

300-208.examcollection.premium.exam.208q

Number: 300-208
Passing Score: 800
Time Limit: 120 min
File Version: 7.0



300-208

Implementing Cisco Secure Access Solutions

Version 7.0

Exam A**QUESTION 1**

A network administrator needs to implement a service that enables granular control of IOS commands that can be executed. Which AAA authentication method should be selected?

- A. TACACS+
- B. RADIUS
- C. Windows Active Directory
- D. Generic LDAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

An administrator can leverage which attribute to assign privileges based on Microsoft Active Directory user groups?

- A. member of
- B. group
- C. class
- D. person

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Cisco 802.1X phasing enables flexible deployments through the use of open, low-impact, and closed modes. What is a unique characteristic of the most secure mode?

- A. Granular ACLs applied prior to authentication
- B. Per user dACLs applied after successful authentication
- C. Only EAPoL traffic allowed prior to authentication

D. Adjustable 802.1X timers to enable successful authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A network administrator must enable which protocol extension to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2
- D. PEAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Changes were made to the ISE server while troubleshooting, and now all wireless certificate authentications are failing. Logs indicate an EAP failure.

What is the most likely cause of the problem?

- A. EAP-TLS is not checked in the Allowed Protocols list
- B. Certificate authentication profile is not configured in the Identity Store
- C. MS-CHAPv2 is not checked in the Allowed Protocols list
- D. Default rule denies all traffic
- E. Client root certificate is not included in the Certificate Store

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

The NAC Agent uses which port and protocol to send discovery packets to an ISE Policy Service Node?

- A. tcp/8905
- B. udp/8905
- C. http/80
- D. https/443

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Which two conditions are valid when configuring ISE for posturing? (Choose two.)

- A. Dictionary
- B. member Of
- C. Profile status
- D. File
- E. Service

Correct Answer: DE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9

Refer to the exhibit.

```
device (config) #aaa new-model
device (config) #tacacs-server host 209.165.200.226
device (config) #tacacs-server host 209.165.200.227
device (config) #tacacs-server key 0 $$5@#4%!!1
```

Which three statements about the given configuration are true? (Choose three.)

- A. TACACS+ authentication configuration is complete.
- B. TACACS+ authentication configuration is incomplete.
- C. TACACS+ server hosts are configured correctly.
- D. TACACS+ server hosts are misconfigured.
- E. The TACACS+ server key is encrypted.
- F. The TACACS+ server key is unencrypted.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

In AAA, what function does authentication perform?

- A. It identifies the actions that the user can perform on the device.
- B. It identifies the user who is trying to access a device.
- C. It identifies the actions that a user has previously taken.
- D. It identifies what the user can access.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Which identity store option allows you to modify the directory services that run on TCP/IP?

- A. Lightweight Directory Access Protocol
- B. RSA SecurID server
- C. RADIUS
- D. Active Directory

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which term describes a software application that seeks connectivity to the network via a network access device?

- A. authenticator
- B. server
- C. supplicant
- D. WLC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Cisco ISE distributed deployments support which three features? (Choose three.)

- A. global implementation of the profiler service CoA
- B. global implementation of the profiler service in Cisco ISE
- C. configuration to send system logs to the appropriate profiler node
- D. node-specific probe configuration
- E. server-specific probe configuration
- F. NetFlow probes

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

How frequently does the Profiled Endpoints dashlet refresh data?

- A. every 30 seconds
- B. every 60 seconds
- C. every 2 minutes
- D. every 5 minutes

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Which command in the My Devices Portal can restore a previously lost device to the network?

- A. Reset
- B. Found
- C. Reinstate
- D. Request

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:****QUESTION 16**

What is the first step that occurs when provisioning a wired device in a BYOD scenario?

- A. The smart hub detects that the physically connected endpoint requires configuration and must use MAB to authenticate.
- B. The URL redirects to the Cisco ISE Guest Provisioning portal.
- C. Cisco ISE authenticates the user and deploys the SPW package.
- D. The device user attempts to access a network URL.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 17**

Which three features should be enabled as best practices for MAB? (Choose three.)

