

Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)



NEW QUESTION 1

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 2

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 3

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 4

In a Cisco ISE split deployment model, which load is split between the nodes?

- A. AAA
- B. network admission
- C. log collection
- D. device admission

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.pdf

NEW QUESTION 5

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 6

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 7

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 8

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 9

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_guide

NEW QUESTION 10

When configuring an authorization policy, an administrator cannot see specific Active Directory groups present in their domain to be used as a policy condition. However, other groups that are in the same domain are seen. What is causing this issue?

- A. Cisco ISE only sees the built-in groups, not user created ones
- B. The groups are present but need to be manually typed as conditions
- C. Cisco ISE's connection to the AD join point is failing
- D. The groups are not added to Cisco ISE under the AD join point

Answer: D

Explanation:

https://www.youtube.com/watch?v=0kuEZEo564s&ab_channel=CiscoISE-IdentityServicesEngine

NEW QUESTION 10

What are two differences of TACACS+ compared to RADIUS? (Choose two.)

- A. TACACS+ uses a connectionless transport protocol, whereas RADIUS uses a connection-oriented transport protocol.
- B. TACACS+ encrypts the full packet payload, whereas RADIUS only encrypts the password.
- C. TACACS+ only encrypts the password, whereas RADIUS encrypts the full packet payload.
- D. TACACS+ uses a connection-oriented transport protocol, whereas RADIUS uses a connectionless transport protocol.
- E. TACACS+ supports multiple sessions per user, whereas RADIUS supports one session per user.

Answer: BD

NEW QUESTION 11

An administrator needs to connect ISE to Active Directory as an external authentication source and allow the proper ports through the firewall. Which two ports should be opened to accomplish this task? (Choose two)

- A. TELNET 23
- B. LDAP 389
- C. HTTP 80
- D. HTTPS 443
- E. MSRPC 445

Answer: BE

NEW QUESTION 13

An engineer is working with a distributed deployment of Cisco ISE and needs to configure various network probes to collect a set of attributes from the used to accomplish this task?

- A. policy service
- B. monitoring
- C. pxGrid
- D. primary policy administrator

Answer: B

NEW QUESTION 14

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 Endpoints Cisco 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 17

A network engineer needs to ensure that the access credentials are not exposed during the 802.1x authentication among components. Which two protocols should complete this task?

- A. PEAP
- B. EAP-MD5
- C. LEAP
- D. EAP-TLS
- E. EAP-TTLS

Answer: BD

NEW QUESTION 21

An engineer is configuring ISE for network device administration and has devices that support both protocols. What are two benefits of choosing TACACS+ over RADUs for these devices? (Choose two.)

- A. TACACS+ is FIPS compliant while RADIUS is not
- B. TACACS+ is designed for network access control while RADIUS is designed for role-based access.
- C. TACACS+ uses secure EAP-TLS while RADIUS does not.
- D. TACACS+ provides the ability to authorize specific commands while RADIUS does not
- E. TACACS+ encrypts the entire payload being sent while RADIUS only encrypts the password.

Answer: DE

NEW QUESTION 25

A network administrator must configura endpoints using an 802 1X authentication method with EAP identity certificates that are provided by the Cisco ISE When the endpoint presents the identity certificate to Cisco ISE to validate the certificate, endpoints must be authorized to connect to the network Which EAP type must be configured by the network administrator to complete this task?

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

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificate-requirements-eap-tls-peap> about EAP FAST

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding-EAP-FAST-and->

NEW QUESTION 26

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 29

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 34

How is policy services node redundancy achieved in a deployment?

- A. by enabling VIP
- B. by utilizing RADIUS server list on the NAD
- C. by creating a node group
- D. by deploying both primary and secondary node

Answer: C

NEW QUESTION 35

Which Cisco ISE solution ensures endpoints have the latest version of antivirus updates installed before being allowed access to the corporate network?

