71301X Q&As

Avaya Aura Communication Applications Implement Certified Exam

Pass Avaya 71301X Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/71301x.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Avaya Official Exam Center

QUESTION 1

Which statement regarding the license for the Avaya Aura Web Gateway (AAWG) is true?

A. A non-virtualized AAWG has an embedded local WebLM server where the license file is installed.

B. Each AAWG deployed requires its own license file.

C. Use of AAWG is an entitlement included with a Session Manager (SM) license, and therefore AAWG does not require a separate license.

D. The AAWG license file can be installed on the WebLM server embedded in the System Manager (SMGR), or on a standalone WebLM server.

Correct Answer: D

The Avaya Aura Web Gateway (AAWG) requires a license file to operate and provide WebRTC services for endpoints such as Avaya Workplace clients or Avaya Spaces Calling extension users. The license file can be installed on either of these two options: The WebLM server embedded in System Manager (SMGR): This is a web-based licensing application that is integrated with SMGR and can manage licenses formultiple Avaya products, such as Communication Manager, Session Manager, Presence Services, or Breeze Platform. You can install an AAWG license file on this WebLM server using SMGR web interface, under Elements > Licensing > Licenses5 A standalone WebLM server: This is a web-based licensing application that runs on a separate Linux or Windows server and can manage licenses for multiple Avaya products, such as Communication Manager, Session Manager, Presence Services, or Breeze Platform. You can install an AAWG license file on this WebLM server using its web interface, under Licenses > Add License File6

QUESTION 2

In some deployments, the Avaya Session Border Controller for Enterprise (ASBCE) might not trust the Certificate Authority (CA) which signed the WebLM server identity certificate.

Which tool would you use to fix the trust issue?

A. the "Fix ASBCE WebLM Cert" option under Device Management > Licensing

B. the sbceconfigurator.py fix-weblm-cert command issued from the EMS CLI

C. the sbceconfigurator.py change-ssl-certs command issued from the SBC CLI

D. the "Verify Existing Certificate" option under Device Management > Licensing

Correct Answer: B

If the Avaya Session Border Controller for Enterprise (ASBCE) does not trust the Certificate Authority (CA) that signed the WebLM server identity certificate, you can use the sbceconfigurator.py fix-weblm-cert command issued from the EMS CLI to fix the trust issue. The WebLM server is a web-based licensing application that manages licenses for various Avaya products, such as Communication Manager, Session Manager, Presence Services, or Breeze Platform. The WebLM server uses an identity certificate to authenticate itself to other entities that communicate with it using HTTPS or REST APIs. The identity certificate is signed by a CA, which is an entity that issues and verifies certificates. The ASBCE server needs to trust the CA that signed the WebLM server identity certificate in order to communicate with it securely and obtain licenses from it. If the ASBCE server does not trust the CA, you can use the sbceconfigurator.py fix-weblm-cert command to install the CA certificate on the ASBCE server and establish trust with it. The sbceconfigurator.py tool is a Python script that runs on the EMS component of the ASBCE server and performs various

configuration tasks. The EMS component is responsible for managing and monitoring the ASBCE server. You can access the EMS CLI using SSH or Telnet and run the sbceconfigurator.py tool from there.

QUESTION 3

Refer to the exhibit.

An investigator at a financial institution (FI) receives an automated transaction alert based on average KYC data within the institution.

Client name	Risk rating	Profession	Country of Tax Residence	Annual Income as per KYC	Monthly Transaction Volume (Month 1)	Monthly Transaction Volume (Month 2)	Monthly Transaction Volume (Month 3)	Average Monthly Spending
Mike Jacob	Low	Accountant	Cyprus	$ 45,000	$ 3,251.00	$ 8,777.70	$11,378.50	$ 525.00
Carl Ahmad	High	Car Dealer	Cyprus	$ 350,000	$ 9,333.33	$12,600.00	$10,360.00	$ 6,708.33
Farah Zein	Medium	Owner of Travel Agency	Cyprus	$ 180,000	$ 4,800.00	$ 6,480.00	$ 5,328.00	$ 4,200.00
Henry Lock	High	Owner of Jewelry Store	Cyprus	$ 630,000	$ 16,800.00	$36,960.00	$18,648.00	$ 9,975.00
Jason Right	Low	Teacher	Cyprus	$ 62,000	$ 1,653.33	$ 2,232.00	$ 1,835.20	$ 1,395.00
Nadine Kien	High	Trader	Cyprus	$ 280,000	$ 7,466.67	$ 10,080.00	$ 8,288.00	$ 5,600.00
May Clous	Low	Employee at a bank	Cyprus	$ 54,000	$ 1,440.00	$ 1,944.00	$ 1,598.40	$ 765.00
Richard Aston	Medium	Hotel Manager	Cyprus	$ 120,000	$ 3,200.00	$ 4,320.00	$ 3,552.00	$ 1,800.00
Mason Jacob	High	Ecommerce business owner	Cyprus	$ 430,000	$ 11,466.67	$15,480.00	$28,666.67	$ 9,316.67
Joshua White	Low	Manager at engineering company	Cyprus	$ 90,000	$ 2,400.00	$ 3,240.00	$ 2,664.00	$1,470.00

