

100% Money Back
Guarantee

Vendor: IBM

Exam Code: C2150-198

Exam Name: IBM Security Access Manager V7.0
Implementation

Version: Demo

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which utility provides backup, restore, and extract capabilities for Security Access Manager data?

- A. pdinfo
- B. pdbackup
- C. pdservice
- D. pd_backup

Answer: B

Question No : 2 - (Topic 1)

What pdbackup command restores the contents of an Access Manger archived file on a Windows operating system to a specific folder?

- A. pdbackup -a extract
- B. pdabckup -a backup
- C. pdbackup -a restore
- D. pdbackup -a retrieve

Answer: A

Question No : 3 - (Topic 1)

When performing an upgrade, which utility is used to back up the information in Tivoli Directory Server?

- A. ldapadd
- B. bulkload
- C. idsdb2ldif
- D. idscreateldif

Answer: C

Question No : 4 - (Topic 1)

Which registry is NOT supported by ISAM 7?

- A. Lotus?Domino?Lotus?Domino
- B. IBM?Tivoli?Directory Server
- C. Microsoft Active Directory 2008
- D. Sun Java?System Directory Server 7

Answer: A

Question No : 5 - (Topic 1)

Which statement is FALSE regarding local response redirection?

- A. We need to use External authentication interface to implement local response redirection.
- B. When local response redirection is enabled, change password must be handled by WebSEAL.
- C. When using local response redirection, WebSEAL no longer has the responsibility of generating responses to client requests.
- D. When local response redirection is enabled, the redirection is used for all local WebSEAL response types: login, error, informational, and password management.

Answer: A

Question No : 6 - (Topic 1)

Which statement is true for the ISAM appliance snapshot?

- A. It is only a backup of the LMI.
- B. It is a backup of all WebSEAL instances.
- C. It is a copy of the state of the appliance at a certain time.
- D. It is a backup of the Policy Server and WebSEAL instances.

Answer: C

Question No : 7 - (Topic 1)

What is the correct archive file If pdbackup -a backup -list C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst is executed using ISAM on a Windows Server?

- A. C:\Program Files\Tivoli\Policy Director\pdbackup\pdbackup.lst_30aug2013.11.30.dar
- B. C:\Program Files\Tivoli\Policy Director\pdbackup\pdbackup.lst_30.08.2013.11.30.dar
- C. C:\Program Files\Tivoli\Policy Director\pdbackup\pdbackup.lst_30aug2013.11_30.dar
- D. C:\Program Files\Tivoli\Policy Director\pdbackup\pdbackup.lst_30.08.2013.11_30.dar

Answer: C

Question No : 8 - (Topic 1)

You have a default setup of ISAM, ITDS and a Microsoft SharePoint backend. A Web environment is experiencing performance issues. In order to conduct analysis, tracing is temporarily switched on using the following commands:

```
server task web04-webseald-unix08 trace set pdweb.debug 2 file path=/tmp/trace.log
```

```
server task web04-webseald-unix08 trace set pdweb.debug 0
```

During analysis of the trace.log various common occurrences appear, the following trace.log extract displays only the lines important for this question.

```
2013-05-26-22:08:01.681+02:00| ----- Browser ==> PD ----- 2013-05-26-22:08:01.684+02:00| ----- Browser <=== PD ----- 2013-05-26-22:08:09.283+02:00| ----- Browser ==> PD ----- 2013-05-26-22:08:16.682+02:00| ----- PD ==> BackEnd ----- 2013-05-26-22:08:17.049+02:00| ----- PD <=== BackEnd ----- 2013-05-26-22:08:17.051+02:00| ----- Browser <=== PD -----
```

What can be concluded by analyzing this trace excerpt?

You indicate you wish to make this a sample question, remove the reference here.

- A. This excerpt indicates no performance or other issues.
- B. This excerpt indicates that ITDS has a performance issue.
- C. This excerpt indicates that the user has given a wrong password.
- D. This excerpt indicates that the backend has a performance issue

Answer: B

Question No : 9 - (Topic 1)

You have a default setup of ISAM, ITDS and a Microsoft SharePoint backend. A Web environment is experiencing performance issues. In order conduct analysis, tracing is temporarily switched on using the following commands:

```
server task web04-webseald-unix08 trace set pdweb.debug 2 file path=/tmp/trace.log
```

```
server task web04-webseald-unix08 trace set pdweb.debug 0
```

During analysis of the trace.log various common occurrences appear, the following trace.log extract displays only the lines important for this question.

```
2013-05-26-22:08:01.681+02:00| ----- Browser ==> PD ----- 2013-05-26-22:08:01.682+02:00| ----- PD ==> BackEnd ----- 2013-05-26-22:08:07.216+02:00| ----- PD <=== BackEnd ----- 2013-05-26-22:08:07.217+02:00| ----- Browser <=== PD -----
```

What can be concluded by analyzing this trace excerpt?

