

Check Point Certified Maestro Expert (CCME) R81.X

Checkpoint 156-836

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Maestro Overview	5
Topic 2, Maestro Components	23
Topic 3, Maestro Security Groups	25
Topic 4, Maestro Configuration	14
Topic 5, Maestro Management	12
Topic 6, Maestro Troubleshooting	28
Total	107

QUESTION NO: 1

In a Maestro Dual Site environment, what is the definition of the term Active Site.

- A. The Active Site is the site that is not handling any traffic for the specific SG, but its connections are synced to its SGMs from the MHOs to be ready in the event of a failover.
- B. The Active Site is the site where the SMO Master exists.
- C. There is no such thing as an active site. In a Dual Site environment, traffic is load balanced.
- D. The Active Site is the site currently handling the enforcement on traffic passing for a specific SG.

ANSWER: D

Explanation:

The Active Site is the site currently handling the enforcement on traffic passing for a specific SG. In a Maestro Dual Site deployment, the active/standby designation is evaluated per Security Group rather than being a blanket designation for every Security Group at an entire physical site. For a given Security Group, the Active Site contains the active Security Group Members that process and enforce the traffic flow. This includes applying the installed Access Control, Threat Prevention, and other relevant security policies while maintaining the live connection state required for ongoing traffic handling.

This per-Security-Group model provides operational flexibility: different Security Groups can have their enforcement role assigned according to the Dual Site design and configured resiliency behavior. The term therefore identifies the location presently responsible for traffic enforcement for that particular Security Group. Check Point's Scalable Platforms documentation describes Maestro architecture, Security Groups, and the Dual Site operational model in the [R81.20 Scalable Platforms Administration Guide](#). Current Check Point technical documentation and product guides are also available through the [Check Point Maestro documentation resources](#).

QUESTION NO: 2

In a Maestro Dual Site environment, what is the definition of the term Active Site.

- A. The Active Site is the site that is not handling any traffic for the specific SG, but its connections are synced to its SGMs from the MHOs to be ready in the event of a failover.
- B. The Active Site is the site where the SMO Master exists.
- C. There is no such thing as an active site. In a Dual Site environment, traffic is load balanced.
- D. The Active Site is the site currently handling the enforcement on traffic passing for a specific SG. Connections are synced within the SGMs in the Active Site.

ANSWER: D

Explanation:

The Active Site is the site currently handling the enforcement on traffic passing for a specific SG. Connections are synced within the SGMs in the Active Site. In a Maestro Dual Site deployment, each Security Group has an operational role assignment across the two physical sites. The Active Site is the location whose Security Group Members are actively receiving and enforcing policy on that Security Group's production traffic. This designation is made per Security Group, rather than being a universal designation for the entire Maestro deployment, so one Security Group may be active at one site while another Security Group is active at the other site. The active Security Group maintains the relevant connection state among its members to support scalable firewall processing. Dual Site also provides a standby counterpart at the alternate location so that the Security Group can continue service following a site failure or a controlled switchover. Consequently, "active" describes the current traffic-enforcement role for the specific Security Group, not the physical location of the SMO Master and not a general traffic-load-balancing state. Check Point's Maestro Administration Guide describes Dual Site operation and Security Group site roles in its [Maestro Dual Site documentation](#). Additional product documentation is available from the [Check Point documentation portal](#).

QUESTION NO: 3

Where should `sx_api_ports_dump.py` command be ran?

- A. Management server
- B. Security Group
- C. Orchestrator
- D. SMO Appliance

ANSWER: C

Explanation:

`sx_api_ports_dump.py` should be run on the **Orchestrator**. In a Check Point Maestro deployment, the Orchestrator provides the control-plane services used to manage the Maestro environment and communicate with Security Groups. The script is an Orchestrator-side diagnostic utility intended to display information about the API-related ports used by the Maestro infrastructure. Running it in the Orchestrator context ensures that it can access the relevant local configuration, processes, and port mappings that the utility is designed to inspect.

This aligns with the Maestro architecture, in which Orchestrators centrally coordinate Security Groups and expose management and operational services. Before running operational scripts, connect to the appropriate Orchestrator through its Gaia command-line interface and use the applicable administrative privileges. For general Maestro architecture and Orchestrator responsibilities, see the [Check Point Maestro Administration Guide](#). Check Point's [Support Center](#) also provides the applicable Maestro release documentation and maintenance guidance for diagnostic commands.

QUESTION NO: 4

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

ANSWER: D

Explanation:

QSFP, QSFP28 is correct. The Maestro Hyperscale Orchestrator MHO-170 provides thirty-two high-speed 100 GbE interfaces designed for Quad Small Form-factor Pluggable family optics. These ports support QSFP-based transceivers for 40 GbE connectivity and QSFP28 transceivers for 100 GbE connectivity. QSFP28 retains the QSFP physical form factor while enabling four lanes that operate at up to 28 Gb/s each, allowing a 100 GbE Ethernet link. This hardware design gives the MHO-170 the dense, high-bandwidth interconnect capability required to connect Maestro Security Groups and upstream or downstream network infrastructure. Selecting optics from the QSFP/QSFP28 family also ensures that the transceiver form factor matches the physical cages and port speeds implemented on the appliance. Administrators should use Check Point-supported and compatible optical modules or DAC cables for the intended link speed and media type, and should confirm supported parts against the platform documentation and compatibility information before deployment. See Check Point's [Maestro product information](#) and the [Check Point Maestro community resources](#) for platform and deployment guidance.

QUESTION NO: 5

A network team proposes NAT between the Security Group Members and the management network because the existing management address ranges overlap. What is the expected effect on this management traffic?

