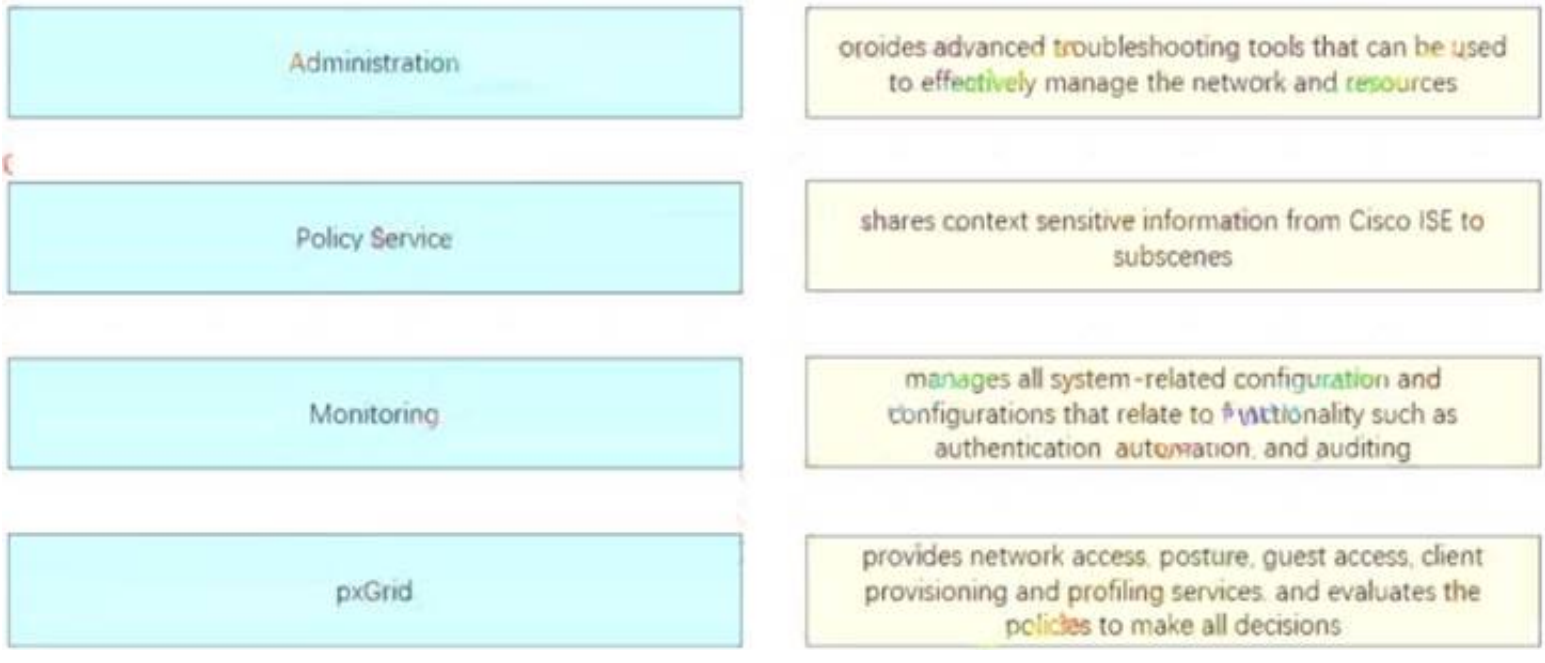
Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)

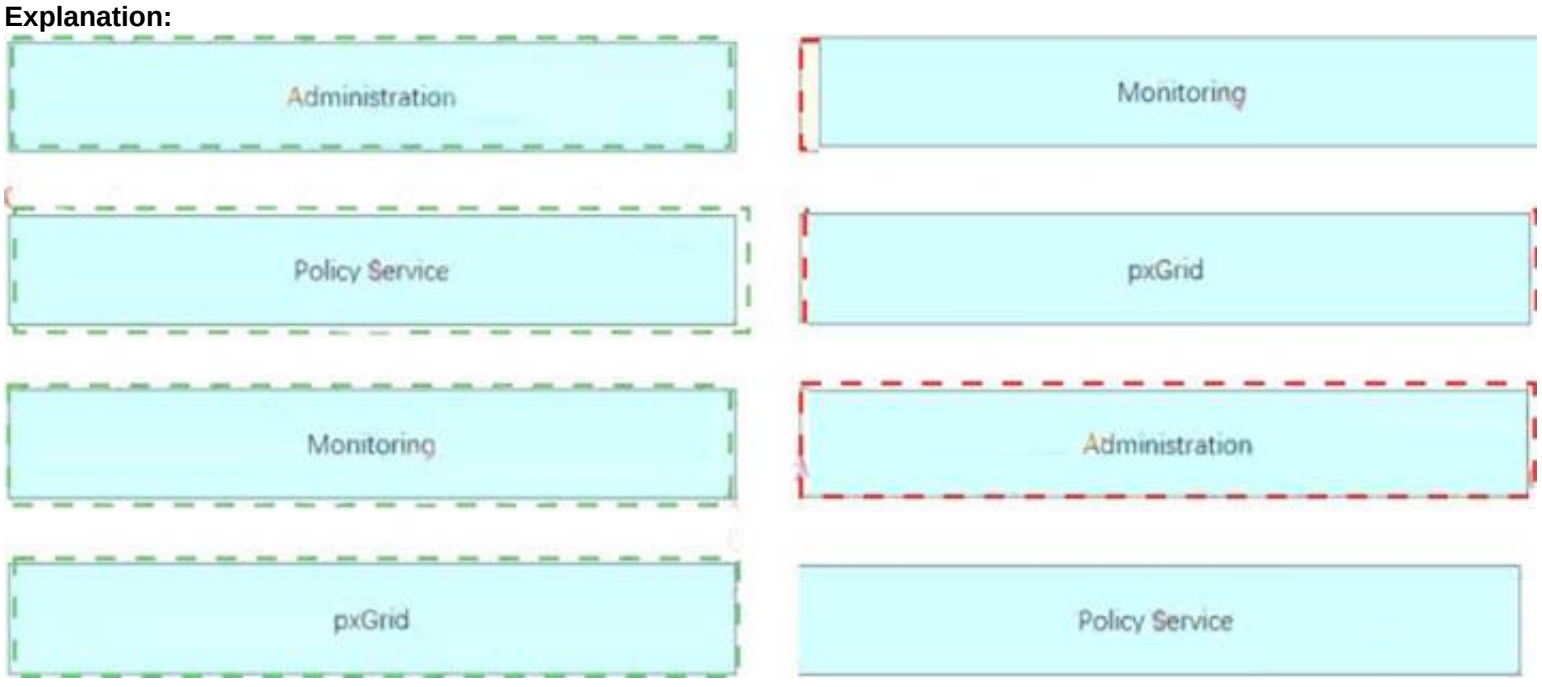
NEW QUESTION 1
Select and Place



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2
What should be considered when configuring certificates for BYOD?

A. An endpoint certificate is mandatory for the Cisco ISE BYOD
B. An Android endpoint uses EST whereas other operation systems use SCEP for enrollment
C. The CN field is populated with the endpoint host name.
D. The SAN field is populated with the end user name

Answer: A

NEW QUESTION 3
A Cisco ISE administrator must restrict specific endpoints from accessing the network while in closed mode. The requirement is to have Cisco ISE centrally store the endpoints to restrict access from. What must be done to accomplish this task"

A. Add each MAC address manually to a blocklist identity group and create a policy denying access
B. Create a logical profile for each device's profile policy and block that via authorization policies.
C. Create a profiling policy for each endpoint with the cdpCacheDeviceId attribute.
D. Add each IP address to a policy denying access.

Answer: B

NEW QUESTION 4
Refer to the exhibit.

```
Switch(config)# gigabitEthernet 1/0/2

Switch(config)# authentication port-control auto

Switch(config)# authentication host-mode multi-auth
```

In which scenario does this switch configuration apply?

A. when allowing a hub with multiple clients connected
B. when passing IP phone authentication
C. when allowing multiple IP phones to be connected
D. when preventing users with hypervisor

Answer: A

Explanation:
https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari#:~:text=Multi%2Dauthentication%

NEW QUESTION 5
An organization wants to standardize the 802 1X configuration on their switches and remove static ACLs on the switch ports while allowing Cisco ISE to communicate to the switch what access to provide What must be configured to accomplish this task?

A. security group tag within the authorization policy
B. extended access-list on the switch for the client
C. port security on the switch based on the client's information
D. dynamic access list within the authorization profile

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_sga_pol.html#

NEW QUESTION 6
A user changes the status of a device to stolen in the My Devices Portal of Cisco ISE. The device was originally onboarded in the BYOD wireless Portal without a certificate. The device is found later, but the user cannot re-onboard the device because Cisco ISE assigned the device to the Blocklist endpoint identity group. What must the user do in the My Devices Portal to resolve this issue?

A. Manually remove the device from the Blocklist endpoint identity group.
B. Change the device state from Stolen to Not Registered.
C. Change the BYOD registration attribute of the device to None.
D. Delete the device, and then re-add the device.

Answer: B

NEW QUESTION 7
An administrator is configuring the Native Supplicant Profile to be used with the Cisco ISE posture agents and needs to test the connection using wired devices to determine which profile settings are available. Which two configuration settings should be used to accomplish this task? (Choose two.)

