Vendor: Avaya

Exam Code:71301X

Exam Name: Avaya Aura Communication Applications Implement Certified Exam

Version: Demo

QUESTION 1

When deploying a Survivable Communication Manager (CM), which statement about the Server ID value is true?

A. The Server ID of a Survivable CM needs to match the server ID of the Main CM. The Server IDs must be an even/odd pair (N, N+l).

B. Every CM server in the network needs to be assigned a unique Server ID including servers in a duplex pair.

C. Every CM server in the network needs to be assigned a unique server ID, but both servers in a duplex pair must have the same Server ID.

D. The Server ID Is a value found in the license file.

Correct Answer: B

QUESTION 2

The customer plans to have 50 SIP Trunks and 100 Remote Workers supported by the Avaya Session Border Controller for Enterprise (ASBCE). How many ASBCE licenses will they require?

A. 150 standard services licenses, and 150 advanced services licenses

B. 50 standard services licenses, and 100 advanced services licenses

C. 150 standard services licenses

D. 150 standard services licenses, and 100 advanced services licenses

Correct Answer: B

The Avaya Session Border Controller for Enterprise (ASBCE) requires licenses to support different types of services, such as SIP Trunking or Remote Worker. The ASBCE licenses are based on the number of concurrent sessions that are handled by the ASBCE server. There are two types of licenses: standard services licenses and advanced services licenses. A standard services license is required for each SIP Trunking session, which is a session between the ASBCE server and a SIP service provider. An advanced services license is required for each Remote Worker session, which is a session between the ASBCE server and a remote endpoint, such as an IP phone or a softphone. Therefore, if the customer plans to have 50 SIP Trunks and100 Remote Workers supported by the ASBCE, they will need 50 standard services licenses and 100 advanced services licenses.

QUESTION 3

When in System Manager (SMGR), which statement about enabling IM and Presence for an Avaya Aura user is true?

A. Edit the Communication Profile of the user to assign an Avaya Presence/IM handle and enable and configure the Presence profile.

B. Edit the Communication Profile of the user to assign an Avaya E.164 handle and enable and configure the Presence profile.

C. Edit the Communication Profile of the user to assign a XMPP handle and enable and configure the Presence profile.

D. Edit the Communication Profile of the user to assign an Avaya SIP handle and enable and configure the Presence profile.

Correct Answer: A

To enable IM and Presence for an Avaya Aura user, you need to edit the Communication Profile of the user in System Manager, under Users > User Management > Manage Users. In the Communication Profile tab, you need to assign an Avaya Presence/IM handle to the user, which is a unique identifier that follows the format username@domain.com. You also need to enable and configure the Presence profile for the user, which specifies the Presence Services snap-in that will provide presence and instant messaging features for the user.

QUESTION 4

Which statement about the Avaya Aura Media Server (AAMS) associated with the Avaya Aura Web Gateway (AAWG) is true?

A. The AAMS is only used for calls to Avaya Spaces Calling from outside the corporate network.

B. When a call is established using Avaya Spaces Calling, the AAMS processes the media until the Avaya Communication Manager shuffles the call.

C. When Avaya Spaces Calling is used by a User to make a call to another User, the media path is always direct, bypassing the AAMS.

D. For a call established to or from Avaya Spaces Calling, the AAMS processes the media for the duration of the call.

Correct Answer: D

The Avaya Aura Media Server (AAMS) associated with the Avaya Aura Web Gateway (AAWG) is used for media processing for calls to or from Avaya Spaces Calling. Avaya Spaces Calling is a softphone that provides calling features to users of Avaya Spaces by leveraging their existing Avaya infrastructure. When a user makes or receives a call using Avaya Spaces Calling, the AAWG handles the WebRTC call signaling and the AAMS handles the media. The AAMS converts the WebRTC media to SIP media and vice versa, and provides services such as announcements, music on hold, conferencing, transcoding, and recording. The AAMS processes the media for the duration of the call, regardless of whether the call is shuffled or not by Communication Manager

---

QUESTION 5

To allow communications between the Avaya Aura Device Services (AADS) and the Avaya Aura Web Gateway (AAWG), which three configuration steps are required? (Choose three.)