- A. Threat Services
- B. Profiling Services
- C. Provisioning Services
- D. Posture Services

Answer: D

NEW QUESTION 36

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 39

An administrator is adding network devices for a new medical building into Cisco ISE. These devices must be in a network device group that is identifying them as "Medical Switch" so that the policies can be made separately for the endpoints connecting through them. Which configuration item must be changed in the network device within Cisco ISE to accomplish this goal?

- A. Change the device type to Medical Switch.
- B. Change the device profile to Medical Switch.
- C. Change the model name to Medical Switch.
- D. Change the device location to Medical Switch.

Answer: A

NEW QUESTION 42

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 43

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 48

A network engineer must enforce access control using special tags, without re-engineering the network design. Which feature should be configured to achieve this in a scalable manner?

- A. SGT
- B. dACL
- C. VLAN
- D. RBAC

Answer: A

NEW QUESTION 51

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 55

Which RADIUS attribute is used to dynamically assign the inactivity active timer for MAB users from the Cisco ISE node'?

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

Answer: C

NEW QUESTION 56

An engineer is enabling a newly configured wireless SSID for tablets and needs visibility into which other types of devices are connecting to it. What must be done on the Cisco WLC to provide this information to Cisco ISE9

- A. enable IP Device Tracking
- B. enable MAC filtering
- C. enable Fast Transition
- D. enable mDNS snooping

Answer: B

NEW QUESTION 59

A laptop was stolen and a network engineer added it to the block list endpoint identity group What must be done on a new Cisco ISE deployment to redirect the laptop and restrict access?

- A. Select DenyAccess within the authorization policy.
- B. Ensure that access to port 8443 is allowed within the ACL.
- C. Ensure that access to port 8444 is allowed within the ACL.
- D. Select DROP under If Auth fail within the authentication policy.

Answer: C

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 63

What is a valid guest portal type?

- A. Sponsored-Guest
- B. My Devices
- C. Sponsor
- D. Captive-Guest

Answer: A

NEW QUESTION 64

There are several devices on a network that are considered critical and need to be placed into the ISE database and a policy used for them. The organization does not want to use profiling. What must be done to accomplish this goal?

- A. Enter the MAC address in the correct Endpoint Identity Group.
- B. Enter the MAC address in the correct Logical Profile.
- C. Enter the IP address in the correct Logical Profile.
- D. Enter the IP address in the correct Endpoint Identity Group.

Answer: A

NEW QUESTION 66

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 68

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 72

Which type of identity store allows for creating single-use access credentials in Cisco ISE?

- A. OpenLDAP
- B. Local
- C. PKI
- D. RSA SecurID

Answer: D

NEW QUESTION 77

An administrator needs to allow guest devices to connect to a private network without requiring usernames and passwords. Which two features must be configured to allow for this? (Choose two.)

- A. hotspot guest portal
- B. device registration WebAuth
- C. central WebAuth
- D. local WebAuth
- E. self-registered guest portal

Answer: AB

NEW QUESTION 79

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 83

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 84

Which two ports do network devices typically use for CoA? (Choose two)

- A. 443
- B. 19005
- C. 8080
- D. 3799
- E. 1700

Answer: DE

NEW QUESTION 86

Drag and drop the configuration steps from the left into the sequence on the right to install two Cisco ISE nodes in a distributed deployment.

Register the secondary node.	1
Define personas for the secondary node.	2
Enable Administration and Monitoring personas on the first node.	3
Configure the first node as the primary node.	4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

NEW QUESTION 87

An engineer is configuring static SGT classification. Which configuration should be used when authentication is disabled and third-party switches are in use?

- A. VLAN to SGT mapping
- B. IP Address to SGT mapping
- C. L3IF to SGT mapping
- D. Subnet to SGT mapping

Answer: B

Explanation:

<https://community.cisco.com/t5/security-knowledge-base/segmentation-strategy/ta-p/3757424>: "The method of sending out IP to SGT mappings from ISE is particularly useful if the access switch does not support TrustSec"

NEW QUESTION 90

An organization is migrating its current guest network to Cisco ISE and has 1000 guest users in the current database. There are no resources to enter this information into the Cisco ISE database manually. What must be done to accomplish this task efficiently?