- A. This excerpt indicates no performance or other issues.
- B. This excerpt indicates that ITDS has a performance issue.
- C. This excerpt indicates that the user has given a wrong password.
- D. This excerpt indicates that the backend has a performance issue.

Answer: D

Question No : 10 - (Topic 1)

Which configuration enables the day time error page?

- A. [acct-mgt]
client-alert-tod = yes
- B. [acct-mgt]
client-alert-dot = yes
- C. [acct-mgt]

client-notify-tod = yes
D. [acct-mgt]
client-notify-dot = yes

Answer: C

Question No : 11 - (Topic 1)

What is the default credential to log on to ISAM 7 WGA command-line interface?

- A. root, root
- B. admin, admin
- C. superadmin, secret
- D. sec_master, object00

Answer: B

Question No : 12 - (Topic 1)

What will help reduce the volume of audit event, while preserving important audit information?

- A. complete disablement of event generation
- B. generation of events for successful HTTP accesses only
- C. generation of events for unsuccessful HTTP accesses only
- D. reconfiguration of WebSEAL to use CARS auditing instead of native auditing

Answer: C

Question No : 13 - (Topic 1)

Recently the Risk Officer of your organization discovered that all key databases containing web certificates in the organization are protected with a very weak password. You are assigned to change the password on every key database into a more complex one. How can this be accomplished?

- A. Open iKeyman, open the appropriate key database, enter the current password, and

select "Change Password".

B. Generate a new stash file using command "ibmstash -db key.kdb -stash key.sth -password <current password> -newpassword <new password>"

C. This is not possible, a new key database has to be created; the current certificates can be exported from the old KDB into the new one.

D. Edit the webseald-default.conf configuration file and change the pointers to the key database password from a stash file to a plain text password and specify the password.

Answer: A

Question No : 14 - (Topic 1)

How are ISAM users and groups logically separated within a single policy server?

A. By creating multiple object spaces.

B. By installing multiple user registries.

C. By creating multiple secure domains.

D. By installing multiple policy proxy servers.

Answer: C

Question No : 15 - (Topic 1)

What are two installable components of the Common Auditing and Reporting Serve?
(Choose two.)

A. Audit Service.

B. Report Service

C. Audit Client Setup Utilities

D. Audit Configuration Console

E. Report Configuration Console

Answer: A,D

Question No : 16 - (Topic 1)

An Administrator wants to restore the amwebbackup.lst_22dec2011.10_22.tar archive file that is stored in the /var/pdbackup directory to the /amwebtest directory. Which command should the administrator run?

- A. pdrestore --f /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar -p /amwebtest
- B. pdinfo -a restore -f /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar -p /amwebtest
- C. pdbackup -a restore -f /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar -p /amwebtest
- D. pd_backup -a restore -f /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar -p /amwebtest

Answer: C

Question No : 17 - (Topic 1)

What would the command "ldapsearch -p 389 -D cn=root -w ? -b cn=connections,cn=monitor -s base objectclass=*" return?

- A. The current_workqueue_size.
- B. The auto_connection_cleaner_run.
- C. The number of monitor threads available.
- D. The current established client connections.

Answer: D

Question No : 18 - (Topic 1)

Which statement is true when using the WGA with the internal LDAP?

- A. The internal LDAP cannot be tuned.
- B. Tuning can only be performed using the LMI.
- C. Tuning can only be performed using a RESTful API.
- D. Tuning can be performed using both the LMI and a RESTful API.

Answer: A

Question No : 19 - (Topic 1)

Which two aspects of logging event activity can be controlled? (Choose two.)

- A. How large each log file can be for each event class
- B. Generate HTML-formatted logging for specific event classes
- C. Where to direct the output for each event class
- D. Send the output to third party application for specific classes
- E. How often log files are changed

Answer: A,C

Question No : 20 - (Topic 1)

What are two advantages of using persistent connections between WebSEAL and a junctioned backend server? (Choose two.)

