy Management Data Plane Separation (MDPS) for all their Check Point Security Gateway(s)/Cluster(s). Which of the following statement is true?

Options:

A- Each network environment is dependent and includes interfaces, routes, sockets, and processes

B- Management Plane -- To access, provision and monitor the Security Gateway

C- Data Plane -- To access, provision and monitor the Security Gateway

D- Management Plane -- for all other network traffic and processing

Answer:

B

Explanation:

Management Data Plane Separation (MDPS) is a feature that allows the separation of the management plane and the data plane on a Security Gateway or a cluster. The management plane is responsible for accessing, provisioning and monitoring the Security Gateway, while the data plane is responsible for all other network traffic and processing.Each network environment is independent and includes interfaces, routes, sockets, and processes1. Reference:Check Point R81 Administration Guide

20%
DISCOUNT