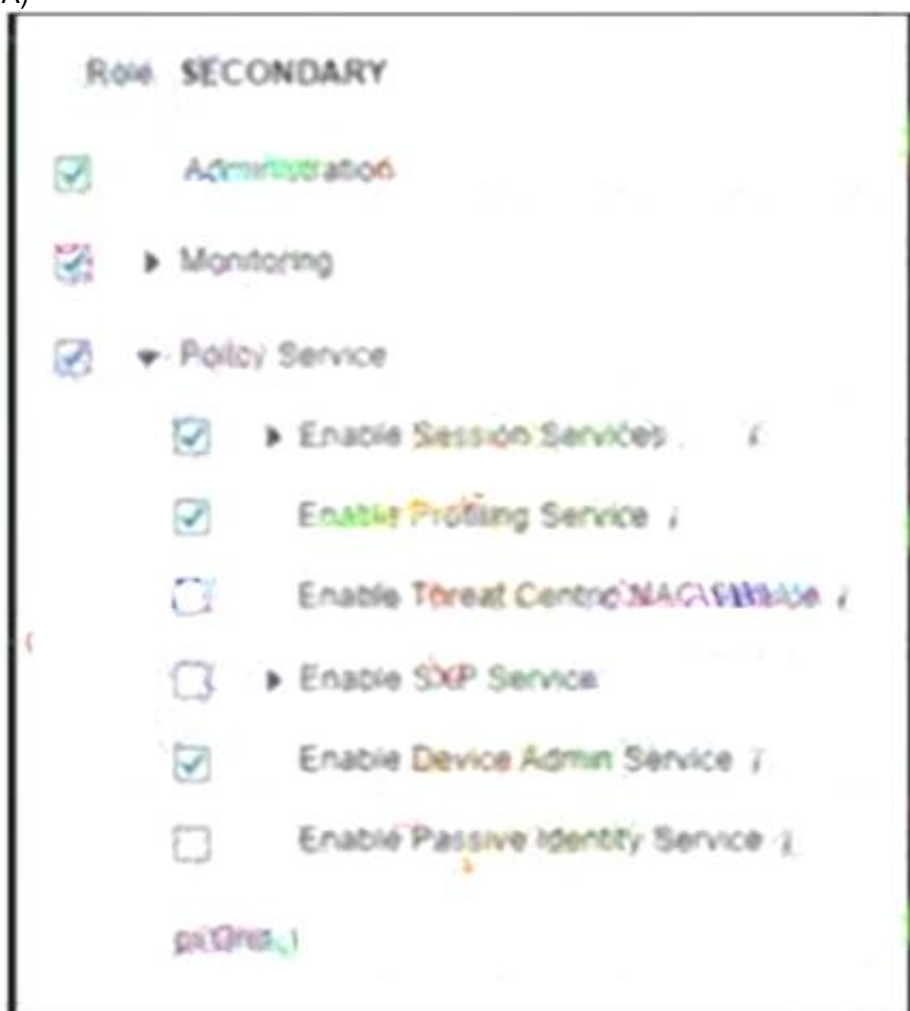
- A. Use a CSV file to import the guest accounts
- B. Use SQL to link the existing database to Cisco ISE
- C. Use a JSON file to automate the migration of guest accounts
- D. Use an XML file to change the existing format to match that of Cisco ISE

Answer: A

NEW QUESTION 92

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 Center (TAC) Service

☐ Enable SXP Service

☒ Enable Device Admin Service

☐ Enable Passive Identity Service

☐ End

C)

