ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

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

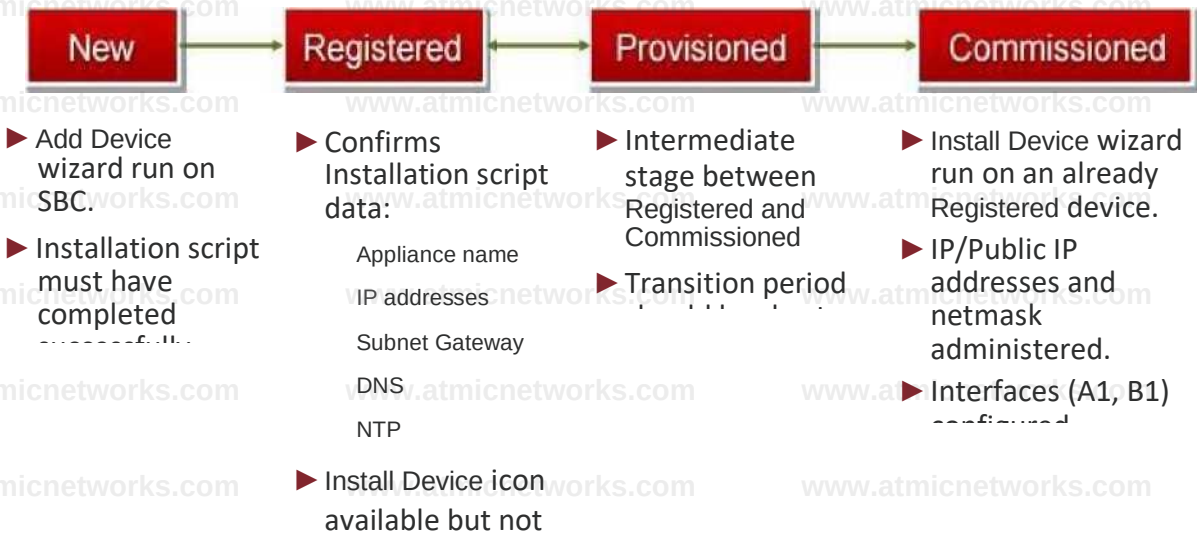
Question: 2

After the initial provisioning script has been run you see your Avaya Session Border Controller for Enterprise (SBCE) displaying a Registered state in the Web GUI. You click on the install link in the EMS System Management > Devices menu to continue the installation.
After displaying a status of Provisioning for a short while, which status does the SBCE display?

A. Commissioned
B. Up
C. Busyout
D. Maintenance-Busy

Answer: A

Explanation:
SBC states:



References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 201

Question: 3

From a remote worker's SIP Endpoint connected via Mobile Workspace, which tool is used to trace the successful way through Avaya Session Border Controller for Enterprise (SBCE) of an Invite message?

A. traceRT
B. traceSM
C. traceMW
D. traceSBC

Answer: B

Explanation:
traceSM is an interactive perl script that allows an administrator to capture, view, and save call processing activity on a Session Manager. While not as powerful or versatile as wireshark, traceSM is absolutely essential when it comes to working with Avaya SIP. First off, it allows you to view SIP messages even if they have been encrypted with TLS.

Question: 4

The provisioning script automatically runs as part of the first boot-up of the Avaya Session Border Controller for Enterprise (SBCE). During this process you assign the Management IP address to the SBCE. You browse to the Element Management System (EMS) to continue to install the SBCE.
On the System Management > Devices web page, which status does the SBCE display before the Install link is clicked?

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

Answer: C

Explanation:

► Add Device wizard run on SBC.

► installation script must have completed successfully.

► Confirms Installation

IPaddresses

„ ,

Subnet

Gateway

DNS

NTP

► Intermediate stage between Registered and Commissioned. Registered

* Transition period should be short.

► Install Device wizard script data: run on an already administered. device.

► IP/Public IP addresses and netmask

, . . .

. . ,

.,.,....

► Interfaces (A1, B1) configured.

► Install Device icon available but not run.

References: Avaya Aura Session Border Controller Enterprise (2012), page 201

Question: 5

To watch Avaya Session Border Controller for Enterprise (SBCE) messages in real-time as they pass through the SBCE, which tool on the SIP command line do you use?

A. traceSBC
B. traceSM –m
C. traceTOOL
D. trace

Answer: A

Explanation:

The tcpdump tool is the main troubleshooting tool of Avaya SBCE, which can capture network traffic.

Using tcpdump is a reliable way to analyze the information arriving to and sent from the SBC.

However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

The traceSBC tool offers solutions for both issues.

In Real-time mode, traceSBC must be on active Avaya SBCE. traceSBC is started without specifying a file in the command line parameters. The tool automatically starts processing the log files. The live

capture can be started and stopped anytime without affecting service.

Example:

traceSBC

References: Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise (December 2015), page 27
https://downloads.avaya.com/css/P8/documents/101014063

Question: 6

On Avaya Session Border Controller for Enterprise (SBCE), which two ways can be used to view System Logs? (Choose two.)

A. from CLI execute cat > var > log > Avaya > syslog
B. from System Manager web GUI > Alarms and Events
C. from CLI execute cat archive > syslog > ipcs.log
D. from EMS web GUI SBCE Dashboard access Logs > System Logs

Answer: C,D

Explanation:
C: Call Trace data are written to this location:
– /archive/syslog/ipcs/octeon.log
D: Viewing system logsProcedure
1. Log on to the EMS web interface with administrator credentials.
2. Select the Logs option from the toolbar, and click the System Logs menu.
The system displays the Syslog Viewer screen. On this screen, you can specify criteria in the Query Options section to filter the results displayed.
3. In the Start Date and End Date fields, filter the results displayed in a search report to fall within starting and ending dates and times. In previous Avaya SBCE Syslog Viewer windows, there were four separate fields: Start Date, Start Time, End Date, and End Time.
References: Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise (December 2015), page 21
Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 478

Question: 7

In the Avaya Session Border Controller for Enterprise (SBCE), before a traffic carrying Network Interface (A1 or B1) can be pinged, to which state do you have to toggle the status on Device Specific Settings > Network Management / Interfaces?