- A. MD5
- B. IP source guard
- C. DHCP snooping
- D. storm control
- E. DAI
- F. URPF

Correct Answer: BCE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 18**

When MAB is configured, how often are ports reauthenticated by default?

- A. every 60 seconds
- B. every 90 seconds
- C. every 120 seconds
- D. never

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

What is a required step when you deploy dynamic VLAN and ACL assignments?

- A. Configure the VLAN assignment.
- B. Configure the ACL assignment.
- C. Configure Cisco IOS Software 802.1X authenticator authorization.
- D. Configure the Cisco IOS Software switch for ACL assignment.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

Which model does Cisco support in a RADIUS change of authorization implementation?

- A. push
- B. pull
- C. policy
- D. security

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

An organization has recently deployed ISE with the latest models of Cisco switches, and it plans to deploy Trustsec to secure its infrastructure. The company also wants to allow different network access policies for different user groups (e.g., administrators). Which solution is needed to achieve these goals?

- A. Cisco Security Group Access Policies in order to use SGACLs to control access based on SGTs assigned to different users
- B. MACsec in Multiple-Host Mode in order to open or close a port based on a single authentication
- C. Identity-based ACLs on the switches with user identities provided by ISE
- D. Cisco Threat Defense for user group control by leveraging Netflow exported from the switches and login information from ISE

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Security Group Access requires which three syslog messages to be sent to Cisco ISE? (Choose three.)

- A. IOS-7-PROXY_DROP
- B. AP-1-AUTH_PROXY_DOS_ATTACK
- C. MKA-2-MACDROP
- D. AUTHMGR-5-MACMOVE
- E. ASA-6-CONNECT_BUILT
- F. AP-1-AUTH_PROXY_FALLBACK_REQ

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Which administrative role has permission to assign Security Group Access Control Lists?

- A. System Admin

- B. Network Device Admin
- C. Policy Admin
- D. Identity Admin

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Refer to the exhibit.

```
asa1(config)# time-range WeekendHours
asa1(config-time-range)# periodic friday 18:00 to monday 8:00
asa1(config)# access-list Outside extended deny ip any object-group vpnservers time-range WeekendHours log
asa1(config)# access-group Outside in outside
```

If the given configuration is applied to the object-group vpnservers, during which time period are external users able to connect?

- A. From Friday at 6:00 p.m. until Monday at 8:00 a.m.
- B. From Monday at 8:00 a.m. until Friday at 6:00 p.m.
- C. From Friday at 6:01 p.m. until Monday at 8:01 a.m.
- D. From Monday at 8:01 a.m. until Friday at 5:59 p.m.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which set of commands allows IPX inbound on all interfaces?

- A. ASA1(config)# access-list IPX-Allow ethertype permit ipx
ASA1(config)# access-group IPX-Allow in interface global

- B. ASA1(config)# access-list IPX-Allow ethertype permit ipx
ASA1(config)# access-group IPX-Allow in interface inside
- C. ASA1(config)# access-list IPX-Allow ethertype permit ipx
ASA1(config)# access-group IPX-Allow in interface outside
- D. ASA1(config)# access-list IPX-Allow ethertype permit ipx
ASA1(config)# access-group IPX-Allow out interface global

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which command enables static PAT for TCP port 25?

- A. nat (outside,inside) static 209.165.201.3 209.165.201.226 eq smtp
- B. nat static 209.165.201.3 eq smtp
- C. nat (inside,outside) static 209.165.201.3 service tcp smtp smtp
- D. static (inside,outside) 209.165.201.3 209.165.201.226 netmask 255.255.255.255

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which command is useful when troubleshooting AAA Authentication between a Cisco router and the AAA server?

- A. test aaa-server test cisco cisco123 all new-code
- B. test aaa group7 tacacs+ auth cisco123 new-code
- C. test aaa group tacacs+ cisco cisco123 new-code
- D. test aaa-server tacacs+ group7 cisco cisco123 new-code

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 28**

In a multi-node ISE deployment, backups are not working on the MnT node. Which ISE CLI option would help mitigate this issue?