A. authentication mode
B. proxy host/IP
C. certificate template
D. security
E. allowed protocol

Answer: CE

NEW QUESTION 8
Which RADIUS attribute is used to dynamically assign the Inactivity active timer for MAB users from the Cisco ISE node?

A. session timeout
B. idle timeout
C. radius-server timeout
D. termination-action

Answer: B

Explanation:
When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session. The inactivity timer for MAB can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute

NEW QUESTION 9
An engineer is configuring web authentication using non-standard ports and needs the switch to redirect traffic to the correct port. Which command should be used to accomplish this task?

A. permit tcp any any eq <port number>
B. aaa group server radius proxy
C. ip http port <port number>
D. aaa group server radius

Answer: C

NEW QUESTION 10
An administrator is configuring RADIUS on a Cisco switch with a key set to Cisc403012128 but is receiving the error “Authentication failed: 22040 Wrong password or invalid shared secret. “what must be done to address this issue?

A. Add the network device as a NAD inside Cisco ISE using the existing key.
B. Configure the key on the Cisco ISE instead of the Cisco switch.
C. Use a key that is between eight and ten characters.
D. Validate that the key is correct on both the Cisco switch as well as Cisco ISE.

Answer: D

NEW QUESTION 10
A network engineer has been tasked with enabling a switch to support standard web authentication for Cisco ISE. This must include the ability to provision for URL redirection on authentication Which two commands must be entered to meet this requirement? (Choose two)

A. Ip http secure-authentication
B. Ip http server
C. Ip http redirection
D. Ip http secure-server
E. Ip http authentication

Answer: BD

Explanation:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuratio

NEW QUESTION 14
An engineer is testing Cisco ISE policies in a lab environment with no support for a deployment server. In order to push supplicant profiles to the workstations for testing, firewall ports will need to be opened. From which Cisco ISE persona should this traffic be originating?

A. monitoring
B. policy service
C. administration
D. authentication

Answer: B

NEW QUESTION 17
An engineer needs to configure Cisco ISE Profiling Services to authorize network access for IP speakers that require access to the intercom system. This traffic needs to be identified if the ToS bit is set to 5 and the destination IP address is the intercom system. What must be configured to accomplish this goal?

A. NMAP
B. NETFLOW
C. pxGrid
D. RADIUS

Answer: B

NEW QUESTION 18
Which protocol must be allowed for a BYOD device to access the BYOD portal?

A. HTTP
B. SMTP
C. HTTPS
D. SSH

Answer: C

NEW QUESTION 19
During a 802 1X deployment, an engineer must identify failed authentications without causing problems for the connected endpoint. Which command will successfully achieve this''

A. dot1x system-auth-control
B. dot1x pae authenticator
C. authentication open
D. authentication port-control auto

Answer: C

NEW QUESTION 20
Which supplicant(s) and server(s) are capable of supporting EAP-CHAINING?

A. Cisco AnyConnect NAM and Cisco Identity Service Engine
B. Cisco AnyConnect NAM and Cisco Access Control Server
C. Cisco Secure Services Client and Cisco Access Control Server
D. Windows Native Supplicant and Cisco Identity Service Engine

Answer: A

NEW QUESTION 24
An engineer is configuring sponsored guest access and needs to limit each sponsored guest to a maximum of two devices. There are other guest services in production that rely on the default guest types. How should this configuration change be made without disrupting the other guest services currently offering three or more guest devices per user?

A. Create an ISE identity group to add users to and limit the number of logins via the group configuration.
B. Create a new guest type and set the maximum number of devices sponsored guests can register
C. Create an LDAP login for each guest and tag that in the guest portal for authentication.
D. Create a new sponsor group and adjust the settings to limit the devices for each guest.

Answer: D

NEW QUESTION 27
What must be configured on the WLC to configure Central Web Authentication using Cisco ISE and a WLC?

A. Set the NAC State option to SNMP NAC.
B. Set the NAC State option to RADIUS NAC.
C. Use the radius-server vsa send authentication command.
D. Use the ip access-group webauth in command.

Answer: B

NEW QUESTION 30
What is a requirement for Feed Service to work?

A. TCP port 3080 must be opened between Cisco ISE and the feed server
B. Cisco ISE has a base license.
C. Cisco ISE has access to an internal server to download feed update
D. Cisco ISE has Internet access to download feed update

Answer: C

NEW QUESTION 33
Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)

A. The device queries the internal identity store
B. The Cisco ISE server queries the internal identity store
C. The device queries the external identity store
D. The Cisco ISE server queries the external identity store.
E. The device queries the Cisco ISE authorization server

Answer: AD

NEW QUESTION 34
A network administrator changed a Cisco ISE deployment from pilot to production and noticed that the JVM memory utilization increased significantly. The administrator suspects this is due to replication between the nodes What must be configured to minimize performance degradation?

A. Review the profiling policies for any misconfiguration
B. Enable the endpoint attribute filter
C. Change the reauthenticate interval.
D. Ensure that Cisco ISE is updated with the latest profiler feed update

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/admin_guide/b_ise_admin_guide_23/b_ise_admin_guide

NEW QUESTION 37
An administrator enables the profiling service for Cisco ISE to use for authorization policies while in closed mode. When the endpoints connect, they receive limited access so that the profiling probes can gather information and Cisco ISE can assign the correct profiles. They are using the default values within Cisco ISE. but the devices do not change their access due to the new profile. What is the problem'?

A. In closed mode, profiling does not work unless CDP is enabled.
B. The profiling probes are not able to collect enough information to change the device profile
C. The profiler feed is not downloading new information so the profiler is inactive
D. The default profiler configuration is set to No CoA for the reauthentication setting

Answer: D

NEW QUESTION 39
Which two components are required for creating a Native Supplicant Profile within a BYOD flow? (Choose two)

A. Windows Settings
B. Connection Type
C. iOS Settings
D. Redirect ACL
E. Operating System

Answer: BE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_

NEW QUESTION 44
Which two endpoint compliance statuses are possible? (Choose two.)

A. unknown
B. known
C. invalid
D. compliant
E. valid

Answer: AD

NEW QUESTION 48
An administrator needs to give the same level of access to the network devices when users are logging into them using TACACS+ However, the administrator must restrict certain commands based on one of three user roles that require different commands How is this accomplished without creating too many objects using Cisco ISE?

A. Create one shell profile and multiple command sets.
B. Create multiple shell profiles and multiple command sets.
C. Create one shell profile and one command set.
D. Create multiple shell profiles and one command set

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide
https://www.youtube.com/watch?v=IlZwB71Szog&ab_channel=JasonMaynard

NEW QUESTION 53
What must match between Cisco ISE and the network access device to successfully authenticate endpoints?

A. SNMP version
B. shared secret
C. certificate
D. profile

Answer: B

Explanation:
https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_network_devices.html

NEW QUESTION 57
What is the deployment mode when two Cisco ISE nodes are configured in an environment?

A. distributed
B. active
C. standalone
D. standard

Answer: A

NEW QUESTION 58
Which two default endpoint identity groups does Cisco ISE create? (Choose two)

A. block list
B. endpoint
C. profiled
D. allow list
E. unknown

Answer: CE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide
Default Endpoint Identity Groups Created for EndpointsCisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.
Cisco ISE creates the following endpoint identity groups:

- Blacklist—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are block listed in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
- GuestEndpoints—This endpoint identity group includes endpoints that are used by guest users.
- Profiled—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
- RegisteredDevices—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays “Unauthorised Network Access”, a default portal page to the blocked devices.
- Unknown—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE. In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint

identity groups, which are associated to the Profiled identity group:

- Cisco-IP-Phone—An identity group that contains all the profiled Cisco IP phones on your network.
- Workstation—An identity group that contains all the profiled workstations on your network.

NEW QUESTION 62
What are two components of the posture requirement when configuring Cisco ISE posture? (Choose two)

A. updates
B. remediation actions
C. Client Provisioning portal
D. conditions
E. access policy

Answer: BD

NEW QUESTION 64
Which two ports must be open between Cisco ISE and the client when you configure posture on Cisco ISE? (Choose two).

A. TCP 8443
B. TCP 8906
C. TCP 443
D. TCP 80
E. TCP 8905

Answer: AE

NEW QUESTION 68
What is a difference between RADIUS and TACACS+?

A. RADIUS uses connection-oriented transport, and TACACS+ uses best-effort delivery.
B. RADIUS offers multiprotocol support, and TACACS+ supports only IP traffic.
C. RADIUS combines authentication and authorization functions, and TACACS+ separates them.
D. RADIUS supports command accounting, and TACACS+ does not.

Answer: C

NEW QUESTION 69
Users in an organization report issues about having to remember multiple usernames and passwords. The network administrator wants the existing Cisco ISE deployment to utilize an external identity source to alleviate this issue. Which two requirements must be met to implement this change? (Choose two.)

A. Enable IPC access over port 80.
B. Ensure that the NAT address is properly configured
C. Establish access to one Global Catalog server.
D. Provide domain administrator access to Active Directory.
E. Configure a secure LDAP connection.

Answer: CD

NEW QUESTION 71
An engineer is creating a new authorization policy to give the endpoints access to VLAN 310 upon successful authentication The administrator tests the 802.1X authentication for the endpoint and sees that it is authenticating successfully What must be done to ensure that the endpoint is placed into the correct VLAN?

A. Configure the switchport access vlan 310 command on the switch port
B. Ensure that the security group is not preventing the endpoint from being in VLAN 310
C. Add VLAN 310 in the common tasks of the authorization profile
D. Ensure that the endpoint is using The correct policy set

Answer: C

NEW QUESTION 74
What does the dot1x system-auth-control command do?