A. Enabled
B. In-Service
C. Accept Service
D. Active

Answer: A

Explanation:

Commission the SBC—SBC Configuration

3. Click the Toggle link for both the A1 and the B1 interfaces.

The Administrative Status for both A1 and B1 changes to Enabled:

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 203

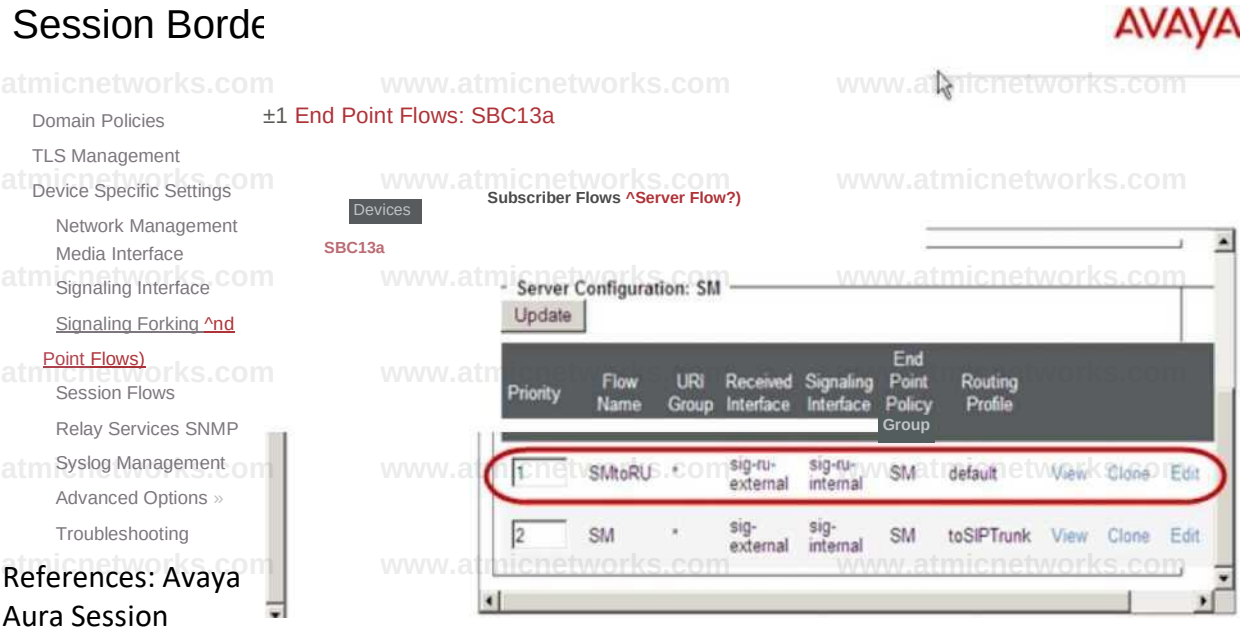
Question: 8

How many Server Flows and/or Subscriber Flows are required for SIP Trunking?

A. one Subscriber Flow and two Server Flows
B. a minimum of two Subscriber Flows
C. one Subscriber Flow and one Server Flow
D. a minimum of two Server Flows

Answer: A

Explanation:
Two types of flows need to be defined for the proper routing of SIP messages from and to the endpoints and the SIP server.
Example, Server Flows:



References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 540, 546

Question: 9

In Avaya Session Border Controller for Enterprise (SBCE) 7.x, you need to download the 46xxsettings.txt file to a Remote Worker device.
What needs to be configured under DMZ Services > Relay Services?

A. Application Relay and File Transfer
B. Reverse Proxy
C. Application Relay
D. Application Relay and Reverse Proxy

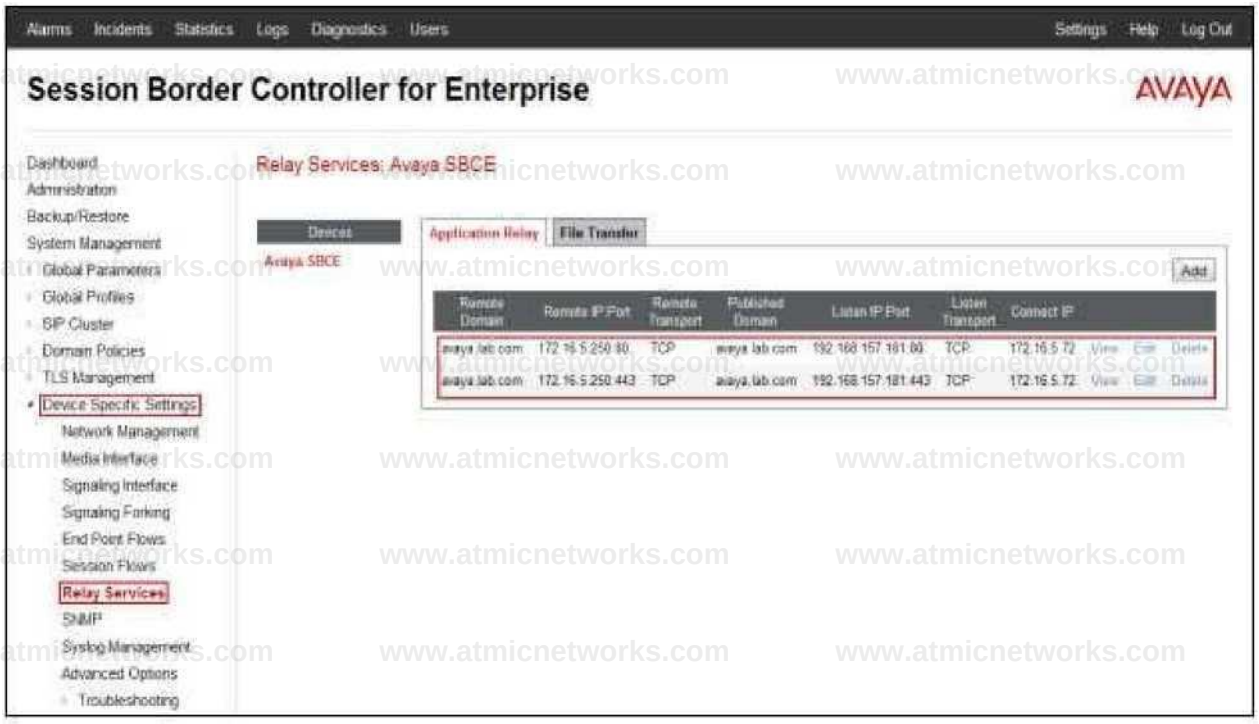
Answer: C

Explanation:

Relay Services are used to define how file transfers (e.g., for phone firmware upgrades and configuration), are routed to the Remote Worker endpoints.

Example: 2 For accessing the file server using HTTPS protocol

The following screenshot shows the newly created Relay Services



References: Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura Communication Manager Rel. 6.3 and Avaya Aura Session Managers Rel. 6.3 - Issue 1.0, page 73
https://downloads.avaya.com/css/P8/documents/100183254

Question: 10

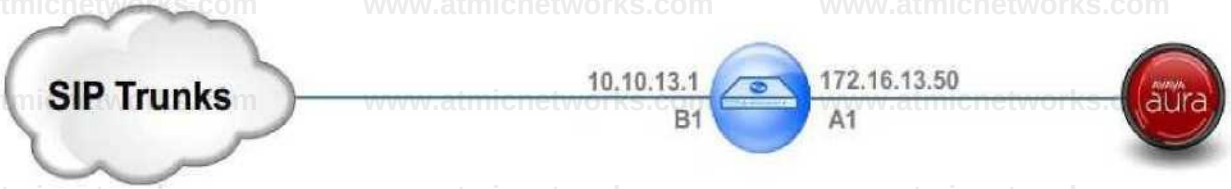
When planning the Avaya Session Border Controller for Enterprise (SBCE) for SIP Trunking, what is a good practice to adopt?