With Dynamic Licensing configured in the Avaya Session Border Controller for Enterprise (ASBCE), when will the ASBCE issue a request to the WebLM server to allocate additional licenses based on "Fetch Count" value?

A. when the percentage of free (available) standard sessions licenses reaches 50% (High Watermark)

B. when the percentage of free (available) standard sessions licenses reaches 30% (Low Watermark)

C. when the percentage of free (available) standard sessions licenses drops below 30% (Low Watermark)

D. when the percentage of free (available) standard sessions licenses drops below 50% (High Watermark)

Correct Answer: C

With Dynamic Licensing configured in the Avaya Session Border Controller for Enterprise (ASBCE), the ASBCE will issue a request to the WebLM server to allocate additional licenses based on the Fetch Count value when the percentage of free (available) standard sessions licenses drops below 30% (Low Watermark). Dynamic Licensing is a feature that allows the ASBCE to dynamically allocate and release licenses from a pool of licenses managed by the WebLM server. The Fetch Count value is a parameter that specifies how many licenses are requested from the WebLM server at a time. The Low Watermark value is a parameter that specifies the threshold percentage of free licenses that triggers a request for more licenses from the WebLM server. The High Watermark value is a parameter that specifies the threshold percentage of free licenses that triggers a release of unused licenses to the WebLM server

QUESTION 4

How does an Avaya Workplace client learn about a Survivability Server assigned in its User Profile?

A. An Avaya Workplace client receives this information from the AADS via the Dynamic Configuration.

B. The Survivability Server details must be manually configured in the Avaya Workplace client.

C. An Avaya Workplace client receives this information from the Session Manager (SM) via PPM.

D. An Avaya Workplace client receives this information from the System Manager (SMGR) via Data Replication Service (DRS).

Correct Answer: A

An Avaya Workplace client learns about a Survivability Server assigned in its User Profile from the Avaya Aura Device Services (AADS) via the Dynamic Configuration. TheDynamic Configuration is a set of parameters that are sent by the AADS to the Avaya Workplace client during login or registration. The Dynamic Configuration contains information such as the SIP domain, SIP proxy, SIP registrar, and Survivability Server for the Avaya Workplace client. The Survivability Server is an Avaya Aura Communication Manager instance that provides call processing and voice mail access for the Avaya Workplace client in case of a network failure or loss of connectivity with the core servers34

QUESTION 5

Which Avaya Aura Platform component does Application Enablement Services (AES) communicate with?

A. Avaya Aura Communication Manager (CM) using SIP

B. Avaya Aura Communication Manager (CM) using H.323

C. Avaya Aura Session Manager (SM) using SIP

D. Avaya Aura Media Server (AAMS) using H.323

Correct Answer: A

Application Enablement Services (AES) communicates with Avaya Aura Communication Manager (CM) using SIP, which is a protocol for initiating and managing multimedia sessions, such as voice, video, or instant messaging. AES is a server that provides APIs and interfaces for developing and integrating CTI applications with CM and other Avaya Aura Platform components. AES supports various APIs and interfaces, such as TSAPI, JTAPI, DMCC, Web Services, and ASAI. AES uses SIP to communicate with CM for various purposes, such as registering endpoints, sending and receiving SIP messages, controlling calls, and capturing media. AES also uses SIP to communicate with other Avaya

Aura Platform components, such as Session Manager (SM), System Manager (SMGR), Presence Services (PS), or Breeze Platform.