A. On the AAWG, the Server-to-server interface port needs to be opened using a shell script.

B. The AAWG FQDN needs to be configured as a Trusted Host on the AADS.

C. The AADS FQDN needs to be configured as a Trusted Host on the AAWG.

D. The AADS FQDN, Client interface port and Server-to-server interface port needs to be configured on the AAWG.

E. On the AADS, the Server-to-server interface port needs to be opened using a shell script.

Correct Answer: BCD

To allow communications between the Avaya Aura Device Services (AADS) and the Avaya Aura Web Gateway (AAWG), you need to perform the following configuration steps: Configure the AAWG FQDN as a Trusted Host on the AADS: A Trusted Host is an entity that is allowed to communicate with the AADS server using HTTPS or REST APIs. You need to configure the Fully Qualified Domain Name (FQDN) of the AAWG server as a Trusted Host on the AADS server, using the System Manager web interface. This allows the AAWG server to access the AADS server for device management and configuration purposes3 Configure the AADS FQDN as a Trusted Host on the AAWG: Similarly, you need to configure the FQDN of the AADS server as a Trusted Host on the AAWG server, using the app configure command line utility. This allows the AADS server to send dynamic configuration parameters and certificates to the AAWG server for WebRTC call signaling and media processing4 Configure the AADS FQDN, Client interface port and Server-to-server interface port on the AAWG: You also need to configure the FQDN, Client interface port and Server-to-server interface port of the AADS server on the AAWG server, using the app configure command line utility. These parameters are used by the AAWG server to establish secure connections with the AADS server for device management and configuration purposes. The default Client interface port is 9443, while the default Server-to-server interface port is 84434

QUESTION 6

When registering as a Remote Worker via the Avaya Session Border Controller for Enterprise (ASBCE), which IP address should be configured in the Server List of the Avaya one-X?Communicator?

A. Avaya Aura Session Manager (SM) External (Public) Interface IP address allocated for Remote Workers

B. The Avaya Aura^ Session Manager (SM) Security Module IP Address

C. ASBCE External (Public) Interface IP address allocated for Remote Workers

D. ASBCE Internal (Private) Interface IP address allocated for Remote Workers

Correct Answer: C

When registering as a Remote Worker via the Avaya Session Border Controller for Enterprise (ASBCE), you should configure the ASBCE External (Public) Interface IP address allocated for Remote Workers in the Server List of the Avaya one-X?Communicator. The ASBCE External (Public) Interface is the interface that connects the ASBCE server to the public Internet and allows communication with external entities, such as Remote Workers or SIP service providers. The ASBCE server acts as a proxy for the Remote Workers and handles the SIP registration and call signaling with the Avaya Aura Session Manager (SM). Therefore, you need to specify the ASBCE External (Public) Interface IP address as the SIP server address in the Avaya one-X?Communicator settings

---

QUESTION 7

In the context of Avaya Aura Presence Services, what is a Watcher?

A. It represents a user whose device is sending status on their behalf using a Publish message.

B. It represents a Presence information about a user that the system reports.

C. It is a user who is subscribing to the current and future presence status of another user.

D. It is a user who requests a one-time view of another user\\'s current presence status. However, it does not get the future presentity updates.

Correct Answer: C

In the context of Avaya Aura Presence Services, a Watcher is a user who is interested in the presence information of another user, called a Presentity. A Watcher sends a Subscribe message to the Presence Services snap-in on the Avaya Breeze?server, requesting to receive notifications about the current and future presence status of the Presentity. The Presence Services snap-in then sends a Notify message to the Watcher, containing the presence information of the Presentity. The Watcher can use this information to decide how and when to communicate with the Presentity12

QUESTION 8

What is the correct procedure for connecting to the Application Enablement Services (AES) command-line interface (CLI), and the default login ID?

A. Use PuTTY or equivalent to SSH to using port 22, then enter login=cust.

B. Use PuTTY or equivalent to SSH to using port 22, then enter login=craft.

C. Use PuTTY or equivalent to connect to using port 21, then enter login=admin.

D. Use PuTTY or equivalent to SSH to using port 222, then enter login = ipcs.

Correct Answer: B

To connect to the Application Enablement Services (AES) command-line interface (CLI), you need to use a secure shell (SSH) client, such as PuTTY, and thedefault login ID. The AES CLI is a text-based interface that allows you to configure

and manage the AES server and its features. You can access the AES CLI using any SSH client that supports SSH version 2. The procedure for connecting to the AES CLI is as follows:

Launch the SSH client on your administrative workstation. Enter the IP address of the AES server that you want to connect to, and specify port 22 for SSH communication.