A. Name Interfaces consistently, for example, A1 for Internal network to Call Server and B1 for external to Trunk Server.
B. Name all internal and external interfaces exactly the same.
C. Use the same IP address on both, internal and external sides of the network.
D. Use one Avaya Session Border Controller for Enterprise on the internal and external sides of the network.

Answer: A

Explanation:

Use the same interface mapping throughout! Examples in this section use:



References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 304

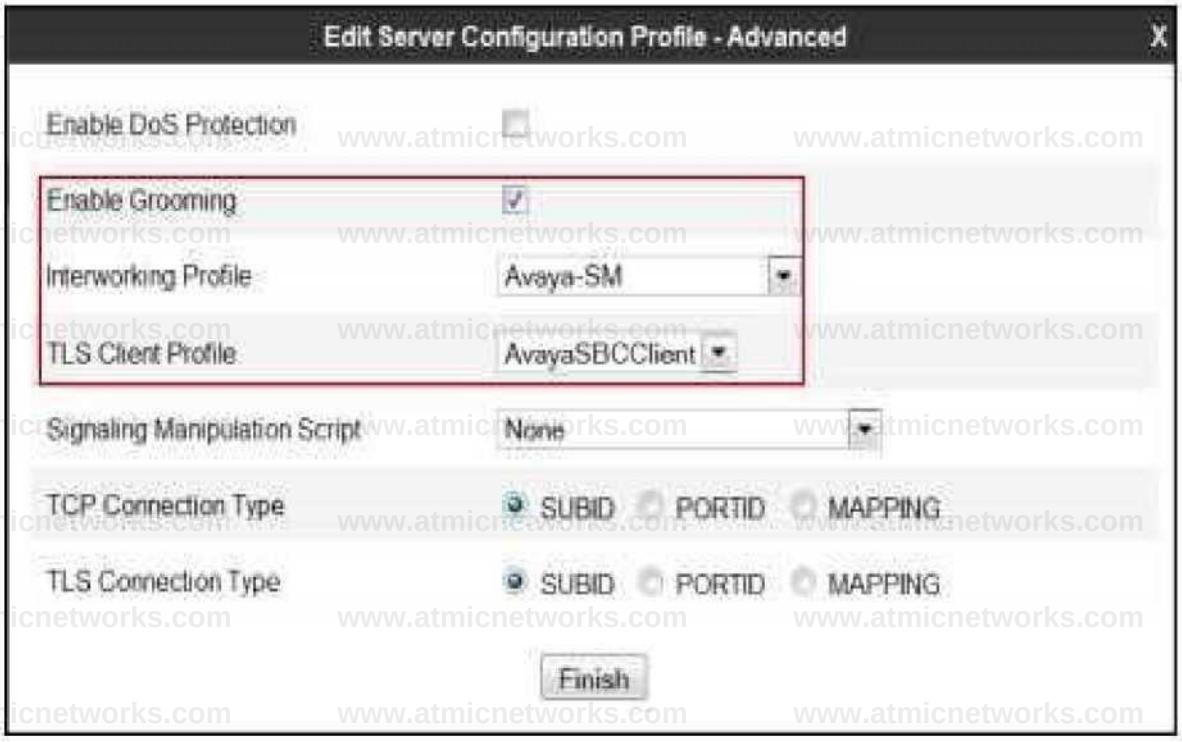
Question: 11

You want to multiplex all remote workers SIP messages to Avaya Aura® Session Manager (SM) over the same TCP connection, rather than open a dedicated TCP connection for each user.
Which feature needs to be enabled for Avaya Session Border Controller for Enterprise (SBCE)?

A. the Enable Grooming feature in the Advanced tab of the Avaya Aura® Session Manager (SM) Server Profile
B. the Enable Shared Control feature in the Signaling Interface.
C. the Stream Users Over Transport Link feature in the Signaling Interface
D. the Share Transport Link feature in the Advanced tab of the Avaya Aura® Session Manager (SM) Server Profile

Answer: A

Explanation:
Example:



References: Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3 - Issue 1.0, page 36
https://downloads.avaya.com/css/P8/documents/100183254

Question: 12

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: C

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.

Question: 13

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)?

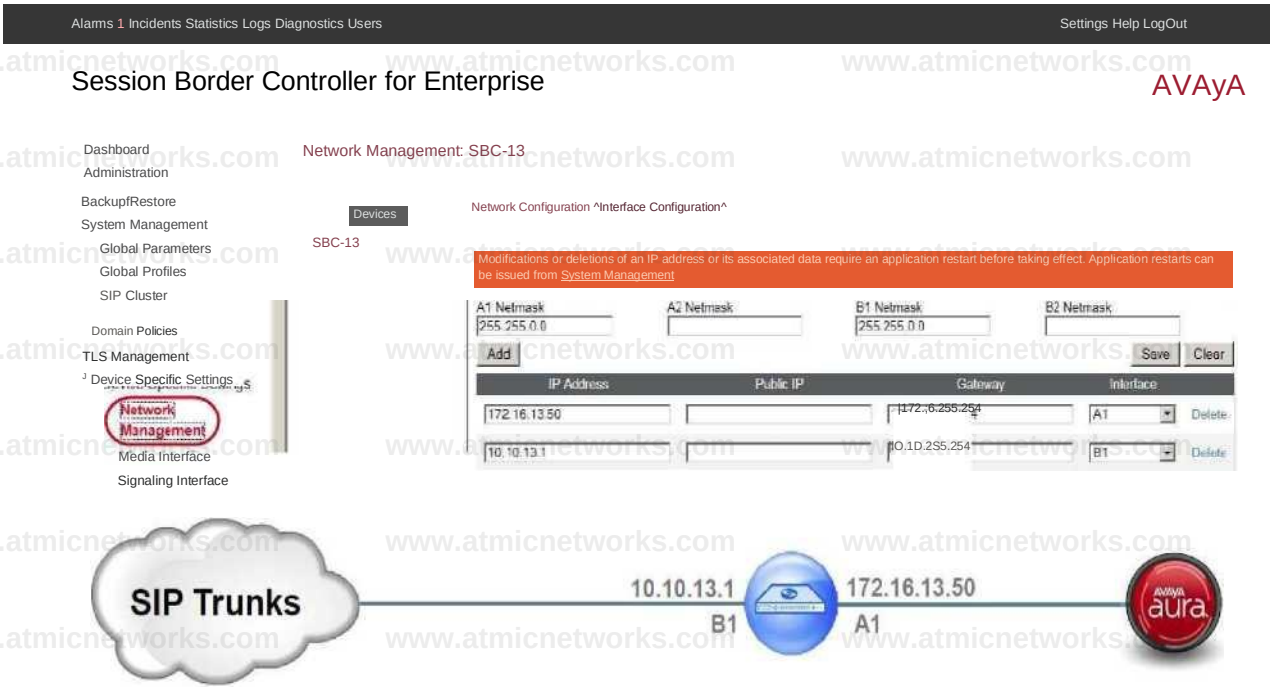
A. Two addresses are assigned to the private NIC and two addresses are assigned to the public NIC.
B. One address is assigned to the private NIC and one address is assigned to the public NIC.
C. Two addresses are assigned to the private NIC and one address is assigned to the public NIC.
D. One address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

Answer: B

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.