- A. Faster response time for the request.
- B. Reduces the chance of thread overrun.
- C. Less entries in the in the WebSEAL session cache.
- D. Less CPU usage for both the WebSEAL and the junction application server.
- E. A significant benefit of response times only if the objects requested are large.

Answer: A,D

Question No : 21 - (Topic 1)

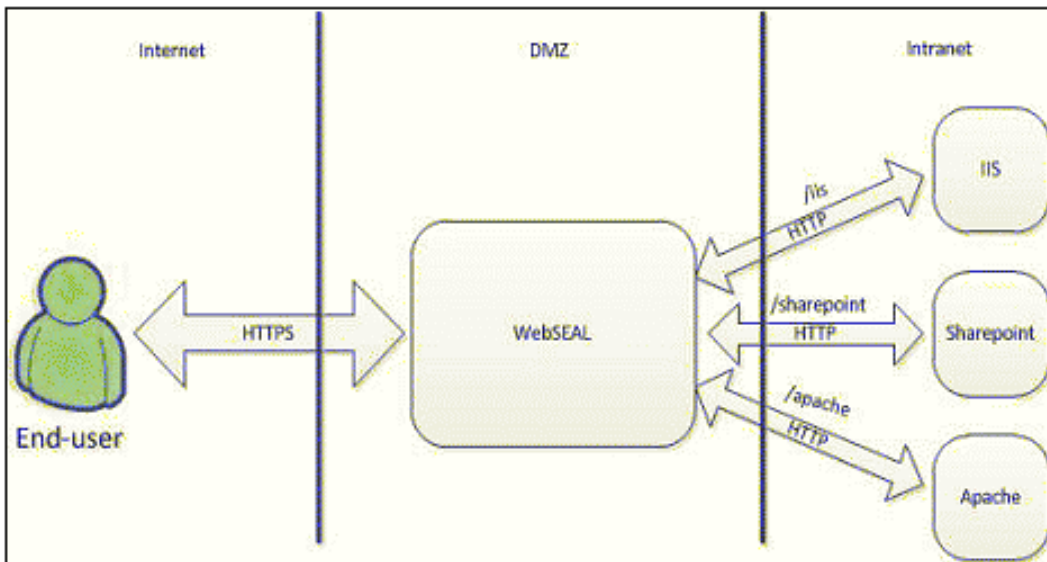
Each routing file contains entries that control the logging of events. What type of events?

- A. Message events and Error events
- B. Message events and Trace events
- C. Message events, Trace events and Error Events
- D. Message events, Trace events, Error events and Fatal events

Answer: B

Question No : 22 - (Topic 1)

Click on the Exhibit.



The exhibit displays a high-level setup of a basic Security Access Implementation. All communication between end-user and WebSEAL happens over HTTPS. The communication between DMZ and Intranet is HTTP-based. What information is gathered if 'pdweb.https' is enabled on WebSEAL?

- A. Information about the WebSEAL session cache.
- B. Information about successful and failed client certificate authentication attempts.
- C. Information about response times of HTTPS-requests between end-user and WebSEAL.
- D. Information about response times of HTTPS-requests between WebSEAL and backend servers (in case of SSL-junctions).

Answer: C

Question No : 23 - (Topic 1)

What command will list all components that are available to gather and report statistics for the given WebSEAL instance 'internet'?

- A. Server task internet-webseald-www.ibm.com stats
- B. Server task internet-webseald-www.ibm.com stats on
- C. Server task internet-webseald-www.ibm.com stats list
- D. Server task internet-webseald-www.ibm.com stats show

Answer: C

Question No : 24 - (Topic 1)

Given the following conditions:

pdweb.authn

For the pdweb.authn component:

- 1.The frequency is set to 40 seconds.
- 2.The destination for the statistics report is the /tmp/auth.log file.

pdweb.jct.1

For the pdweb.jct.1 component:

- 1.The frequency is set to 50 seconds,
- 2.The destination for the statistics report is the /tmp/jct.log file.

pdweb.jmt

For the pdweb.jmt component:

- 1.The frequency is set to 20 seconds.
- 2.The destination for the statistics report is the /tmp/jmtA.log and the /tmp/jmtB.log files

What would the configuration in the stanza [aznapi-configuration] look like?

