

300-715 Dumps

Implementing and Configuring Cisco Identity Services Engine (SISE)

<https://www.certleader.com/300-715-dumps.html>



NEW QUESTION 1

Select and Place

Administration	provides advanced troubleshooting tools that can be used to effectively manage the network and resources
Policy Service	shares context sensitive information from Cisco ISE to subscenes
Monitoring	manages all system-related configuration and configurations that relate to functionality such as authentication, automation, and auditing
pxGrid	provides network access, posture, guest access, client provisioning and profiling services, and evaluates the policies to make all decisions

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Administration	Monitoring
Policy Service	pxGrid
Monitoring	Administration
pxGrid	Policy Service

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

An engineer is designing a new distributed deployment for Cisco ISE in the network and is considering failover options for the admin nodes. There is a need to ensure that an admin node is available for configuration of policies at all times. What is the requirement to enable this feature?

- A. one primary admin and one secondary admin node in the deployment
- B. one policy services node and one secondary admin node
- C. one policy services node and one monitoring and troubleshooting node
- D. one primary admin node and one monitoring and troubleshooting node

Answer: A

NEW QUESTION 8

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 9

An administrator is configuring a new profiling policy within Cisco ISE The organization has several endpoints that are the same device type and all have the same Block ID in their MAC address. The profiler does not currently have a profiling policy created to categorize these endpoints. therefore a custom profiling policy must be created Which condition must the administrator use in order to properly profile an ACME AI Connector endpoint for network access with MAC address <MAC ADDRESS>?

- A. MAC_OUI_STARTSWITH_<MACADDRESS>
- B. CDP_cdpCacheDeviceID_CONTAINS_<MACADDRESS>
- C. MAC_MACAddress_CONTAINS_<MACADDRESS>
- D. Radius Called Station-ID STARTSWITH <MACADDRESS>

Answer: D

NEW QUESTION 10

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 10

What is the minimum certainty factor when creating a profiler policy?

- A. the minimum number that a predefined condition provides
- B. the maximum number that a predefined condition provides
- C. the minimum number that a device certainty factor must reach to become a member of the profile
- D. the maximum number that a device certainty factor must reach to become a member of the profile

Answer: C

NEW QUESTION 15

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 19

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 24

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 29

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

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

Answer: AD

NEW QUESTION 30

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 32

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 34

An engineer is using Cisco ISE and configuring guest services to allow wireless devices to access the network. Which action should accomplish this task?

- A. Create the redirect ACL on the WLC and add it to the WLC policy
- B. Create the redirect ACL on the WLC and add it to the Cisco ISE policy.
- C. Create the redirect ACL on Cisco ISE and add it to the WLC policy
- D. Create the redirect ACL on Cisco ISE and add it to the Cisco ISE Policy

Answer: B

NEW QUESTION 36

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 39

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 41

Which Cisco ISE service allows an engineer to check the compliance of endpoints before connecting to the network?

- A. personas
- B. qualys
- C. nexpose
- D. posture

Answer: D

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 Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a 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 50

Which two fields are available when creating an endpoint on the context visibility page of Cisco IS? (Choose two)

- A. Policy Assignment
- B. Endpoint Family
- C. Identity Group Assignment
- D. Security Group Tag
- E. IP Address

Answer: AC

NEW QUESTION 53

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 55

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 60

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 65

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 66

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 71

What service can be enabled on the Cisco ISE node to identify the types of devices connecting to a network?

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

Answer: B

NEW QUESTION 76

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 81

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 85

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 88

An engineer is configuring Cisco ISE policies to support MAB for devices that do not have 802.1X capabilities. The engineer is configuring new endpoint identity groups as conditions to be used in the AuthZ policies, but noticed that the endpoints are not hitting the correct policies. What must be done in order to get the devices into the right policies?

- A. Manually add the MAC addresses of the devices to endpoint ID groups in the context visibility database.
- B. Create an AuthZ policy to identify Unknown devices and provide partial network access prior to profiling.
- C. Add an identity policy to dynamically add the IP address of the devices to their endpoint identity groups.
- D. Identify the non 802.1X supported device types and create custom profiles for them to profile into.

Answer: D

NEW QUESTION 89

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 90

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 95

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 96

Which two features must be used on Cisco ISE to enable the TACACS. feature? (Choose two)

- A. Device Administration License
- B. Server Sequence
- C. Command Sets
- D. Enable Device Admin Service
- E. External TACACS Servers

Answer: AD

NEW QUESTION 98

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 102

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 103

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 104

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 109

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 111

Which portal is used to customize the settings for a user to log in and download the compliance module?