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

Question: 14

In Avaya Session Border Controller for Enterprise (SBCE), what is the default state of an Interface?

A. Deployed
B. Enabled
C. Disabled
D. Active

Answer: C

Explanation:
Example:
Commission the SBC—SBC Configuration

1. The A1 and B1 interfaces display on the Network Configuration tab.
2. Click on the Interface Configuration tab:

3. Click the Toggle link for both the A1 and the B1 interfaces.

The Administrative Status for both A1 and B1 changes to Enabled:

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 203

Question: 15

To set Timers, URI Manipulation, and Header Manipulation that the Avaya Session Border Controller for Enterprise (SBCE) will use when signaling to the far-end server; a profile like "avaya-ru" is provided by default.

When configuring the Server Configuration, you must link to which type of Global profile?

A. Signaling
B. Routing
C. Topology Hiding
D. Server Interworking

Answer: D

Explanation:

The standard Avaya profile "avaya-ru" is cloned for the Call Server Interworking Profile.

The Interworking function of the Global Profiles feature enables the SBCE to function in an enterprise VoIP network using different SIP protocols.

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 339

Question: 16

On Avaya Session Border Controller for Enterprise (SBCE), where do you access the tool that displays SIP messages, in real time, as they pass through the SBCE?

A. from Avaya Aura® System Manager, navigate to "Session Border Controller for Enterprise > SBCE

Administration" menu
B. from the SBCE EMS Web Console
C. from the SBCE Server command line via SSH session, using PuTTY
D. from the traceSIP client installed on a local PC

Answer: C

Explanation:
Stat the tue Tracing Tools, TraceSM, SSH to Session Manager

1. Launch PuTTY (or similar client application) for a SSH session to Session Manager (port 22). Use the Session Manager IP Address (172.16.255.107).
2. Log in.
3. At the Session Manager command line type traceSM –x and press Enter.

Note: The traceSM tool shows the SIP call flow in Session Manager.
It gives insight into Session Manager's decisions.
Benefit: can filter certain types of SIP messages
References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 485

Question: 17

For an Avaya SIP telephone, working as a Remote Worker via the Avaya Session Border Controller for Enterprise (SBCE), which IP address should be configured in the Server List of the one-X® Communicator?

A. the SBCE Internal Interface allocated for Mobile Workspace Endpoint
B. the SBCE External Interface allocated for Mobile Workspace Endpoint
C. the Internal Avaya Aura® Session Manager SM100 IP Address
D. the Avaya Aura® Session Manager External Interface allocated for Mobile Workspace Endpoints.

Answer: D

Explanation:
Remote Worker Avaya one-X Communicator Configuration
The following screens illustrate Avaya one-X Communicator administration settings for the Remote Worker used in the reference configuration.
Example:
1. On the Avaya one-X Communicator application running on the PC, click on the Settings icon on the top right to display the Settings window.2. Click on Telephony, the General Settings window will appear.
The following values were used in the reference configuration:
Under Using: select SIP (SIP must be selected; H.323 is not supported for Remote Workers).
* Under Server List, click Add (the Add Server window to the right will appear).
* Under Proxy Server enter 192.168.157.180 (This is one of the two "public" IP addresses for interface B1 on the Avaya SBCE used for Remote Worker access to Session Manager (public IP not used for relay services).
Etc.
References: Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel.

6.3 - Issue 1.0, page 81
https://downloads.avaya.com/css/P8/documents/100183254

Question: 18

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: A,B

Explanation:
8: 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

Question: 19

On Avaya Session Border Controller for Enterprise (SBCE), which statement about how to examine messages with Wireshark is true?

A. You have to start and stop the .pcap file using command line.
B. You can start and stop a Packet Capture in the EMS web GUI and then you can open the .pcap file with Wireshark.
C. Wireshark runs directly on Avaya Session Border Controller for Enterprise (SBCE).
D. They cannot be examined on this version.

Answer: B

Explanation:
Viewing the Packet Capture with Wireshark.
0. Start a Packet Capture in the EMS web GUi.
1. After the capture completes, click the Capture tab.
2. Double-click on the capture file name.
3. The File Download window opens.
4. Click Open.

The Wireshark application opens the trace.
Note: The Wireshark call tracing tool can be used on virtual desktop for vLabs.

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 468

Question: 20

After running the Install wizard on Avaya Session Border Controller for Enterprise (SBCE), you added a Public Outside IP address to the B1 interface. You try to ping this IP address from a PC in the same subnet but it falls.

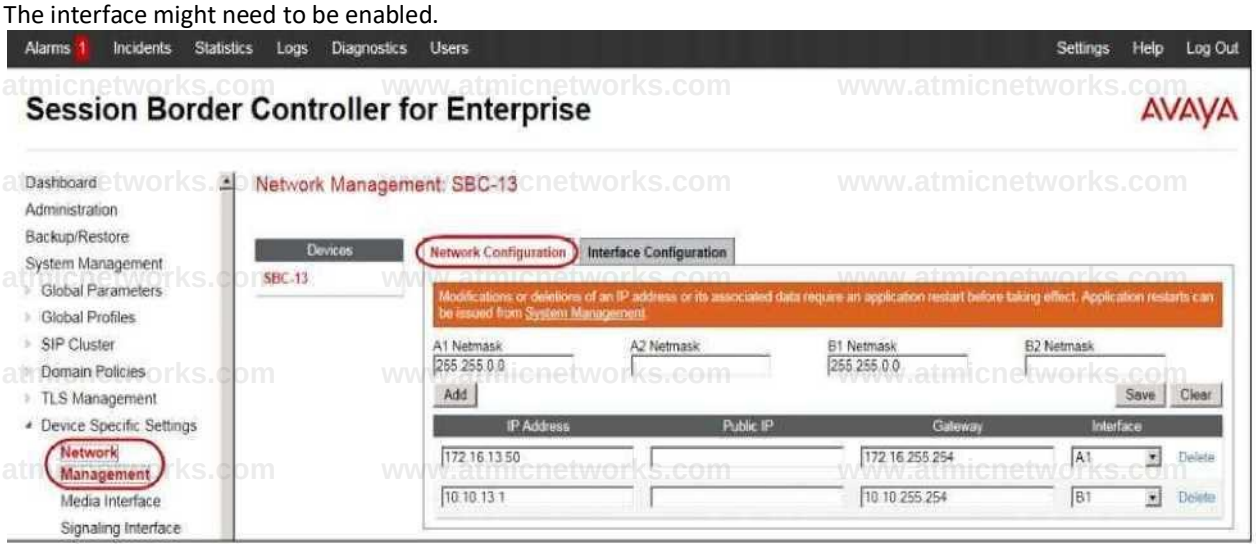
What would you do first to resolve the issue?

A. Restart Applications.
B. Set the Default Gateway router IP address, navigate to the Interfaces and Enable the B1 Interface.
C. Reboot SBCE.
D. Navigate to Device Specific Settings > Network Management > Interfaces and Enable the B1 interface.

Answer: D

Explanation:

The interface might need to be enabled.



