000-039

IBM Tivoli Access Manager for e-business V6.1.1 Implementation

Version 14.23

Topic 1, Volume A

QUESTION NO: 1

What is included in the high level configuration document when WebSEAL clustering must provide high availability to back-end Web servers as part of the configuration?

A. Policy Server Replication
B. WebSEAL Junction Replication
C. Back-end Web Server Replication
D. LDAP High Availability and Replication

Answer: B

QUESTION NO: 2

What are two supported options when determining which user registry to use in an IBM Tivoli Access Manager for e-business V6.1.1 environment? (Choose two.)

A. IBM Tivoli Directory Server
B. Open Source LDAP Server
C. Novell Java Directory Server
D. Oracle User Directory Server
E. Microsoft Active Directory Application Mode (ADAM)

Answer: A, E

QUESTION NO: 3

What meets the solution requirements of a large number of user sessions that need to be tracked using a fault tolerant and scalable IBM Tivoli Access Manager for e-business V6.1.1 Session Management Server (SMS) architecture where session information can be recovered after a failure?

A. An SMS server deployed on a cluster WebSphere V7.0 server that uses a 64-bit JVM and uses in-memory storage location for session information.
B. An SMS server deployed on a cluster WebSphere V7.0 server that uses a 32-bit JVM and uses a cluster IBM DB2 database storage location for session information.

C. An SMS server deployed on a cluster WebSphere V7.0 server that uses a 64-bit JVM and uses a cluster IBM DB2 database storage location for session information.
D. An SMS server deployed on a cluster WebSphere V7.0 server that uses a 32-bit JVM and uses WebSphere eXtreme Scale V7.0 storage location for session information.

Answer: D

QUESTION NO: 4

How can five IBM Tivoli Access Manager for e-business V6.1.1 (Tivoli Access Manager) administrators be given a different password policy than the rest of the employees in a single Tivoli Access Manager environment?

A. When creating an administrator, apply a custom password policy which is different from the global password policy.
B. When creating an administrator, add them to a special Tivoli Access Manager group with a different password policy.
C. Configure the password policy for the Tivoli Access Manager administrator in LDAP for the other employees in Tivoli Access Manager.
D. Configure the password policy in the WebSEAL configuration file which enables the special Tivoli Access Manager administrator setting.

Answer: A

QUESTION NO: 5

A customer is planning an IBM Tivoli Access Manager for e-business V6.1.1 environment which includes a WebSEAL instance. What are three considerations for this implementation? (Choose three.)

A. authentication type
B. authorization server location
C. stateful junctions requirements
D. junctions created as SMTP or TCP
E. administration type (pdadmin or WPM)
F. junction type (standard, virtualhost, transparent)

Answer: A, C, F

QUESTION NO: 6

Corporate policy states that the service desk resets passwords after five failed logon attempts. Which report provides the user identity qualifying for a password reset?

A. Locked Account History
B. User Password Change History
C. Failed Authorization Event History
D. Failed Authentication Event History

Answer: D

QUESTION NO: 7

While creating a high level configuration document, the IBM Tivoli Access Manager for e-business V6.1.1 (Tivoli Access Manager) architect has to express the location of the Tivoli Access Manager components network zones. The WebSEAL will be accessible from the Internet for external customers. Which three installation options will the architect include in the configuration document? (Choose three.)

A. WebSEAL installed in the DMZ
B. Policy Server installed in the DMZ
C. WebSEAL installed in the Intranet
D. User Registry installed in the DMZ
E. Policy Server installed in the Intranet
F. User Registry installed in the Intranet

