

## Avaya.71300X.v2022-06-23.q23

<b>Exam Code:</b>	71300X
<b>Exam Name:</b>	Avaya Aura® Communication Applications Integration Exam
<b>Certification Provider:</b>	Avaya
<b>Free Question Number:</b>	23
<b>Version:</b>	v2022-06-23
<b># of views:</b>	208
<b># of Questions views:</b>	443
<a href="https://www.freecram.net/torrent/Avaya.71300X.v2022-06-23.q23.html">https://www.freecram.net/torrent/Avaya.71300X.v2022-06-23.q23.html</a>	

### NEW QUESTION: 1

You are setting up the SIP connection between Avaya Aura Messaging (AAM) and the Avaya Aura Core, and the information you have entered for the Far-end connection is:

What should you conclude from all this information?

- A.** There will be conflicts in the TLS connections given that 5061 is a well-known port that other Endpoints and Servers use within the same network.
- B.** The connection cannot work because 5061 is not the Well-known port corresponding to TLS by standard.
- C.** The IP address is wrong because its range does not correspond to a valid TLS-compatible IP address.
- D.** A Security Certificate from the same Certificate Authority as the other Avaya Aura components, must be installed on the AAM Server to guarantee successful TLS Connections.

**Answer:** ([SHOW ANSWER](#))

### NEW QUESTION: 2

Which statement describes Cross-Origin Resource Sharing (CORS)?

- A.** It allows for signaling-groups to be used by more than one trunk-group.
- B.** It is a W3C specification that allows cross-domain communication from the browser.
- C.** It is making DSP resources available regardless of the originating location of a call.
- D.** It is a network setup by which an Avaya Aura Media Server (AAMS) can be used by more than one Avaya Aura Communications Manager (CM).

**Answer:** ([SHOW ANSWER](#))

Explanation

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the first resource was served. A web page may freely embed cross-origin images, stylesheets, scripts, iframes, and videos.

Note on the History of CORS:

Cross-origin support was originally proposed by Matt Oshry, Brad Porter, and Michael Bodell of Tellme Networks in March 2004 for inclusion in VoiceXML 2.1 to allow safe cross-origin data requests by VoiceXML browsers.

In May 2006 the first W3C Working Draft was submitted. In March 2009 the draft was renamed to "Cross-Origin Resource Sharing" and in January 2014 it was accepted as a W3C Recommendation.

References: [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)

### **NEW QUESTION: 3**

In the context of Avaya Aura Presence Services 7.x, what is a Fetcher?

- A.** It is a kind of watcher that requests a one-time view of the user's current presentity information, but does not get future presentity information for a user.
- B.** It is a user whose devices are sending status or presentity information on his behalf using a Publish message regarding his communication status.
- C.** It is a watcher that is subscribing to current and future presentity information from another user.
- D.** It is the presence information about a user that the system reports.

**Answer: (SHOW ANSWER)**

Explanation

Fetchers pull the value of presence information for a specific presentity from the presence service. If a fetcher is fetching information on a regular basis, it is called a poller. Subscribers, on the other hand, subscribe to presentity information on the presence service.

### **NEW QUESTION: 4**

Which three functionalities does WebRTC provide? (Choose three.)

- A.** NAT / Firewall Traversal
- B.** adds click-to-call capabilities from a web application to an Avaya endpoint
- C.** Internet-friendly codecs and Privacy
- D.** real-time audio and video conferencing

**Answer: (SHOW ANSWER)**

Explanation

\* One of the primary differentiating features for the WebRTC Snap-in is that the web application handles authentication and authorization of calls. This includes the capability to assert a calling user's phone number and restrict the numbers that can be called.

\* The Avaya SBCE enables secure firewall traversal for HTTP and SRTP packets, facilitates sending DTLS to provide secured key exchange for the SRTP flow, and takes care of all security requirements mentioned in the TURN protocol for the solution.