2. Click on the Interface Configuration tab.

3. Click the Toggle link for both the A1 and the B1 interfaces.

The Administrative Status for both A1 and B1 changes to Enabled

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 204

Question: 21

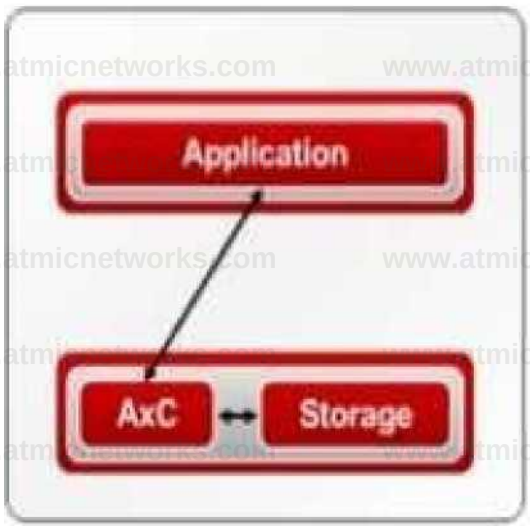
What are the three components of Avaya Aura® Messaging (AAM)? (Choose three.)

A. Messaging Distributor
B. Application Server
C. Messaging Store
D. AxC/Directory
E. SM100 Module

Answer: B,C,D

Explanation:

The AXC connector is always co-resident with the Avaya message store.



References: Administering Avaya Aura® Messaging Release 6.2, Issue 2.2 (December 2013)
https://downloads.avaya.com/css/P8/documents/100172127

Question: 22

In Avaya Aura® Messaging 6.3, which statement is true about Avaya Aura® Messaging (AAM) capacities of a system utilizing the Standard Capacity (non-High Capacity) Message Store template?

A. One Message Store Server supports up to 60000 user mailboxes and you can have 5 active + 1 Redundant Application Servers in a cluster.
B. One Message Store Server supports up to 6000 user mailboxes and you can have 3 active + 1 Redundant Application Servers in a cluster.
C. One Message Store Server supports up to 600 user mailboxes and you can have 5 active + 1 Redundant Application Servers in a cluster.
D. One Message Store Server supports up to 1000 user mailboxes and you can have 3 active + 1 Redundant Application Servers in a cluster.

Answer: B

Explanation:
Dedicated AxC/Directory server: A physical server that manages notification capabilities and the LDAP database and provides communications between application servers and the thirdparty storage server. This server also stores user properties and name and greeting recordings.
Not all configurations require a dedicated AxC/Directory server because the AxC/Directory role runs on the Avaya-provided message store. You only need a dedicated AxC/Directory server for: References: Avaya Aura® Messaging Overview and Specification, Release 6.3.2 (January 2015) , page 20
https://downloads.avaya.com/css/P8/documents/101004642

Question: 23

To route calls to Avaya Aura® Messaging (AAM), which routing strategy is used by Avaya Aura® Session Manager (SM)?

A. Automatic Route Selection (ARS)
B. Automatic Alternate Routing (AAR)
C. Network Routing Policies (NRP)
D. Registry Routing

Answer: C

Explanation:
Routing policies describe the conditions under which Session Manager will route calls between Communication Manager and Avaya Aura Messaging.
References: Application Notes for Configuring Avaya Aura® Messaging 6.1 as a Voice Messaging Solution for Avaya Aura® Communication Manager 6.0.1 Feature & Evolution Server Using SIP Trunks and Avaya Aura® Session Manager 6.1 –Issue 1.0, page 25
https://www.devconnectprogram.com/fileMedia/download/08ad7375-7c2e-4767-929f- 15f4e8130a0d

Question: 24

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. The connection cannot work because 5061 is not the Well-known port corresponding to TLS by standard.
B. 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.
C. 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.
D. The IP address is wrong because its range does not correspond to a valid TLS-compatible IP address.

Answer: C

Question: 25

When configuring a SIP Entity for Avaya Aura® Messaging (AAM) in Avaya Aura® System Manager, which Type of SIP entity needs to be selected?

A. Messaging
B. Avaya Aura® Messaging
C. Communication Manager Messaging
D. Other

Answer: D

Explanation:
Define SIP Entity
Expand Elements, Routing and select SIP Entities from the left navigation menu.
Click New (not shown). In the General section, enter the following values and use default values for remaining fields.
* Name: Enter an identifier for the SIP Entity
* FQDN or IP Address: Enter IP address of Avaya Aura® Messaging.
* Type: Select "Other"
Etc.
References: Application Notes for Configuring Avaya Aura® Messaging 6.1 as a Voice Messaging Solution for Avaya Aura® Communication Manager 6.0.1 Feature & Evolution Server Using SIP Trunks and Avaya Aura® Session Manager 6.1 – Issue 1.0 , page 22
https://www.devconnectprogram.com/fileMedia/download/08ad7375-7c2e-4767-929f-15f4e8130a0d

Question: 26

To allow trust between Avaya Aura® System Manager (SMGR) and Avaya Aura® Messaging

(AAM), there is a password set when you add the Trusted Server on AAM. This password must match with the password also configured in SMGR.
Which statement about the password in SMGR is true?

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: C

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

Question: 27

In Avaya Aura® System Manager, how is Avaya Aura® Messaging (AAM) added to the list of Managed Elements?

A. It is added when you configure the AAM SIP Entity in SMGR.
B. It is automatically added during the enrollment process.
C. It can only be manually added.
D. It is automatically added using initTM –f command on the Command Line Interface of AAM.

Answer: D

Explanation:
In System Manager, element installation sets up the trust between System Manager and its managed elements. . Similarly, UCM has a trust management process to set up the trust between UCM and its managed elements. To enable managed elements of UCM to be in the same trust domain as the System Manager managed elements, you must import the UCM Certificate Authority (CA) certificate to the System Manager managed element's trusted certificate list.
Note: To force a re-initialization of trust management

1. Ensure the enrollment password in the System Manager Security -> Enrollment Password screen is valid and set. Make note of this password as it will be needed when running the trust management initialization command.
2. Log into the Session Manager virtual machine IP address with an ssh client as the craft or customer account login
3. Execute the following shell command once at the shell prompt:

$ initTM –f

This will prompt you for the enrollment password and then initialize trust management and the database replication service of the Session Manager.
References: Administering Avaya Aura System Manager for Release 6.3.11 and later, Release 6.3, Issue 8, November 2016, page 1073
https://downloads.avaya.com/css/P8/documents/101008185
https://downloads.avaya.com/css/P8/documents/100161692

Question: 28

In Avaya Aura® Messaging (AAM) 6.3, how many Call Answering Ports can one Application Server support?

A. up to 100 Ports
B. up to 10 Ports
C. up to 1000 Ports
D. up to 10000 Ports

Answer: A

Explanation:
The Call Answer Ports range is 2–100.
References: Administering Avaya Aura Messaging, page 34
https://downloads.avaya.com/css/P8/documents/100112131

Question: 29

An Avaya Aura® Messaging (AAM) server intended to store Voice Messages in Avaya Message Store Mode, and you are configuring that server for integration with an Avaya Aura® Core.
In Messaging Administration > Server Settings > Server Role/AxC Address, which Server Role must be chosen at the “Roles for this server” field?