Answer: A, E, F

QUESTION NO: 8

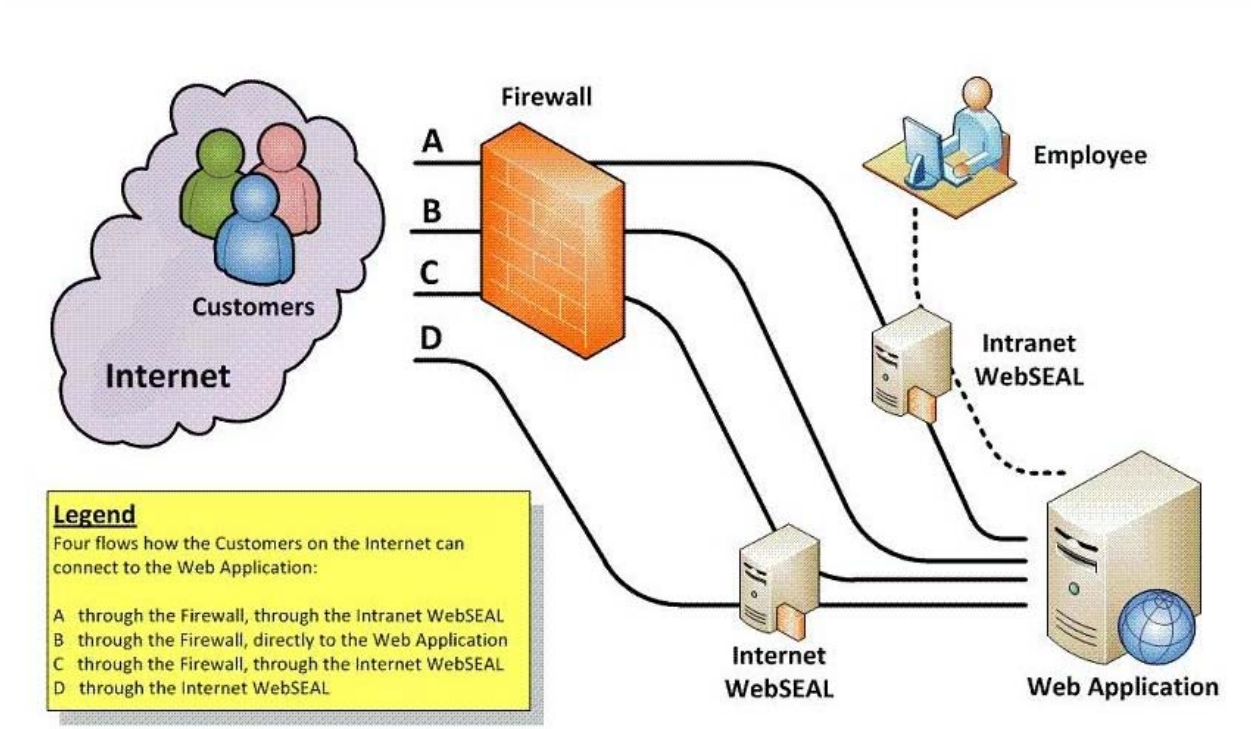
A user's password was stolen. The incident report team needs to know exactly which applications were used during the incident before the user changed the password. Which report is needed?

A. Audit Event History by User
B. Resource Access by Accessor
C. User Password Change History
D. Authorization Event History by Action

Answer: A

QUESTION NO: 9

Click the Exhibit button.



An existing IBM Tivoli Access Manager for e-business V6.1.1 infrastructure already protects a Web application for employees by using an intranet WebSEAL. The next step is to make the Web application accessible for Internet customers. What would be the most secure and logical flow?

A. Flow A
B. Flow B
C. Flow C
D. Flow D

Answer: C

QUESTION NO: 10

What are two functions of the Policy Server? (Choose two.)

A. It maintains the operating file system.

B. It gets the latest information about the patch level.
C. It gives the date and time for the current transaction.
D. It maintains the location information about other IBM Tivoli Access Manager servers.
E. It maintains the master authorization database and processes updates for the authorization database.

Answer: D, E

QUESTION NO: 11

Which statement(s) are true about the Policy Proxy Server?

1) It reduces the number of inbound firewall ports that must be opened to the real Policy Server.
2) It serves as a standby Policy Server.
3) It reduces the number of outbound firewall ports that must be opened on the firewall.
4) It caches the master authorization database of the secure IBM Tivoli Access Manager domains.

A. only statement 1
B. only statement 2
C. statements 1 and 3
D. statements 1 and 4

Answer: D

QUESTION NO: 12

Which two components are required to create an initial management domain? (Choose two.)

A. Policy Server
B. Registry Server
C. Policy Proxy Server
D. Authorization Server
E. Session Management Server

Answer: A, B

QUESTION NO: 13

On which three operating systems can IBM Tivoli Access Manager Policy Server be installed and configured? (Choose three.)

A. AIX V5.1
B. AIX V5.2
C. Windows XP
D. z/OS V1.11
E. Linux on x86_64
F. Windows 2003 / 2008 Advance Enterprise

Answer: B, E, F

QUESTION NO: 14

What happens if the Policy Server goes down?

