156-315.81 Q&As

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

QUESTION 1

You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

A. fw unloadlocal

B. fw unloadpolicy

C. fwm unload local

D. fwm unload policy

Correct Answer: A

The command fw unloadlocal removes the current security policy from the local gateway and returns it to its initial state2. This command can be used as a last resort to restore traffic flow through the gateway if the policy is causing problems. The command fw unloadpolicy is not valid, and the commands fwm unload local and fwm unload policy are used to remove policies from remote gateways3. References: 2: Check Point Software, Getting Started, Unloading Security Policies;

3: Check Point Software, Getting Started, Unloading Security Policies from Remote Gateways.

QUESTION 2

You have enabled "Full Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.

B. Data Awareness is not enabled.

C. Identity Awareness is not enabled.

D. Logs are arriving from Pre-R81 gateways.

Correct Answer: B

The most likely reason why you are not seeing any data type information in your logs even though you have enabled Full Log as a tracking option to a security rule is that Data Awareness is not enabled on your Security Gateway. Data Awareness is a feature that allows you to monitor and control data types that are transferred over HTTP, HTTPS, FTP, SMTP, POP3, or IMAP protocols. Data Awareness can identify over 700 data types, such as credit card numbers, social security numbers, bank account numbers, medical records, etc., and provide visibility into the data usage patterns of your users. Data Awareness can also enforce data loss prevention (DLP) policies to prevent sensitive data from leaving your network or entering your network from untrusted sources. To enable Data Awareness on your Security Gateway, you need to activate the Data Awareness Software Blade in SmartConsole and install the policy on the Security Gateway.

QUESTION 3

CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

A. MySQL

B. Postgres SQL

C. MarisDB

D. SOLR

Correct Answer: B

CPM process stores objects, policies, users, administrators, licenses and management data in a Postgres SQL database. This database is located in $FWDIR/conf and can be accessed using the pg_client command2. The other options are not the correct database type for CPM. References: Check Point R81 Security Management Administration Guide

QUESTION 4

What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.

B. Security Gateway failover as well as Security Management Server failover is a manual procedure.

C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.

D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

Correct Answer: A

The correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution is: Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure. Security Gateway failover is a feature that allows a cluster of Security Gateways to provide high availability and load balancing for network traffic. If one Security Gateway fails or becomes unreachable, another Security Gateway in the cluster automatically takes over its role and handles the traffic without interrupting the service. Security Management Server failover is a feature that allows a backup Security Management Server to take over the role of the primary Security Management Server in case of failure or disaster. However, this feature requires manual intervention to activate the backup server and restore the database from a backup file.

QUESTION 5

What is false regarding prerequisites for the Central Deployment usage?

A. The administrator must have write permission on SmartUpdate

B. Security Gateway must have the latest CPUSE Deployment Agent

C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.

D. The Security Gateway must have a policy installed

Correct Answer: C

Establishing SIC between gateways and the management server is a prerequisite for Central Deployment usage, as the CDT tool will not take care of this automatically1. The administrator must have write permission on SmartUpdate, the Security Gateway must have the latest CPUSE Deployment Agent, and the Security Gateway must have a policy installed2. These are the basic requirements for using the Central Deployment Tool (CDT), which is a utility that lets you manage a deployment of software packages from your Management Server to the multiple managed Security gateways and cluster members at the same time2. The CDT can perform various actions, such as installation of software packages, taking snapshots, running shell scripts, pushing/pulling files, and automating the RMA backup and restore process2. The CDT is supported on Check Point Appliances with R80.40 and higher versions2. References: How to keep your Security Gateways up to date - Check Point Software, Central Deployment Tool (CDT) - Check Point CheckMates.