QUESTION 6

In the Avaya Session Border Controller for Enterprise (ASBCB), which feature allows reusing the same TCP connection to the Avaya Aura Session Manager (SM) for all SIP messages related to the same Remote Worker?

A. "Enable Shared Control" in the Signaling Interface used for the SM

B. "Share Transport Link" in the Advanced tab of the SIP Server Profile for the SM

C. "Stream Users Over Transport Link" in the Signaling Interface used for the SM

D. "Enable Grooming" in the Advanced tab of the SIP Server Profile for the SM

Correct Answer: C

In some deployments, you can enable a feature called "Stream Users Over Transport Link" in the Signaling Interface used for the Avaya Aura Session Manager (SM) on the Avaya Session Border Controller for Enterprise (ASBCB). This feature allows reusing the same TCP connection to SM for all SIP messages related to Remote Workers registered with SM through ASBCB. A Signaling Interface is a configuration object that defines how ASBCB handles SIP signaling with other entities, such as endpoints or servers. A Signaling Interface can include parameters such as source and destination IP addresses, ports, protocols, encryption modes, authentication modes, and timers. The "Stream Users Over Transport Link" parameter is an option that can be enabled or disabled in the Advanced tab of the Signaling Interface configuration screen. When this option is enabled, ASBCB will use the same TCP connection to SM for all SIP messages related to the same Remote Worker. This can reduce the number of TCP connections and improve the performance and scalability of ASBCB and SM.

QUESTION 7

Which two key configuration steps are needed to associate the Avaya Call Park and Page snap-in to an Avaya Workplace Client? (Choose two.)

A. Add an Implicit User Profile.

B. Add a Service Profile.

C. Configure a Call Park activation and deactivation feature code.

D. Add a SIP Entity for the Call Park and Page snap-in.

Correct Answer: BC

To associate the Avaya Call Park and Page snap-in to an Avaya Workplace Client, you need to perform the following key configuration steps: Add a Service Profile: A Service Profile is a set of parameters that defines the features and capabilities of a user or device in System Manager. You need to create a Service Profile for the Call Park and Page snap-in, under Users > User Management > Service Profiles. In the Service Profile, you need to specify the name, type, domain, and SIP Entity of the Call Park and Page snap-in. You also need to enable the Call Park feature and configure the Call Park activation and deactivation feature codes1 Configure a Call Park activation and deactivation feature code: A feature code is a numeric sequence that activates or deactivates a specific feature on Communication Manager. You need to configure a Call Park activation and deactivation feature code on Communication Manager, using the change feature- access-codes command. The Call Park activation feature code allows a user to park a call on a specified

extension, while the Call Park deactivation feature code allows a user to retrieve a parked call from any extension2

QUESTION 8

Which two pieces of information in an output from the show mgc command (issued on a G430/G450 Gateway CLI), indicate that the G430/G450 is operating as an Internet Friendly (Edge) Gateway as opposed to an Enterprise Gateway? (Choose two.)

A. The Management Link Mode displays Tunnelled.

B. The H.248 Link Mode displays IFG.

C. The Gateway Mode displays Edge.

D. The H.248 Link Status displays UP/Encrypted.

E. The Controller displays sbc@.

Correct Answer: BD

The output from the show mgc command (issued on a G430/G450 Gateway CLI) can indicate whether the G430/G450 is operating as an Internet Friendly (Edge) Gateway or an Enterprise Gateway. An Internet Friendly (Edge) Gateway is a device that provides secure and reliable connectivity between endpoints on different networks, such as the public internet and a private enterprise network. An Enterprise Gateway is a device that provides connectivity between endpoints on the same network, such as a LAN or a WAN. The show mgc command displays information about the Media Gateway Controller (MGC), which is the entity that controls the media gateway functions of the G430/G450, such as call processing, routing, and signaling. The MGC can be an Avaya Communication Manager (CM) server or an Avaya Session Border Controller for Enterprise (ASBCE) server. The output from the show mgc command includes these fields: Management Link Mode: This field indicates how the G430/G450 communicates with the MGC for management purposes, such as configuration, monitoring, and troubleshooting. The possible values are Direct or Tunnelled. Direct means that the G430/G450 communicates with the MGC using a direct IP connection over TCP port 5022. Tunnelled means that the G430/G450 communicates with the MGC using a tunnel over TCP port 2944 and secured using TLS. This mode is used when the G430/G450 operates as an Internet Friendly (Edge) Gateway and communicates with ASBCE as the MGC.

