DUMPSARENA

Oracle Communications Session Border Controller 7 Basic Implementation Essentials

Oracle 1z0-404

Version Demo

Total Demo Questions: 9

Total Premium Questions: 96

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (SIMULATION)

Which statement is true about the Host In Path (HIP) feature In the Session Border Controller?

A) By default, the Session Border Controller's FTP, ICMP, SNMP, and Telnet services cannot be accessed via the management interfaces.

B) To enable these services (FTP ICMP, SNMP, and Telnet services), the enable host-in-path command must be executed from the superuser mode.

C) To enable these services, the Session Border Controller includes a software license that enables administrative traffic over the media interfaces.

D) By default, the Session Border Controller's FTP, ICMP, SNMP, and Telnet services cannot be accessed via the media interfaces.

E) These four fields (FTP, ICMP, SNMP, and Telnet services) are collectively known as the Host Interface Priority.

ANSWER: Check the explanation for the answer

Explanation:

Correct answer: D) By default, the Session Border Controller's FTP, ICMP, SNMP, and Telnet services cannot be accessed via the media interfaces.

The *Host In Path (HIP)* feature controls whether traffic destined for the SBC itself (host services such as FTP, ICMP, SNMP, and Telnet) is permitted through media-side interfaces. For security, these host services are disabled on media interfaces by default. HIP can be configured when administrative access through a media interface is required.

QUESTION NO: 2

You made a configuration change to a media interface.

Which command must be executed to commit the change to volatile (RAM) memory?

A. From configuration mode, execute the done command.

B. From superuser mode, execute the write-config command.

C. From user mode, execute the save-config command.

D. From user mode, execute the commit-config command.

E. From superuser mode, execute the save-config command.

ANSWER: A

Explanation:

`From configuration mode, execute the done command.` is correct because `done` completes editing of the current configuration object—in this case, the media interface—and applies the entered values to the SBC's active configuration in volatile memory. In the ACLI's hierarchical configuration workflow, a change is not fully accepted for the edited object until the administrator exits that object with `done`. The updated setting can then take effect as part of the running configuration.

This action concerns the active, RAM-resident configuration, rather than preserving the configuration through a reboot. Persisting accepted configuration changes is a separate operation performed after the relevant configuration objects have been completed. Oracle's ACLI documentation describes using `done` to finish configuration-element editing and return to the parent configuration level, with the entered configuration becoming active. This distinction between completing an edit and saving persistent configuration is important when administering media interfaces, because interface addressing and port settings must first be accepted by the running system before they can be retained for subsequent restarts. See Oracle's ACLI Configuration Basics documentation and the Media Interfaces configuration documentation.

QUESTION NO: 3

Which three options are valid ways to apply Header Manipulation Rules (HMRs) to your existing configuration?

A. Navigate to the network-interface configuration element and configure the in-manipulationid parameter.

B. Navigate to the session-agent configuration element and configure the in-manipulationid parameter.

C. Navigate to the sip-interface configuration element and configure the in-manipulationid parameter.

D. Navigate to the session-agent configuration element and configure the in-manipulationid parameter.

E. Navigate to the session-group configuration element and configure the in-manipulationid parameter.

ANSWER: B C D E

Explanation:

HMRs are associated with SIP signaling processing points, allowing the Oracle Communications Session Border Controller to select and execute a named manipulation set as messages enter the SBC. A SIP interface is a valid attachment point because it identifies a SIP-facing ingress context, and its `in-manipulationid` parameter specifies the HMR set to apply to inbound SIP messages. A session agent is also a valid attachment point; configuring its `in-manipulationid` associates the named rule set with signaling received from that peer. Finally, a session group can carry an inbound manipulation identifier so that inbound signaling associated with the group can receive the configured treatment. The question contains a duplicated session-agent option; because both entries have identical text, both have the same technically correct truth value. These configuration associations let an implementation apply header transformations in the appropriate SIP routing or peer context while retaining reusable, centrally defined manipulation rules. Oracle documents HMR configuration and the use of manipulation identifiers in its SBC documentation: Oracle Communications SBC Header Manipulation Rules and Oracle Communications SBC ACLI Configuration Reference.