A. causes a network access switch not to track 802.1x sessions
B. globally enables 802.1x
C. enables 802.1x on a network access device interface
D. causes a network access switch to track 802.1x sessions

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380

NEW QUESTION 76
An administrator is configuring sponsored guest access using Cisco ISE Access must be restricted to the sponsor portal to ensure that only necessary employees can issue sponsored accounts and employees must be classified to do so What must be done to accomplish this task?

A. Configure an identity-based access list in Cisco ISE to restrict the users allowed to login
B. Edit the sponsor portal to only accept members from the selected groups
C. Modify the sponsor groups assigned to reflect the desired user groups
D. Create an authorization rule using the Guest Flow condition to authorize the administrators

Answer: C

NEW QUESTION 80
Which two probes must be enabled for the ARP cache to function in the Cisco ISE profile service so that a user can reliably bind the IP address and MAC addresses of endpoints? (Choose two.)

A. NetFlow
B. SNMP
C. HTTP
D. DHCP
E. RADIUS

Answer: DE

Explanation:
Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

NEW QUESTION 85
An administrator is configuring a Cisco ISE posture agent in the client provisioning policy and needs to ensure that the posture policies that interact with clients are monitored, and end users are required to comply with network usage rules Which two resources must be added in Cisco ISE to accomplish this goal? (Choose two)

A. AnyConnect
B. Supplicant
C. Cisco ISE NAC
D. PEAP
E. Posture Agent

Answer: AE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_An
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_clie

NEW QUESTION 87
Which permission is common to the Active Directory Join and Leave operations?

A. Create a Cisco ISE machine account in the domain if the machine account does not already exist
B. Remove the Cisco ISE machine account from the domain.
C. Set attributes on the Cisco ISE machine account
D. Search Active Directory to see if a Cisco ISE machine account already ex.sts.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_

NEW QUESTION 89

An engineer is configuring the remote access VPN to use Cisco ISE for AAA and needs to conduct posture checks on the connecting endpoints After the endpoint connects, it receives its initial authorization result and continues onto the compliance scan What must be done for this AAA configuration to allow compliant access to the network?

A. Configure the posture authorization so it defaults to unknown status
B. Fix the CoA port number
C. Ensure that authorization only mode is not enabled
D. Enable dynamic authorization within the AAA server group

Answer: D

NEW QUESTION 91
An engineer needs to export a file in CSV format, encrypted with the password C1$c0438563935, and contains users currently configured in Cisco ISE. Drag and drop the steps from the left into the sequence on the right to complete this task.

Click Export Selected, click Key, and enter the password.	1
Click Administration, and then click Identity Management.	2
Click Start Export, and then click OK.	3
Click Identities, click Users, and then select the list of users.	4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 94
An ISE administrator must change the inactivity timer for MAB endpoints to terminate the authentication session whenever a switch port that is connected to an IP phone does not detect packets from the device for 30 minutes. Which action must be taken to accomplish this task?

A. Add the authentication timer reauthenticate server command to the switchport.
B. Add the authentication timer inactivity 3600 command to the switchport.
C. Change the idle-timeout on the Radius server to 3600 seconds for IP Phone endpoints.
D. Configure the session-timeout to be 3600 seconds on Cisco ISE.

Answer: B

NEW QUESTION 95
What service can be enabled on the Cisco ISE node to identity the types of devices connecting to a network?

A. MAB
B. profiling
C. posture
D. central web authentication

Answer: B

NEW QUESTION 100
Refer to the exhibit.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A network engineers configuring the switch to accept downloadable ACLs from a Cisco ISC server Which two commands should be run to complete the configuration? (Choose two)

A. aaa authorization auth-proxy default group radius
B. radius server vsa sand authentication
C. radius-server attribute 8 include-in-access-req
D. ip device tracking
E. dot1x system-auth-control

