Number: 156-836
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 156-836

Exam Name: Check Point Certified Maestro Expert - R81.X

Exam A

QUESTION 1
Maestro allows running commands globally in Expert mode by using global prefixes, such as:

A. asg all
B. g_all
C. all
D. global

Correct Answer: B
Section:
Explanation:
The g_all prefix is used to run commands globally in Expert mode on all Security Group Members of the current Security Group. For example, g_all cpstop will stop the Check Point services on all SGMs. The other prefixes are not valid for global commands in Expert mode.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 4: Using the Command Line Interface and WebUI, Lesson 4.3: Global Commands, page 4-11
* Check Point R81 Maestro Administration Guide, Chapter 4: Using the Command Line Interface and WebUI, Section: Global Commands, page 4-9
* Global Expert Mode Commands - Check Point CheckMates

QUESTION 2
The _____ command will allow users to update the specified file on all SGMs.

A. g_update_conf_file
B. g_all'
C. sed
D. g_cat

Correct Answer: A
Section:
Explanation:
The g_update_conf_file command is a global command that allows users to update the specified file on all Security Group Members of the current Security Group. The command takes the file name and the parameter-value pair as arguments and updates the file accordingly. For example, g_update_conf_file fwkern.conf fwha_enable_arp=1 will add or modify the fwha_enable_arp parameter in the fwkern.conf file on all SGMs.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 4: Using the Command Line Interface and WebUI, Lesson 4.3: Global Commands, page 4-12
* Check Point R81 Maestro Administration Guide, Chapter 4: Using the Command Line Interface and WebUI, Section: Global Commands, page 4-10
* Maestro Commands for Security Groups - Check Point CheckMates

QUESTION 3
What happens when you make changes from Clish on the SMO Master?

A. The changes are synchronized to the SMS/MDS as a backup.
B. The changes are synchronized to the MHO as a backup.
C. Changes are only applied on the SMO Master.
D. Changes are applied to all members in the SG.

Correct Answer: C
Section:
Explanation:
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 2: Maestro Security Groups, Lesson 2.2: Security Group Configuration, page 2-10
* Check Point R81 Maestro Administration Guide, Chapter 2: Maestro Security Groups, Section: Security Group Configuration, page 2-9
* Security Group Configuration - Check Point Software

QUESTION 4
What type of license is required for an MHO?

A. The MHO requires a NGTP license.
B. The MHO requires a VSX license.
C. The MHO does not require a license.
D. A license is needed for each attached SGM.

Correct Answer: C
Section:
Explanation:
The MHO (Maestro Hyperscale Orchestrator) does not require a license by itself, but each SGM (Security Group Module) that is attached to the MHO needs a license. The license type depends on the features and blades that are enabled on the SGM. For example, if the SGM is running VSX, it needs a VSX license.
* Maestro Expert (CCME) Course - Check Point Software, page 71
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline

QUESTION 5
What Maestro component acts as a load balancer and network switch?

A. Security Switching Module (SSM)
B. Maestro Hyperscale Orchestrator (MHO)
C. Security Group (SG)
D. Security Gateway Module (SGM)

Correct Answer: B
Section:
Explanation:
* The Quantum Maestro Orchestrator uses the Distribution Mode to assign incoming traffic to Security Group Members.
*
Reference: Working with the Distribution Mode

QUESTION 6
What is an uplink interface used for?

A. To connect in between appliances
B. To connect appliances to customer's infrastructure
C. To connect Orchestrators to customer's infrastructure
D. To connect in between Orchestrators

Correct Answer: C

Section:
Explanation:
Uplink interfaces are used to connect Maestro Hyperscale Orchestrators (MHOs) to the customer's network infrastructure, such as switches, routers, or firewalls. They are also used to send and receive management and control traffic from the customer's network to the MHOs.
* Maestro Expert (CCME) Course - Check Point Software, page 41
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline

QUESTION 7
When working with Maestro, what is the difference between using Clish and gClish?

