

Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)



NEW QUESTION 1

Select and Place

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:

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

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 2

When planning for the deployment of Cisco ISE, an organization's security policy dictates that they must use network access authentication via RADIUS. It also states that the deployment provide an adequate amount of security and visibility for the hosts on the network. Why should the engineer configure MAB in this situation?

- A. The Cisco switches only support MAB.
- B. MAB provides the strongest form of authentication available.
- C. The devices in the network do not have a supplicant.
- D. MAB provides user authentication.

Answer: C

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

An organization wants to enable web-based guest access for both employees and visitors. The goal is to use a single portal for both user types. Which two authentication methods should be used to meet this requirement? (Choose two.)

- A. LDAP
- B. 802.1X
- C. Certificate-based
- D. LOCAL
- E. MAC based

Answer: DE

NEW QUESTION 9

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 10

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 10

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

NEW QUESTION 12

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 14

A user is attempting to register a BYOD device to the Cisco ISE deployment, but needs to use the onboarding policy to request a digital certificate and provision the endpoint. What must be configured to accomplish this task?

- A. A native supplicant provisioning policy to redirect them to the BYOD portal for onboarding
- B. The Cisco AnyConnect provisioning policy to provision the endpoint for onboarding
- C. The BYOD flow to ensure that the endpoint will be provisioned prior to registering
- D. The posture provisioning policy to give the endpoint all necessary components prior to registering

Answer: A

NEW QUESTION 15

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 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 21

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 23

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

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 30

A security administrator is using Cisco ISE to create a BYOD onboarding solution for all employees who use personal devices on the corporate network. The administrator generates a Certificate Signing Request and signs the request using an external Certificate Authority server. Which certificate usage option must be selected when importing the certificate into ISE?

- A. RADIUS
- B. DLTS
- C. Portal
- D. Admin

Answer: C

NEW QUESTION 35

When creating a policy within Cisco ISE for network access control, the administrator wants to allow different access restrictions based upon the wireless SSID to which the device is connecting. Which policy condition must be used in order to accomplish this?

- A. Network Access NetworkDeviceName CONTAINS <SSID Name>
- B. DEVICE Device Type CONTAINS <SSID Name>
- C. Radius Called-Station-ID CONTAINS <SSID Name>
- D. Airespace Airespace-Wlan-Id CONTAINS <SSID Name>

Answer: C

Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115734-ise-policies-ssid-00.h>

NEW QUESTION 40

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 45

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 46

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 48

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 50

An engineer is configuring Cisco ISE for guest services They would like to have any unregistered guests redirected to the guest portal for authentication then have a CoA provide them with full access to the network that is segmented via firewalls Why is the given configuration failing to accomplish this goal?

- A. The Guest Flow condition is not in the line that gives access to the quest portal
- B. The Network_Access_Authentication_Passed condition will not work with guest services for portal access.
- C. The Permit Access result is not set to restricted access in its policy line
- D. The Guest Portal and Guest Access policy lines are in the wrong order

Answer: D

NEW QUESTION 51

A network administrator is configuring a secondary cisco ISE node from the backup configuration of the primary cisco ISE node to create a high availability pair The Cisco ISE CA certificates and keys must be manually backed up from the primary Cisco ISE and copied into the secondary Cisco ISE Which command must be issued for this to work?

- A. copy certificate lse
- B. application configure lse
- C. certificate configure lse
- D. Import certificate lse

Answer: B

Explanation:

<https://community.cisco.com/t5/network-access-control/ise-certificate-import-export/m-p/3847746>

NEW QUESTION 52

When configuring Active Directory groups, what does the Cisco ISE use to resolve ambiguous group names?

- A. MIB
- B. TGT
- C. OMAB
- D. SID

Answer: D

NEW QUESTION 54

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 57

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 62

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 67

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 70

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 75

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 78

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 80

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 83

An engineer is implementing network access control using Cisco ISE and needs to separate the traffic based on the network device ID and use the IOS device sensor capability. Which probe must be used to accomplish this task?

- A. HTTP probe
- B. NetFlow probe
- C. network scan probe
- D. RADIUS probe

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor> <http://www.network-node.com/blog/2016/1/2/ise-20-profiling>

NEW QUESTION 85

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 90

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 91

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 92

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 95

An administrator for a small network is configuring Cisco ISE to provide dynamic network access to users. Management needs Cisco ISE to not automatically trigger a CoA whenever a profile change is detected. Instead, the administrator needs to verify the new profile and manually trigger a CoA. What must be configuring in the profiler to accomplish this goal?

- A. Port Bounce
- B. No CoA
- C. Session Query
- D. Reauth

Answer: B

Explanation:

<https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-policies>

NEW QUESTION 97

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 99

An organization wants to improve their BYOD processes to have Cisco ISE issue certificates to the BYOD endpoints. Currently, they have an active certificate authority and do not want to replace it with Cisco ISE. What must be configured within Cisco ISE to accomplish this goal?