Answer: BC

NEW QUESTION 104
Refer to the exhibit:

```
Interface: GigabitEthernet2/0/36
MAC Address: 000e.84af.59af
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

Which command is typed within the CU of a switch to view the troubleshooting output?

A. show authentication sessions mac 000e.84af.59af details
B. show authentication registrations
C. show authentication interface gigabitethemet2/0/36
D. show authentication sessions method

Answer: A

NEW QUESTION 106
An engineer needs to configure a compliance policy on Cisco ISE to ensure that the latest encryption software is running on the C drive of all endpoints. Drag and drop the configuration steps from the left into the sequence on the right to accomplish this task.

Answer Area

select Posture and Disk Encryption Condition	step 1
access the Disk Encryption Condition window	step 2
select the Encryption settings	step 3
access Policy Elements and Conditions	step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 107
An engineer needs to configure a Cisco ISE server to issue a CoA for endpoints already authenticated to access the network. The CoA option must be enforced on a session, even if there are multiple active sessions on a port. What must be configured to accomplish this task?

A. the Reauth CoA option in the Cisco ISE system profiling settings enabled
B. an endpoint profiling policy with the No CoA option enabled
C. an endpoint profiling policy with the Port Bounce CoA option enabled
D. the Port Bounce CoA option in the Cisco ISE system profiling settings enabled

Answer: A

NEW QUESTION 109
An administrator must block access to BYOD endpoints that were onboarded without a certificate and have been reported as stolen in the Cisco ISE My Devices Portal. Which condition must be used when configuring an authorization policy that sets DenyAccess permission?

A. Endpoint Identity Group is Blocklist, and the BYOD state is Registered.

B. Endpoint Identify Group is Blocklist, and the BYOD state is Pending.
C. Endpoint Identity Group is Blocklist, and the BYOD state is Lost.
D. Endpoint Identity Group is Blocklist, and the BYOD state is Reinstate.

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ISE_26_admin_guide/b_ISE_admin_26_

NEW QUESTION 114
An engineer tests Cisco ISE posture services on the network and must configure the compliance module to automatically download and install on endpoints Which action accomplishes this task for VPN users?

A. Create a Cisco AnyConnect configuration and Client Provisioning policy within Cisco ISE.
B. Configure the compliance module to be downloaded from within the posture policy.
C. Push the compliance module from Cisco FTD prior to attempting posture.
D. Use a compound posture condition to check for the compliance module and download if needed.

Answer: A

NEW QUESTION 117
Which two responses from the RADIUS server to NAS are valid during the authentication process? (Choose two)

A. access-response
B. access-request
C. access-reserved
D. access-accept
E. access-challenge

Answer: BD

NEW QUESTION 119
A company manager is hosting a conference. Conference participants must connect to an open guest SSID and only use a preassigned code that they enter into the guest portal prior to gaining access to the network. How should the manager configure Cisco ISE to accomplish this goal?

A. Create entries in the guest identity group for all participants.
B. Create an access code to be entered in the AUP page.
C. Create logins for each participant to give them sponsored access.
D. Create a registration code to be entered on the portal splash page.

Answer: B

NEW QUESTION 123
Which two default guest portals are available with Cisco ISE? (Choose two.)

A. visitor
B. WIFI-access
C. self-registered
D. central web authentication
E. sponsored

Answer: CE

NEW QUESTION 125
A network administrator is configuring client provisioning resource policies for client machines and must ensure that an agent pop-up is presented to the client when attempting to connect to the network Which configuration item needs to be added to allow for this'?

A. the client provisioning URL in the authorization policy
B. a temporal agent that gets installed onto the system
C. a remote posture agent proxying the network connection
D. an API connection back to the client

Answer: C

NEW QUESTION 127
A network administrator must use Cisco ISE to check whether endpoints have the correct version of antivirus installed Which action must be taken to allow this capability?

A. Configure a native supplicant profile to be used for checking the antivirus version
B. Configure Cisco ISE to push the HostScan package to the endpoints to check for the antivirus version.
C. Create a Cisco AnyConnect Network Visibility Module configuration profile to send the antivirus information of the endpoints to Cisco ISE.
D. Create a Cisco AnyConnect configuration within Cisco ISE for the Compliance Module and associated configuration files

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html About Anyconnect Network Visibility Module
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect45/administration/guide/b_An

NEW QUESTION 128
An administrator is configuring a Cisco WLC for web authentication Which two client profiling methods are enabled by default if the Apply Cisco ISE Default Settings check box has been selected'? (Choose two.)

A. CDP
B. DHCP
C. HTTP
D. SNMP
E. LLDP

Answer: AE

NEW QUESTION 130
An engineer is configuring a guest password policy and needs to ensure that the password complexity requirements are set to mitigate brute force attacks. Which two requirement complete this policy? (Choose two)

A. minimum password length
B. active username limit
C. access code control
D. gpassword expiration period
E. username expiration date

Answer: AD

NEW QUESTION 131
If a user reports a device lost or stolen, which portal should be used to prevent the device from accessing the network while still providing information about why the device is blocked?

A. Client Provisioning
B. Guest
C. BYOD
D. Blacklist

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Desi The Blacklist identity group is system generated and maintained by ISE to prevent access to lost or stolen devices. In this design guide, two authorization profiles are used to enforce the permissions for wireless and wired devices within the Blacklist:

- Blackhole WiFi Access
- Blackhole Wired Access

NEW QUESTION 135
Which profiling probe collects the user-agent string?

A. DHCP
B. AD
C. HTTP
D. NMAP

Answer: C

NEW QUESTION 139
Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after togging into the device with this command set authorization Which configuration is causing this issue?

A. Question marks are not allowed as wildcards for command sets.
B. The command set is allowing all commands that are not in the command list
C. The wildcard command listed is in the wrong format
D. The command set is working like an ACL and denying every command.

Answer: A

NEW QUESTION 142
A network administrator is currently using Cisco ISE to authenticate devices and users via 802 1X There is now a need to also authorize devices and users using EAP-TLS. Which two additional components must be configured in Cisco ISE to accomplish this'? (Choose two.)

A. Network Device Group
B. Serial Number attribute that maps to a CA Server
C. Common Name attribute that maps to an identity store
D. Certificate Authentication Profile
E. EAP Authorization Profile

Answer: CD

NEW QUESTION 147
What are two benefits of TACACS+ versus RADIUS for device administration? (Choose two)

A. TACACS+ supports 802.1X, and RADIUS supports MAB
B. TACACS+ uses UDP, and RADIUS uses TCP
C. TACACS+ has command authorization, and RADIUS does not.
D. TACACS+ provides the service type, and RADIUS does not
E. TACACS+ encrypts the whole payload, and RADIUS encrypts only the password.

Answer: CE

NEW QUESTION 149
An engineer is configuring 802.1X and is testing out their policy sets. After authentication, some endpoints are given an access-reject message but are still allowed onto the network. What is causing this issue to occur?

A. The switch port is configured with authentication event server dead action authorize vlan.
B. The authorization results for the endpoints include a dACL allowing access.
C. The authorization results for the endpoints include the Trusted security group tag.
D. The switch port is configured with authentication open.

Answer: D

NEW QUESTION 152
A network engineer is configuring Cisco TrustSec and needs to ensure that the Security Group Tag is being transmitted between two devices Where in the Layer 2 frame should this be verified?

A. CMD filed
B. 802.1Q filed
C. Payload
D. 802.1 AE header

Answer: A

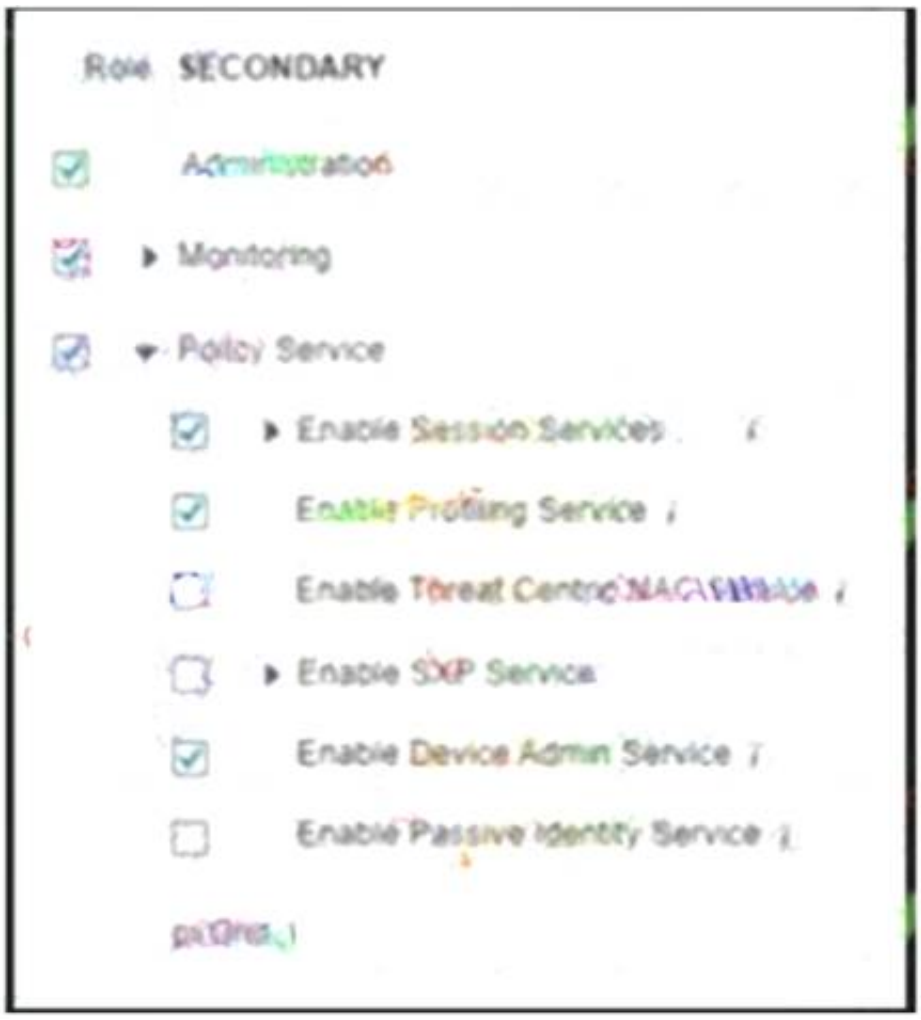
Explanation:
https://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs/policy_defined_segmentation_with_tr (slide 25)

NEW QUESTION 155
Which interface-level command is needed to turn on 802 1X authentication?

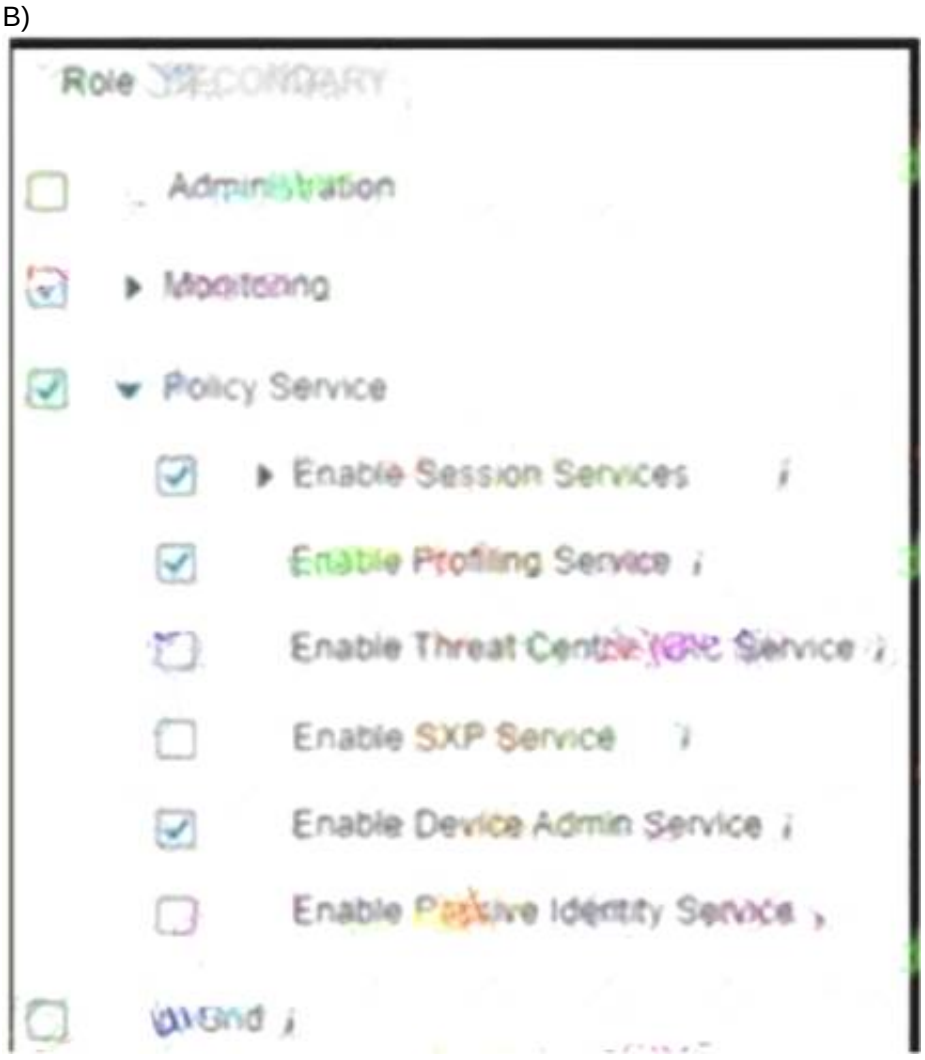
A. Dofl1x pae authenticator
B. dot1x system-auth-control
C. authentication host-mode single-host
D. aaa server radius dynamic-author

Answer: A

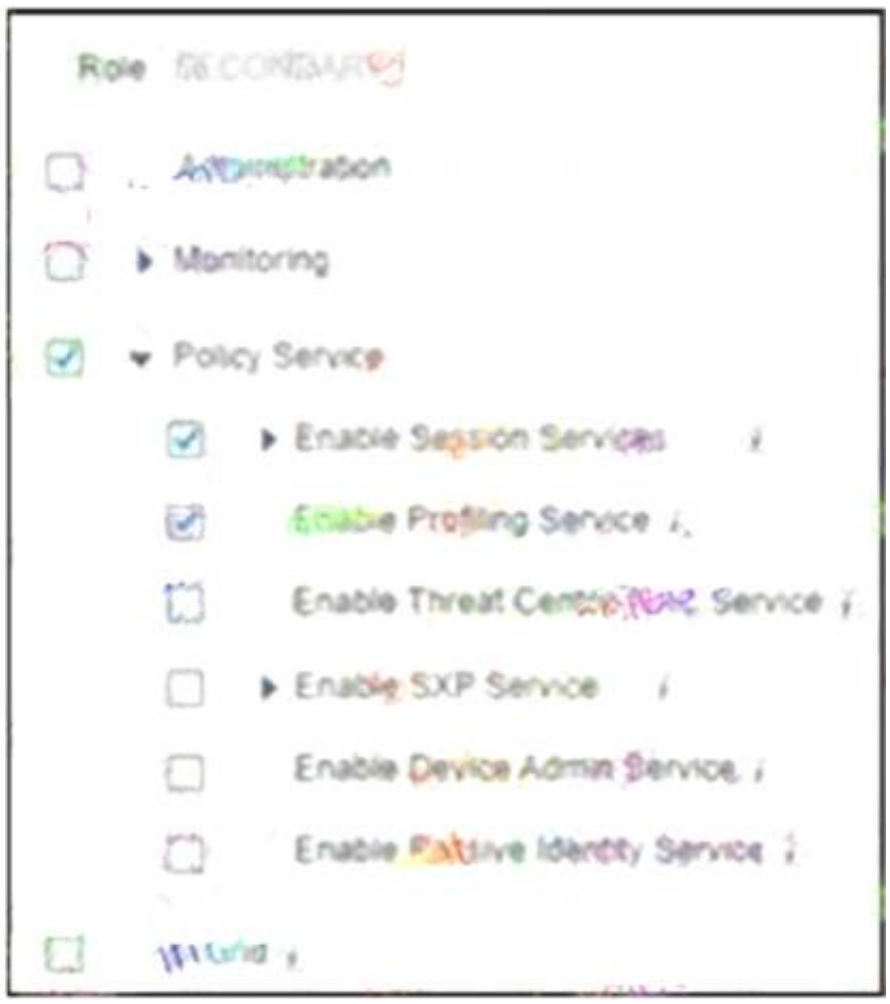
NEW QUESTION 159
An engineer builds a five-node distributed Cisco ISE deployment The first two deployed nodes are responsible for the primary and secondary administration and monitoring personas Which persona configuration is necessary to have the remaining three Cisco ISE nodes serve as dedicated nodes in the Cisco ISE cube that is responsible only for handling the RADIUS and TACACS+ authentication requests, identity lookups, and policy evaluation?
A)


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

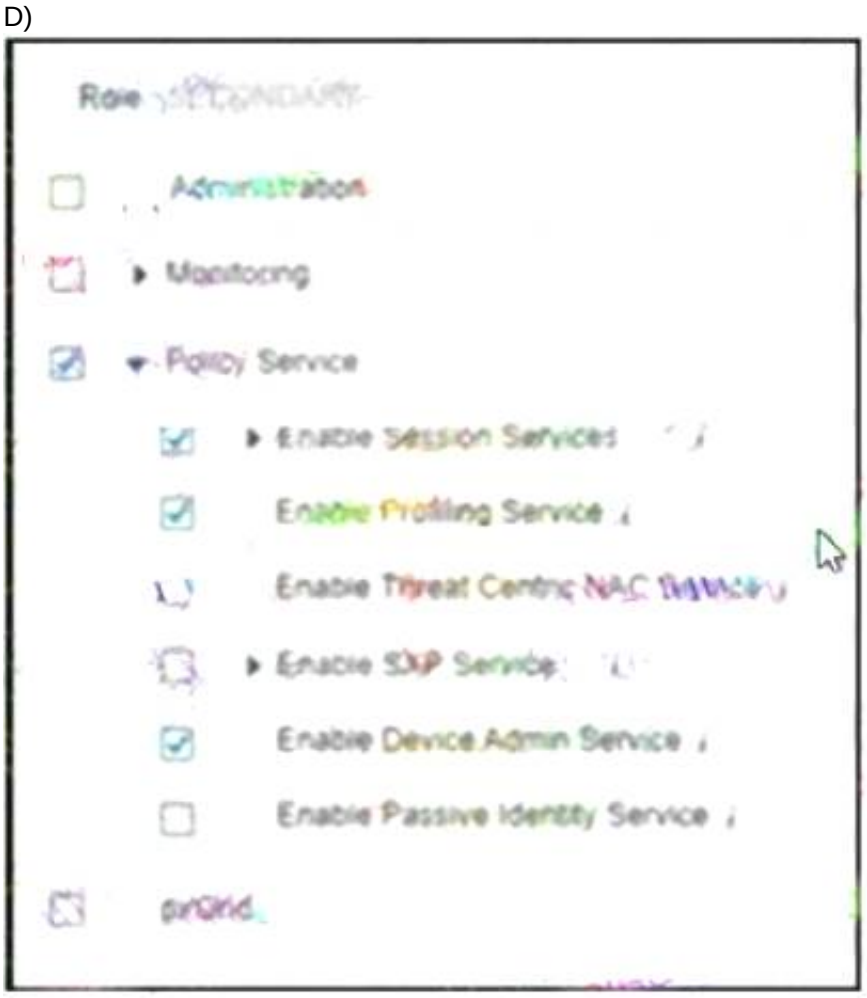
B)


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

C)



D)



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

Answer: D

NEW QUESTION 163
Which two actions must be verified to confirm that the internet is accessible via guest access when configuring a guest portal? (Choose two.)

A. The guest device successfully associates with the correct SSID.
B. The guest user gets redirected to the authentication page when opening a browser.
C. The guest device has internal network access on the WLAN.
D. The guest device can connect to network file shares.
E. Cisco ISE sends a CoA upon successful guest authentication.

Answer: BE

NEW QUESTION 168
Refer to the exhibit.

An organization recently implemented network device administration using Cisco ISE. Upon testing the ability to access all of the required devices, a user in the Cisco ISE group IT Admins is attempting to login to a device in their organization's finance department but is unable to. What is the problem?

A. The IT training rule is taking precedence over the IT Admins rule.
B. The authorization conditions wrongly allow IT Admins group no access to finance devices.
C. The finance location is not a condition in the policy set.
D. The authorization policy doesn't correctly grant them access to the finance devices.

Answer: D

NEW QUESTION 171
Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. endpoint marked as lost in My Devices Portal
B. addition of endpoint to My Devices Portal
C. endpoint profile transition from Apple-Device to Apple-iPhone
D. endpoint profile transition from Unknown to Windows 10-Workstation
E. updating of endpoint dACL.

Answer: CD

NEW QUESTION 176
Which two authentication protocols are supported by RADIUS but not by TACACS+? (Choose two.)

A. MSCHAPv1
B. PAP
C. EAP
D. CHAP
E. MSCHAPV2

Answer: CE

NEW QUESTION 179
An engineer must configure Cisco ISE to provide internet access for guests in which guests are required to enter a code to gain network access. Which action accomplishes the goal?

A. Configure the hotspot portal for guest access and require an access code.
B. Configure the sponsor portal with a single account and use the access code as the password.
C. Configure the self-registered guest portal to allow guests to create a personal access code.
D. Create a BYOD policy that bypasses the authentication of the user and authorizes access codes.

Answer: A

NEW QUESTION 183
A new employee just connected their workstation to a Cisco IP phone. The network administrator wants to ensure that the Cisco IP phone remains online when the user disconnects their Workstation from the corporate network Which CoA configuration meets this requirement?

A. Port Bounce
B. Reauth
C. NoCoA
D. Disconnect

Answer: C

Explanation:
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

NEW QUESTION 188

There is a need within an organization for a new policy to be created in Cisco ISE. It must validate that a specific anti-virus application is not only installed, but running on a machine before it is allowed access to the network. Which posture condition should the administrator configure in order for this policy to work?

A. file
B. registry
C. application
D. service

Answer: C

NEW QUESTION 190
Refer to the exhibit.
Which two configurations are needed on a catalyst switch for it to be added as a network access device in a Cisco ISE that is being used for 802 1X authentications? (Choose two)