\* WebRTC can be a game changer for enterprise communications and customer engagement. Enterprises can now add real-time communications to any website.

References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 9

**NEW QUESTION: 5**

Before SIP Trunking configuration can begin, which state must the Avaya Session Border Controller for Enterprise (SBCE) be in?

- A. Registered
- B. Provisioned
- C. Commissioned
- D. Ready

**Answer: C** ([LEAVE A REPLY](#))

Explanation

Prerequisite Conditions for SIP Trunking

Starting point for SIP-trunking administration:

System Management > Installed tab shows SBC(s) Commissioned indicates a successful initial console configuration.

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 302

**NEW QUESTION: 6**

In which two locations is the Switch Password configured?

- A. In 'ip-services' form on Avaya Aura Communication Manager (CM) and in 'TSAPI link' on Avaya Aura Application Enablement Services (AES)
- B. In 'ip-services' form on Avaya Aura Communication Manager (CM) and in 'Switch Connection' on Avaya Aura Application Enablement Services (AES)
- C. In 'cti-link' form on Avaya Aura Communication Manager (CM) and in 'Switch Connection' on Avaya Aura Application Enablement Services (AES)
- D. In 'cti-link' form on Avaya Aura Communication Manager (CM) and in 'TSAPI link' on Avaya Aura Application Enablement Services (AES)

**Answer: (SHOW ANSWER)**

Explanation

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services.

Procedure

1. Type change ip-services. Communication Manager displays the IP SERVICES form
2. Complete Page 1 of the IP SERVICES form
3. Complete Page 3 of the IP SERVICES form as follows.
  - a. In the AE Services Server field, type the name of the AE Services server
  - b. In the Password field, create a password.

This is the password that the AE Services administrator must set on the AE Server (Communication Manager Interface > Switch Connections > Edit Connection > Switch Password).

The passwords must exactly match on both Communication Manager and the AE Services server.

References: Avaya Aura Application Enablement Services Administration and Maintenance Guide, Release

6.3 (June 2014) , page 26

<https://downloads.avaya.com/css/P8/documents/100171737>

### **NEW QUESTION: 7**

Which statement about enabling IM and Presence for a user is true?

- A.** In SMGR, edit the Communication Profile of the user to assign an Avaya E.164 handle and check the Presence profile checkbox.
- B.** In SMGR, edit the Communication Profile of the user to assign an Avaya SIP handle and check the Presence profile checkbox.
- C.** In SMGR, edit the Communication Profile of the user to assign a XMPP handle and check the Presence profile checkbox.
- D.** In SMGR, edit the Communication Profile of the user to assign an Avaya Presence/IM handle and check the Presence profile checkbox.

**Answer: ([SHOW ANSWER](#))**

Explanation

Communication Profile tab: Presence Profile

Fields include:

- \* The SIP Entity field used to route SIP based messages through the Presence Services.
- \* IM Gateway The IP address of the IM gateway

Note: Avaya SMGR stands for Avaya System Manager.

References: Administering Avaya Aura System Manager for Release 6.3.11 and later, Release 6.3 November

2016, page 554

<https://downloads.avaya.com/css/P8/documents/101008185>

### **NEW QUESTION: 8**

By default, which Codec does Avaya Aura Messaging (AAM) support?

- A.** G.726
- B.** G.722
- C.** G.711
- D.** G.729

**Answer: ([SHOW ANSWER](#))**

Explanation

You must configure the Messaging system to use the G.711 encoding format.

Note: The G.711 format provides the highest audio quality especially when voice networks use multiple encodings and decodings. Avaya requires that you use the G.711 encoding format in Messaging systems that support TTY devices.

The G.711 encoding format uses a higher encoding rate than GSM. The G.711 encoding format therefore produces larger files and requires more storage space for messages. Messaging provides customers with adequate storage space for message playback and networking. References: Administering Avaya Aura Messaging, Release 6.2 Issue 2.2 (December 2013) , page 201

<https://downloads.avaya.com/css/P8/documents/100172127>

**NEW QUESTION: 9**

WebRTC is used for which type of calls?

