156-315.81 Q&As

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

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

https://www.pass4itsure.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which command shows the current Security Gateway Firewall chain?

A. show current chain

B. show firewall chain

C. fw ctl chain

D. fw ctl firewall-chain

Correct Answer: C

QUESTION 2

In which formats can Threat Emulation forensics reports be viewed in?

A. TXT, XML and CSV

B. PDF and TXT

C. PDF, HTML, and XML

D. PDF and HTML

Correct Answer: C

The formats in which Threat Emulation forensics reports can be viewed in are PDF, HTML, and XML. Threat Emulation is a feature that detects and prevents zero-day attacks by emulating files in a sandbox environment and analyzing their behavior. Threat Emulation generates forensics reports that provide detailed information about the emulated files, such as verdict, severity, activity summary, screenshots, network activity, registry activity, file activity, and process activity. These reports can be viewed in PDF, HTML, or XML formats from SmartConsole or SmartView.

QUESTION 3

Which SmartEvent component is responsible to collect the logs from different Log Servers?

A. SmartEvent Server

B. SmartEvent Database

C. SmartEvent Collector

D. SmartEvent Correlation Unit

Correct Answer: D

The SmartEvent component that is responsible to collect the logs from different Log Servers is the SmartEvent Correlation Unit. The SmartEvent Correlation Unit is a daemon that runs on the SmartEvent Server and receives logs from one or more Log Servers. The SmartEvent Correlation Unit analyzes the logs and generates correlated events

according to the SmartEvent policy2. References: Check Point R81 SmartEvent Administration Guide

QUESTION 4

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.

B. Change the Standby Security Management Server to Active.

C. Change the Active Security Management Server to Standby.

D. Manually synchronize the Active and Standby Security Management Servers.

Correct Answer: A

The hostname of the Standby member should not be changed to match the hostname of the Active member, as this would cause a conflict in the network. The correct procedure is to change the hostname of the Active member to a different name, and then change the Standby member to the original hostname of the Active member1. References: 1: Check Point Resource Library, Certified Security Expert (CCSE) R81.20 Course Overview, page 9.

QUESTION 5

What command lists all interfaces using Multi-Queue?

A. cpmq get

B. show interface all

C. cpmq set

D. show multiqueue all

Correct Answer: A

The command that lists all interfaces using Multi-Queue is cpmq get. Multi- Queue is a feature that allows network interfaces to use multiple transmit and receive queues, which improves the performance and scalability of the Security Gateway by distributing the network load among several CPU cores. Cpmq is a command that allows administrators to configure and manage Multi-Queue settings on network interfaces. Cpmq get lists all interfaces using Multi-Queue and shows their queue count and core distribution.

QUESTION 6

When simulating a problem on ClusterXL cluster with cphaprob STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

A. cphaprob STOP unregister

B. cphaprob STOP unregister

C. cphaprob unregister STOP

D. cphaprob unregister STOP

Correct Answer: A

When simulating a problem on a ClusterXL cluster with the command "cphaprob STOP -s problem -t 0 register" to initiate a failover on an active cluster member, you can use the command "cphaprob STOP unregister" to remove the

problematic state and return the cluster to normal operation.

Option A correctly identifies the command that allows you to remove the problematic state, making it the verified answer.

References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

QUESTION 7

By default, what type of rules in the Access Control rulebase allow the control connections?

A. Implicit Rules

B. Explicitly Implied Rules

C. Implied Rules

D. Explicit Rules

Correct Answer: C

QUESTION 8

SmartEvent Security Checkups can be run from the following Logs and Monitor activity:

A. Reports

B. Advanced

C. Checkups

D. Views

Correct Answer: A

SmartEvent Security Checkups can be run from the Reports activity in Logs and Monitor. A Security Checkup is a report that analyzes network traffic and security events and provides recommendations for improving security posture. To run a Security Checkup, go to Logs and Monitor > Reports > New Report > Security Checkup. The other activities in Logs and Monitor do not have the option to run a Security Checkup. References: : Check Point Software, Getting Started, Running a Security Checkup Report.

QUESTION 9

Which statements below are CORRECT regarding Threat Prevention profiles in Smart Dashboard?

A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.

B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.

C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.

D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Correct Answer: C

In SmartDashboard, Threat Prevention profiles can be assigned to one or more rules. This means that you can have multiple profiles assigned to a single gateway, and each of these profiles can be associated with one or more rules. This allows for granular control over threat prevention settings for different rules or scenarios.