Role **SECONDARY**

☐ Administration

☐ Monitoring

☒ Policy Service

☒ Enable Session Services

☒ Enable Profiling Service

☐ Enable Threat Center (TAC) Service

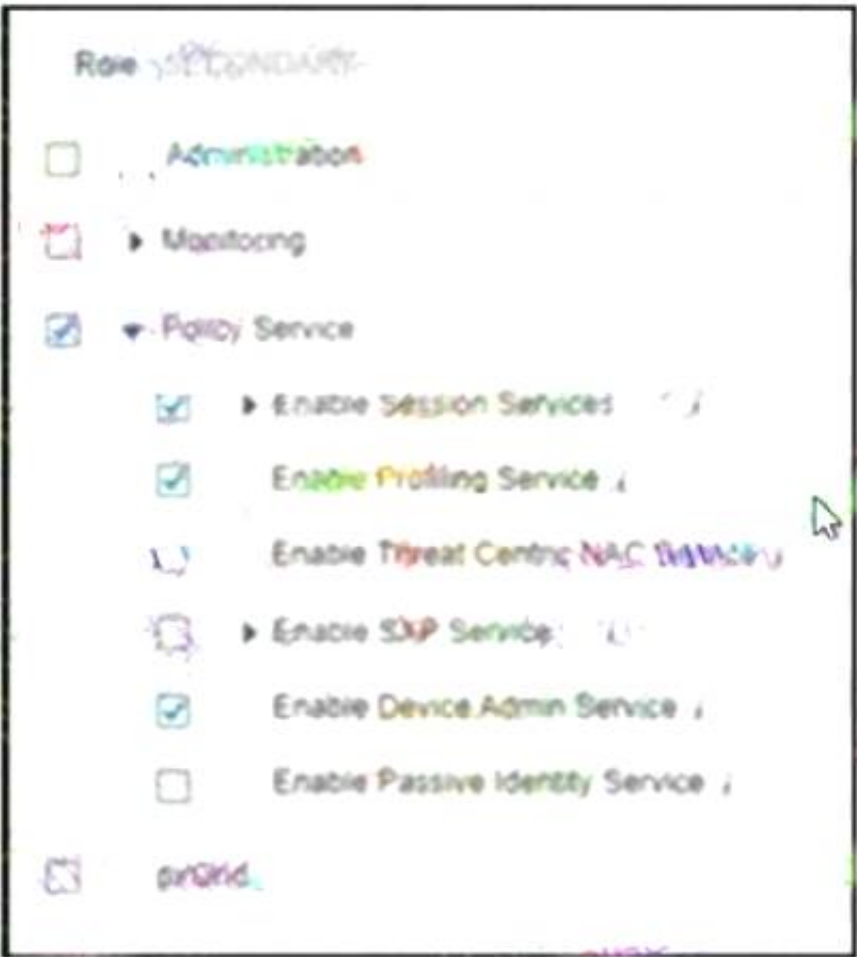
☐ Enable SXP Service

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

☐ End

D)



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

Answer: D

NEW QUESTION 94

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 99

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 102

An organization is hosting a conference and must make guest accounts for several of the speakers attending. The conference ended two days early but the guest accounts are still being used to access the network. What must be configured to correct this?

- A. Create an authorization rule denying sponsored guest access.
- B. Navigate to the Guest Portal and delete the guest accounts.
- C. Create an authorization rule denying guest access.
- D. Navigate to the Sponsor Portal and suspend the guest accounts.

Answer: D

NEW QUESTION 105

Which command displays all 802 1X/MAB sessions that are active on the switch ports of a Cisco Catalyst switch?

- A. show authentication sessions output
- B. Show authentication sessions
- C. show authentication sessions interface Gi 1/0/x
- D. show authentication sessions interface Gi1/0/x output

Answer: B

NEW QUESTION 110

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 111

Which three default endpoint identity groups does cisco ISE create? (Choose three)

- A. Unknown
- B. whitelist
- C. end point
- D. profiled
- E. blacklist

Answer: ADE

Explanation:

Default Endpoint Identity Groups Created for Endpoints

Cisco 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.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide

NEW QUESTION 114

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 115

An engineer has been tasked with standing up a new guest portal for customers that are waiting in the lobby. There is a requirement to allow guests to use their social media logins to access the guest network to appeal to more customers What must be done to accomplish this task?