A. Clish commands are for testing purposes only and cannot be saved, gClish commands apply to all SG members, by default.
B. Clish commands apply to all UP SG members, by default. gClish commands apply to all SG members, by default.
C. Clish commands are run on the SG members. gClish commands are run on the MHO and applied to all connected SG members in a specified group.
D. Clish commands apply only to a specific SG member. gClish commands apply to all UP SG members, by default.

Correct Answer: C
Section:

QUESTION 8
What cannot be learned from the output of lldpctl?

A. Serial number of Appliance
B. Appliance model
C. Distribution mode
D. Orchestrator's IP

Correct Answer: C
Section:
Explanation:
The lldpctl command is a tool to display information about the devices discovered by the Link Layer Discovery Protocol (LLDP) on all ports of the Maestro Orchestrator and the Security Group Members. LLDP is a protocol that enables devices to exchange information about their identity, capabilities, and configuration. LLDP can help to discover the topology and connectivity of the Maestro environment. The output of lldpctl can show the serial number, appliance model, and orchestrator's IP of the connected devices, but it cannot show the distribution mode of the Security Group. The distribution mode is the algorithm that determines how the Maestro Orchestrator distributes the traffic among the Security Group Members. To view the distribution mode, other commands such as asg monitor or asg stat can be used.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 4: Using the Command Line Interface and WebUI, Lesson 4.2: LLDP, page 4-9
* Check Point R81 Maestro Administration Guide, Chapter 3: Working with Security Group Modules, Section: LLDP, page 3-9
* Check Point R81 Maestro Administration Guide, Chapter 2: Maestro Security Groups, Section: Traffic Distribution, page 2-7
* Maestro basic setup documentation - Page 2 - Check Point CheckMates
* Log and Configuration Files - Check Point Software

QUESTION 9
What is the purpose of Management ports located on the Rear Panel of the Orchestrator MHO-140?

A. 1Gbps connectivity for Security Groups
B. Reserved for internal purposes. Not in use.
C. Out-of-band interfaces for access to Orchestrator itself
D. Additional ports used as uplinks

Correct Answer: C
Section:
Explanation:
The Management ports located on the Rear Panel of the Orchestrator MHO-140 are out-of-band interfaces that provide access to the Orchestrator itself for configuration and management purposes. They are not used for traffic distribution or connectivity to the Security Groups or the external networks. They are 1Gbps RJ-45 ports that can be connected to a switch or a router.
Reference
* Maestro Hyperscale Orchestrator Datasheet - Check Point Software1, page 2
* Quantum Maestro Getting Started Guide - Check Point CheckMates2, page 4

QUESTION 10
There are two 10Gbps dual-port NIC installed on a 6800 appliance. Which interfaces should be connected to Orchestrator 1 for downlinks' intra-orchestrator redundancy when using two Orchestrators?

A. Any pair of available ports
B. Port 1 in Slot 1 and Port 1 in Slot 2
C. Port 1 in Slot 1 and Port 2 in Slot 1
D. Port 1 in Slot 2 and Port 2 in Slot 1

Correct Answer: B
Section:
Explanation:
The correct interfaces to connect to Orchestrator 1 for downlinks' intra-orchestrator redundancy when using two Orchestrators are Port 1 in Slot 1 and Port 1 in Slot 2. This is because each slot represents a different NIC, and each port represents a different physical link. By connecting two ports from different slots, the appliance can have redundant connections to the same orchestrator, and avoid a single point of failure in case of a NIC or link failure.
Reference
* Check Point 156-835 Certification Flashcards | Quizlet1
* Maestro Expert (CCME) Course - Check Point Software, page 182
* Maestro Technical Training, Module 2: Maestro Security Groups and the Single Management Object, slide 163

QUESTION 11
What is one benefit of a Dual MHO environment?

