IBM Security Access Manager V9.0 Deployment

1. A customer has a developed an OAuth 2.0 Client application to access resources on behalf of a user. The customer states that the OAuth client has the following two constraints:
1. The OAuth client is not capable of maintaining its credentials confidential for authentication with the authorization server.
2. The resource owner does not have a trust relationship with the client What is the suitable OAuth 2.0 grant type for the API Protection Policy if the user resource accessed by the OAuth 2.0 client is to be protected by IBM Security Access Manager V9.0?

A. Implicit Grant

B. Client Credentials Grant

C. Authorization Code Grant

D. Resource Owner Password Credentials Grant

Answer(s): B

---

2. In a customer environment, a REST API client is being developed to carry out Reverse Proxy configuration and maintenance. As part of one of the activities the customer needs to update the junction information with an additional Backend Server. The customer has written a REST API client but is not able modify the junction.
Which HTTP headers should the customer pass?

A. Host, Authorization

B. Host, Accept: Application/json

C. Authorization, Accept:Application/json

D. content-type:application/json, Authorization

Answer(s): C

---

3. During installation WebSEAL provides a default certificate key database that is used to authenticate both clients and junctioned servers.
Which stanza entry of the WebSEAL configuration file points to the default certificate key database (i.e. kdb file)?

A. ssl-keyfile

B. jct-cert-keyfile

C. webseal-cert-keyfile

D. webseal-cert-keyfile-label

Answer(s): B

---

4. A company has a large number of users who use mobile applications. The company wants to implement context-aware access controls for these resources.
Which module of IBM Security Access Manager V9.0 should the company enable to support this requirement?

A. Federation module

B. Protocol Analysis module

C. Mobile Access Control modulo

D. Advanced Access Control module

Answer(s): A

---

5. A request for a virtual host junction shows an unexpected source IP address.
Which troubleshooting tool can be used to investigate this issue?

A. Host File

B. Snapshots

C. Support Files

D. Packet Tracing

Answer(s): A

---

6. An IBM Security Access Manager V9.0 deployment professional is charged with monitoring request response times from WebSEAL to the backend. The deployment professional wants the flexibility to see response times per request, per junction, per HTTP return code, or other criteria that may come up in the future.
What action will generate the required data for this analysis?

A. Customize the request.log to include response times

B. Run pdadmin "stats get pdweb.jct" on all junctions on a regular basis

C. Run pdadmin "stats get pdweb.https" and "stats get pdweb.http" on a regular basis

D. Write a REST API script to pull "application interface statistics" on a regular basis

Answer(s): D

---

7. A deployment professional attempts to log into an appliance which is part of a cluster to run pdadmin commands and receives the following message:
pdadmin> login -a sec_master -p password
2016-03-03-02:04:38.683-06:001------0x1354A420 pdadmin ERROR ivc socket mtsclient.cpp 2376 0x7fc2b7b0c720
HPDCO1056E Could not connect to the server 192.168.254.11, on port 7135. Error: Could not connect to the server. (status 0x1354a426) What should the deployment professional check concerning the login target?

A. Login was attempted on a special node

B. Login was attempted on a restricted node

C. Login was attempted on a secondary master that has not been promoted to the primary

D. Login was attempted on a non-primary master of a cluster and the primary policy server is down

Answer(s): A

---

8. A customer is migrating from TAM v6.1 running on AIX to IBM Security Access Manager (ISAM) V9.0 hardware appliances.
Which information from the TAM v6.1 environment will be useful in sizing the new ISAM V9.0 hardware configuration?

A. WebSEAL request logs

B. WebSEAL CDAS specifics

C. Number of LDAP replicas

D. Number of objects in the protected object space

Answer(s): D

---

9. There is an SSL connectivity issue between the IBM Security Access Manager V9.0 Reverse Proxy and the backend business application.
Which two troubleshooting commands under Tools in the application SSH interface can be used to validate the Reverse Proxy can successfully connect to the backend host:secure-port? (Choose two.)

- [ ] A. ping
- [ ] B. session
- [ ] C. connect

- [ ] D. traceroute
- [ ] E. connections

Answer(s): B C

---

10. An IBM Security Access Manager V9.0 Reverse Proxy has a stateful junction to a Portal application called "/wps". There is no web server in front of Portal. This junction has three Portal servers defined behind it. The Portal team needs to do maintenance on each of the three servers. The team wants to accomplish this with least impact to end users.
Which pdadmin "server task" based steps will accomplish this?

A. Stop a server, have Portal team apply maintenance, bring server online - repeat for the other two servers

B. Delete a server, have Portal team apply maintenance then add server back - repeat for the other two servers

C. Take a server offline, have Portal team apply maintenance, bring server online - repeat for the other two servers

D. Throttle a server, ensure activity has ceased for that server, have Portal team apply maintenance, bring server online - repeat for the other two servers

Answer(s): C

---

11. A customer received a replacement hardware appliance, but on boot up it has a different firmware than that for IBM Security Access Manager (ISAM) V9.0. The appliance needs to be flashed to ISAM V9.0. The appliance needs to be rebooted with a bootable USB drive formatted as FAT32.
Which file format is needed to create the bootable drive?