-
- A. [aznapi-configuration]
stats = pdweb.jmt 20
stats = pdweb.authn 40
stats = pdweb.jct.1 50
logcfg = stats.pdweb.jmt:file path=/tmp/jmtA.log,rollover_size=-1,flush=20
logcfg = stats.pdweb.jmt:file path=/tmp/jmtB.log,rollover_size=-1,flush=20
logcfg = stats.pdweb.authn:file path=/tmp/auth.log,rollover_size=-1,flush=20
logcfg = stats.pdweb.jct.1:file path=/tmp/jct.log,rollover_size=-1,flush=20
 - B. [aznapi-configuration]
logcfg = pdweb.jmt:file path=/tmp/jmtA.log,rollover_size=-1,flush=20,frequency=20
logcfg = pdweb.jmt:file path=/tmp/jmtB.log,rollover_size=-1,flush=20,frequency=20
logcfg = pdweb.authn:file path=/tmp/auth.log,rollover_size=-1,flush=20,frequency=40
logcfg = pdweb.jct.1:file path=/tmp/jct.log,rollover_size=-1,flush=20,frequency=50
 - C. [aznapi-configuration]
stats = pdweb.jmt:file path=/tmp/jmtA.log,rollover_size=-1,flush=20,frequency=20
stats = pdweb.jmt:file path=/tmp/jmtB.log,rollover_size=-1,flush=20,frequency=20
stats = pdweb.authn:file path=/tmp/auth.log,rollover_size=-1,flush=20,frequency=40
stats = pdweb.jct.1:file path=/tmp/jct.log,rollover_size=-1,flush=20,frequency=50
 - D. [aznapi-configuration]
stats = pdweb.jmt 20
stats = pdweb.authn 40
stats = pdweb.jct.1 50
logcfg = stats.pdweb.jmt:file path=/tmp/jmtA.log: path=/tmp/jmtB.log,rollover_size=-1,flush=20
logcfg = stats.pdweb.authn:file path=/tmp/auth.log,rollover_size=-1,flush=20
logcfg = stats.pdweb.jct.1:file path=/tmp/jct.log,rollover_size=-1,flush=20

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Question No : 25 - (Topic 1)

Statistical reporting can be enabled dynamically, making it possible to overrule the static configuration. How can this be achieved?

- A. Using the WebSEAL routing file
- B. Using the pdadmin-statement 'stats on'
- C. Using the stanza '[aznapi-configuration]'
- D. Using the configuration file 'stats.monitor'

Answer: B

Question No : 26 - (Topic 1)

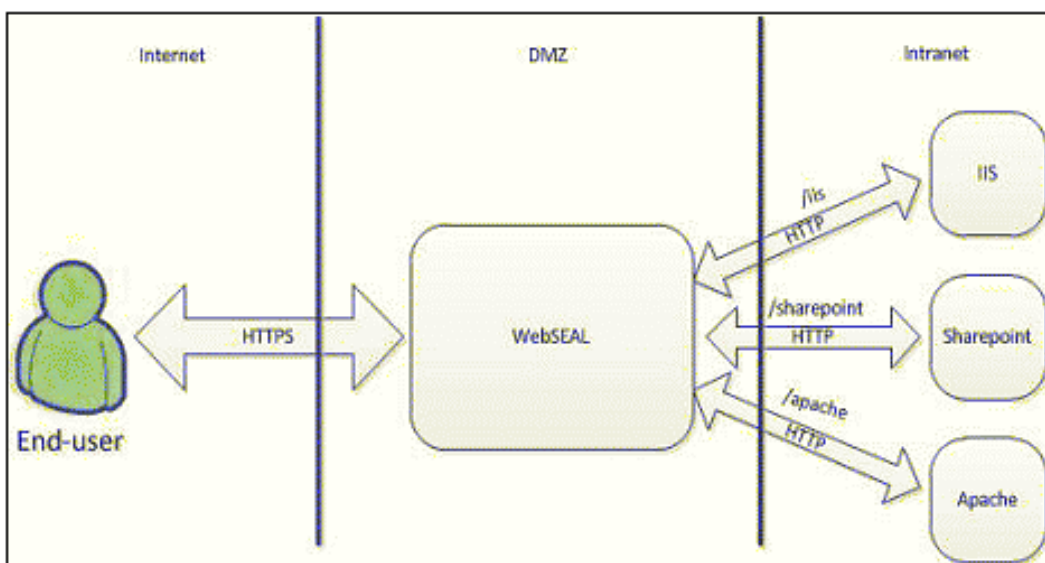
In a Windows production environment, the "netstat -a" command indicates a large number of sockets in the TIMEWAIT-state between the WebSEAL and the junctioned backend server. To avoid WebSEAL eventually running out of sockets, what action should be taken?

