Question: 1

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

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: 2

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: 3

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

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: 4

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

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: 5

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

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: 6

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

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

Question: 7

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