QUESTION NO: 4

You finished configuring a not Real Time Change (not RTC)-supported configuration element and you want to apply the change in your service.

Which two options are valid in order to accomplish this? (Choose two.)

A. From user mode, execute the save-config and activate-config commands.

B. From configuration mode, execute the save-config, activate-config, and reboot commands.

C. From superuser mode, execute the save-config and activate-config and reboot commands.

D. From superuser mode, execute the save-config and activate-config commands.

E. From superuser mode, execute the save-config, activate-config, and reboot force commands.

ANSWER: C E

Explanation:

A configuration change to an element that is not Real-Time Change (RTC) supported cannot become operational solely by saving and activating the configuration. The configuration must first be saved so that the edited running configuration is written to the system's saved configuration, and then activated to make that saved configuration the active boot configuration. Because the changed element is not RTC-capable, a system reboot is required before the SBC can instantiate the changed setting in service.

"From superuser mode, execute the save-config and activate-config and reboot commands." is valid because it completes the required save, activation, and normal restart sequence. "From superuser mode, execute the save-config, activate-config, and reboot force commands." is also valid because `reboot force` is the forced-reboot form of the reboot operation and likewise restarts the system so that non-RTC changes take effect. Operationally, the forced form should be used with appropriate awareness of its service impact.

Oracle's SBC documentation describes the ACLI configuration lifecycle, including saving and activating configuration, and identifies that non-RTC changes require a reboot to take effect. See the Oracle Communications Session Border Controller ACLI Configuration Guide and the Oracle Communications Session Border Controller documentation library.

QUESTION NO: 5

You are configuring the boot parameters in the Session Border Controller.

Which three statements are true about the boot parameters? (Choose three.)

A. A reboot is always required to apply any change to the boot parameters.

B. The target name is used for domain name resolution.

C. The system clock is a boot parameter.

D. The boot parameters are stored in Non-Volatile Random Access Memory (NVRAM).

E. The boot parameters are not affected by the activate-config command.

ANSWER: A D E

Explanation:

Boot parameters are the low-level startup settings the Oracle Communications Session Border Controller needs before its normal configuration can be loaded. They are retained in nonvolatile memory (NVRAM), so essential startup information such as management-network boot settings persists across a power cycle. Because these parameters control the boot environment, a reboot is required for a changed boot parameter to be used by the running system. This is distinct from ordinary configuration changes, which can be made active using the configuration activation process.

The `activate-config` command operates on the saved SBC configuration; it does not alter the separately maintained boot-parameter values. Consequently, boot parameters remain unaffected when a configuration is activated. This separation ensures that configuration activation cannot inadvertently replace the management and startup information required to boot and access the SBC. Oracle's SBC documentation describes boot parameters as startup-specific settings and treats boot-parameter configuration separately from the standard ACLI configuration activation workflow. See the Oracle Communications Session Border Controller documentation library and the Oracle SBC ACLI Reference.

QUESTION NO: 6

You are configuring access rules in a Session Border Controller Peering architecture.

Which configuration step is required to allow access from any User Agent (UA)?

A. Navigate to the sip-port configuration element and set the allow-anonymous parameter to all.

B. Navigate to the realm-config configuration element and set the addr-prefix parameter to the IP subnet of your trusted User Agent (UA).

C. Navigate to the sip-port configuration element and set the allow-anonymous parameter to address-prefix.

D. Navigate to the session-agent configuration element and set the ip-address parameter to the IP subnet of your trusted User Agent (UA).

E. Navigate to the sip-port configuration element and set the allow-anonymous parameter to agents-only.

ANSWER: A

Explanation:

Navigate to the sip-port configuration element and set the allow-anonymous parameter to all. This setting instructs the Oracle Communications Session Border Controller to accept SIP requests from any User Agent rather than limiting

anonymous access to defined session agents, registered endpoints, or sources matched through address-prefix access controls. In a peering deployment, the SIP port is the appropriate configuration location because it governs how inbound SIP traffic arriving on that port is admitted before more specific routing and policy processing occurs. The value `all` is specifically intended for unrestricted anonymous SIP access, making it the required setting when the requirement is to permit access from any UA regardless of its source address or prior endpoint definition. This setting should be applied deliberately, since allowing any UA broadens the set of systems that can send SIP signaling to the SBC; production deployments normally pair such access with suitable security, topology, and signaling-policy controls. Oracle's Session Border Controller documentation provides configuration guidance and product documentation at Oracle Communications Session Border Controller documentation. Oracle's communications product documentation portal is also available at Oracle Communications documentation.