- A. Create a sponsor portal to allow guests to create accounts using their social media logins.
- B. Create a sponsored guest portal and enable social media in the external identity sources.
- C. Create a self-registered guest portal and enable the feature for social media logins
- D. Create a hotspot portal and enable social media login for network access

Answer: C

NEW QUESTION 116

An engineer wants to learn more about Cisco ISE and deployed a new lab with two nodes. Which two persona configurations allow the engineer to successfully test redundancy of a failed node? (Choose two.)

- A. Configure one of the Cisco ISE nodes as the Health Check node.
- B. Configure both nodes with the PAN and MnT personas only.
- C. Configure one of the Cisco ISE nodes as the primary PAN and MnT personas and the other as the secondary.
- D. Configure both nodes with the PAN, MnT, and PSN personas.
- E. Configure one of the Cisco ISE nodes as the primary PAN and PSN personas and the other as the secondary.

Answer: CE

NEW QUESTION 118

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 122

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 125

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.

uses username and password for authentication

uses certificates for authentication

changes credentials through the admin portal

supports fragmentation after the tunnel is established

uses the X.509 format

supports auto-enrollment for obtaining credentials

PEAP-MSCHAPv2

PEAP-EAP-TLS

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

PEAP-MSCHAPv2

uses username and password for authentication

changes credentials through the admin portal

supports fragmentation after the tunnel is established

PEAP-EAP-TLS

uses certificates for authentication

uses the X.509 format

supports auto-enrollment for obtaining credentials

NEW QUESTION 126

Drag and drop the description from the left onto the protocol on the right that is used to carry out system authentication, authentication, and accounting.

combines authentication and authorization

encrypts the entire payload

encrypts only the password field

separates authentication and authorization

primary use is device administration

primary use is network access

TACACS+

RADIUS

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, chart, application Description automatically generated
<https://www.mbne.net/tech-notes/aaa-tacacs-radius>

NEW QUESTION 128

Which two roles are taken on by the administration person within a Cisco ISE distributed environment? (Choose two.)

- A. backup
- B. secondary
- C. standby
- D. primary
- E. active

Answer: BD

NEW QUESTION 132

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

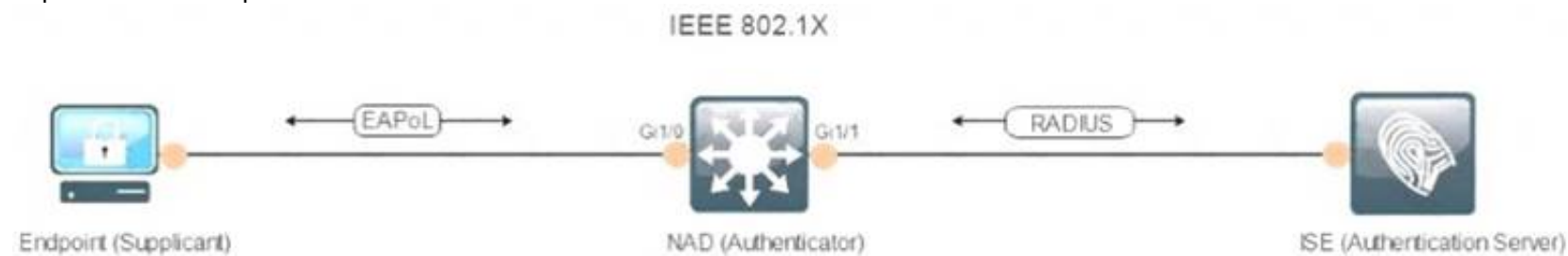
software on the endpoint that communicates with EAP at layer 2	authenticator
device that controls physical access to the network based on the endpoint authentication status	supplicant
device that validates the identity of the endpoint and provides results to another device	authentication server

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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



NEW QUESTION 136

What allows an endpoint to obtain a digital certificate from Cisco ISE during a BYOD flow?