- A. video calls only
- B. calls originated from internal web browsers only
- C. calls originated from external web browsers only
- D. calls originated from internal and external web browsers

**Answer: (SHOW ANSWER)**

Explanation

The Avaya WebRTC Snap-in enables users inside or outside the Enterprise to make a secure call from their web browser to any endpoint to which Avaya Aura can deliver calls.

References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 6

<https://downloads.avaya.com/css/P8/documents/101013939>

**NEW QUESTION: 10**

- A. Verify that Avaya Breeze™ is configured as a Managed Element in Avaya Aura System Manager.
- B. Verify that an enrollment password is configured on System Manager and that it has not expired.
- C. Verify that a valid Certificate is installed on the Avaya Breeze™ instance.
- D. Verify that Avaya Breeze™ is licensed.

**Answer: (SHOW ANSWER)**

Explanation

See step 8 and step 9 below.

Repairing replication between Avaya Breeze™ and System Manager

Procedure

1. On the System Manager web console, navigate to Services > Replication.
2. In Replica Group column, click CollaborationEnvironment\_3.1.
3. In Replica Node Host Name column, locate Avaya Breeze™.
4. Verify that the status of the Synchronization Status field is green. If not, go to Step 5.
5. If Presence Services Snap-in has been deployed, in the Product column, verify that both Avaya Breeze™ and Presence Services are displayed.
6. Select Avaya Breeze™, and click Repair.
7. After 2-15 minutes, verify that the status of the Synchronization Status field is green. If not, go to Step 8.

8. Verify that Enrollment Password is not expired.
  - a. Navigate to Services > Security.
  - b. In the navigation pane, click Certificates > Enrollment Password.

9. If the Enrollment Password is expired:

- a. Enter a password, and click Commit.

It is highly recommended that the same password must be used. Otherwise, Avaya Breeze™ and Presence Services must be re-administered, because System Manager Enrollment Password was configured during deployment of Avaya Breeze™.

- b. Open an SSH session to the Avaya Breeze™ Management Module IP address as sroot.
- c. On the command line interface, enter `initTM -f`.
- d. When prompted for the enrollment password, enter the password that you provided in Step 9a.
- e. Repeat Step 1 to Step 6.

References: Avaya Aura Presence Services Snap-in Reference, Release 7.0.1 (December 2016), page 223

<https://downloads.avaya.com/css/P8/documents/101013646>

#### **NEW QUESTION: 11**

Avaya Aura Presence Services 7.x is implemented on Avaya Breeze™ (formerly known as Engagement Development Platform (EDP)).

When looking at Elements > Engagement Development Platform > Service Management, which status would you expect for a Presence Services snap-in that is ready to support Avaya Aura Presence Services?

- A. Loaded
- B. Installed
- C. Accepting
- D. Active

**Answer: (SHOW ANSWER)**

Explanation

Enabling Avaya Breeze cluster running Presence Services

Before you begin

Ensure that the Avaya Breeze™ servers running the Presence Services are recovered / powered up.

Procedure

1. On the System Manager web console, navigate to Elements > Avaya Breeze > Cluster Administration.
2. Select the Presence Services cluster, and change the Cluster State to Accept New Service.

References: Avaya Aura Presence Services Snap-in Reference. Release 7.0.1 (December 2016), page 48

<https://downloads.avaya.com/css/P8/documents/101013646>

#### **NEW QUESTION: 12**

When looking at Avaya Aura System Manager - Home > Services > Replication, what is the name of the replica group representing the EDP / Avaya Breeze™ instances?

