

3102^{Q&As}

Avaya IP Office Implementation

Pass Avaya 3102 Exam with 100% Guarantee

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

<https://www.pass2lead.com/3102.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1



When creating a New User Profile, an administrator is asked to enter, two separate passwords for the new user. Which statement best describes the need for two different passwords?

- A. The Identity password is used in authenticating the user when accessing the user's management console, while the Communication Profile is used to authenticate the user when logging in on a telephone.
- B. The Communication Profile is the prime password for authenticating the user while the Identity password is a backup password used to reset the Communication Profile in cases where the prime password is forgotten.
- C. The Identity password is used when logging in to a telephone that connected to the corporate network while the Communication Profile is used while logging in with a VPN telephone or the corporate network.
- D. The Identity password is used when logging into a telephone in to a communication profile password enables further privileges and capability.

Correct Answer: A

QUESTION 2

Review the error message in the installation log shown in the exhibit. What is the probable cause for initDRs to fail and how can it be fixed?

- A. There is a non-bidirectional FQDN resolution between Session Manager and System Manager. Verify the enrollment password used to initialize trust management has not expired
- B. There is a JMX connection error. Verify the enrollment password used to initialize trust management has not expired.
- C. There is a non-bidirectional FQDN resolution between Session Manager and System Manager. Verify that either the System Manager or the Session Manager has updated DNS records or the hostnames have been added to the

/etc/hosts file on the Session Manager and the System Manager.

D. There is a JMX connection error. Verify that either the System Manager or the Session Manager has updated DNS records, or the hostnames have been added to the /etc/hosts file on the Session Manager and the System Manager.

Correct Answer: C

QUESTION 3

A technician has been asked to apply an Application Sequence to call made from / to a non-SIP user who does not have Session Manager Profile. Which sequence describes the steps that should be taken?

A. Add an Avaya-SIP Communication Address to the user\'s User Profile. Add a Session Manager Profile to the user\'s User Profile. Select appropriate Originating and Terminating Sequences for the user from the options in the new Session Manager Profile.

B. Create a new Implicit User rule. Define a number pattern that can be compared with dialed numbers. Select appropriate Originating and Terminating Sequences to be applied when a match occurs.

C. Navigate to the list of Application Sequences and select the sequence to apply to the non-SIP user. Add the user\'s extension number to the list of associated users. Select appropriate check box options to determine if the sequence should be applied In originating

mode, terminating mode or both.

D. Create a new Non-SIP User Application Sequence Policy. Define the address and location of the non-SIP user. Select appropriate Originating and Terminating Sequences for the non-sip user from the given options.

Correct Answer: B

QUESTION 4

Which statement expresses the relationship between users, roles, and groups?

A. Roles grant permissions. Users are not directly assigned roles but inherit them through belonging to groups.

B. A group is a name for a collection of roles and each role is assigned its own administrator user.

C. Users can belong to groups for easy management and can be assigned roles which grant them access rights.

D. Groups and roles directly correspond to sections of the SMGR Web Console navigation pane and, unless a user belongs to a specific role group, they cannot access the corresponding management screens.

Correct Answer: C

QUESTION 5

How is call Admission Control enabled for Session Manager Release 6.1?

A. Call Admission Control is enabled in the SIP Entity by specifying a value for Managed Bandwidth.

- B. Call Admission Control is enabled on the Session Manager instance by specifying a value for Managed Bandwidth.
- C. Call Admission Control is enabled on a Location by specifying a value for Managed Bandwidth.
- D. Call Admission Control is enabled on an Entity Link specifying a value for Managed Bandwidth on the Locations screen in Session Manager.

Correct Answer: D

[Latest 3102 Dumps](#)

[3102 VCE Dumps](#)

[3102 Braindumps](#)