A. Application Only
B. Storage Only

C. Storage & Application
D. AMSM

Answer: C

Question: 30

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

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

Answer: C

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

Question: 31

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: D

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),

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

Question: 32

What is the process for Web browsing to the AES Management Console, and logging in with the default account and default password?

A. Error! Hyperlink reference not valid. Management IP Addr>:8443, then enter login=craft password=crftpw
B. Error! Hyperlink reference not valid. Management IP Addr> then enter login=admin password=admin01
C. Error! Hyperlink reference not valid. Management IP Addr> then enter login=admin password=admin
D. Error! Hyperlink reference not valid. Management IP Addr> then enter login=cust password-custpw

Answer: D

Explanation:
Log in to the AE Server as the default administrator (cust).
Make sure that the URL begins with "https://" and the host name or IP address of the AE Services Server is correct.
References: Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3 (June 2014), page 56
https://downloads.avaya.com/css/P8/documents/100171737

Question: 33

In Avaya Aura® Communication Manager (CM) for TSAPI, which type of CTI-link needs to be configured?

A. ASAI-IP
B. TSAPI-IP
C. ADJ-IP
D. DMCC-IP

Answer: C

Explanation:
The Avaya AES server forwards CTI requests, responses, and events between Invision CTI
Server and Communication Manager. The Avaya AES server communicates with
Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Invision CTI.
Step 1: Enter the display system-parameters customer-options command. On Page 3, verify that Computer Telephony Adjunct Links is set to y.
Step 2: Enter the add cti-link m command, where m is a number between 1 and 64, inclusive.
Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set

the
Type field to ADJ-IP, and assign a descriptive Name to the CTI link.
Etc.
References: Application Notes for Invision CTI with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0, page 6
https://www.devconnectprogram.com/fileMedia/download/edd26666-ae98-4f15-9a2a- a156d0807160

Question: 34

Which four kinds of services does the TSAPI standard provide for third-party call control over Avaya Aura® Communication Manager (CM)? (Choose four.)

A. receiving notifications of events
B. controlling specific calls or stations
C. invoking CM features
D. performing a remote reboot to the CM server
E. completing the routing of incoming calls
F. adding new feature buttons to agent sets

Answer: A,B,C,E

Explanation:
A: The services in the Event Report group provide a client application with the reports of events that cause a change in the state of a call, a connection, or a device.
B: The services in the call control group enable a telephony client application to control a call or connection on Communication Manager. Typical uses of these services are:
placing calls from a device
controlling a connection for a single call.
C: The services in the query group allow a client to query device features and static attributes of a Communication Manager device.
E: The services in the routing group allow Communication Manager to request and receive routing instructions for a call from a client application.
References: Avaya Aura® Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference Release 6.1, page 128
https://downloads.avaya.com/css/P8/documents/100141354

Question: 35

Which configuration must be completed before configuring a TSAPI link on Avaya Aura® Application Enablement Services (AES)?

A. A CTI link must be configured on Avaya Aura® Communication Manager (CM) first.
B. A Switch Connection must be configured on Avaya Aura® Application Enablement Services (AES) first.
C. A signaling-group must be configured on Avaya Aura® Communication Manager (CM) first.
D. A CTI-user must be configured on Avaya Aura® Application Enablement Services (AES) first.

Answer: A

Explanation:
If you are administering the AE Server for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft or IBM Sametime), you must administer a CTI link from Communication Manager to AE Services.
Follow these steps from a Communication Manager SAT to administer a CTI link type ADJ-IP.
Procedure
1. Type add cti-link <link number>, for example add cti-link 5.
2. Complete the CTI LINK form as follows:
a. In the Extension field, type <station extension>, for example 70001.
b. In the Type field, type ADJ-IP.
c. In the Name field, type <name of AE Server>, for example aeserver1.
References: Avaya Aura® Application Enablement Services Administration and Maintenance, page 30
Guide
https://downloads.avaya.com/css/P8/documents/100171737

Question: 36

What are three ways of accessing Avaya Aura® Application Enablement Services (AES) to perform administration? (Choose three.)

A. with an Open X.11 terminal window
B. with web access
C. with remote access using Rlogin
D. with local access using a system console
E. with remote access using SSH

Answer: B,D,E

Explanation:
8: You can use a Web browser to access the Application Enablement Services Management Console (AE Services Management Console).
DE: Administrators can access the AE Services Linux shell (command prompt) either locally using a system console or remotely using a secure shell (ssh) client. This access method applies primarily to AE Services Technicians (craft users) who perform specific tasks, such as viewing trace logs, installing patches, and so forth.
References: Avaya Aura® Application Enablement Services Administration and Maintenance Guide , page 52
https://downloads.avaya.com/css/P8/documents/100171737

Question: 37

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: C

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 Manager6.3.6 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

Question: 38

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: B

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

Question: 39

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: B

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

Question: 40

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: A,B,D

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

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

Question: 41

Which component converts WebRTC Media Stream to SIP Media Stream?

A. HTTP Reverse Proxy
B. Avaya Aura® Media Server (AAMS)
C. STUN/TURN server
D. G.450/430 or G.650 Medpro board

Answer: C

Explanation:
Provisioning Avaya Aura® Media Server for the WebRTC Snap-in. Procedure
1. Log in to the Avaya Aura®
Media Server Element Manager.
2. Check that Avaya Aura®
Media Server nodes and routes are set up correctly.
See Deploying Avaya Breeze™ for details on configuring Avaya Aura® Media Server for Avaya Breeze™.
3. Go to System Configuration > Server Profile > General Settings, enable Firewall NAT Tunneling Media Processor and then click Save.
4. Go to System Configuration > Signaling Protocols > SIP > General Settings, enable Always use SIP default outbound proxy, and then click Save.
Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Accounts and create a TURN/STUN account. This account ID and password must match the account created on the Avaya SBCE.
6. Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Servers to add the TURN/STUN connection to the Avaya SBCE server Etc.
References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 23
https://downloads.avaya.com/css/P8/documents/101013939

Question: 42

Which three steps are necessary to make a successful Implementation of Avaya Breeze™ WebRTC
Snap-in? (Choose three.)

A. Load the Snap-in.
B. Download and Install WebRTC License file.
C. Busy and Release the WebRTC snap-in.
D. Manually configure the WebLM IP address in the WebRTC configuration attributes.
E. Install the Snap-in.

Answer: A,B,E

Explanation:
Step 1: Download and install the license file
Procedure
0. Download the snap-in license file from PLDS.
1. On System Manager navigate to Home > Services > Licenses.

2. Select Install License.
3. Browse to the location of the snap-in license.
4. Select the license file and click Open.
5. Click Accept the License Terms & Conditions and click Install.

The system installs the license file.

In the left navigation pane, the system displays the snap-in under Licensed Products.

Step 2: Load the snap-in

Step 3: Install the snap-in

References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 15

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

Question: 43

The WebRTC snap-in needs to be loaded on which of Avaya Breeze™ cluster?