- A. Network Access Control
- B. My Devices Portal
- C. Application Visibility and Control
- D. Supplicant Provisioning Wizard

Answer: D

NEW QUESTION 139

An administrator is configuring TACACS+ on a Cisco switch but cannot authenticate users with Cisco ISE. The configuration contains the correct key of Cisc039712287. but the switch is not receiving a response from the Cisco ISE instance What must be done to validate the AAA configuration and identify the problem with the TACACS+ servers?

- A. Check for server reachability using the test aaa group tacacs+ admin <key> legacy command.
- B. Test the user account on the server using the test aaa group radius server CUCS user admin pass <key> legacy command.
- C. Validate that the key value is correct using the test aaa authentication admin <key> legacy command.
- D. Conrm the authorization policies are correct using the test aaa authorization admin drop legacy command.

Answer: A

Explanation:

<https://medium.com/training-course-ccna-security-210-260/ccna-security-part-3-implementing-aaa-in-cisco-ios>

NEW QUESTION 144

An administrator is migrating device administration access to Cisco ISE from the legacy TACACS+ solution that used only privilege 1 and 15 access levels. The organization requires more granular controls of the privileges and wants to customize access levels 2-5 to correspond with different roles and access needs. Besides defining a new shell profile in Cisco ISE. what must be done to accomplish this configuration?

- A. Enable the privilege levels in Cisco ISE
- B. Enable the privilege levels in the IOS devices.
- C. Define the command privileges for levels 2-5 in the IOS devices
- D. Define the command privileges for levels 2-5 in Cisco ISE

Answer: B

Explanation:

<https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>

NEW QUESTION 147

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 152

Which two Cisco ISE deployment models require two nodes configured with dedicated PAN and MnT personas? (Choose two.)

- A. three PSN nodes
- B. seven PSN nodes with one PxGrid node
- C. five PSN nodes with one PxGrid node
- D. two PSN nodes with one PxGrid node
- E. six PSN nodes

Answer: CD

NEW QUESTION 154

An engineer is configuring posture assessment for their network access control and needs to use an agent that supports using service conditions as conditions for the assessment. The agent should be run as a background process to avoid user interruption but when it is run, the user can see it. What is the problem?

- A. The engineer is using the "Anyconnect" posture agent but should be using the "Stealth Anyconnect posture agent
- B. The posture module was deployed using the headend instead of installing it with SCCM
- C. The user was in need of remediation so the agent appeared in the notifications
- D. The proper permissions were not given to the temporal agent to conduct the assessment

Answer: A

NEW QUESTION 158

An administrator is manually adding a device to a Cisco ISE identity group to ensure that it is able to access the network when needed without authentication. Upon testing, the administrator notices that the device never hits the correct authorization policy line using the condition EndPoints LogicalProfile EQUALS static_list. Why is this occurring?

- A. The dynamic logical profile is overriding the statically assigned profile
- B. The device is changing identity groups after profiling instead of remaining static
- C. The logical profile is being statically assigned instead of the identity group
- D. The identity group is being assigned instead of the logical profile

Answer: C

NEW QUESTION 160

An administrator adds a new network device to the Cisco ISE configuration to authenticate endpoints to the network. The RADIUS test fails after the administrator configures all of the settings in Cisco ISE and adds the proper configurations to the switch. What is the issue?

- A. The endpoint profile is showing as "unknown."
- B. The endpoint does not have the appropriate credentials for network access.
- C. The shared secret is incorrect on the switch or on Cisco ISE.
- D. The certificate on the switch is self-signed not a CA-provided certificate.

Answer: B

NEW QUESTION 165

An engineer is configuring a posture policy for Windows 10 endpoints and wants to ensure that users in each AD group have different conditions to meet to be compliant. What must be done to accomplish this task?

- A. identify The users groups needed for different policies and create service conditions to map each one to its posture requirement
- B. Configure a simple condition for each AD group and use it in the posture policy for each use case
- C. Use the authorization policy within the policy set to group each AD group with their respective posture policy
- D. Change the posture requirements to use an AD group for each use case then use those requirements in the posture policy

Answer: C

NEW QUESTION 169

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 173

What are the minimum requirements for deploying the Automatic Failover feature on Administration nodes in a distributed Cisco ISE deployment?