- A. Client Profiling
- B. Client Endpoint
- C. Client Provisioning
- D. Client Guest

Answer: C

NEW QUESTION 112

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 113

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 118

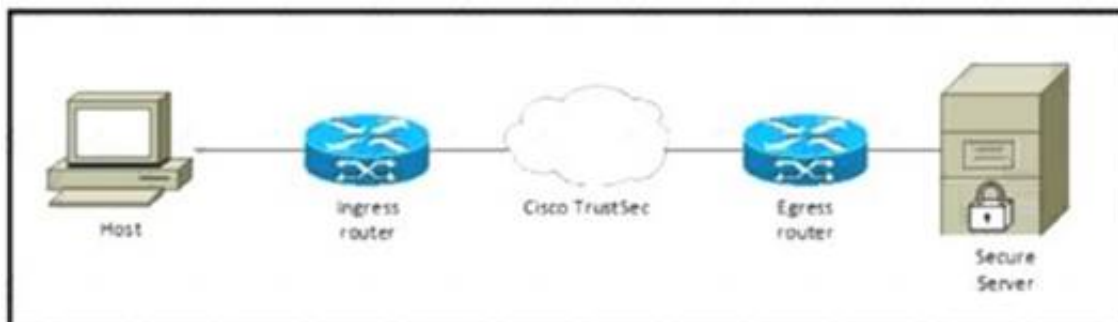
An engineer is configuring 802.1X and is testing out their policy sets. After authentication, some endpoints are given an access-reject message but are still allowed onto the network. What is causing this issue to occur?

- 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 121

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 123

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 125

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 127

What are two requirements of generating a single signing in Cisco ISE by using a certificate provisioning portal, without generating a certificate request? (Choose two)

- A. Location the CSV file for the device MAC
- B. Select the certificate template
- C. Choose the hashing method
- D. Enter the common name
- E. Enter the IP address of the device

Answer: BD

Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provi>

NEW QUESTION 128

Which personas can a Cisco ISE node assume'?

- A. policy service, gatekeeping, and monitoring
- B. administration, policy service, and monitoring
- C. administration, policy service, gatekeeping
- D. administration, monitoring, and gatekeeping

Answer: B

Explanation:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_dis_deploy.html

The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. The menu options that are available through the administrative user interface are dependent on the role and personas that an ISE node assumes. See Cisco ISE Nodes and Available Menu Options for more information.

NEW QUESTION 131

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 134

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 139

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 140

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 141

What happens when an internal user is configured with an external identity store for authentication, but an engineer uses the Cisco ISE admin portal to select an internal identity store as the identity source?

- A. Authentication is redirected to the internal identity source.
- B. Authentication is redirected to the external identity source.
- C. Authentication is granted.
- D. Authentication fails.

Answer: D

NEW QUESTION 143

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 145

MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gain access to the network Which alternate method should be used to tell users how to remediate?

- A. URL link
- B. message text
- C. executable
- D. file distribution

Answer: A

Explanation:

<https://www.sciencedirect.com/topics/computer-science/remediation-action>

NEW QUESTION 148

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 151

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 152

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 156

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 160

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 164

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 168

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 173

What is a difference between TACACS+ and RADIUS in regards to encryption?

- A. TACACS+ encrypts only the password, whereas RADIUS encrypts the username and password.
- B. TACACS+ encrypts the username and password, whereas RADIUS encrypts only the password.
- C. TACACS+ encrypts the password, whereas RADIUS sends the entire packet in clear text.
- D. TACACS+ encrypts the entire packet, whereas RADIUS encrypts only the password.

Answer: D

NEW QUESTION 178

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 180

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 185

What is a method for transporting security group tags throughout the network?

- A. by enabling 802.1AE on every network device
- B. by the Security Group Tag Exchange Protocol
- C. by embedding the security group tag in the IP header
- D. by embedding the security group tag in the 802.1Q header

Answer: B

NEW QUESTION 186

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 188

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 189

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 191

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 194

An administrator is configuring Cisco ISE to authenticate users logging into network devices using TACACS+. The administrator is not seeing any of 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 195

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 196

Which two features should be used on Cisco ISE to enable the TACACS+ feature? (Choose two)

- A. External TACACS Servers
- B. Device Admin Service
- C. Device Administration License
- D. Server Sequence
- E. Command Sets

Answer: BC

NEW QUESTION 201

An administrator replaced a PSN in the distributed Cisco ISE environment. When endpoints authenticate to it, the devices are not getting the right profiles or attributes and as a result, are not hitting the correct policies. This was working correctly on the previous PSN. Which action must be taken to ensure the endpoints get identified?

- A. Verify that the MnT node is tracking the session.
- B. Verify the shared secret used between the switch and the PSN.
- C. Verify that the profiling service is running on the new PSN.
- D. Verify that the authentication request the PSN is receiving is not malformed.

Answer: C

NEW QUESTION 206

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 210

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 radius

Answer: A

NEW QUESTION 211

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 endpoints on the network. Which node should be used to accomplish this task?

- A. PSN
- B. primary PAN
- C. pxGrid
- D. MnT

Answer: A

NEW QUESTION 216

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 220

A policy is being created in order to provide device administration access to the switches on a network. There is a requirement to ensure that if the session is not actively being used, after 10 minutes, it will be disconnected. Which task must be configured in order to meet this requirement?

- A. session timeout
- B. idle time
- C. monitor
- D. set attribute as

Answer: A

Explanation:

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

NEW QUESTION 222

Which use case validates a change of authorization?

- A. An authenticated, wired EAP-capable endpoint is discovered
- B. An endpoint profiling policy is changed for authorization policy.
- C. An endpoint that is disconnected from the network is discovered
- D. Endpoints are created through device registration for the guests

Answer: B

Explanation:

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

NEW QUESTION 224

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 227

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-715 Exam with Our Prep Materials Via below:

<https://www.certleader.com/300-715-dumps.html>