A. Dual MHOs provide redundancy to the Maestro environment by increasing throughput by at least 50 percent.
B. Dual MHOs allow better synchronization to occur between SGMs.
C. Dual MHOs allow additional SGMs to be added to the SG.
D. Dual MHOs can be used to achieve increased scalability and redundancy. .

Correct Answer: D
Section:
Explanation:
One of the benefits of a Dual MHO environment is that it can provide both scalability and redundancy to the Maestro system. Scalability means that the system can handle more traffic and SGMs as the demand grows, and redundancy means that the system can survive the failure of one or more components without losing functionality or performance. Dual MHOs can achieve these benefits by distributing the load and the management tasks among two orchestrators, and by providing backup and failover mechanisms for each other.
Reference
* Maestro Expert (CCME) Course - Check Point Software, page 251
* CheckPoint Certified Maestro Expert (CCME) - Skillzcafe, page 22
* Check Point Certified Maestro Expert (CCME) R81.X, page 23

QUESTION 12
What cannot be a reason for 'Failed to get remote orchestrator interfaces' error message, when clicking on 'Orchestrator' in WebUI

A. Remote orchestrator has no empty interfaces
B. Single orchestrator environment, but configured Orchestrator amount is 2
C. One orchestrator only, but Orchestrator amount is 2 or no Sync in between orchestrators
D. No Sync between orchestrators

Correct Answer: A
Section:
Explanation:
One of the possible reasons for the ''Failed to get remote orchestrator interfaces'' error message, when clicking on ''Orchestrator'' in WebUI, is that the remote orchestrator has no empty interfaces that can be assigned to a security group. This can happen if all the interfaces on the remote orchestrator are already part of configured security groups, or if the remote orchestrator has no physical interfaces at all. In this case, the WebUI cannot display the unassigned interfaces of the remote orchestrator, and shows the error message.
Reference
* Not able to see unassigned interfaces on checkpoint Orchestrator
* Maestro 140 not detecting Interfaces
* Maestro Expert (CCME) Course - Check Point Software, page

QUESTION 13
What Maestro component is automatically designated the SMO Master?

A. The SGM with the lowest member ID (the first one added to the security group.)
B. The MDS that pushes policy to the SMO is considered the SMO Master.
C. The first MHO configured is considered the SMO Master.
D. The SGM with the highest member ID (the last one added to the security group.)

Correct Answer: A
Section:
Explanation:
The SMO Master is the SGM that is responsible for synchronizing the configuration and policy with the other SGMs in the security group. The SMO Master is automatically designated as the SGM with the lowest member ID, which is usually the first one added to the security group. The SMO Master can be changed manually if needed.
* Maestro Frequently Asked Questions (FAQ), under ''What is a Single Management Object (SMO)?''
* Check Point Jump Start Course: Maestro, under ''Maestro Security Groups''

QUESTION 14
What is a downlink interface used for?

A. To connect appliances to Orchestrators
B. To connect appliances to customer's infrastructure
C. To connect in between Orchestrators
D. To connect Orchestrators to customer's infrastructure

Correct Answer: B
Section:

QUESTION 15
What is a security group?

A. A solution for Security Gateway redundancy and Load Sharing.

B. A set of appliances of the same model that are collectively managed by the MHO.
C. A set of network interfaces and individual SGMs assigned to a logical group.
D. A set of objects in SmartConsole that are responsible for enforcing an access policy.

Correct Answer: A
Section:
Explanation:
Security groups are used to simplify management and policy enforcement across multiple devices or network segments, often offering redundancy and load balancing features

QUESTION 16
What is the Orchestrator?

A. Network Switch
B. Manager of compute and network resources, load balancer and network switch
C. Load balancer
D. None of above

Correct Answer: B
Section:
Explanation:
The Orchestrator is a Maestro component that manages the compute and network resources of the Security Group Modules (SGMs) in a Security Group. It also acts as a load balancer and a network switch, distributing traffic among the SGMs and connecting them to the customer's network infrastructure.
* Maestro Expert (CCME) Course - Check Point Software, page 41
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline

QUESTION 17
What is the Correction Layer?