- A. Increase the number of WebSEAL worker threads.
- B. Configure hard- and/or soft limits on the slow backend junctions.
- C. Decrease the TIMEWAIT-related Windows registry parameters on the WebSEAL and the backend server.
- D. Configure a redundant WebSEAL-instance instance on the same machine, using a clustered environment.

Answer: C

Question No : 27 - (Topic 1)

Click on the Exhibit.



The exhibit displays a high-level setup of a basic Security Access Implementation. All communication between end-user and WebSEAL occurs over HTTPS. The communication between DMZ and Intranet is HTTP-based. End-users are complaining about a slow performing backend IIS-server. In an effort to pinpoint the problem, the average and maximum response times of a request sent to IIS is collected by the administrator. What pdadmin-statement should the administrator use to collect this information?

- A. s t internet-webseald-www.ibm.com stats get /iis
- B. s t internet-webseald-www.ibm.com stats show /iis

-
- C. s t internet-webseald-www.ibm.com stats get pdweb.jct.1
 - D. s t internet-webseald-www.ibm.com stats show pdweb.jct.1

Answer: C

Question No : 28 - (Topic 1)

An organization is facing the following challenge: Customers authenticate using a username and password, Business Partners are using a certificate to authenticate, and employees are using a token device. Within the WebSEAL architecture, how can this be achieved?

- A. Configure multiple authentication mechanism in the webseald-default.conf configuration file.
- B. Define three WebSEAL instances and configure each with a different authentication mechanism and a different URL.
- C. Use PDCONFIG to configure three Authorization servers each with a different authorization mechanism. Configure the receiving WebSEAL to redirect to the Authorization servers.
- D. Create a WebSEAL instance; make two copies of its webseald-default.conf, naming the copies webseald-certificate.conf and webseald-token.conf. Restart WebSEAL to activate the new configuration.

Answer: B

Question No : 29 - (Topic 1)

Which component should be used for WebSEAL high availability while avoiding repeated requests for log-ons?

- A. Policy Proxy Server
- B. Plug-In for Web servers
- C. Session Integration Server
- D. Session Management Server

Answer: D

Question No : 30 - (Topic 1)

Which external component is NOT required to use IBM Security Access Manager Web Gateway Appliance?

- A. Policy Server
- B. Backend web server
- C. Common Auditing and Reporting Service
- D. Lightweight Directory Access Protocol (LDAP) registry

Answer: C

Question No : 31 - (Topic 1)

An organization planning to implement IBM Security Access Manager V7 solution for existing Web Applications has indicated that an external third party authentication system will be required for some users. In order to authenticate against a custom user registry, what information should be included in a high level design document?

- A. Authentication service plug-in
- B. External authorization service
- C. Custom authentication service
- D. External authentication interface

Answer: D

Question No : 32 - (Topic 1)

Which statement is true for the Local Management Interface (LMI)?

- A. LMI cannot be used to update a routing control file.
- B. LMI does not provide provision to stop, start and restart a web reverse proxy instances.
- C. LMI cannot be used to stop, start and restart a web application configured with a web reverse proxy instances.
- D. LMI does not provide provision to control trace level, manage the trace files and rollover files for an appliance component.

Answer: C

Question No : 33 - (Topic 1)

Which out-of-the-box report shows the availability status of security software servers on a specific machine?

- A. Server Availability Report
- B. General Availability Report
- C. Failed Authorization Events History
- D. Security Server Audit Event History

Answer: A

Question No : 34 - (Topic 1)

In an ISAM 7.0 solution, which two servers are included by default? (Choose two.)

- A. IBM Cognos
- B. IBM Tivoli Directory Server
- C. IBM Websphere Process Server
- D. IBM WebSphere Application Server
- E. IBM Security Privileged Identity Manager

Answer: B,D

Question No : 35 - (Topic 1)

If a user's account was compromised and the password was immediately changed by an unauthorized user, which report details all events executed for a specific period in time?

- A. Failed Authorization History Report
- B. Audit Event History by User Report
- C. Failed Authentication History Report
- D. User Password Change History Report

Answer: B

Question No : 36 - (Topic 1)

In an ISAM 7.0 solution, in which network zone should the WebSEAL Server component for

internet access reside?