- A. Create a certificate signing request and have the root certificate authority sign it.
- B. Add the root certificate authority to the trust store and enable it for authentication.
- C. Create an SCEP profile to link Cisco ISE with the root certificate authority.
- D. Add an OCSP profile and configure the root certificate authority as secondary.

Answer: C

Explanation:

Ref:<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-pr>

NEW QUESTION 104

Refer to the exhibit.

Policy Name	Conditions	Results	Actions
IT Training	AND - NetworkSource: NetworkSource: Group: IT Training	IT_Training	
IT Admins	AND - NetworkSource: NetworkSource: Group: IT Admins	IT_Admin_Limit	
Network Engineering	AND - NetworkSource: NetworkSource: Group: Network Engineering	Net_Eng_Limit	
Finance	AND - NetworkSource: NetworkSource: Group: Finance	Fin_Limit	

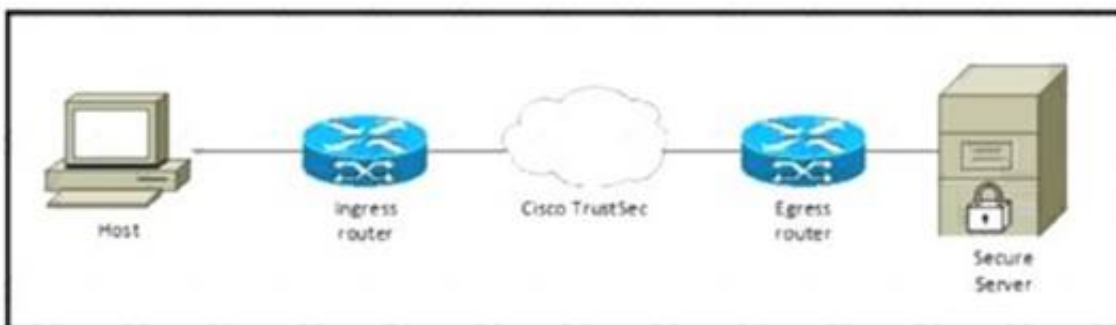
An organization recently implemented network device administration using Cisco ISE. Upon testing the ability to access all of the required devices, a user in the Cisco ISE group IT Admins is attempting to login to a device in their organization's finance department but is unable to. What is the problem?

- 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 105

Refer to the exhibit



Which component must be configured to apply the SGACL?

- A. egress router
- B. host
- C. secure server
- D. ingress router

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html#52796

NEW QUESTION 106

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 111

Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after toggling 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 113

What are two differences between the RADIUS and TACACS+ protocols'? (Choose two.)

- A. RADIUS is a Cisco proprietary protocol, whereas TACACS+ is an open standard protocol
- B. TACACS+ uses TCP port 49. whereas RADIUS uses UDP ports 1812 and 1813.
- C. RADIUS offers multiprotocol support, whereas TACACS+ does not
- D. RADIUS combines authentication and authorization, whereas TACACS+ does not
- E. RADIUS enables encryption of all the packets, whereas with TACACS+. only the password is encrypted.

Answer: BD

NEW QUESTION 114

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 117

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 122

An administrator wants to configure network device administration and is trying to decide whether to use TACACS* or RADIUS. A reliable protocol must be used that can check command authorization. Which protocol meets these requirements and why?

- A. TACACS+ because it runs over TCP
- B. RADIUS because it runs over UDP
- C. RADIUS because it runs over TCP.
- D. TACACS+ because it runs over UDP

Answer: A

NEW QUESTION 125

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 128

During BYOD flow, from where does a Microsoft Windows PC download the Network Setup Assistant?

- A. Cisco App Store
- B. Microsoft App Store
- C. Cisco ISE directly
- D. Native OTA functionality

Answer: C

NEW QUESTION 132

A network engineer is configuring guest access and notices that when a guest user registers a second device for access, the first device loses access. What must be done to ensure that both devices for a particular user are able to access the guest network simultaneously?

- A. Configure the sponsor group to increase the number of logins.
- B. Use a custom portal to increase the number of logins
- C. Modify the guest type to increase the number of maximum devices
- D. Create an Adaptive Network Control policy to increase the number of devices

Answer: C

Explanation:

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-7/admin_guide

NEW QUESTION 136

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 device 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 141

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 142

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 147

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	TACACS+	
encrypts the entire payload		
encrypts only the password field		
separates authentication and authorization	RADIUS	
primary use is device administration		
primary use is network access		

- 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 149

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 153

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 154

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 158

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 161

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 163

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 167

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 172

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 176

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 lor each use case then use those requirements in the posture policy

Answer: C

NEW QUESTION 180

.....

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](#)