QUESTION NO: 7

Which two statements correctly describe SIP response classes? (Choose two.)

A. A 1xx response is a provisional response.

B. A 2xx response is a successful final response.

C. A 3xx response indicates a successful session establishment.

D. A 4xx response is a provisional response.

E. A 6xx response applies only to the session agent that generated it.

ANSWER: A B

Explanation:

A 1xx response is a provisional response. It indicates that the request has been received and that processing is continuing, but it does not complete the SIP transaction. Examples include 100 Trying and 180 Ringing.

A 2xx response is a successful final response. For example, 200 OK indicates that the request was successfully processed. Responses in the 4xx class represent client failure conditions, while 5xx responses represent server failure conditions. See RFC 3261, section 21.

QUESTION NO: 8

What is the first thing you should do when you want the Session Border Controller to detect that an endpoint is behind a NAT/firewall device?

A. Navigate to the sip-port configuration element and set the nat-traversal parameter to disabled.

B. Navigate to the sip-interface configuration element and set the nat-traversal parameter to never.

C. Navigate to the sip-interface configuration element and set the nat-traversal parameter to always.

D. Navigate to the sip-port configuration element and set the nat-traversal parameter to enabled.

E. Navigate to the sip-interface configuration element and set the nat-traversal parameter to detect.

ANSWER: C

Explanation:

Navigate to the sip-interface configuration element and set the nat-traversal parameter to always. NAT traversal behavior is configured on the SIP interface because that is where the Oracle Communications Session Border Controller processes SIP signaling received from the applicable network side. Setting `nat-traversal` to `always` instructs the SBC to perform NAT-traversal processing for SIP endpoints on that interface, allowing it to identify and accommodate endpoints whose SIP message addressing does not correspond to the address from which signaling is received. This is the appropriate initial

configuration when endpoints may be located behind NAT or firewall devices and the SBC must apply its address-handling logic consistently. NAT devices commonly alter address and port information in transit, so signaling equipment needs NAT-aware processing to maintain reachable SIP and media routing. Oracle's Session Border Controller documentation is available through the Oracle Communications Session Border Controller documentation library. The general network behavior and requirements associated with NAT are also described in RFC 4787, Network Address Translation Behavioral Requirements.

QUESTION NO: 9

You are examining a SIP packet. There is no final response to the ACK method.

What is the reason for this?

A. The ACK method was defined only in RFC 2543 and it has been deprecated.

B. The ACK method is part of the INVITE transaction.

C. The ACK method is an exception in RFC 3261.

D. The ACK method is an optional SIP method.

E. The ACK method was replaced with the CANCEL method in RFC 3261.

ANSWER: B

Explanation:

The ACK method is part of the INVITE transaction. SIP uses ACK to confirm that a User Agent Client has received a final response to an INVITE, so ACK is not a request for which the receiving endpoint sends another final SIP response. This avoids creating an acknowledgment loop, such as a response requiring another acknowledgment. RFC 3261 specifies that ACK is used for both successful and non-successful final responses to INVITE, with slightly different transaction handling depending on whether the INVITE final response was a 2xx response. For a non-2xx final response, the ACK is handled within the INVITE client/server transaction state machines. For a 2xx response, ACK is a separate end-to-end request, but it still does not receive a response. In either case, observing no final response to an ACK in a SIP trace is therefore expected protocol behavior, not evidence of a missing packet or failed SIP processing. The relevant SIP transaction behavior is defined in RFC 3261 section 17, while ACK handling for INVITE responses is described in section 13.2.2.4. See RFC 3261, section 17 and RFC 3261, section 13.2.2.4.