Click Connect or Open to initiate the connection. The server displays a security alert window the first time you connect. If you see this window, click Yes or Accept to accept the server\\'s host key. The system displays a login prompt. Enter the

login ID for accessing the AES CLI. The default login ID for the AES CLI is craft, which is a system administrator account that has full access to all features and functions of the AES server. The system displays a password prompt. Enter the

password for the craft account. The default password for the craft account is craft. You can change the password or create other user accounts with different access levels using the Security Database feature of the AES web interface.

QUESTION 9

Avaya Session Border Controller for Enterprise (ASBCE) can be deployed on the Kernel- based Virtual Machine (KVM) infrastructure. What is the template file type to be used for the KVM deployment?

A. OVA

B. QCOW2

C. OVF

D. EC2

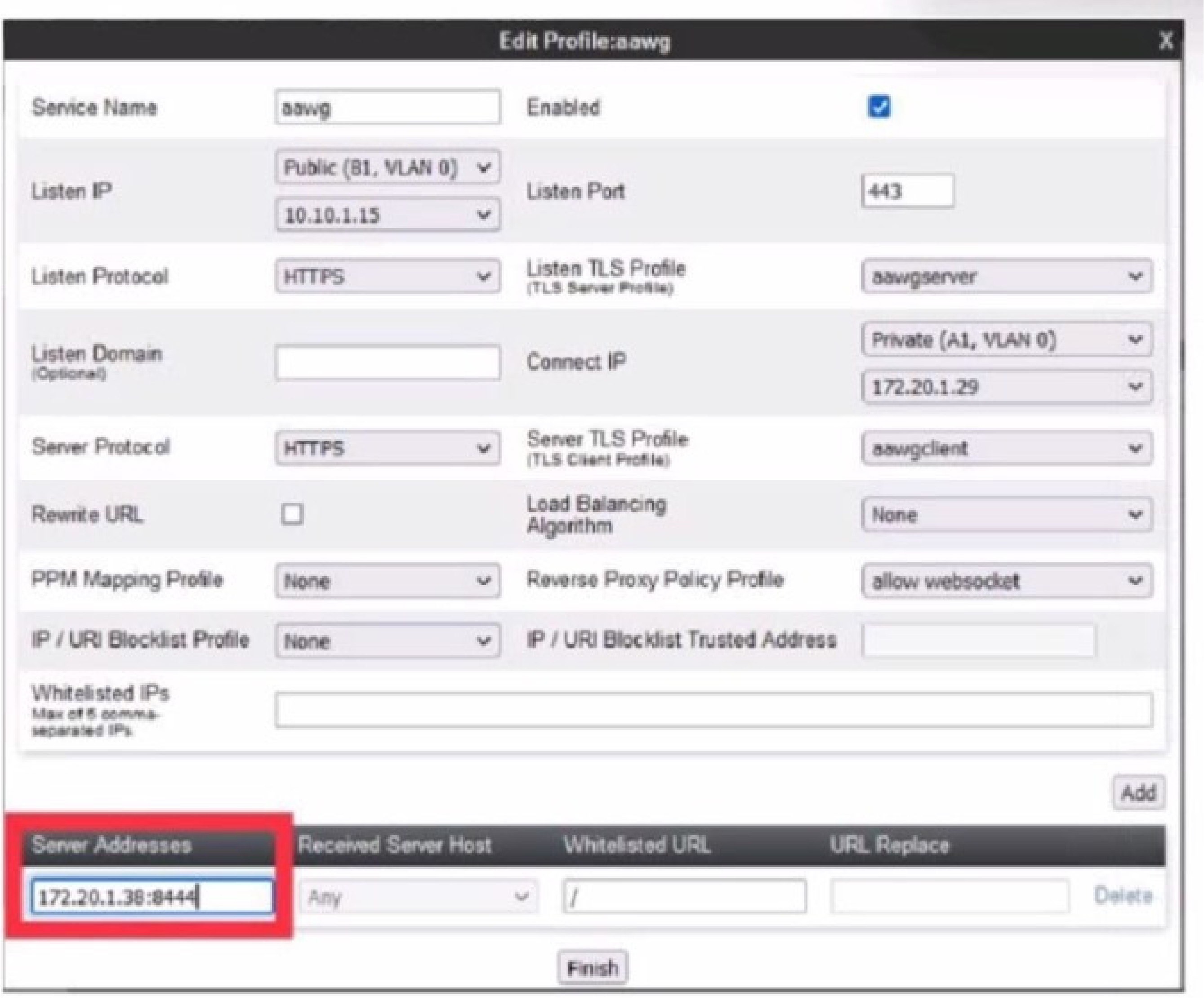
Correct Answer: B

Avaya Session Border Controller for Enterprise (ASBCE) can be deployed on the Kernel-based Virtual Machine (KVM) infrastructure. KVM is a virtualization technology that allows multiple operating systems to run on a single physical machine. To deploy ASBCE on KVM, you need to use a template file that contains the ASBCE software image and configuration parameters. The template file type to be used for KVM deployment is QCOW2, which stands for QEMU CopyOn-Write version 2. QCOW2 is a file format for disk images that can be used by QEMU, which is an open source emulator and virtualizer that can run KVM virtual machines. QCOW2 files support features such as compression, encryption, snapshots, and backing files

---

QUESTION 10

Refer to the exhibit.



Edit Profile:aawg

Service Name	aawg	Enabled	☑
Listen IP	Public (B1, VLAN 0) 10.10.1.15	Listen Port	443
Listen Protocol	HTTPS	Listen TLS Profile (TLS Server Profile)	aawgserver
Listen Domain (Optional)		Connect IP	Private (A1, VLAN 0) 172.20.1.29
Server Protocol	HTTPS	Server TLS Profile (TLS Client Profile)	aawgclient
Rewrite URL	□	Load Balancing Algorithm	None
PPM Mapping Profile	None	Reverse Proxy Policy Profile	allow websocket
IP / URI Blocklist Profile	None	IP / URI Blocklist Trusted Address	
Whitelisted IPs Max of 5 comma-separated IPs			

Server Addresses	Received Server Host	Whitelisted URL	URL Replace	
172.20.1.38:8444	Any	/		Delete

When configuring a Reverse Proxy for the Avaya Aura Web Gateway (AAWG) in the Avaya Session Border Controller for Enterprise (ASBCE), what is the significance of using port 8444 in the Server Address field?

A. This port should match the Front-end port for external access on the AAWG so that AAWG sends the media path for external calls through the ASBCE STUN/TURN server.

B. It is the default listen port on the AAWG used for all WebRTC call signalling.