```
radius server ISE1
 address ipv4 192.168.255.17 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

tacacs server ISE1
 address ipv4 192.168.255.15 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52
```

```
radius server ISE1
 address ipv4 192.168.255.19 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

radius server ISE1
 address ipv4 192.168.255.16 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

tacacs server ISE1
 address ipv4 192.168.255.18 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52
```

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

Answer: AC

NEW QUESTION 195
A customer wants to set up the Sponsor portal and delegate the authentication flow to a third party for added security while using Kerberos Which database should be used to accomplish this goal?

A. RSA Token Server
B. Active Directory
C. Local Database
D. LDAP

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide

NEW QUESTION 198
An engineer is configuring 802.1X and wants it to be transparent from the users' point of view. The implementation should provide open authentication on the switch ports while providing strong levels of security for non-authenticated devices. Which deployment mode should be used to achieve this?

A. closed
B. low-impact
C. open
D. high-impact

Answer: B

Explanation:
https://www.lookingpoint.com/blog/cisco-ise-wired-802.1x-deployment-monitormode#:~:text=Low%20im

NEW QUESTION 202
An administrator is attempting to join a new node to the primary Cisco ISE node, but receives the error message "Node is Unreachable". What is causing this

error?

A. The second node is a PAN node.
B. No administrative certificate is available for the second node.
C. The second node is in standalone mode.
D. No admin privileges are available on the second node.

Answer: B

Explanation:
https://www.ciscopress.com/articles/article.asp?p=2812072

NEW QUESTION 204
An administrator is configuring posture assessment in Cisco ISE for the first time. Which two components must be uploaded to Cisco ISE to use Anyconnect for the agent configuration in a client provisioning policy? (Choose two.)

A. Anyconnect network visibility module
B. Anyconnect compliance module
C. AnyConnectProfile.xml file
D. AnyConnectProfile.xsd file
E. Anyconnect agent image

Answer: BD

NEW QUESTION 208
The IT manager wants to provide different levels of access to network devices when users authenticate using TACACS+. The company needs specific commands to be allowed based on the Active Directory group membership of the different roles within the IT department. The solution must minimize the number of objects created in Cisco ISE. What must be created to accomplish this task?

A. one shell profile and one command set
B. multiple shell profiles and one command set
C. one shell profile and multiple command sets
D. multiple shell profiles and multiple command sets

Answer: C

NEW QUESTION 211
In a standalone Cisco ISE deployment, which two personas are configured on a node? (Choose two)

A. publisher
B. administration
C. primary
D. policy service
E. subscriber

Answer: BD

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide

NEW QUESTION 215
A network security engineer needs to configure 802.1X port authentication to allow a single host to be authenticated for data and another single host to be authenticated for voice. Which command should the engineer run on the interface to accomplish this goal?

A. authentication host-mode single-host
B. authentication host-mode multi-auth
C. authentication host-mode multi-host
D. authentication host-mode multi-domain

Answer: D

NEW QUESTION 218
Which are two characteristics of TACACS+? (Choose two)

A. It uses TCP port 49.
B. It combines authorization and authentication functions.
C. It separates authorization and authentication functions.
D. It encrypts the password only.
E. It uses UDP port 49.

Answer: AC

NEW QUESTION 223
A network administrator is configuring authorization policies on Cisco ISE There is a requirement to use AD group assignments to control access to network resources After a recent power failure and Cisco ISE rebooting itself, the AD group assignments no longer work What is the cause of this issue?

A. The AD join point is no longer connected.
B. The AD DNS response is slow.
C. The certificate checks are not being conducted.
D. The network devices ports are shut down.

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/ise_active_directory_integration/b_ISE_AD_integration_

NEW QUESTION 225
A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for one day When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the guest network after that period. Which configuration is causing this problem?

A. The Endpoint Purge Policy is set to 30 days for guest devices
B. The RADIUS policy set for guest access is set to allow repeated authentication of the same device
C. The length of access is set to 7 days in the Guest Portal Settings
D. The Guest Account Purge Policy is set to 15 days

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide

NEW QUESTION 227
Which advanced option within a WLAN must be enabled to trigger Central Web Authentication for Wireless users on AireOS controller?

A. DHCP server
B. static IP tunneling
C. override Interface ACL
D. AAA override

Answer: D

NEW QUESTION 229
What is the maximum number of PSN nodes supported in a medium-sized deployment?

A. three
B. five
C. two
D. eight

Answer: B

NEW QUESTION 234
An engineer is configuring TACACS+ within Cisco ISE for use with a non-Cisco network device. They need to send special attributes in the Access-Accept response to ensure that the users are given the appropriate access. What must be configured to accomplish this'?

A. dACLs to enforce the various access policies for the users
B. custom access conditions for defining the different roles
C. shell profiles with custom attributes that define the various roles
D. TACACS+ command sets to provide appropriate access

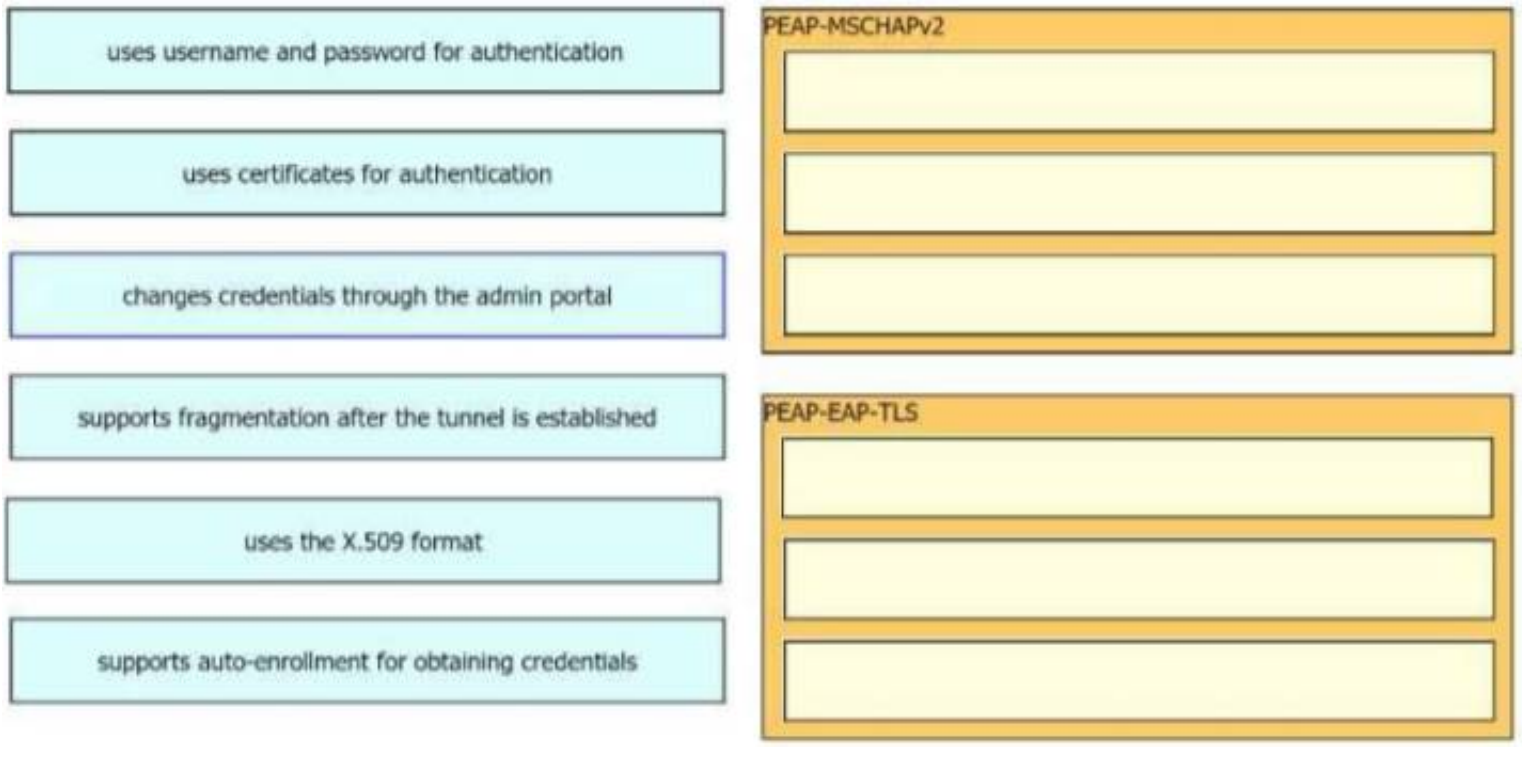
Answer: C

NEW QUESTION 236
Which Cisco ISE deployment model provides redundancy by having every node in the deployment configured with the Administration. Policy Service, and Monitoring personas to protect from a complete node failure?

A. distributed
B. dispersed
C. two-node
D. hybrid

Answer: C

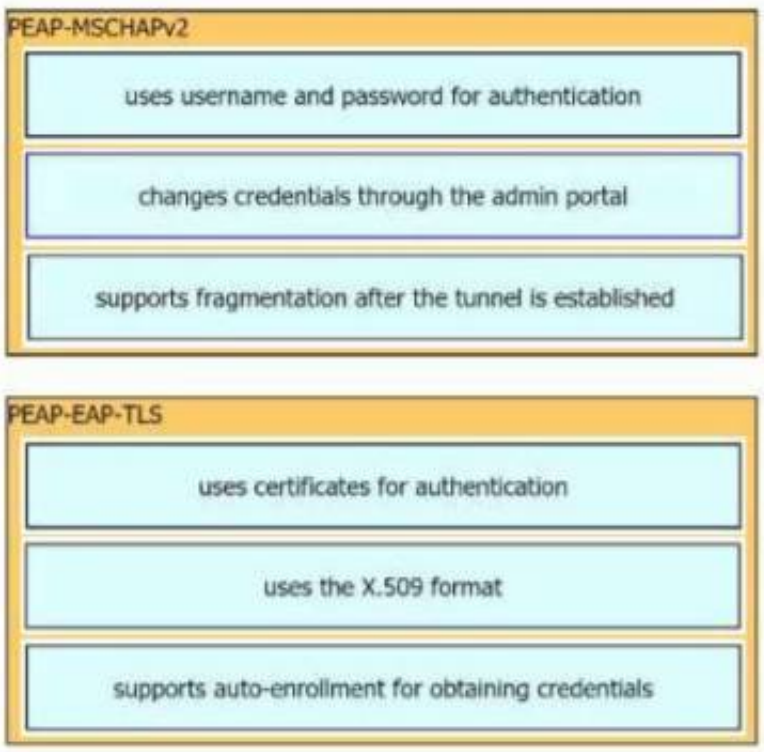
NEW QUESTION 240
An organization wants to implement 802.1X and is debating whether to use PEAP-MSCHAPv2 or
PEAP-EAP-TLS for authentication. Drag the characteristics on the left to the corresponding protocol on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 242
An engineer is using the low-impact mode for a phased deployment of Cisco ISE and is trying to connect to the network prior to authentication. Which access will be denied in this?

A. HTTP
B. DNS
C. EAP
D. DHCP

Answer: A

NEW QUESTION 247
What is an advantage of using EAP-TLS over EAP-MS-CHAPv2 for client authentication?

A. EAP-TLS uses a username and password for authentication to enhance security, while EAP-MS-CHAPv2 does not.
B. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.
C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.
D. EAP-TLS uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.

Answer: C

NEW QUESTION 251
An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP port 1812 RADIUS

B. TCP port 161
C. TCP port 514
D. UDP port 79
E. UDP port 16666

Answer: BC

NEW QUESTION 253
Refer to the exhibit.

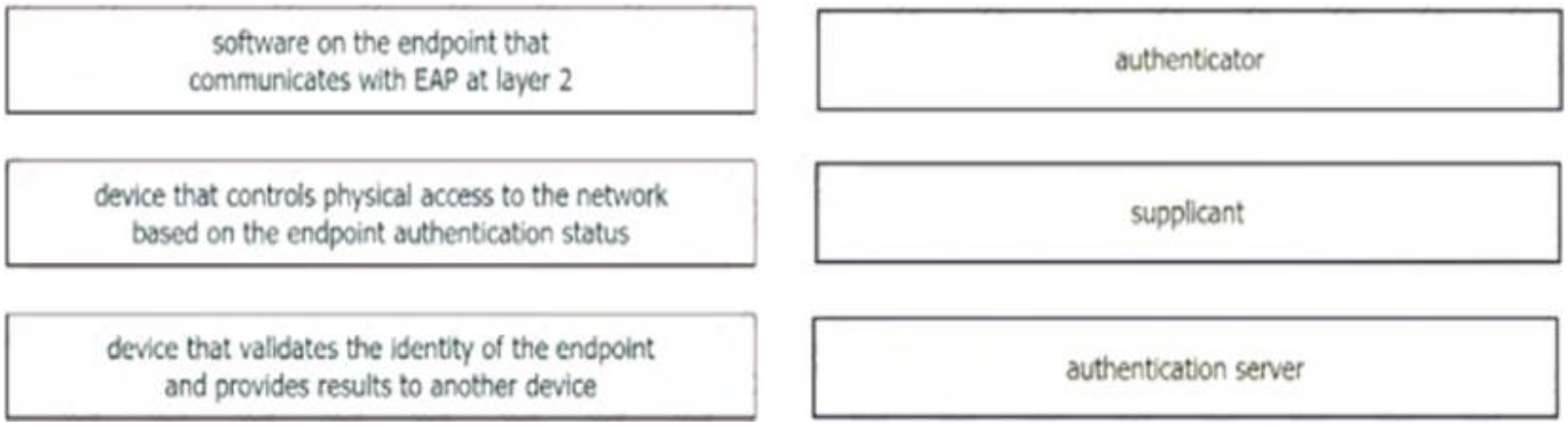
Interface	MAC Address	Method	Domain	Status Fg	Session ID
Gi1/0/6	0024.142d.e47f	mab	UNKNOWN	Auth	C0A829020000000C2BBAF5D3
Gi1/0/1	0050.5698.0720	dot1x	UNKNOWN	Unauth	C0A82902000000152BCD0BE7

An engineer is configuring a client but cannot authenticate to Cisco ISE During troubleshooting, the show authentication sessions command was issued to display the authentication status of each port Which command gives additional information to help identify the problem with the authentication?

A. show authentication sessions
B. show authentication sessions Interface Gil/0/1 output
C. show authentication sessions interface Gi1/0/1 details
D. show authentication sessions output

Answer: C

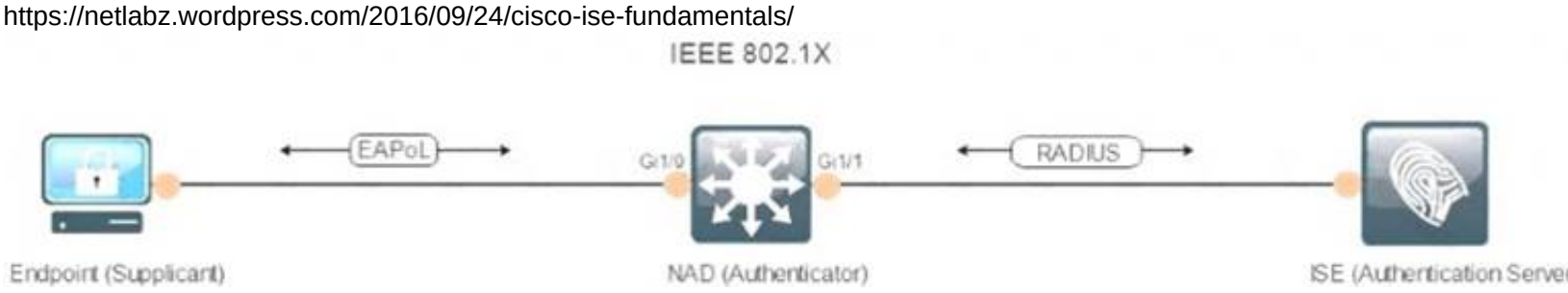
NEW QUESTION 257
Drag the descriptions on the left onto the components of 802.1X on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://netlabz.wordpress.com/2016/09/24/cisco-ise-fundamentals/



NEW QUESTION 259
An organization has a fully distributed Cisco ISE deployment When implementing probes, an administrator must scan for unknown endpoints to learn the IP-to-MAC address bindings. The scan is complete on one FPSN. but the information is not available on the others. What must be done to make the information available?

A. Scanning must be initiated from the PSN that last authenticated the endpoint
B. Cisco ISE must learn the IP-MAC binding of unknown endpoints via DHCP profiling, not via scanning
C. Scanning must be initiated from the MnT node to centrally gather the information
D. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning

Answer: B

NEW QUESTION 261
A network administrator is setting up wireless guest access and has been unsuccessful in testing client access. The endpoint is able to connect to the SSID but is unable to grant access to the guest network through the guest portal. What must be done to identify the problem?

A. Use context visibility to verify posture status.
B. Use the endpoint ID to execute a session trace.
C. Use the identity group to validate the authorization rules.
D. Use traceroute to ensure connectivity.

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide

NEW QUESTION 263
A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for 1 day. When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the guest network after that period. Which configuration is causing this problem?

A. The RADIUS policy set for guest access is set to allow repeated authentication of the same device.
B. The length of access is set to 7 days in the Guest Portal Settings.
C. The Endpoint Purge Policy is set to 30 days for guest devices.
D. The Guest Account Purge Policy is set to 15 days.

Answer: C

NEW QUESTION 264
An administrator is configuring a new profiling policy in Cisco ISE for a printer type that is missing from the profiler feed The logical profile Printers must be used in the authorization rule and the rule must be hit. What must be done to ensure that this configuration will be successful^

A. Create a new logical profile for the new printer policy
B. Enable the EndPoints:EndPointPolicy condition in the authorization policy.
C. Add the new profiling policy to the logical profile Printers.
D. Modify the profiler conditions to ensure that it goes into the correct logical profile

Answer: B

NEW QUESTION 269
What occurs when a Cisco ISE distributed deployment has two nodes and the secondary node is deregistered?

A. The primary node restarts
B. The secondary node restarts.
C. The primary node becomes standalone
D. Both nodes restart.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_deploy.html if your deployment has two nodes and you deregister the secondary node, both nodes in this
primary-secondary pair are restarted. (The former primary and secondary nodes become standalone.)

NEW QUESTION 270
Refer to the exhibit

