Free Questions for 300-715 by braindumpscollection

Shared by Kennedy on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network security administrator needs a web authentication configuration when a guest user connects to the network with a wireless connection using these steps:

. An initial MAB request is sent to the Cisco ISE node.

. Cisco ISE responds with a URL redirection authorization profile if the user's MAC address is unknown in the endpoint identity store.

. The URL redirection presents the user with an AUP acceptance page when the user attempts to go to any URL.

Which authentication must the administrator configure on Cisco ISE?

Options:

A- device registration WebAuth

B- WLC with local WebAuth

C- wired NAD with local WebAuth

D- NAD with central WebAuth

Answer:

D

Explanation:

Central Web Authentication (CWA) is a feature that allows the network access device (NAD) to redirect the web traffic of a guest user to a web portal hosted by Cisco ISE1. The NAD acts as a proxy between the guest user and the ISE node, and performs the authentication and authorization based on the RADIUS attributes returned by ISE1. To configure CWA on ISE, the administrator must create an authorization profile that contains the URL redirection attribute and assign it to the guest user1. The other options are not correct because they do not use CWA. Device registration WebAuth is a feature that allows users to register their devices on ISE before they can access the network2. WLC with local WebAuth is a feature that allows the wireless LAN controller (WLC) to host the web portal and authenticate the guest user locally3. Wired NAD with local WebAuth is a feature that allows the switch to host the web portal and authenticate the guest user locally

Question 2

Question Type: MultipleChoice

The security team identified a rogue endpoint with MAC address 00:46:91:02:28:4A attached to the network. Which action must security engineer take within Cisco ISE to effectively

restrict network access for this endpoint?

Options:

A- Configure access control list on network switches to block traffic.

B- Create authentication policy to force reauthentication.

C- Add MAC address to the endpoint quarantine list.

D- Implement authentication policy to deny access.

Answer:

C

Explanation:

Cisco ISE provides a feature called Adaptive Network Control (ANC) that allows administrators to apply policies to endpoints based on their behavior or status1. One of the ANC policies is Quarantine, which restricts network access for an endpoint by assigning it to a limited-access VLAN or applying an access control list (ACL) on the switch port2. To use the Quarantine policy, the administrator must add the MAC address of the rogue endpoint to the endpoint quarantine list in ISE2. This will trigger a change of authorization (CoA) for the endpoint and apply the Quarantine policy. The other options are not effective for restricting network access for a rogue endpoint, as they do not use the ANC feature of ISE.

Question 3

Question Type: MultipleChoice

An enterprise uses a separate PSN for each of its four remote sites. Recently, a user reported receiving an "EAP-TLS authentication failed" message when moving between remote sites. Which configuration must be applied on Cisco ISE?

Options:

A- Use a third-party certificate on the network device.

B- Add the device to all PSN nodes in the deployment.

C- Renew the expired certificate on one of the PSN.

D- Configure an authorization profile for the end users.

Answer:

B

Explanation:

When using separate PSNs for different sites, the network device must be added to all PSN nodes in the deployment, so that the device can communicate with the appropriate PSN based on the location of the user1. If the device is not added to all PSN nodes, the user may encounter an EAP-TLS authentication failure when moving between sites, as the device may not be able to reach the PSN that issued

the certificate2. The other options are not relevant for this scenario, as they do not address the issue of PSN communication.

Question 4

Question Type: MultipleChoice

An engineer is working on a switch and must tag packets with SGT values such that it learns via SXP. Which command must be entered to meet this requirement?

Options:

A- ip source guard

B- ip dhcp snooping

C- ip device tracking maximum

D- ip arp inspection

Answer:

C

Explanation:

The ip device tracking maximum command is used to configure the maximum number of IP-to-SGT bindings that can be learned via SXP on a switch1. This command also enables the switch to tag packets with SGT values based on the bindings learned from SXP peers. The other commands are not related to SGT tagging or SXP learning.

Question 5

Question Type: MultipleChoice

An engineer is starting to implement a wired 802.1X project throughout the campus. The task is for failed authentication to be logged to Cisco ISE and also have a minimal impact on the users. Which command must the engineer configure?