A. Correction Layer is a daemon which corrects errors on Backplane interfaces
B. Correction Layer is a mechanism which handles asymmetric connections in multi-appliance system. For example, in case of NAT
C. Correction Layer is a mechanism which activated in case of asymmetric routing
D. Correction Layer is a Layer of GAIA OS which corrects misspelled commands and allows them to execute

Correct Answer: B
Section:
Explanation:
The Correction Layer is a Maestro component that ensures that packets from the same connection are handled by the same Security Group Module (SGM) in a multi-appliance system. This is especially important when NAT is involved, as packets sent from the client to the server can be distributed to a different SGM than packets from the same session sent from the server to the client. The Correction Layer must then forward the packet to the correct SGM.
* NAT and the Correction Layer on a Security Gateway - Check Point Software1
* Solved: Maestro queries - Check Point CheckMates

QUESTION 18
What is the Correction Layer mechanism?

A. Ensures asymmetric traffic is handled properly, especially in the case of NAT or VPNs.
B. The load-balancing mechanism used by the MHO.
C. The MHO's distribution algorithm which determines the handling SGM for a given connection.

D. Enforces the access policy on the SGMs and synchronizes the enforcement verdict to other SGMs in the SG.

Correct Answer: A
Section:
Explanation:
The Correction Layer mechanism is a Maestro component that ensures that packets from the same connection are handled by the same Security Group Module (SGM) in a multi-appliance system. This is especially important when NAT or VPNs are involved, as packets sent from the client to the server can be distributed to a different SGM than packets from the same session sent from the server to the client. The Correction Layer must then forward the packet to the correct SGM.
* NAT and the Correction Layer on a VSX Gateway - Check Point Software1
* Solved: Maestro queries - Check Point CheckMates

QUESTION 19
What is the maximum number of Appliances within Security group in Dual-Site configuration?

A. 28
B. 31
C. 15
D. 16

Correct Answer: A
Section:

QUESTION 20
At a minimum, how many management and Uplink ports does a SG require?

A. Only one of the two interfaces is needed for the Security Group.
B. Neither are required.
C. Two of each.
D. One each.

Correct Answer: D
Section:
Explanation:
A Security Group (SG) requires at least one management port and one uplink port to function properly. The management port is used to connect the SG to the Maestro Hyperscale Orchestrator (MHO) and the customer's management infrastructure, such as SmartConsole or SmartDomain Manager. The uplink port is used to connect the SG to the customer's network infrastructure, such as switches, routers, or firewalls. The uplink port is also used to send and receive traffic from the customer's network to the SG.
* Maestro Expert (CCME) Course - Check Point Software, page 41
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline

QUESTION 21
What is the maximum number of Appliances within the same Security Group?

A. 31
B. 8
C. 52
D. 16

Correct Answer: A

Section:
Explanation:
The maximum number of appliances within the same security group is 31. This is because a security group can have up to 31 Security Group Modules (SGMs) of the same or different models, and each SGM is an appliance that runs the Check Point software. A security group can span across multiple chassis, and each chassis can have up to 16 SGMs. However, the total number of SGMs in a security group cannot exceed 31.
* Maestro Expert (CCME) Course - Check Point Software, page 51
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline

QUESTION 22
For the MHO-175, which ports are Management ports?

A. Ports 49 - 55 are Management ports.
B. Ports 1 - 4 are Management ports.
C. Ports 27 - 47 are Management ports.
D. Ports 5 - 26 are Management ports.

Correct Answer: B
Section:
Explanation:
According to the Port Mapping for the Check Point Maestro HyperScale Orchestrator MHO-175 document1, ports 1 - 4 are Management ports that are used to connect the MHO to the customer's management infrastructure, such as SmartConsole or SmartDomain Manager. Ports 5 - 26 are Uplink ports that are used to connect the MHO to the customer's network infrastructure, such as switches, routers, or firewalls. Ports 27 - 47 are Downlink ports that are used to connect the MHO to the Security Group Modules (SGMs) in the Security Group. Ports 49 - 55 are Backplane ports that are used to connect the MHO to another MHO in a Dual Orchestrator environment.
* Maestro Expert (CCME) Course - Check Point Software, page 42
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline3
* Port Mapping for the Check Point Maestro HyperScale Orchestrator MHO-1751

QUESTION 23
What kinds of transceivers are supported on Orchestrator MHO-140?

A. SFP, QSFP, QSFP28
B. SFP+, SFP28, QSFP
C. SFP, SFP+, SFP28
D. SFP, SFP+, QSFP, QSFP28

Correct Answer: C
Section:
Explanation:
According to the Maestro Hyperscale Orchestrator Datasheet1, the Orchestrator MHO-140 supports the following transceiver types: SFP, SFP+, SFP28. These transceivers can be used for the management, uplink, and downlink ports of the Orchestrator. The SFP transceivers support 1 GbE, the SFP+ transceivers support 10 GbE, and the SFP28 transceivers support 25 GbE.
* Maestro Expert (CCME) Course - Check Point Software, page 42
* Check Point Certified Maestro Expert (CCME) R81.X - Global Knowledge, course outline3
* Maestro Hyperscale Orchestrator Datasheet - Check Point Software, page 2

QUESTION 24
What happens if the SMO Master fails?

A. The next SGM with the current lowest SGM ID assumes the role of the SMO Master.
B. The Backup SMO Master will take over in the event of a failure with the SMO Master.
C. A failover will occur on the MHO and traffic will continue to pass.

D. The Security Group will no longer pass traffic and the issue must be resolved with the SMO Master.

Correct Answer: B
Section:
Explanation:
The SMO Master is the SGM that is responsible for managing the Security Group and communicating with the MHO. If the SMO Master fails, the Backup SMO Master, which is the SGM with the next lowest SGM ID, will take over the role of the SMO Master and ensure the continuity of the Security Group operations.
Reference=Maestro Expert (CCME) Course - Check Point Software, page 14;Check Point Accredited Maestro Expert - New exam a... - Check Point CheckMates, page 1.

QUESTION 25
What does the lldpctl command do?

A. Show all devices discovered by LLDP protocol on downlink ports
B. Show all devices discovered by LLDP protocol on all ports
C. Discover orchestrators
D. Show all devices discovered by LLDP protocol on uplink ports

Correct Answer: B
Section:
Explanation:
The lldpctl command is a tool to display information about the devices discovered by the Link Layer Discovery Protocol (LLDP) on all ports of the Maestro Orchestrator and the Security Group Members. LLDP is a protocol that enables devices to exchange information about their identity, capabilities, and configuration. LLDP can help to discover the topology and connectivity of the Maestro environment.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 4: Using the Command Line Interface and WebUI, Lesson 4.2: LLDP, page 4-9
* Check Point R81 Maestro Administration Guide, Chapter 3: Working with Security Group Modules, Section: LLDP, page 3-9

QUESTION 26
There are two appliances within the same Security Group. One of them is connected by One downlink only, another one by Two downlinks. Assuming there's no NAT and no VPN, what would be proportion of traffic distribution done by Orchestrator?

A. 100%/0%
B. 33%/66%
C. 50%/50%
D. 66%/33%

Correct Answer: B
Section:

QUESTION 27
While looking at your system's correction statistics, you notice you have a correction rate approaching 100 percent. Is this a problem?

A. A correction rate above 90 percent indicates a need to disable Layer 4 Distribution.
B. A correction rate approaching 100 percent of all connections is unusual. This is a cause for concern because the SGMs may fail to process traffic.
C. If correction rates are higher than 80 percent, latency is expected.
D. In some scenarios, a correction rate approaching 100 percent of all connections is not unusual. This is not usually a cause for concern as the correction mechanism is fast and efficient.

Correct Answer: D
Section:

Explanation:
The correction rate is the percentage of connections that require correction by the correction layer, which is a mechanism that ensures that the traffic is processed by the correct SGM in the Security Group. The correction rate depends on the distribution mode (Layer 3 or Layer 4) and the traffic pattern. In some scenarios, such as when the traffic is asymmetric or when the distribution mode is Layer 4, the correction rate can approach 100 percent of all connections.This is not a problem, as the correction layer is designed to handle such situations without affecting the performance or availability of the Security Group1.
Reference=Maestro Expert (CCME) Course - Check Point Software, page 16.

QUESTION 28
What type of cluster can a Security Group can be compared to?

A. Load Sharing Active / Active
B. VSLS
C. Active / Backup
D. Active / Standby

Correct Answer: A
Section:
Explanation:
A Security Group can be compared to a Load Sharing Active / Active cluster because it consists of multiple Security Group Members that share the traffic load and provide high availability and scalability. Each Security Group Member is an active firewall that processes traffic according to the Security Group policy and synchronizes its state with other members. The Maestro Orchestrator acts as a load balancer that distributes the traffic among the Security Group Members based on their capacity and availability.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 2: Maestro Security Groups, Lesson 2.1: Introduction to Security Groups, page 2-4
* Check Point R81 Maestro Administration Guide, Chapter 2: Maestro Security Groups, Section: Security Group Overview, page 2-3

QUESTION 29
What kinds of transceivers are supported on Orchestrator MHO-170?

A. SFP, QSFP, QSFP28
B. SFP+, SFP28, QSFP
C. SFP, SFP+, SFP28
D. QSFP, QSFP28

Correct Answer: D
Section:
Explanation:
The Orchestrator MHO-170 supports QSFP and QSFP28 transceivers on its 32x 100 GbE ports. QSFP stands for Quad Small Form-factor Pluggable and QSFP28 is an enhanced version of QSFP that supports up to 28 Gbps per lane. These transceivers can provide high-speed and high-density connectivity for the Maestro environment.
Reference
* Maestro Hyperscale Orchestrator Datasheet - Check Point Software1, page 2
* Maestro Transceiver & DAC Inventory - Check Point CheckMates

QUESTION 30
There are two 10Gbps dual-port NICs and one 40Gbps NIC installed on a 23800 Appliance in slots 1, 2 and 3 accordingly. Which interfaces should be connected to Orchestrator 1 for downlinks' intra-orchestrator redundancy when using two Orchestrators?

A. Port 1 in Slot 2 and Port 2 in Slot 1
B. This configuration is not supported
C. Any pair of available ports

D. Port 1 in Slot 1 and Port 2 in Slot 1

Correct Answer: D
Section:
Explanation:
This configuration likely provides balanced and redundant connectivity for orchestrator redundancy.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 3: Dual Orchestrator Environment, Lesson 3.1: Introduction to Dual Orchestrator Environment, page 3-7
* Check Point R81 Maestro Administration Guide, Chapter 3: Working with Security Group Modules, Section: Downlinks, page 3-8
* Check Point 23800 Appliance Datasheet - Check Point Software, page 2

QUESTION 31
Which licenses should be issued for the Orchestrator?

A. No licenses are required for Orchestrator
B. Depends on Software Blades enabled on connected appliances
C. The Orchestrator is considered a Management server, hence it's licensed the same way
D. The Orchestrator requires NGTX license

Correct Answer: A
Section:
Explanation:
Orchestrators in many network environments do not require separate licenses, as they primarily function to manage and distribute network traffic.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 1: Introduction to Check Point Maestro, Lesson 1.2: Maestro Licensing, page 1-8
* Check Point R81 Maestro Administration Guide, Chapter 1: Introduction to Check Point Maestro, Section: Maestro Licensing, page 1-6
* Activation of a Quantum Maestro Orchestrator - Check Point Software

QUESTION 32
When security policy is installed

A. All SGMs receive the security policy and one by one performs an independent policy verification. Then, all SGMs simultaneously install the policy.
B. The SMO Master receives the policy and performs a policy verification the policy is installed on the SMO Master, the SMO Master broadcasts the available package, other members retrieve the new policy from the SMO Master, then the non-SMO Master SGMs install the policy.
C. All SGMs receive the security policy and simultaneous policy installation occurs.
D. The policy is installed on the SMO, the SMO Master broadcasts the available package, other members retrieve the new policy from the SMO Master and perform an independent policy verification, then the non-SMO Master SGMs install the policy.

Correct Answer: B
Section:
Explanation:
This is the correct answer because it describes the security policy installation flow for a Maestro Security Group. The SMO Master is the Security Group Member that acts as the leader and the single point of contact for the Management Server. The SMO Master verifies the policy and installs it first, then notifies the other SGMs that a new policy is available. The other SGMs fetch the policy from the SMO Master and install it in parallel.
Reference
* Check Point Certified Maestro Expert (CCME) R81.X Courseware, Module 2: Maestro Security Groups, Lesson 2.3: Security Policy Installation, page 2-15
* Check Point R81 Maestro Administration Guide, Chapter 2: Maestro Security Groups, Section: Security Policy Installation, page 2-13
* Policy installation flow - Check Point Software

QUESTION 33

What cannot be learned from the output of asg monitor command?

A. Uptime
B. Port status
C. Security Policy status
D. Appliances cluster status

Correct Answer: D
Section:

QUESTION 34
What happens if you apply a hotfix using gClish?

A. If you apply a hotfix using gclish, it causes an outage for the entire SG as all members reboot at roughly the same time.
B. If you apply a hotfix using gclish, each SG members installs the hotfix and reboots after waiting it's turn to do so.
C. Logical groups 'A' and 'B' are created. Members of group 'A' install and reboot first. Then members of group 'B' does the same once reboots have finished with group 'A.'
D. If you apply a hotfix using gclish, the operation will fail because an outage would occur.

Correct Answer: B
Section:
Explanation:
According to theInstalling and Uninstalling a Hotfix on Quantum Maestro Orchestrators, page 1, when you apply a hotfix using gclish, the MHO distributes the hotfix to all SGMs in the Security Group. The SGMs install the hotfix and reboot one by one, in ascending order of their SGM IDs. The SGMs wait for the previous SGM to finish rebooting before starting their own reboot. This ensures that there is no outage for the entire Security Group.
Reference=Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators, page 1;Maestro R81.10 Jumbo Hotfix install - Check Point CheckMates, page 1.

QUESTION 35
What type of license is required for an MHO?

A. The MHO requires a NGTP license.
B. The MHO requires a VSX license.
C. The MHO does not require a license.
D. A license is needed for each attached SGM.

Correct Answer: D
Section:
Explanation:
For Quantum Maestro setups, an individual license is required for each appliance in the Security Group1.This applies to both regular appliances and appliances with MHO SKUs2.
Reference=Maestro Frequently Asked Questions (FAQ) - Check Point Software,Solved: license maestro - Check Point CheckMates,Check Point License Guide - Check Point Software.

QUESTION 36
What is a security group?

A. A solution for Security Gateway redundancy and Load Sharing.
B. A set of appliances of the same model that are collectively managed by the MHO.
C. A set of network interfaces and individual SGMs assigned to a logical group.
D. A set of objects in SmartConsole that are responsible for enforcing an access policy.

Correct Answer: B
Section:
Explanation:
A security group is a scalable network security system that connects multiple Check Point security appliances into a unified system. It is represented by a single management object (SMO) in SmartConsole and consists of security gateway modules (SGMs) that share the same security policy, configuration, software versions, and routing information.
Reference=Check Point Maestro Hyperscale Network Security,Maestro Frequently Asked Questions (FAQ) - Check Point Software,Introducing Maestro -- The Industry's First Hyperscale Network Security Solution - Check Point Blog.