H.248 Link Mode: This field indicates how the G430/G450 communicates with the MGC for media gateway control purposes, such as controlling media streams, allocating resources, and creating connections. The possible values areEGW or

IFG. EGW means that the G430/G450 communicates with the MGC using H.248 protocol over UDP port 2944. This mode is used when the G430/G450 operates as an Enterprise Gateway and communicates with CM as the MGC. IFG means

that the G430/G450 communicates with the MGC using H.248 protocol over TCP port 2944 and secured using TLS. This mode is used when the G430/G450 operates as an Internet Friendly (Edge) Gateway and communicates with ASBCE

as the MGC.

H.248 Link Status: This field indicates whether the H.248 link between the G430/G450 and the MGC is up or down, and whether it is encrypted or not. The possible values are UP/Encrypted, UP/Unencrypted, DOWN/Encrypted, or DOWN/

Unencrypted. UP means that the H.248 link is established and functional. DOWN means that the H.248 link is not established or not functional. Encrypted means that the H.248 link is secured using TLS encryption. Unencrypted means that

the H.248 link is not secured using TLS encryption. Therefore, to determine whether the G430/G450 is operating as an Internet Friendly (Edge) Gateway or an Enterprise Gateway, you can look at these two fields in the output from the show

mgc command:

If the H.248 Link Mode displays IFG, it means that the G430/G450 is operating as an Internet Friendly (Edge) Gateway and communicating with ASBCE as the MGC using H.248 over TCP port 2944 and secured using TLS. If the H.248 Link

Status displays UP/Encrypted, it means that the G430/G450 is operating as an Internet Friendly (Edge) Gateway and communicating with ASBCE as the MGC using a secure and functional H.248 link.

QUESTION 9

Which three SIP headers should be overwritten with a SIP domain in a Topology Hiding Profile associated with a Session Manager in a typical Avaya Session Border Controller for Enterprise (ASBCE) deployment? (Choose three.)

A. From

B. Refer-To

C. To

D. Request-Line

E. Referred-By

Correct Answer: ABC

When configuring a Topology Hiding Profile associated with a Session Manager in a typical Avaya Session Border Controller for Enterprise (ASBCE) deployment, you should overwrite the following three SIP headers with a SIP domain: From, Refer-To, and To. A Topology Hiding Profile is a configuration object that masks the FQDN or IP address portion of SIP headers to hide the internal topology of the network. For example, SBCE@avaya.com can become SBCE@135.122.18.7, or just the opposite. The From header indicates the identity of the originator of a SIP request or response. The Refer-To header indicates the identity of the recipient of a REFER request, which is used to transfer calls or sessions. The To header indicates the identity of the intended recipient of a SIP request or response. These headers should be overwritten with a SIP domain to prevent exposing internal FQDNs or IP addresses to external entities

QUESTION 10

Which End Point Flows are required when setting up the Avaya Session Border Controller for Enterprise (ASBCE) SIP Trunking?

A. a minimum of two Subscriber Flows

B. a minimum of two Server Flows

C. one Subscriber Flow and one Server Flow

D. one Subscriber Flow and two Server Flows

Correct Answer: C

When setting up the Avaya Session Border Controller for Enterprise (ASBCE) SIP Trunking, you need one Subscriber Flow and one Server Flow. A Subscriber Flow is a configuration object that defines how the ASBCE handles SIP requests and responses from or to an endpoint, such as an IP phone or a softphone. A Server Flow is a configuration object that defines how the ASBCE handles SIP requests and responses from or to a server, such as a Communication Manager or a Session Manager. For SIP Trunking, you need one Subscriber Flow that connects the ASBCE to the internal SIP server, and one Server Flow that connects the ASBCE to the external SIP service provider. These flows specify parameters such as source and destination IP addresses, ports, protocols, codecs, encryption, authentication, and routing rules3

QUESTION 11

In the Avaya Session Border Controller for Enterprise (ASBCE), what is the state of a Network Interface, after the deployment?