- A. CollaborationEnvironment\_7.0
- B. Avaya Breeze™\_7.0
- C. CollaborationEnvironment\_3.1
- D. Engagement Development Platform EDP\_7.0

**Answer: (SHOW ANSWER)**

Explanation

Confirming that Avaya Breeze successfully replicates with System Manager Procedure

1. On the System Manager web console, navigate to Services > Replication.
2. In Replica Group column, click CollaborationEnvironment\_3.1.
3. In Replica Node Host Name column, locate your newly-deployed Avaya Breeze.
4. After 2 - 15 minutes, verify that the status of the Synchronization Status field is green/Synchronized. If not, see Repairing replication between Avaya Breeze™ and System Manager

References: Avaya Aura Presence Services Snap-in Reference, Release 7.0.1, (December 2016), page 24

<https://downloads.avaya.com/css/P8/documents/101013646>

### NEW QUESTION: 13

A customer reports that when using Presence services, the users cannot see the Presence status.

Which two tools are used to trace a PUBLISH message. In the Avaya Breeze™ server? (Choose two.)

- A. tracePS
- B. traceSM
- C. traceCE
- D. traceSBC
- E. tracePRS

**Answer: (SHOW ANSWER)**

### NEW QUESTION: 14

A company is deploying Avaya Session Border Controller for Enterprise (SBCE) to support SIP trunking.

What is the minimum number of IP-addresses they need to assign to the private and public Network Interface Cards (NICs)?

- A. Two addresses are assigned to the private NIC and two addresses are assigned to the public NIC.
- B. One address is assigned to the private NIC and one address is assigned to the public NIC.
- C. Two addresses are assigned to the private NIC and one address is assigned to the public NIC.
- D. One address is assigned to the private NIC and two addresses are assigned to the public NIC.

**Answer: B (LEAVE A REPLY)**

Explanation

Example configuration:

## Ensure Interfaces are Enabled

- ▶ Select **System Management > Device Specific Settings > Network Management**.
- ▶ Click on the **Interface Configuration** tab to enable the **A1** and **B1** interfaces.

Session Border Controller for Enterprise

Network Management: SBC-13

Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

IP Address	Public IP	Gateway	Interface	
172.16.13.50		172.16.255.254	A1	Delete
10.10.13.1		10.10.255.254	B1	Delete



References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 305

### NEW QUESTION: 15

In which location is the AAMS URI 'ce-msml@avaya.com' configured?

- A. Elements > Breeze > Configuration > HTTP Security and as a Regular Expression
- B. Elements > Breeze > Configuration > HTTP Security and as a Dial Pattern
- C. Home > Elements > Breeze > Configuration > Avaya Aura Media Server and as a Dial Pattern
- D. Home > Elements > Breeze > Configuration > Avaya Aura Media Server and as a Regular Expression

**Answer: (SHOW ANSWER)**

Explanation

Creating the Avaya Aura Media Server Routing Pattern

Procedure

1. On System Manager, click Elements > Routing > Routing Policies.
2. Click New.
3. Type a Name for the Routing Policy.
4. From the SIP Entity as Destination field, click Select.



5. Select the Avaya Aura

Media Server SIP Entity that you created.

Select the Local Host Name FQDN SIP Entity if you are using High Availability for the Avaya Aura Media Server routing.

6. Click Commit.

7. Navigate to Home > Elements > Routing > Regular Expressions and click New.

8. In the Pattern field, type ce-msml@<sip-domain>.\*

This sip-domain value must match:

\* The SIP domain that you entered in the Home > Elements > Routing > Domains page.

\* The default SIP domain that you entered on the Avaya Breeze™ Cluster Administration page.

9. Click Commit

<https://downloads.avaya.com/css/P8/documents/101014426>

References: Deploying Avaya Breeze, Release 3.1, (September 2016), page 55

### **NEW QUESTION: 16**

In Avaya Session Border Controller for Enterprise (SBCE) 7.x, which two configuration screens must be configured for Personal Profile Management (PPM) to be successfully downloaded to an Avaya SIP Telephone (AST)? (Choose two.)

A. PPM Services Mapping Profile

B. Application Relay

C. File Transfer

D. Reverse Proxy

**Answer: (SHOW ANSWER)**

Explanation

B: Application relays function as port forwards. Different clients require different application relays.

A: An Avaya SIP phone downloads and processes a configuration file, sends out a slew of SUBSCRIBE messages, and uses something called Personal Profile Manager (PPM).

Note: The PPM is a software module that runs as part of an Avaya Session Manager. It consists of a series of web services that phones use to retrieve and manage SIP related user data.

References:

<https://andrewjprokop.wordpress.com/2014/03/28/understanding-avayas-personal-profile-manager-ppm/>

<https://downloads.avaya.com/css/P8/documents/101028355>

**Valid 71300X Dumps** shared by Fast2test.com for Helping Passing 71300X Exam!

Fast2test.com now offer the **newest 71300X exam dumps**, the Fast2test.com 71300X exam **questions have been updated** and **answers have been corrected** get the **newest**

Fast2test.com 71300X dumps with Test Engine here: <https://www.fast2test.com/71300X-premium-file.html> (70 Q&As Dumps, **30%OFF Special Discount: freecram**)

#### **NEW QUESTION: 17**

A field engineer runs the Installation Wizard to install the Avaya Session Border Controller for Enterprise (SBCE).

Which statement about the Domain Name Service (DNS) configuration is true?

- A.** A DNS address always needs to be configured for both the Primary and Secondary DNS, even if only the DNS is available.
- B.** A DNS address does not need to be configured.
- C.** A DNS address needs to be configured, even if it is unused and/or unreachable.
- D.** A DNS address should not be configured here.

**Answer: (SHOW ANSWER)**

Explanation

The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. You must supply a DNS address entry, even if it is unused and/or unreachable.

#### **NEW QUESTION: 18**

Which Avaya Breeze™ Cluster type is the Avaya Aura Presence Services snap-in installed on?

- A.** Presence Services
- B.** Core Platform
- C.** General Purpose
- D.** IM\_Presence

**Answer: B (LEAVE A REPLY)**

Explanation

Verifying that Presence Services snap-in is ready to support Presence and IM Procedure

1. On the System Manager web console, navigate to Elements > Avaya Breeze > Cluster Administration.

2. Locate the row for the cluster, and verify that:

\* The Cluster Profile field shows Core Platform.

etc.

References: Avaya Aura Presence Services Snap-in Reference. Release 7.0.1 (December 2016), page 224

<https://downloads.avaya.com/css/P8/documents/101013646>

#### **NEW QUESTION: 19**

To which other component does the Avaya Aura Application Enablement Services (AES) Switch Connections connect?

- A.** Avaya Aura Media Server (AAMS) using H.323
- B.** Avaya Aura Session Manager (SM) using SIP

C. Avaya Aura Communications Manager (CM) using H.323

D. Avaya Aura Communications Manager (CM) using SIP

**Answer: (SHOW ANSWER)**

Explanation

Adding a switch connection

The procedure include the following steps:

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections.

2. On the Switch Connections page, in the Add Connection field, type a switch connection name (for example Switch1) For the Secure H323 Connection check box, do one of the following:

\* For Communication Manager 6.3.6 or later and TLS for the H.323 Signaling Channel (normally associated with FIPS Mode), select the Secure H323 Connection check box.

\* For any previous release of Communication Manager without TLS for the H.323 Signaling Channel, uncheck the Secure H323 Connection check box.

Etc.

References: Avaya Aura Application Enablement Services Administration and Maintenance Guide, page 73

<https://downloads.avaya.com/css/P8/documents/100171737>

### **NEW QUESTION: 20**

A. It needs to match the Enrollment Password.

B. It needs to match the admin password used to login to SMGR using a web browser.

C. It needs to match the Attributes of the Messaging Managed Element in the Inventory.

D. It needs to match the root password used to login to SMGR command line.

**Answer: (SHOW ANSWER)**

Explanation

Configuring Messaging in the normal operational mode

Before you begin

\* Add both the primary and secondary servers as Trusted Servers in the Messaging system.