References: Check Point Certified Security Expert R81 documentation and learning resources.

QUESTION 10

Which features are only supported with R81.20 Gateways but not R77.x?

A. Access Control policy unifies the Firewall, Application Control and URL Filtering, Data Awareness, and Mobile Access Software Blade policies.

B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.

C. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.

D. Time object to a rule to make the rule active only during specified times.

Correct Answer: C

The features that are only supported with R81.20 Gateways and not with R77.x are described in option C:

"C. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence."

This feature, known as Rule Base Layers, allows for greater flexibility and control in organizing and prioritizing security rules within the rule base.

Options A, B, and D do not specifically pertain to features introduced in R81.20 and are available in earlier versions as well.

References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

QUESTION 11

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

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

Correct Answer: D

The command switch to specify the Gaia API context is mgmt_cli --context gaia_api . 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. References: Check Point R81 Management API Reference Guide

QUESTION 12

What is the responsibility of SOLR process on R81.20 management server?

A. Validating all data before it\\'s written into the database

B. It generates indexes of data written to the database

C. Communication between SmartConsole applications and the Security Management Server

D. Writing all information into the database

Correct Answer: B

The responsibility of SOLR process on R81.20 management server is to generate indexes of data written to the database. SOLR is an open source search platform that provides fast and scalable indexing and querying capabilities. SOLR is used by the R81.20 management server to index data such as logs, objects, policies, tasks, and events, and to enable quick and efficient searches on this data by SmartConsole and SmartView applications.

QUESTION 13

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.

B. Fill Layer4 VPN SL VPN that gives users network access to all mobile applications.

C. Full Layer3 VPN PSec VPN that gives users network access to all mobile applications.

D. You can make sure that documents are sent to the intended recipients only.

Correct Answer: C

The feature that provides Full Layer3 VPN PSec VPN, giving users network access to all mobile applications, is the correct answer.

Capsule Connect/VPN is used to establish secure VPN connections for mobile devices, and the Full Layer3 VPN (IPSec VPN) option provides comprehensive network access.

References: Check Point documentation or training materials related to Mobile Access Methods and VPN configurations.

QUESTION 14

Which of the following is NOT an internal/native Check Point command?

A. fwaccel on

B. fw ct1 debug

C. tcpdump

D. cphaprob

Correct Answer: C

The command tcpdump is not an internal/native Check Point command. It is a common command-line tool that captures and analyzes network traffic. The other commands are internal/native Check Point commands that perform various functions. For example: fwaccel on enables SecureXL acceleration on the Security Gateway. fw ctl debug sets the debug flags for the Firewall kernel module. cphaprob displays the status and information about ClusterXL or VRRP members. References: Check Point R81 CLI Reference Guide, pages 11, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27; Check Point R81 Gaia Administration Guide, page 9

QUESTION 15

John is using Management HA. Which Smartcenter should be connected to for making changes?

A. secondary Smartcenter

B. active Smartenter

C. connect virtual IP of Smartcenter HA

D. primary Smartcenter

Correct Answer: B

Management HA is a feature that allows the Security Management server to have one or more backup Standby Security Management servers that are ready to take over in case of failure1. The Active Security Management server is the one that handles all the management operations, such as policy installation, object creation, configuration backup, etc. The Standby Security Management servers are synchronized with the Active Security Management server and store the same data, such as databases, certificates, CRLs, etc. The Standby Security Management servers can also perform some operations, such as fetching a Security Policy or retrieving a CRL1. To make changes to the system, such as editing objects or policies, the administrator needs to connect to the Active Security Management server. This is because the Active Security Management server is the only one that can modify the data and synchronize it with the Standby Security Management servers. The administrator can use SmartConsole to connect to the Active Security Management server by entering its IP address or hostname1. The administrator can also use SmartDashboard to connect to the Active Security Management server by selecting Policy > Management High Availability. This shows information about the Security Management server that includes its peers - displayed with the name, status and type of Security Management server1. The other options are incorrect because:

A. secondary Smartcenter: This is a synonym for a Standby Security Management server, which cannot be used to

make changes to the system. C. connect virtual IP of Smartcenter HA: This is not a valid option because there is no virtual IP for Smartcenter HA. Each Security Management server has its own IP address and hostname.

D. primary Smartcenter: This is a synonym for the Active Security Management server, but it is not the correct term to use. The term primary implies that there is only one Active Security Management server, which is not true. The administrator can put the Active Security Management server on standby and promote a Standby Security Management server to active at any time1. References: How to Configure Management HA