A. Context Store EDP Cluster
B. Core Platform EDP Cluster
C. General Purpose EDP Cluster
D. Work Assignment EDP Cluster

Answer: B

Explanation:

A cluster profile is a pre-loaded template that contains cluster attributes.

The Core Platform cluster profile: A closed cluster that supports up to 10 Avaya Breeze servers.

Question: 44

The media stream in WebRTC is anchored on which Avaya Aura® component?

A. Avaya Aura® Media Gateway G430/G450
B. Avaya Aura® Media Server (AAMS)
C. No DSP Resources are required
D. G650 Medpro

Answer: B

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.

The WebRTC Snap-in supports 1800 simultaneous calls at a rate of 28,000 BHCC in the following deployment model:

1 Avaya Breeze server

1 Avaya Session Border Controller for Enterprise (Avaya SBCE) server

8 Avaya Aura Media Servers

References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 26

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

Question: 45

Which three statements about Avaya Breeze™ are true? (Choose three.)

A. It allows application developers to quickly add new capabilities to their Avaya solutions.
B. It is used by Avaya, Partner, and Enterprise Developers.
C. It does not require a license.
D. It was formerly called Collaboration POD but has been renamed to Avaya Breeze™.
E. It is a development platform that enables rapid development for applications that are targeted to meet a customer's communications needs.

Answer: A,B,E

Explanation:
Avaya Breeze provides a virtualized and secure application platform where Java programmers can develop and dynamically deploy advanced collaboration capabilities that extend the power of Avaya Aura.
Customers, partners, and Avaya organizations can rapidly develop snap-ins and applications that are deployed on Avaya Breeze.

Question: 46

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: B

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

Question: 47

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: D

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

Question: 48

What identifies that the Avaya Breeze™ server is using Identity Certificates that have been signed by Avaya Aura® System Manager (SMGR)?

A. if the Issuer Name states "O=AVAYA, OU=MGMT, CN= System Manager CA" for the Security Module SIP Identity Certificate

B. if the replication status is showing 'Synchronized' with a green background color
C. if a successfully installed WebRTC snap-in is used
D. if the Entity Link between Avaya Aura® Session Manager (SM) and Avaya Breeze™ server is up

Answer: A

Question: 49

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: B

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

Question: 50

The Avaya WebRTC solution uses the web intensively to make media calls from a standard web browser in the internet, into internal and secure communication premises in the enterprise.
Which statement about security between the Enterprise-edge and those standard Web browsers in the internet is true?

A. A trust relationship based on certificates must be built to make WebRTC work.
B. No trust relationship exists between enterprise edge security and web browsers; therefore, the security strategy is based on an Authorization Token instead.
C. There must be a VPN connection between the Web Browser and the Enterprise-edge to build a WebRTC link.
D. WebRTC only works within the Enterprise network. External Web Browsers must connect through an Avaya Session Border Controller for Enterprise (SBCE) via a SIP trunk.

Answer: B

Explanation:
Validation of the authorization token.
The WebRTC Snap-in will validate the authorization token created and encrypted by the web server. If the snap-in can decrypt the token and ensure that the time stamp is valid, it knows that the incoming HTTP request is valid. The time stamp will usually be short lived; on the order of 5- 10seconds to protect against reply attacks.
References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 27
https://downloads.avaya.com/css/P8/documents/101013939

Question: 51

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: D

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

Question: 52

To log on the one-X® Communicator to Avaya Aura® Presence Services server, what do you enter in the IM and Presence / Server field of the one-X® Communicator?

A. the management IP-Address of FQDN of Avaya Breeze™ server
B. the management IP-Address of FQDN of Avaya Aura® Session Manager (SM)
C. the SM100 IP-Address of FQDN of Avaya Aura® Session Manager (SM)
D. the SM100 IP-Address or FQDN of Avaya Breeze™ server

Answer: C

Explanation:

The SIP one-X Communicator needs to be configured to use a specific protocol and port when registering to Session Manager.Enter the IP address of the Session Manager virtual SM-100 card for Session Manager SIP Element.

References: Application Notes for Configuring Avaya AuraTM Presence Services 6.0 with Avaya AuraTM Session Manager 6.0, and Avaya AuraTM Communication Manager for one-XTM Communicator clients as part of Avaya Unified Communication Mobile Worker Solution - Issue 1.0, page 30

https://www.devconnectprogram.com/fileMedia/download/dba93412-03c6-4fda-8d6a- 280ae2193d6f

Question: 53

You are creating a SIP Entity for Avaya Aura® Engagement Development Platform - EDP / Avaya Breeze™.

What do you have to enter in the field labeled FQDN or IP Address?

A. the Management IP-Address or FQDN of the Avaya Breeze™ platform.
B. the SM100 IP-address or FQDN of the Avaya Breeze™ platform
C. the IP-Address or FQDN of Core Platform Cluster
D. the IP-Address or FQDN of general Purpose Cluster

Answer: A

Explanation:

Administering an Avaya Breeze instance

Before you begin

To complete this task you will need:

* The IP address of the Avaya Breeze Management Network Interface.
This is the same IP address you used when deploying the Virtual Machine (VM).
* The IP address including the network mask, and default gateway for the Avaya Breeze Security Module.
Procedure (see step 6 below)
1. On System Manager, in Elements, click Avaya Breeze.
2. Click Server Administration.
3. In the Avaya Breeze Server Instances list, click New.
4. In the SIP Entity field, select the SIP Entity that you created.
5. Ensure that the value in the UCID Network Node ID field is unique across the solution deployment so that it does not conflict with other UCID-generating entities like Avaya Aura Communication Manager or Avaya Aura Experience Portal.
6. In the Management Network Interface FQDN or IP Address field, type the IP address of the Avaya Breeze Management Network Interface.
References: Deploying Avaya Breeze, Release 3.1, (September 2016), page 47
https://downloads.avaya.com/css/P8/documents/101014426

Question: 54

Which two options describe the purpose of TraceSM in the Avaya Aura® Presence Services? (Choose two.)

A. It captures Packet-Size statistics from every telephone call in Avaya Aura® 7.
B. It captures real-time XMPP traffic.
C. It captures Voice and Video Calls media packets in real-time.
D. It captures live traces for both SIP and H323/XMPP clients.
E. It captures Contact details from every user connected to Avaya Aura® Presence Services.

Answer: B,D

Explanation:
It's important to know that traceSM is a real-time capture tool.
traceSM is an interactive perl script that allows an administrator to capture, view, and save call processing activity on a Session Manager. While not as powerful or versatile as wireshark, traceSM is absolutely essential when it comes to working with Avaya SIP. First off, it allows you to view SIP messages even if they have been encrypted with TLS.
References: https://andrewjprokop.wordpress.com/2014/06/02/a-necessary-guide-to-the-avaya- tracesm-utility/

Question: 55

When Avaya Aura® Presence Services is implemented, which statement is true about Port Management?

A. It allows multi-media services over a standard Web-Browser.
B. It allows independent management capabilities to filter out undesired message to every Avaya Aura® Presence Services user.
C. It collects statistics about Port-Usage from each Presence-compatible endpoint across the network.