- A. a primary and secondary PAN and a health check node for the Secondary PAN
- B. a primary and secondary PAN and no health check nodes
- C. a primary and secondary PAN and a pair of health check nodes
- D. a primary and secondary PAN and a health check node for the Primary PAN

Answer: D

NEW QUESTION 177

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 182

Which statement about configuring certificates for BYOD is true?

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

Answer: C

NEW QUESTION 184

Drag the steps to configure a Cisco ISE node as a primary administration node from the left into the correct order on the right.

Select the check box next to the current node, and then click Edit.	Step 1
Click Save.	Step 2
Choose Administration > System > Deployment.	Step 3
Click Make Primary.	Step 4

- 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 188

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

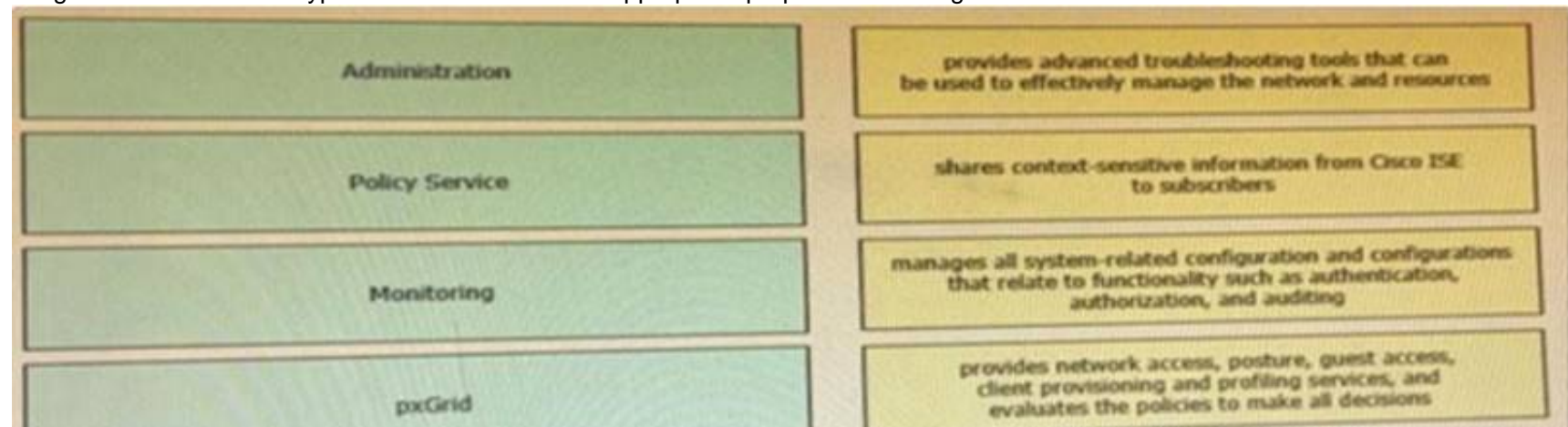
Answer: D

Explanation:

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

NEW QUESTION 190

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 195

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 199

An engineer is configuring a dedicated SSID for onboarding devices. Which SSID type accomplishes this configuration?

- A. dual
- B. hidden
- C. broadcast
- D. guest

Answer: A

Explanation:

<https://community.cisco.com/t5/security-documents/ise-byod-dual-vs-single-ssid-onboarding/ta-p/3641422>

https://www.youtube.com/watch?v=HH_Xasqd9k4&ab_channel=CiscoISE-IdentityServicesEngine

http://www.labminutes.com/sec0053_ise_1_1_byod_wireless_onboarding_dual_ssid

NEW QUESTION 204

What is a valid status of an endpoint attribute during the device registration process?

- A. block listed
- B. pending
- C. unknown
- D. DenyAccess

Answer: B

NEW QUESTION 205

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 206

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 300-715 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 300-715 Practice Test Here](#)