Testpassport Q&A

La meilleure qualité le meilleur service

Exam : **050-V71X-CSESECURID**

Title : RSA SecurID Certified Systems Engineer 7.1x Exam

Version : Demo

1.If the RSA RADIUS server is NOT installed at the time of the RSA Authentication Manager software installation and the RADIUS function is needed at a later date, (Choose two)
A. it can be added to the Authentication Manager server through the Operations Console.
B. it can be added to the Authentication Manager server using the add_rad_svr command line utility.
C. it can be installed on a separate host and connected to the existing Authentication Manager server.
D. Authentication Agents can be configured to proxy RADIUS transactions without the need for a RADIUS server
E. it cannot be added to the Authentication Manager server without uninstalling then reinstalling the server software.
Answer: C E

2.If an organization's general security policy specifies that certain RSA SecurID tokens will be used without a PIN (tokencode only), this can be accomplished by editing the parameters
A. in the records for individual tokens.
B. in the Realm Authentication Policy.
C. in the Security Domain Token Policy.
D. in the Security Domain Password Policy.
Answer: A

3.If manual load balancing has just been set up for an Authentication Agent and it appears that the Agent is not contacting the desired servers, it might be helpful to verify the contents of the
A. sdopts.rec file.
B. sdconf.rec file.
C. sdstatus.12 file.
D. sdagent.rec file.
Answer: A

4.Which of the following statements is true about the RSA RADIUS Server in an RSA Authentication Manager version 7.1 environment?
A. A single RADIUS server can be configured to support multiple realms across a single Authentication Manager deployment.
B. Once the RADIUS server is installed in an Authentication Manager environment, all users default to using the RADIUS protocol for authentication.
C. If RADIUS is integrated with an Authentication Manager deployment, all users who authenticate via RADIUS must be issued an RSA SecurID token.
D. If a RADIUS server is not installed at the same time as a Primary or Replica server, it can NOT be added later without uninstalling and re-installing the Primary or Replica software.
Answer: D

5.As part of the Primary server installation, the installer automatically backs up certain files in the RSA Authentication Manager/backup/ directory. These files
A. include the system private key file.
B. hold the contents of the embedded database.
C. are used to install Replica servers and Server Nodes.
D. are deleted after the Primary services successfully start.
Answer: A

6.When planning an RSA SecurID system deployment, the Agents that will be required are dependent on
A. the type of authenticator assigned to users in the system.
B. the variety and type of entry points to a given network or protected resource.
C. the total number of users that exist in all Authentication Manager Security Domains.
D. the communication (port) configurations of any firewalls separating Agent devices and authentication servers.
Answer: B

7.Ninety (90) days after installation, if the initial Super Admin user's password is not changed, the initial Super Admin user
A. is required to change their password before accessing both the Operations Console and Security Console.
B. can access both the Operations Console and Security Console but is reminded to change passwords after logon.
C. is allowed to access the Operations Console but is required to change their password before accessing the Security Console.
D. is locked out of both the Operations Console and the Security Console until another administrator re-sets the password and unlocks the account.
Answer: C

8.RSA Authentication Agents are typically installed and configured
A. only outside a corporate or internet firewall.
B. according to a general security policy and access control plan.
C. before the installation of the RSA Authentication Manager server.
D. before users have been assigned and trained on the use of RSA SecurID tokens.
Answer: B

9.When using an RSA Authentication Agent for PAM, which of the following statements is true?
A. Users designated for RSA SecurID authentication must have root privileges.
B. A user's account must specify 'sdshell' to allow RSA SecurID authentication.
C. When installing the Agent for PAM, the services file must be edited to add "securid_pam" as a TCP service.
D. Service, rule and module information to support RSA SecurID authentication are

contained in the pam.conf file.
Answer: D

10.To use an LDAP directory server as a source for user and group data in an RSA Authentication Manager database,
A. an Identity Source can be mapped to the LDAP directory through the Authentication Manager Operations Console.
B. individual data transfer jobs can be scheduled through the Scheduled Jobs function of the Authentication Manager Security Console.
C. a data export can be initiated on the directory server to export users and groups to the Authentication Manager database over a secure SSL connection.
D. a new LDAP schema is applied to the directory server to include the attribute "cn=securid" to designate users to be transferred to Authentication Manager.
Answer: A