```
interface GigabitEthernet1/0/1
  authentication host-mode multi-auth
  authentication post-control auto
  mab
  dot1x pae authenticator
```

Which switch configuration change will allow only one voice and one data endpoint on each port?

A. Multi-auth to multi-domain
B. Mab to dot1x
C. Auto to manual
D. Multi-auth to single-auth

Answer: A

Explanation:
https://community.cisco.com/t5/network-access-control/cisco-ise-multi-auth-or-multi-host/m-p/3750907

NEW QUESTION 273
Which default endpoint identity group does an endpoint that does not match any profile in Cisco ISE become a member of?

A. Endpoint
B. unknown
C. blacklist
D. white list
E. profiled

Answer: B

Explanation:
If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_identities.html

NEW QUESTION 276
A Cisco ISE server sends a CoA to a NAD after a user logs in successfully using CWA Which action does the CoA perform?

A. It terminates the client session
B. It applies the downloadable ACL provided in the CoA
C. It applies new permissions provided in the CoA to the client session.
D. It triggers the NAD to reauthenticate the client

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/113362-config-web-auth-ise-00.ht

NEW QUESTION 278
Which two features are available when the primary admin node is down and the secondary admin node has not been promoted? (Choose two.)

A. hotspot
B. new AD user 802 1X authentication
C. posture
D. BYOD
E. guest AUP

Answer: BC

NEW QUESTION 279
What is a restriction of a standalone Cisco ISE node deployment?

A. Only the Policy Service persona can be disabled on the node.
B. The domain name of the node cannot be changed after installation.
C. Personas are enabled by default and cannot be edited on the node.
D. The hostname of the node cannot be changed after installation.

Answer: C

NEW QUESTION 283
An administrator is configuring cisco ISE lo authenticate users logging into network devices using TACACS+ The administrator is not seeing any oí the authentication in the TACACS+ live logs. Which action ensures the users are able to log into the network devices?

A. Enable the device administration service in the Administration persona
B. Enable the session services in the administration persona
C. Enable the service sessions in the PSN persona.
D. Enable the device administration service in the PSN persona.

Answer: D

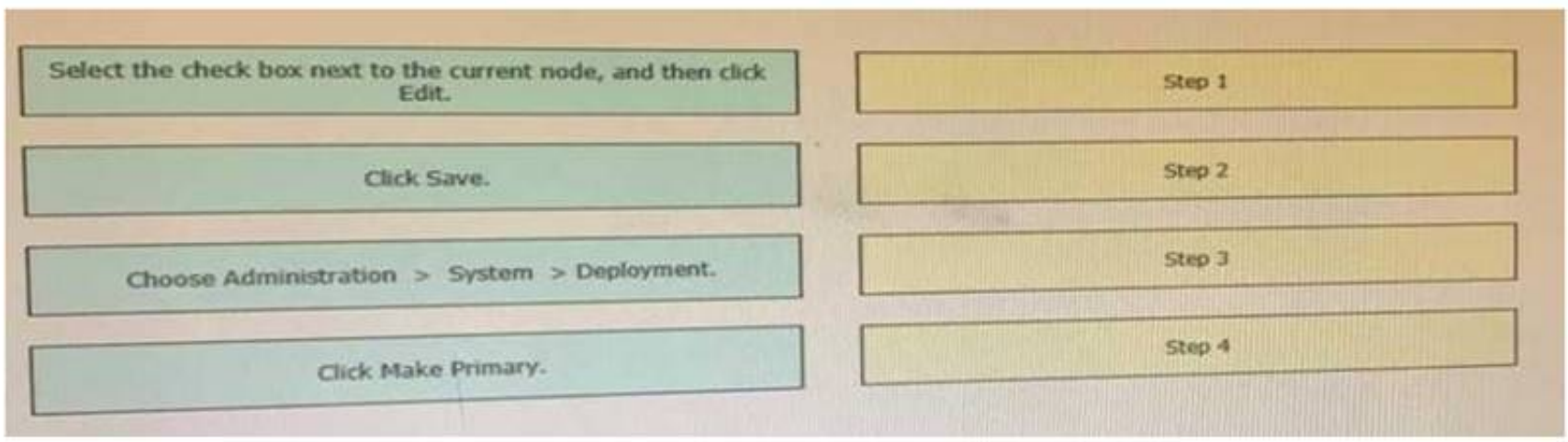
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_tacacs_dev

NEW QUESTION 287
Which port does Cisco ISE use for native supplicant provisioning of a Windows laptop?

A. TCP 8909
B. TCP 8905
C. UDP 1812
D. TCP 443

Answer: B

NEW QUESTION 289
Drag the steps to configure a Cisco ISE node as a primary administration node from the left into the correct order on the night.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide
Step 1
Choose Administration > System > Deployment.
The Register button will be disabled initially. To enable this button, you must configure a Primary PAN.
Step 2
Check the check box next to the current node, and click Edit.
Step 3
Click Make Primary
to configure your Primary PAN.
Step 4
Enter data on the General Settings
Step 5
tab.
Click Save to save the node configuration.

NEW QUESTION 293
An administrator is adding a switch to a network that is running Cisco ISE and is only for IP Phones The phones do not have the ability to authenticate via 802 1X Which command is needed on each switch port for authentication?

A. dot1x system-auth-control
B. enable bypass-mac
C. enable network-authentication
D. mab

Answer: D

Explanation:
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-config-mab.html

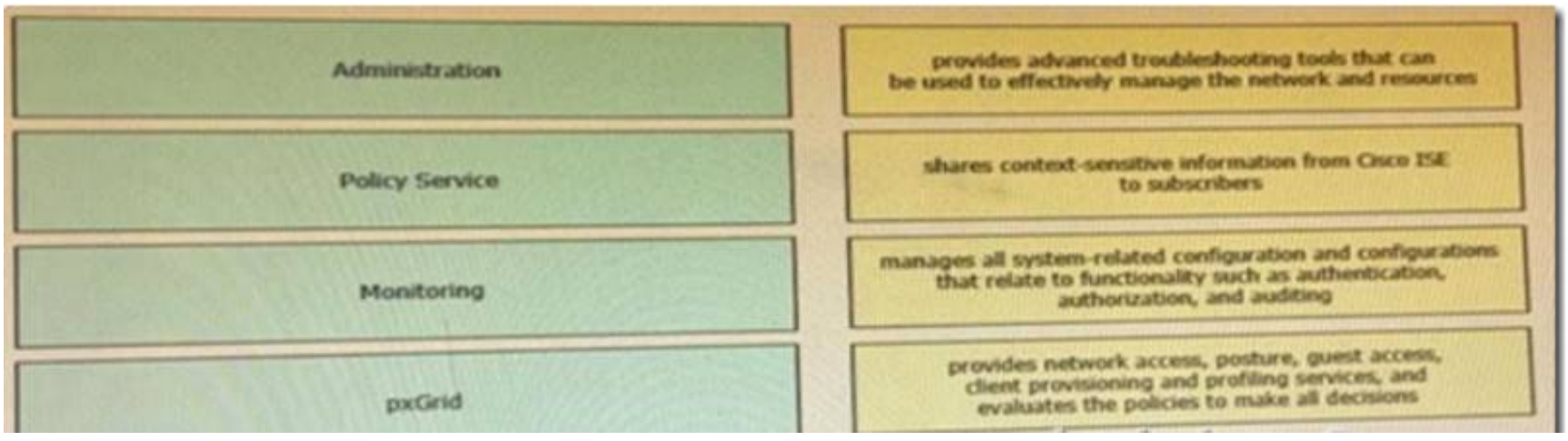
NEW QUESTION 297
An engineer is implementing Cisco ISE and needs to configure 802.1X. The port settings are configured for port-based authentication. Which command should be used to complete this configuration?

A. dot1x pae authenticator
B. dot1x system-auth-control
C. authentication port-control auto
D. aaa authentication dot1x default group radius

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/dot1x.

NEW QUESTION 298
Drag the Cisco ISE node types from the left onto the appropriate purposes on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Monitoring = provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources
Policy Service = provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Administration = manages all system-related configuration and configurations that relate to functionality such as authentication, authorization, auditing, and so on
pxGrid = shares context-sensitive information from Cisco ISE to subscribers
https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide

NEW QUESTION 301
A user reports that the RADIUS accounting packets are not being seen on the Cisco ISE server. Which command is the user missing in the switch's configuration?

A. radius-server vsa send accounting
B. aaa accounting network default start-stop group radius
C. aaa accounting resource default start-stop group radius
D. aaa accounting exec default start-stop group radios

Answer: A

NEW QUESTION 305
An administrator is configuring new probes to use with Cisco ISE and wants to use metadata to help profile the endpoints. The metadata must contain traffic information relating to the endpoints instead of
industry-standard protocol information Which probe should be enabled to meet these requirements?

A. NetFlow probe
B. DNS probe
C. DHCP probe
D. SNMP query probe

Answer: C

Explanation:
http://www.network-node.com/blog/2016/1/2/ise-20-profiling

NEW QUESTION 310
An engineer is configuring Cisco ISE to reprofile endpoints based only on new requests of INIT-REBOOT and SELECTING message types. Which probe should be used to accomplish this task?

A. MMAP
B. DNS
C. DHCP
D. RADIUS

Answer: C

NEW QUESTION 311
In which two ways can users and endpoints be classified for TrustSec? (Choose Two.)

A. VLAN
B. SXP
C. dynamic
D. QoS
E. SGACL

Answer: AE

NEW QUESTION 316
What is a characteristic of the UDP protocol?

A. UDP can detect when a server is down.
B. UDP offers best-effort delivery
C. UDP can detect when a server is slow
D. UDP offers information about a non-existent server

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838

NEW QUESTION 321
Which two task types are included in the Cisco ISE common tasks support for TACACS+ profiles? (Choose two.)

A. Firepower
B. WLC
C. IOS
D. ASA
E. Shell

Answer: BE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide TACACS+ Profile
TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

- Common tasks
- Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.
The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However,
the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

- Shell
- WLC
- Nexus
- Generic

The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using a equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

NEW QUESTION 326
Which two methods should a sponsor select to create bulk guest accounts from the sponsor portal? (Choose two)

A. Random
B. Monthly
C. Daily
D. Imported
E. Known

Answer: AD

NEW QUESTION 330
An administrator is configuring posture with Cisco ISE and wants to check that specific services are present on the workstations that are attempting to access the network. What must be configured to accomplish this goal?

A. Create a registry posture condition using a non-OPSWAT API version.
B. Create an application posture condition using a OPSWAT API version.
C. Create a compound posture condition using a OPSWAT API version.
D. Create a service posture condition using a non-OPSWAT API version.

Answer: D

NEW QUESTION 332
A Cisco device has a port configured in multi-authentication mode and is accepting connections only from hosts assigned the SGT of SGT_0422048549 The VLAN trunk link supports a maximum of 8 VLANS What is the reason for these restrictions?

A. The device is performing inline tagging without acting as a SXP speaker
B. The device is performing mime tagging while acting as a SXP speaker
C. The IP subnet addresses are dynamically mapped to an SGT.
D. The IP subnet addresses are statically mapped to an SGT

Answer: C

NEW QUESTION 334
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-715 Practice Exam Features:

* 300-715 Questions and Answers Updated Frequently

* 300-715 Practice Questions Verified by Expert Senior Certified Staff

* 300-715 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-715 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year