Options:

A- authentication open

B- pae dot1x enabled

C- authentication host-mode multi-auth

D- monitor-mode enabled

Answer:

D

Explanation:

In the context of a wired 802.1X deployment with Cisco ISE, the requirement is to log failed authentications while minimizing user impact. Let's analyze each option:

A) authentication open - This command configures the port to allow network access regardless of the authentication state. It's useful in situations where specific devices can't perform 802.1X authentication but should still be allowed network access. However, it doesn't specifically address the logging of failed authentications.

B) pae dot1x enabled - PAE (Port Access Entity) refers to the entity on a network device that enforces access control. This command enables 802.1X on the port, which is a prerequisite for implementing 802.1X, but doesn't directly relate to logging failed authentication attempts.

C) authentication host-mode multi-auth - This command configures the port to allow multiple authenticated sessions. This mode is used when multiple devices are connected to the same port (like in a conference room). While it's relevant for 802.1X environments, it doesn't specifically cater to logging failed authentications or minimizing user impact.

D) monitor-mode enabled - This command is used in the context of 802.1X to enable Monitor Mode on a port. Monitor Mode allows a port to grant limited network access to endpoints without 802.1X capabilities. It's often used to ease the deployment of 802.1X by monitoring the authentication status without fully enforcing access control, thereby minimizing user impact. It also helps in logging authentication attempts, including failures.

Question 6

Question Type: MultipleChoice

An administrator is configuring a switch port for use with 802 1X What must be done so that the port will allow voice and multiple data endpoints?

Options:

A- Configure the port with the authentication host-mode multi-auth command

B- Connect the data devices to the port, then attach the phone behind them.

C- Use the command authentication host-mode multi-domain on the port

D- Connect a hub to the switch port to allow multiple devices access after authentication

Answer:

A

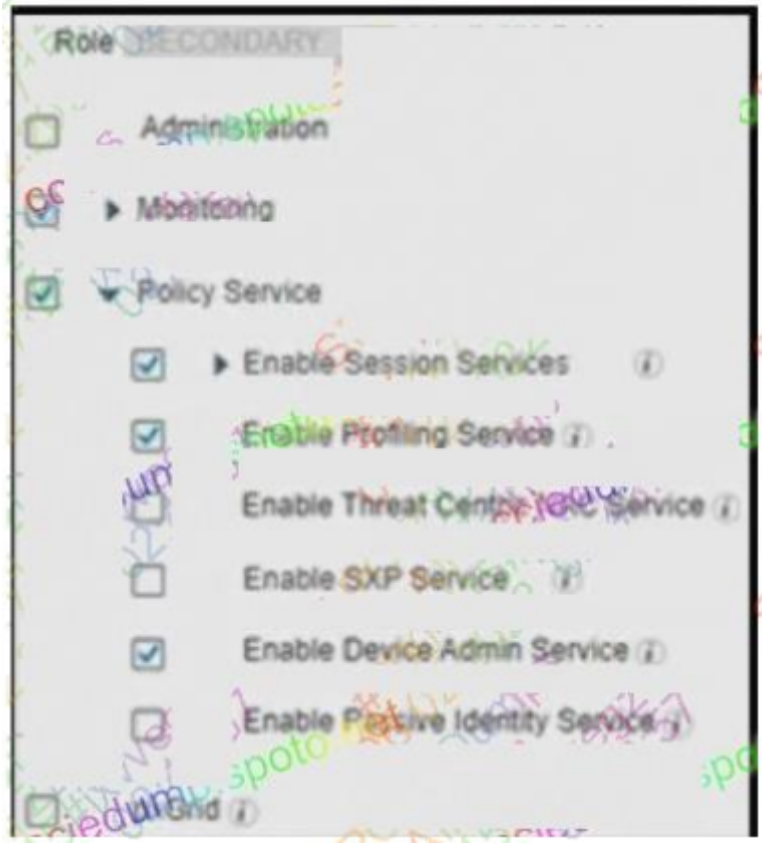
Question 7

Question Type: MultipleChoice

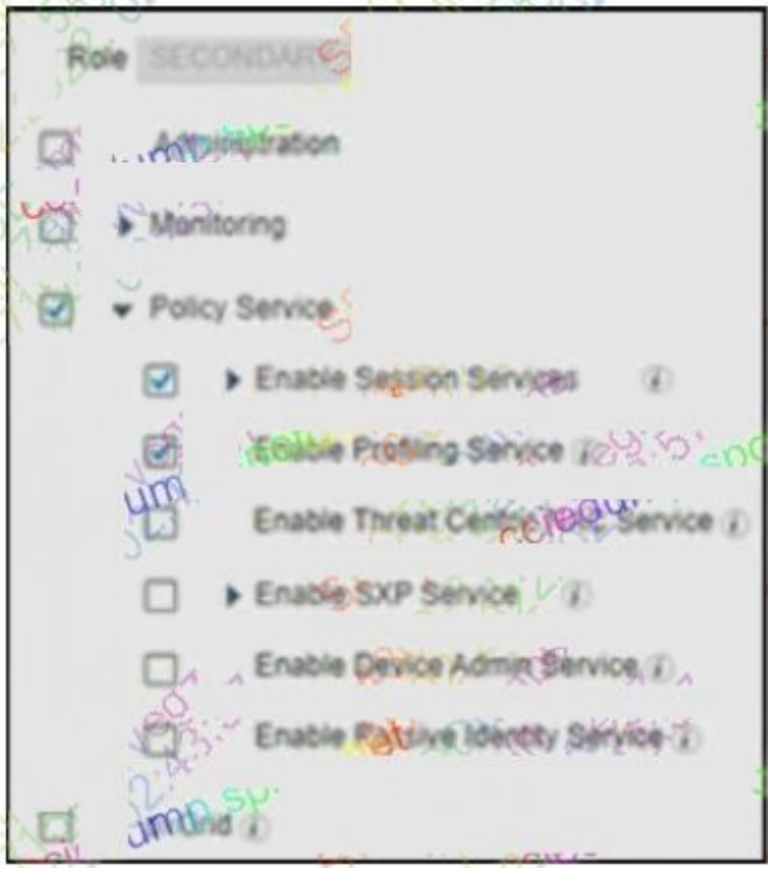
An engineer builds a five-node distributed Cisco ISE deployment The first two deployed nodes are responsible for the primary and secondary administration and monitoring personas Which persona configuration is necessary to have the remaining three Cisco ISE nodes serve as dedicated nodes in the Cisco ISE cube that is responsible only for handling the RADIUS and TACACS+ authentication requests, identity lookups, and policy evaluation?

A)

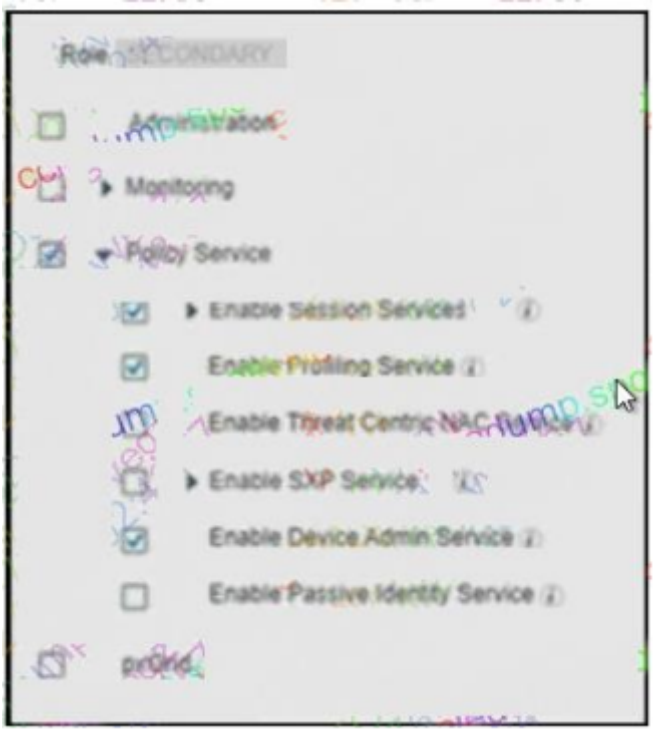
B)


Role SECONDARY
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service
pxGrid

C)


Role
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service
pxGrid

D)



Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

D

Question 8

Question Type: MultipleChoice

Which two default guest portals are available with Cisco ISE? (Choose two.)

Options:

A- visitor

B- WIFI-access

C- self-registered

D- central web authentication

E- sponsored

Answer:

C, E