D. Port 5222 is used for one-X® Endpoints, while Port 5269 is open for connecting with other XMPP 3rd-Party Servers.

Answer: D

Explanation:

Port 5222: XMPP connection configuration

The Connection Manager runs by default when you install the XCP server. It is configured with a JSM Command Processor and two XMPP directors. The XMPP directors handle communication with IM clients. One of the directors is configured to use port 5222 and the other is configured to use port 5223 for secure communications.

Port 5269:Example Obtaining the Server-to-Server Port from an Openfire server

Procedure

1. Log in to the Openfire Web console.
2. Click Server > Server Settings > Server to Server.
3. In the Service Enabled section, the Enabled check box should be checked, and the port value is contained in the box to the right of Remote servers can exchange packets with this server on port.

By default the value is 5269, and it is recommended that this default value be maintained.

References: Administering Avaya Aura Presence Services, Release 6.2.4, (June 2014), pages 110, 154

https://downloads.avaya.com/css/P8/documents/100180467

Question: 56

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

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

Question: 57

Which statement about Avaya Aura® Presence Services 7.x snap-in licensing is true?

A. It requires an instance-license.
B. It requires a per-user license.
C. It does not require a license to work.
D. It requires a license file for each snap-in installed.

Answer: C

Explanation:
Presence Services snap-in does not require a license to work.
References: Avaya Aura® Presence Services Snap-in Reference. Release 7.0.1 (December 2016), page 17
https://downloads.avaya.com/css/P8/documents/101013646

Question: 58

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: C

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

Question: 59

Which statement about the SIP Entities to support Avaya Aura® Presence Services is true?

A. Only one SIP Entity is built of Type = “Presence Services”, which uses the SM100 IP address of the Avaya Breeze™ node.
B. Only one SIP Entity is built of Type = “Engagement Development Platform”, which uses the SM100 IP Address of the Avaya Breeze™ node.
C. Two SIP Entities are built to the same SM100 IP address of each node. One is of Type = “Engagement Development Platform”, and the other is of Type = “Other”.
D. Two SIP Entities are built to the same SM100 IP address of each node. One is of Type = “Engagement Development Platform”, and the other is of Type = “Presence Services”.

Answer: B

Question: 60

You need to connect Avaya Breeze™ platform that is hosting Avaya Aura® Presence Services Snap-in with Avaya Aura® Session Manager (SM).
Which three are needed? (Choose three.)

A. ports UDP 5060 and TLS 5061
B. one Entity Link from SM to Avaya Aura® Presence Services Snap-in
C. one Entity Link from SM to Avaya Breeze™
D. TLS 5061 and TLS 5062
E. ports TCP 5060 and UDP 5060

Answer: B,C,D

Explanation:

BD: Administering Entity Link between Presence Services Cluster SIP Entity and Session Manager Procedure

1. On the System Manager web console, navigate to Elements > Routing > Entity Links.
2. In the Name field, enter a name for Entity Link.
3. In the SIP Entity 1 field, select the Session Manager instance.
4. In the Protocol field, select TLS.
5. In the Port field, type 5062.

Note: Note that this port number cannot be the same as the port number administered in "Administering Entity Link between Avaya Breeze and Session Manager".

CD: Administering Entity Link between Avaya Breeze and Session Manager.

About this task

Create an En2tity Link to connect Session Manager to Avaya Breeze. You must administer separate
Entity Links for Avaya Breeze servers in order to open SIP listeners on the designated ports.
Session Manager requires a Listen Port with the Listen Port as 5061, Protocol as TLS, and Default
Domain as the login domain of endpoint devices. Without this, PPM will fail for SIP endpoints.

References: Avaya Aura® Presence Services Snap-in Reference. Release 7.0.1 (December 2016), pages 25-26
https://downloads.avaya.com/css/P8/documents/101013646

Question: 61

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: A

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.

Question: 62

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: B

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

Question: 63

If more than one Avaya Breeze™ node is available in the cluster, which statement about redundancy and load-balancing is true?

A. IM clients point to any Avaya Breeze™ node SM100 IP address. The client is dynamically informed of alternate Avaya Breeze™ nodes in the cluster.
B. The list of all Avaya Breeze™ nodes SM100 IP addresses must be configured in the client.
C. The Cluster IP address is not used for Presence Services in 7.0. IM clients configure a FQDN instead of IP address which is resolved by a DNS server to all Avaya Breeze™ nodes in the cluster.
D. IM clients point to the Leader Avaya Breeze™ node SM100 IP address which redirects the clients to a particular Avaya Breeze™ node based on load-balancing policy.

Answer: D

Explanation:
Enable load balancing for a cluster if you want to scale the HTTP services without targeting a particular Avaya Breeze™ server. All the requests are sent to the cluster IP address. When you enable load balancing, two Avaya Breeze™ servers are chosen as the active and standby load balancing servers. The active load balancer distributes the HTTP requests to all the other servers in the cluster in a round robin fashion.
References: Administering Avaya Breeze, Release 3.1 (May 2016), page 16
https://downloads.avaya.com/css/P8/documents/101014143

Question: 64

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: C

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

Question: 65

What should be verified before running the initTM -f command on the Command Line Interface of Avaya Breeze™ platform (formerly known as Engagement Development Platform (EDP))?

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: B

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

Question: 66

You are creating the identity certificates that must be installed in the Avaya Session Border Controller for Enterprise (SBCE).
Which statement about installing the certificate files in the SBCE is true?

A. The cert file and the Key filenames generated by the Certificate Authority must match.
B. Both the PEM and Key files must be in a zip file.
C. The SBCE must be rebooted before the files installation.
D. The cert file and the Key filenames generated by the Certificate Authority must be different.

Answer: A

Question: 67

You are starting the process to create a server certificate so it can be installed in the Avaya Session Border Controller (SBC).
What must be done before creating a server certificate for SBC?

A. Generate a Certificate Signing Request (CSR) in SBC.
B. Run initTM -d from SBC CLI.
C. Add End Entity in Session Manager.
D. Download a CA PEM file from System Manager.

Answer: A

Question: 68

Which statement about the SIP Entities to support single node Avaya Aura® Presence Services is true?

A. Only one SIP Entity is built of Type = “Presence Services”, which uses the SM100 IP address of the Avaya Breeze™ node.
B. Only one SIP Entity is built of Type = “Avaya Breeze”, which uses the SM100 IP address of the Avaya Breeze™ node.
C. Two SIP Entities are built to the same SM100 IP address of each node. One is of type = “Avaya Breeze”, and the other is of Type = “Presence Services”.
D. Two SIP Entities are built to the same SM100 IP address of each node. One is of type = “Avaya Breeze”, and the other is of Type = “Other”.

Answer: B

Question: 69

Avaya Aura® Presence Services 7.x is implemented on Avaya Breeze™ (formerly Engagement Development Platform (EDP)).
When looking at Elements > Breeze > Service Management > Services, which status would you expect for a Presence Services snap-in that is ready to support Avaya Aura® Presence Services?

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

Answer: A

Question: 70

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

Answer: C,E