- A. Within the firewall, in the DMZ zone
- B. Outside the firewall, in the Internet zone
- C. In the same network zone as the policy server
- D. This component not required for a customer solution

Answer: A

Question No : 37 - (Topic 1)

In an organization all customer information is stored in an Active Directory (AD). Special applications for customer contracts and transactions are all connected to this AD. This organization wants to enable customers to see their information online. Therefore, a web environment has been deployed including WebSphere Application Server, IBM Tivoli Directory Server (ITDS) and IBM Security Access Manager. For security reasons the organization decided that this web environment cannot directly connect to Active Directory but should use its own directory, ITDS. A letter will be sent to each customer with its personal login details. What is the least labor intensive way to authenticate a customer online?

- A. Configure the ITDS authorization forwarding to AD
- B. Schedule an export of AD into LDIF and load this into ITDS.
- C. Configure WebSEAL's EAI to authenticate directly on the AD
- D. Use IBM Tivoli Directory Integrator to exchange essential data between the directories

Answer: D

Question No : 38 - (Topic 1)

Security Access Manager supports the use of Tivoli Common Directory logging, how is it enabled?

- A. In the TAM-runtime configuration file
- B. Tivoli Common Directory is by default enabled
- C. By setting properties in the Tivoli Common Directory properties file
- D. Select this option during the installation of the Security Access Manager product

Answer: D

Question No : 39 - (Topic 1)

What HTTP header field is used by an external authentication interface (EAI) server to provide to WebSEAL the user identity?

- A. am-user-id
- B. eai-user-id
- C. am-eai-user-id
- D. eai-am-user-id

Answer: C

Question No : 40 - (Topic 1)

What junction flags do you use if the back-end server and Access Manager share a user registry?

- A. -b gso
- B. -b fsso
- C. -b ignore
- D. -b supply

Answer: C

Question No : 41 - (Topic 1)

Which is a supported web server for the Security Access Manager plug-in for Web Servers?

- A. Mozilla Web Server
- B. Oracle HTTP Server
- C. Apache Web Server
- D. LiteSpeed Web Server

Answer: C

Question No : 42 - (Topic 1)

Which two can be used to manage the SSL certificates on the Web Gateway Appliance?
(Choose two.)

- A. The WGA LMI.
- B. The web service.
- C. The WGA CLI shell
- D. The cgi-bin interface.
- E. The WGA pdadmin interface.

Answer: A,B

Question No : 43 - (Topic 1)

How do you configure two different external authentication interface (EAI) servers that use different HTTP header fields for their results?

- A. This is impossible, because the HTTP parameter names EAI servers use to respond are hard coded.
- B. Use the same WebSEAL instance, and specify different HTTP parameters when creating the junction.
- C. Use two different WebSEAL instances, which can be on the same computer, and put different field names in the [eai] stanza of the instance configuration file.
- D. Use two different WebSEAL instances, which have to be on two different computers, and put different field names in the [http-param] stanza of the configuration file, /opt/pdweb/etc/eai.conf.

Answer: C

Question No : 44 - (Topic 1)

Given a registry suffix of o=ibm,c=us, how would you create an "Accounting" group using the commands below?

- A. group create Accounting
- B. create group Accounting cn=Accounting,o=ibm,c=us
- C. add group Accounting cn=Accounting,o=ibm,c=us cn=Accounting Accounting

D. group create Accounting cn=Accounting,o=ibm,c=us cn=Accounting Accounting

Answer: D

Question No : 45 - (Topic 1)

What Security Access Manager pdadmin command will create an object named /Management/application-object that is an application container object (type 14)?

- A. create object /Management/application-object type 14
- B. objectspace create /Management/application-object type 14 ispolicyattachable true
- C. object add /Management/application-object "Application Object" 14 ispolicyattachable yes
- D. object create /Management/application-object "Application Object" 14 ispolicyattachable yes

Answer: D

Question No : 46 - (Topic 1)

What two conditions affect content caching configuration in a WebSEAL environment? (Choose two.)

- A. By default, content caches are not defined at installation.
- B. Content caching occurs only when a cache is not defined in the Policy Server configuration file.
- C. The content caching mechanism does not cache responses to requests containing query strings.
- D. The content caching mechanism cache responses to requests over junctions configured with -b options.
- E. The content caching mechanism does not cache responses to requests over junctions configured with the -c and -C options.