- A. The traffic is dropped and does not pass correction.
- B. The Orchestrator automatically bypasses NAT for management traffic.
- C. The SMO Master corrects the translated traffic and redistributes it to the other members.
- D. The traffic passes without inspection because management traffic is trusted.

ANSWER: A

Explanation:

Management-network traffic that is NATed is dropped and does not pass through the Maestro correction mechanism. The management network is a dedicated control and administration path, not a normal production-data path on which NAT correction can be expected.

The Orchestrator does not disable NAT automatically, and the SMO does not redistribute translated management traffic. The management design must provide the required routable connectivity without relying on Maestro correction for NATed management flows.

QUESTION NO: 6

Two Maestro HyperScale Orchestrators are deployed for redundancy. During a maintenance activity, one MHO is taken offline while the other remains healthy and connected to the Security Group Members. Which operating characteristic allows the remaining MHO to continue participating in traffic handling?

- A. The MHOs process traffic in Active-Standby mode.
- B. The MHOs process traffic in Active-Active mode.
- C. The MHOs process traffic in VSLS mode.
- D. The MHOs process traffic only after an SMO Master election.

ANSWER: B

Explanation:

Maestro HyperScale Orchestrators process traffic in Active-Active mode. Both MHOs can participate in the traffic-distribution fabric during normal operation, rather than one being reserved as an inactive standby unit.

Consequently, the surviving healthy MHO can continue traffic handling when its peer is unavailable, subject to the physical connectivity and topology being intact. This is different from an Active-Standby model, in which the standby device would normally not process production traffic before a failure.

QUESTION NO: 7

During a maintenance window, an administrator must observe current throughput and traffic distribution across all active appliances in one Security Group without capturing packet payloads. Which command should be used?

- A. `asg monitor`
- B. `g_tcpdump`
- C. `asg diag`
- D. `orch_stat -p`

ANSWER: A

Explanation:

`asg monitor` is used to monitor traffic handled by appliances in a Security Group. Its continuously updating output is useful for observing current traffic load and the distribution of traffic among active Security Group Members.

`g_tcpdump` is used for packet capture, not normal throughput monitoring. `asg diag` is a diagnostic utility, and `orch_stat -p` is used to inspect Orchestrator port-related information.

QUESTION NO: 8

Which command is used to set the number of sites in a Maestro environment?

- A. `set maestro orchestrator-site-amount`
- B. `set maestro configuration orchestrator-site-amount`
- C. `set maestro configuration orchestrator-site-number`
- D. `set maestro configuration orchestrator-site-id`

ANSWER: B**Explanation:**

The correct command is `set maestro configuration orchestrator-site-amount`. In a Check Point Maestro deployment, this global Maestro configuration setting defines how many Orchestrator sites participate in the environment. The supported site amounts are one or two, with one being the default. Configuring two sites enables the relevant multi-site behavior, including the site synchronization design and the failover policies used by Security Groups and Security Group Members.

This setting must be planned early because it is intended to establish the Maestro topology before Security Groups are provisioned. Check Point documentation specifies that the site amount can be changed only before creation of the first Security Group. Consequently, an administrator should set the intended value during initial Maestro configuration, verify it as part of the deployment design, and only then create Security Groups and onboard Security Group Members. The command belongs under the Maestro `configuration` command hierarchy, and the parameter name is specifically `orchestrator-site-amount`.

For Maestro architecture and initial configuration guidance, see the [Check Point R81.10 Scalable Platforms Administration Guide](#) and Check Point's [Maestro product documentation overview](#).

QUESTION NO: 9

What command should be used for collecting diagnostic information about the orchestrator?

- A. `cpinfo`
- B. `asg perf -v`
- C. `cpview`
- D. `orch_info`

ANSWER: A**Explanation:**

`cpinfo` is the appropriate command because it creates a comprehensive diagnostic-information package for Check Point Support analysis. On a Maestro Orchestrator, this package gathers relevant system and product details, including configuration data, installed software information, logs, and other troubleshooting artifacts. The resulting archive is intended to provide a consistent snapshot of the appliance's state when investigating operational issues or preparing a Service

Request. Check Point documents `cpinfo` as its standard information-collection utility and describes the generated output as support data that can be transferred to Check Point for diagnosis. This makes it the correct operational command when the requirement is to collect diagnostic information rather than merely inspect a current performance view or display a limited subset of platform information. Run the command from the Orchestrator CLI with the privileges required by the appliance's administrative procedures, then retain or upload the generated package according to the Support engineer's instructions. See Check Point's [R81 CLI Reference Guide entry for cpinfo](#) and the [Maestro R81 Getting Started Guide](#).

QUESTION NO: 10

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.

ANSWER: D

Explanation:

Changes made from Clish on the SMO Master are applied to all members in the Security Group. In a Maestro Security Group, the SMO Master is the designated member through which Security Group-level Gaia configuration is administered. Maestro distributes the applicable configuration changes from that master to the other Security Group Members so that the members remain operationally consistent as one scalable gateway system. This centralized configuration behavior is important because the Security Group forwards traffic collectively; network and system settings that must be common across members are managed from the SMO Master rather than configured independently on each member. Administrators should therefore make intended Security Group configuration changes while connected to the current SMO Master and allow the synchronization process to complete. For configuration that is specifically local to an individual appliance or interface context, administrators must follow the applicable Maestro configuration procedure, but ordinary Security Group Clish administration performed on the SMO Master is propagated throughout the Security Group. Check Point's Maestro product overview describes the Security Group architecture and centralized management model: [Check Point Quantum Maestro](#). The official documentation library, including the Maestro Administration Guide, is available at [Check Point Documentation](#).