A. Deployed

B. Active

C. Disabled

D. Enabled

Correct Answer: C

In the Avaya Session Border Controller for Enterprise (ASBCE), the state of a Network Interface, after the deployment, is Disabled. A Network Interface is a logical interface that represents a physical port on the ASBCE server. A Network Interface can be configured with an IP address, subnet mask, gateway, and VLAN ID. After the deployment of the ASBCE server, the Network Interfaces are in a Disabled state by default. To enable a Network Interface, you need to use the ASBCE web interface or CLI and configure the interface parameters. You also need to assign the interface to a Zone, which is a logical grouping of interfaces that defines the security and routing policies for the ASBCE server

QUESTION 12

You are deploying the Avaya Aura Presence Services on Avaya Breeze?

When looking under Elements > Avaya Breeze> Service Management > Services in Avaya Aura System Manager, which status would you expect to see for a Presence Services snap-in that is ready to support Presence and IM?

A. Active

B. Installed

C. Loaded

D. Accepting

Correct Answer: A

When deploying the Avaya Aura Presence Services on Avaya Breeze? you can check the status of the Presence Services snap-in in System Manager, under Elements > Avaya Breeze> Service Management > Services. The status indicates the state of the snap-in on the Avaya Breeze?cluster. The status Active means that the snap-in is running and ready to support Presence and IM. The other statuses are either intermediate or error states that indicate that the snap-in is not fully functional or operational.

QUESTION 13

Which event triggers a Survivable Communication Manager (CM) to accept IP phones registration requests, and put the configured IP trunks in a working condition?

A. availability of DSP resources from either an Avaya Aura Media Server (AAMS) and/or a G-series Media Gateway

B. a lack of a response to an outbound SIP INVITE

C. a failed IP phone registration attempt

D. a heartbeat failure of the main CM

Correct Answer: D

A Survivable Communication Manager (CM) is a Communication Manager instance that provides local call processing and trunking capabilities for remote sites or branches in case of a WAN outage or loss of connectivity with the core servers. A Survivable CM monitors thestatus of the main CM by sending and receiving heartbeat messages at regular intervals. A heartbeat message is a SIP OPTIONS request that tests the availability of the main CM. If the Survivable CM does not receive a response to its heartbeat message within a specified timeout period, it assumes that the main CM is down and triggers a failover process. During the failover process, the Survivable CM accepts IP phone registration requests from the local endpoints and puts the configured IP trunks in a working condition, allowing the remote site or branch to continue making and receiving calls

QUESTION 14

Before running the initTM -f command from the Avaya Breeze?server CLI, what should be verified?

A. Verify that the Avaya Breeze?is configured as a Managed Element in Avaya Aura System Manager.

B. Verify that an enrollment password is configured in Avaya Aura System Manager, and that it has not expired.

C. Verify that a valid certificate is installed on the Avaya Breeze?server.

D. Verify that the Avaya Breeze?server is licensed.

Correct Answer: B

The initTM -f command is used to initialize the trust management between the Avaya Breeze?server and the Avaya Aura System Manager. This command requires an enrollment password that is configured in the System Manager web interface, under Security > Enrollment Password. The enrollment password has a validity period that can be set by the administrator. If the enrollment password has expired, the initTM -f command will fail. Therefore, before running the initTM -f command, you should verify that the enrollment password is configured and valid12

QUESTION 15

After running the Install wizard on the Avaya Session Border Controller for Enterprise (ASBCE), you add a Public (External) IP address to the Bl interface. You try to ping this IP address from a PC in the same subnet, but it fails.

What is the first step to resolve the problem?

A. Navigate to Network and Flows > Network Management > Interfaces and enable the Bl interface.

B. Navigate to Device Management, and click on Restart Application.

C. Navigate to Device Management, and and click on Reboot.

D. Connect to the ASBCE CLI and reboot the ASBCE.

Correct Answer: A

After running the Install wizard on the Avaya Session Border Controller for Enterprise (ASBCE), you add a Public (External) IP address to the Bl interface. The Bl interface is a logical interface that represents the external network port on the ASBCE server. The Bl interface is used to communicate with external entities, such as SIP service providers or remote workers. If you try to ping the Bl interface IP address from a PC in the same subnet, but it fails, the first step to resolve the problem is to navigate to Network and Flows > Network Management > Interfaces and enable the Bl interface. By default, the Bl interface is disabled after the Install wizard. You need to enable it and assign it to an External Zone, which is a logical grouping of interfaces that defines the security and routing policies for the external network