C. It\\'s the default port used for ICE/STUN/TURN messages on the AAWG.

D. It\\'s used for remote access to the AAWG web interface.

Correct Answer: B

When configuring a Reverse Proxy for the Avaya Aura Web Gateway (AAWG) in the Avaya Session Border Controller for Enterprise (ASBCE), the Server Address field is used to specify the IP address or FQDN and port of the AAWG server. The port used in this field shouldmatch the listen port on the AAWG server that is used for all WebRTC call signalling. The default listen port on the AAWG server is 8444, which is also used by default in the Server Address field of the ASBCE Reverse Proxy configuration. The Reverse Proxy allows external clients to access the AAWG server securely and transparently through the ASBCE

QUESTION 11

To trace SIP messages exchanged during a Remote Worker registration in real-time, which Avaya Session Border Controller for Enterprise (ASBCE) CLI tool is used?

A. tracesbc

B. traceRW

C. tracexu

D. traceReg

Correct Answer: A

To trace SIP messages exchanged during a Remote Worker registration in real-time, you can use the tracesbc CLI tool on the Avaya Session Border Controller for Enterprise (ASBCE). The tracesbc tool is used to capture and display SIP messages and media statistics for calls that traverse the ASBCE server. You can use various filters and options to specify which calls or messages you want to trace. For example, you can filter by source or destination IP address, port, protocol, or call ID. You can also specify how long you want to run the trace and how many messages you want to display. The tracesbc tool can help you troubleshoot and diagnose issues with Remote Worker registration and call setup

---

QUESTION 12

A user has been informed by the Attendant that a call for them has been parked using the Avaya Call Park and Page running on the Breeze?platform. How can the user retrieve the parked call?

A. by pressing the Call Park button on their endpoint

B. by dialing the Answer Back feature access code

C. by dialing the system-wide Pilot extension

D. by dialing the Park extension used to park the call

Correct Answer: D

A user can retrieve a parked call by dialing the Park extension used to park the call. A Park extension is a virtual extension that is assigned to a parked call by the Call Park and Page snap-in on the Avaya Breeze?platform. A Park extension can be either system-wide or location-specific, depending on how the Call Park feature is configured. A system-wide Park extension can be accessed from any endpoint in any location, while a location-specific Park extension can only be accessed from endpoints in the same location as the parked call. When a user dials the Park extension of a parked call, the Call Park and Page snap-in transfers the call to the user\\'s endpoint12