A. WebSEAL returns a 503: service unavailable.
B. WebSEAL denies access for all incoming requests.
C. WebSEAL is no longer able to authenticate and authorize users.
D. WebSEAL continues to work and the end user is unaware of the failure.

Answer: D

QUESTION NO: 15

Which IBM Tivoli Access Manager for e-business V6.1.1 file is used to configure LDAP replicas?

A. pd.conf
B. ldap.conf
C. ibmslapd.conf
D. PDJLog.properties

Answer: B

QUESTION NO: 16

What is the correct order to install and configure a new IBM Tivoli Access Manager for e-business V6.1.1 environment?

A. User Registry, WebSphere, Web Portal Manager, Policy Server
B. User Registry, Web Portal Manager, Policy Server, WebSphere
C. User Registry, Web Portal Manager, WebSphere, Policy Server
D. User Registry, Policy Server, WebSphere, Web Portal Manager

Answer: D

QUESTION NO: 17

Which access control list permission specifies access to an application hosted on WebSphere where Java Access Contract for Containers (JACC) is enabled for IBM Tivoli Access Manager for e-business V6.1.1?

A. x
B. i
C. T
D. r

Answer: B

QUESTION NO: 18

What is the default keystore type used by IBM Tivoli Access Manager for e-business V6.1.1?

A. jks
B. kdb
C. cms
D. pks12

Answer: C

QUESTION NO: 19

When a user makes a request for a resource in a WebSEAL domain, WebSEAL sends the resource to the user upon successful authentication and policy check. As an alternative to this standard response, WebSEAL can be configured to automatically redirect the user to a specially designated home or welcome page. How this is accomplished?

A. Edit the WebSEAL configuration file and uncomment the enable-login-redirect-page in the [acnt-mgt] stanza and specify a page location, for example:

```
[acnt-mgt]
enable-login-redirect-page = /jct/intro-page.html
```

B. Edit the WebSEAL configuration file and uncomment the enable-login-redirect-page in the [enable-redirects] stanza and specify a page location, for example:

```
[enable-redirects]
enable-login-redirect-page = /jct/intro-page.html
```

C. Edit the WebSEAL configuration file and enable the redirect for each authentication method by uncommenting the entry for each method in the [enable-redirects] stanza, for example:

```
[enable-redirects]
redirect = forms-auth
redirect = basic-auth
redirect = cert-auth
redirect = token-auth
redirect = ext-auth-interface
```

Then specify the login-redirect-page in the [acnt-mgt] stanza, for example:

```
[acnt-mgt]
login-redirect-page = /jct/intro-page.html
```

D. Edit the WebSEAL configuration file and enable the redirect for each authentication method by uncommenting the entry for each method in the [enable-redirects] and specify a page location, for example:

```
[enable-redirects]
forms-auth-redir-page = /jct/intro-page-1.html
basic-auth-redir-page = /jct/intro-page-2.html
cert-auth-redir-page = /jct/intro-page-3.html
token-auth-redir-page = /jct/intro-page-4.html
ext-auth-interface-redir-page = /jct/intro-page-5.html
```

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

Answer: C

QUESTION NO: 20

In order to achieve communication between the default configured Policy Server and WebSEAL, which firewall ports must be opened between these two components?

A. ports 80 and 389
B. ports 636 and 6881
C. ports 9080 and 9443
D. ports 7135 and 7234

Answer: B, C

QUESTION NO: 21

Which pdadmin command shows the list of servers on a load balancing junction?

A. server task <instance>-webseald-<computer> show /junction
B. server task <instance>-webseald-<computer> servers list /junction
C. server task <instance>-webseald-<computer> servers show /junction
D. server task <instance>-webseald-<computer> show servers /junction

Answer: A

QUESTION NO: 22

A WebSEAL instance is being configured in a working IBM Tivoli Access Manager for e-business V6.1.1 environment but is failing. What are two possible causes for the configuration failure? (Choose two.)

A. The firewall is preventing communication on default port 443.
B. The firewall is preventing communication on default port 7234.
C. The firewall is preventing communication on default port 7136.
D. The firewall is preventing communication on default port 7135.
E. The firewall is preventing communication on default port 9080.

Answer: B, D

QUESTION NO: 23

Which authentication level order is valid when defining a step-up authentication?