\* Update the Login, Password, and Confirm Password fields with the appropriate trusted server defined on the Messaging system.

Procedure

1. Log on to the Messaging system that System Manager manages. 2. Add the secondary System Manager server as Trusted Servers in the Messaging system.

3. Log on to the secondary System Manager server.

4. On the System Manager web console, click Services > Inventory.

5. In the left navigation pane, click Manage Elements.

6. On the Manage Elements page, select the Messaging system that you want to change to the secondary System Manager server.

7. Click Edit.

8. On the Attributes tab, fill the Login, Password, and Confirm Password fields with the corresponding name and password of the Messaging trusted server.
9. Click Commit.
10. Click Inventory > Synchronization > Messaging System, and select the required Messaging element.
11. Click Now.

The secondary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

References: Administering Avaya Aura System Manager for Release 6.3.11 and later, Release 6.3, Issue 8 (November 2016), page 104

<https://downloads.avaya.com/css/P8/documents/101008185>

### **NEW QUESTION: 21**

Which statement about WebRTC and Media Resources is true?

- A. WebRTC does not use any Media Resources since it only handles Text-Chat sessions.
- B. WebRTC relies on the Avaya Aura Media Server (AAMS) to convert the WebRTC media stream to a SIP media stream.
- C. WebRTC uses its own embedded proprietary technology to handle and process Media Packets.
- D. WebRTC uses Media Resources from a Hard-Based Media Gateway controlled by Avaya Aura Communication Manager (CM).

**Answer: (SHOW ANSWER)**

Explanation

The Avaya Media Server can translate WebRTC media into a SIP media stream.

References:

<http://www.avaya.com/blogs/archives/2014/10/an-introduction-to-the-avaya-webrtc-snap-in.html>

### **NEW QUESTION: 22**

Which access control method is used by the Avaya Aura Application Enablement Services (AES) server for administrators?

- A. Single Administrator simple password login
- B. Challenge-Response shared-key method only
- C. System Manager AES Management Menu
- D. Role-Based Access Control

**Answer: (SHOW ANSWER)**

Explanation

Role Based Access Control (RBAC)

Access to AE Services Management Console Web pages can be restricted by user authorization level. The operations that users are allowed to perform such as read, edit and delete can also be restricted.

References: Avaya Aura Application Enablement Services Overview and Specification, Release 7.0.1, Issue 2 (June 2016), page 20

<https://downloads.avaya.com/css/P8/documents/101014052>

**NEW QUESTION: 23**

What is the process for establishing a command line session to the AES Management IP Address, and logging in with the default account and default password?

- A.** Use PuTTY to Rlogin to > AES Management IP Addr > using port 21, then enter login=admin password=admin.
- B.** Use PuTTY to SSH to > AES Management IP Addr > using port 22, then enter login=craft password=crftpw.
- C.** Use PuTTY to SSH to > AES Management IP Addr > using port 22, then enter login=cust password=custpw.
- D.** Use PuTTY to SSH to > AES Management IP Addr > using port 222, then enter login=admin password=admin01.

**Answer: (SHOW ANSWER)**

Explanation

Use port 22, not port 21 or port 222.

Log in as craft and use the default password.

References: Application Enablement Services Installation and Upgrade Guide for a Bundled Server Release

4.0, page 29

[https://downloads.avaya.com/elmodocs2/AES/4.0/02\\_300356\\_4.pdf](https://downloads.avaya.com/elmodocs2/AES/4.0/02_300356_4.pdf)

**Valid 71300X Dumps** shared by Fast2test.com for Helping Passing 71300X Exam!

Fast2test.com now offer the **newest 71300X exam dumps**, the Fast2test.com 71300X exam **questions have been updated** and **answers have been corrected** get the **newest**

Fast2test.com 71300X dumps with Test Engine here: <https://www.fast2test.com/71300X-premium-file.html> (70 Q&As Dumps, **30%OFF Special Discount: freecram**)