Answer: C,E

Question No : 47 - (Topic 1)

What is the default port number of LDAP traffic that is unencrypted?

-
- A. 389
 - B. 636
 - C. 1389
 - D. 1636

Answer: A

Question No : 48 - (Topic 1)

What are two supported Single Sign-On methods used for WebSphere Application Server?
(Choose two.)

- A. HTTP Authentication Method
- B. Advanced Authentication Method
- C. Trusted Association Interceptor
- D. Lightweight Third Party Association
- E. Client Side Certificate Authentication Method

Answer: C,D

Question No : 49 - (Topic 1)

Which link causes a problem with WebSEAL when it appears in the HTML sent by a backend server behind a virtual host junction?

- A. Links in the HTML are never a problem.
- B. A relative link, such as `click here`.
- C. A server-relative link, such as `click here`.
- D. An absolute link, such as `click here`.

Answer: A

Question No : 50 - (Topic 1)

What command is used to apply necessary ACLs to an ldap suffix in order for Security Access Manager to be able to manage user and group information within that suffix?

-
- A. ivacl -update
 - B. update_schema
 - C. pdadmin acl create
 - D. ivrgy_tool add_acls

Answer: D

Question No : 51 - (Topic 1)

What are two prerequisite components are required when installing and configuring a base Security Access Manager Policy Server environment? (Choose two.)

- A. IBM Security Utilities
- B. Security Access manager Runtime
- C. Security Access Manager Web Server
- D. Security Access Manager Policy Proxy Server
- E. Security Access Manager Authorization Server

Answer: A,B

Question No : 52 - (Topic 1)

When configuring a Standby Policy Server environment for Security Access Manager environment on AIX, what two conditions apply? (Choose two.)

- A. Each AIX system must have access to a different disk array that is configured for data redundancy.
- B. The registry server must be available and installed on a same system.
- C. The registry server must be available and installed on a separate system.
- D. The policy database and the configuration files that are used by the policy server must be on a shared disk array.
- E. Both the primary and standby policy servers must be on separate AIX systems that are part of a High Availability Cluster Multi-Processing (PowerHA) environment.

Answer: D,E

Question No : 53 - (Topic 1)

For an existing junction on the WebSEAL Gateway Appliance, what method should be used to add an additional backend server?

- A. The "Add" tab in the junction management page.
- B. The "Servers" tab in the junction management page.
- C. The "Junction" tab in the junction management page.
- D. The "Add Server" tab in the junction management page.

Answer: B

Question No : 54 - (Topic 1)

How do you avoid an unreliable back-end causing problems with other junctions?

- A. Use -I 60
- B. Use -L 60
- C. Use -L 60%
- D. Use -unreliable

Answer: B

Question No : 55 - (Topic 1)

Which two actions occur when configuring the WebSphere Application Server JACC provider for Security Access Manager? (Choose two.)

- A. sec_master is added to the was_admin group
- B. ACLs are created for WebSphere Application Server Resources
- C. Users are created to map to each WebSphere Application Server J2EE Application Role
- D. WebSEAL junctions are created for each WebSphere Application Server J2EE application
- E. Objects are created in the Security Access Manager objectspace which correspond to WebSphere Application Server Roles and Resources

Answer: B,E

Question No : 56 - (Topic 1)

Which three components are prerequisites for a Web Security development system?
(Choose three.)

- A. Security Access Manager Runtime
- B. Security Access Manager WebSEAL
- C. Security Access Manager Policy Server
- D. Security Access Manager Java Runtime
- E. Security Access Manager Web Security Runtime
- F. Security Access Manager Application Development Kit

Answer: A,E,F

Question No : 57 - (Topic 1)

Which statement is true when referencing WebSEAL Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) support?

- A. WebSEAL supports CRL and OCSP for client certificate authentication and for SSL junctioned server authentication.
- B. WebSEAL supports CRL and OCSP for client certificate authentication but not for SSL junctioned server authentication.
- C. WebSEAL supports both CRL and OCSP for client certificate authentication but only CRL for SSL junctioned server authentication.
- D. WebSEAL supports both CRL and OCSP for client certificate authentication but only OCSP for SSL junctioned server authentication.

Answer: A

Question No : 58 - (Topic 1)

Which configuration file is used to configure LDAP replicas for Security Access Manager HA environment?

- A. pd.conf
- B. ldap.conf
- C. ivmgrd.conf
- D. webseald-default.conf

Answer: B

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.