A. .iso

B. .ova

C. .pkg

D. .img

Answer(s): A

---

12. A risk officer of an organization discovered that a site protected by the IBM Security Access Manager V9.0 solution might be vulnerable to common attacks like cross-site scripting (XSS) and SQL injection.
Which optional component should be configured to protect against these attacks?

A. Federation

B. Secure Web Settings

C. Advanced Access Control

D. Web Application Firewall

Answer(s): D

---

13. A stateful junction /WebApp is added to a Web reverse proxy instance with two backend HTTP servers.
When one of the backend server stops responding to the requests, the users are getting the "Third Party Not Responding" error message even though one of the backend server continues to respond.
Which parameter needs to be added to the configuration file so that "Third Party Not Responding" error page is not rendered and the user is connected to the backend server that is responding?

A. use-same-session = yes

B. use-new-stateful-on-error = yes

C. failover-include-session-id = yes

D. enable-failover-cookie-for-domain = yes

Answer(s): A

---

14. An IBM Security Access Manager V9.0 deployment professional executes the following steps:
1. Navigate to Edit SSL Certificate Database - embedded_ldap_keys
2. Select the embedded LDAP server certificate
3. Click Manage->Export
4. Save the resulting .cer file onto local desktop
Which task was the deployment professional performing?

A. Renewing the embedded LDAP server certificate

B. Replacing the embedded LDAP server certificate

C. Creating a backup of the embedded LDAP server certificate

D. Preparing to configure SSL for a local LDAP client to the embedded LDAP server

Answer(s): B

---

15. An IBM Security Access Manager V9.0 systems deployment professional needs to protect a back-end web applications from SQL injection attacks that match signatures from the IBM X-Force signature database.
Which action needs to be performed?

A. Simulation Mode must be enabled and a Risk Profile must be specified.

B. Web Content Protection must be enabled and a Risk Profile must be specified.

C. Simulation Mode must be enabled and a Registered Resource must be specified.

D. Web Content Protection must be enabled and a Registered Resource must be specified.

Answer(s): A

---

16. The IBM Security Access Manager (ISAM) V9.0 LMI SSL certificate is auto-generated by default.
When the LMI certificate is due to expire, how is it renewed?

A. The ISAM Appliance will renew LMI certificate automatically.

B. The ISAM deployment professional must issue reset_lmi_cert using command line interface

C. The ISAM deployment professional must re-generate it using LMI Manage System Settings -> SSL panels.

D. The ISAM deployment professional must create a new self sign certificate using LMI Manage System Settings -> SSL panels.

Answer(s): C

---

17. The customer currently maintains all its users in Active Directory. As part of its new IBM Security Access Manager (ISAM) V9.0 deployment, the customer understands it will have to implement the ISAM "Global Sign-on (GSO)" to achieve SSO with certain backend applications which do their own authentication and cannot be modified.
Which federated repositories configuration will address the customer requirements?

A. Use an external ISDS LDAP as the ISAM Primary LDAP, federate with the AD and import all AD users into the ISAM TDS

B. Configure the AD as the ISAM Primary LDAP, which will create the necessary secauthority=default suffix. Import all users into the ISAM AD

C. Use the ISAM embedded LDAP as the Primary LDAP, federate with the AD and configure "basic user", and specify "basic-user-principal-attribute = samAccountName"

D. Use an external ISDS LDAP as the Primary LDAP, federate with the AD, configure "basic user", specify "basic-user-principal-attribute = samAccountName" and "basic-user-search-suffix = secauthority=default"

Answer(s): B

---

18. A customer has three LDAP servers: A master (ds1.example.com), another master (ds2.example.com) and a read-only replica (ds3.example.com) used for IBM Security Access Manager (ISAM) V9.0. The deployment professional has configured the ISAM runtime using ds1.example.com as the registration server.
Which configuration will provide load balancing for LDAP read across all three servers and failover to ds2.example.com for LDAP write?

A. replica = ds2.example.com,389,readonly,5replica = ds3.example.com,389,readonly,5replica = ds2.example,com,389,readwrite,6

B. replica = ds1.example.com.389,readonly,6replica = ds2.example.com,389,readonly,6replica = ds3.example.com,389.readonly,6replica = ds2.example.com,389,readwrite,4

C. replica = ds1.example.com,389,readonly,4replica = ds2.exomple.com,389,readonly,4replica = ds3.example.com.389,readonty,4replica = ds2.example com,389,readwrite,6

D. replica = ds1.example.com,389,readonly,1replica = ds2.example.com,389,readonly,2replica = ds3.example.com,389,readonly,3replica = ds2.exomple.com,389,readwrrte,4

Answer(s): A

---

19. Which web resource should be used to keep up to date on support flashes, fixpack announcements, and other product related issues?

A. The IBM Support Portal

B. The IBM Security twitter account

C. The LinkedIn IBM Security Access Manager V9.0 Group

D. The IBM devWorks IBM Security Access Manager V9.0 Forum

Answer(s): D

---

20. A customer has deployed an IBM Security Access Manager V9.0 solution to protect web applications. After the initial authentication between the client and WebSEAL, WebSEAL can build a new Basic Authentication header and use the --b option to provide the authenticated Security Access Manager user name (client's original identity) together with a predefined static password across the junction to the back-end server.
Which configuration option will accomplish this?

A. b gso

B. b filter

C. b ignore

D. b supply

Answer(s): C