- A. repository
- B. ftp-url
- C. application-bundle
- D. collector

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 29**

Which command can check a AAA server authentication for server group Group1, user cisco, and password cisco555 on a Cisco ASA device?

- A. ASA# test aaa-server authentication Group1 username cisco password cisco555
- B. ASA# test aaa-server authentication group Group1 username cisco password cisco555
- C. ASA# aaa-server authorization Group1 username cisco password cisco555
- D. ASA# aaa-server authentication Group1 roger cisco555

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 30**

Which statement about system time and NTP server configuration with Cisco ISE is true?

- A. The system time and NTP server settings can be configured centrally on the Cisco ISE.
- B. The system time can be configured centrally on the Cisco ISE, but NTP server settings must be configured individually on each ISE node.
- C. NTP server settings can be configured centrally on the Cisco ISE, but the system time must be configured individually on each ISE node.

D. The system time and NTP server settings must be configured individually on each ISE node.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Wireless client supplicants attempting to authenticate to a wireless network are generating excessive log messages. Which three WLC authentication settings should be disabled? (Choose three.)

- A. RADIUS Server Timeout
- B. RADIUS Aggressive-Failover
- C. Idle Timer
- D. Session Timeout
- E. Client Exclusion
- F. Roaming

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which two authentication stores are supported to design a wireless network using PEAP EAP-MSCHAPv2 as the authentication method? (Choose two.)

- A. Microsoft Active Directory
- B. ACS
- C. LDAP
- D. RSA Secure-ID
- E. Certificate Server

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:**QUESTION 33**

What is another term for 802.11i wireless network security?

- A. 802.1x
- B. WEP
- C. TKIP
- D. WPA
- E. WPA2

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:**QUESTION 34**

Which two EAP types require server side certificates? (Choose two.)

- A. EAP-TLS
- B. PEAP
- C. EAP-MD5
- D. LEAP
- E. EAP-FAST
- F. MSCHAPv2

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:**QUESTION 35**

Where is client traffic decrypted in a controller-based wireless network protected with WPA2 Security?

- A. Access Point

- B. Switch
- C. Wireless LAN Controller
- D. Authentication Server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

Which setting provides the best security for a WLAN and authenticates users against a centralized directory store?

- A. WPA2 AES-CCMP and 801.X authentication
- B. WPA2 AES-CCMP and PSK authentication
- C. WPA2 TKIP and PSK authentication
- D. WPA2 TKIP and 802.1X authentication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

What is a feature of Cisco WLC and IPS synchronization?

- A. Cisco WLC populates the ACLs to prevent repeat intruder attacks.
- B. The IPS automatically send shuns to Cisco WLC for an active host block.
- C. Cisco WLC and IPS synchronization enables faster wireless access.
- D. IPS synchronization uses network access points to provide reliable monitoring.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which two components are required to connect to a WLAN network that is secured by EAP-TLS authentication? (Choose two.)

- A. Kerberos authentication server
- B. AAA/RADIUS server
- C. PSKs
- D. CA server

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

Which statement about Cisco Management Frame Protection is true?

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

Which three statements about the Cisco wireless IPS solution are true? (Choose three.)

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.
- E. It allows the WLC to failover because of congestion.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

In a basic ACS deployment consisting of two servers, for which three tasks is the primary server responsible? (Choose three.)

- A. configuration
- B. authentication
- C. sensing
- D. policy requirements
- E. monitoring
- F. repudiation

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

In a split ACS deployment with primary and secondary servers, which three statements about AAA load handling are true? (Choose three.)

- A. During normal operations, each server processes the full workload of both servers.
- B. If a AAA connectivity problem occurs, the servers split the full load of authentication requests.
- C. If a AAA connectivity problem occurs, each server processes the full workload of both servers.
- D. During normal operations, the servers split the full load of authentication requests.
- E. During normal operations, each server is used for specific operations, such as device administration and network admission.
- F. The primary servers are used to distribute policy information to other servers in the enterprise.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference: