Cisco.300-715.v2023-03-03.q81

Exam Code:	300-715
Exam Name:	Implementing and Configuring Cisco Identity Services Engine
Certification Provider:	Cisco
Free Question Number:	81
Version:	v2023-03-03
# of views:	1869
# of Questions views:	810
https://www.exam-tests.com/300-715-exam/Cisco.300-715.v2023-03-03.q81.html	

NEW QUESTION: 1
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. RBAC
D. VLAN
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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. Use the ip access-group webauth in command.
C. Set the NAC State option to RADIUS NAC.
D. Use the radius-server vsa send authentication command.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
A network engineer is configuring Cisco TrustSec and needs to ensure that the Security Group Tag is being transmitted between two devices Where in the Layer 2 frame should this be verified?
A. CMD filed
B. 802.1Q filed
C. Payload
D. 802.1 AE header
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs/policy_defined_segmentation_with_trustsec_rob_bleeker.pdf (slide 25)

NEW QUESTION: 4
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: B,D (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010.html

NEW QUESTION: 5
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 Sponsor Portal and suspend the guest accounts.
C. Navigate to the Guest Portal and delete the guest accounts.
D. Create an authorization rule denying guest access.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
Refer to the exhibit:

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

Switch(config)# authentication port-control auto

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

Refer to the exhibit. 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: (SHOW ANSWER)
https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari#:~:text=Multi%2Dauthentication%20host%20mode%3A%20You,allows%20multiple%20source%20MAC%20addresses.

NEW QUESTION: 7

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: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/configure-posture.html

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_client_provisioning.html#task_D1C2E8ECE1D54D259C01BCBF0A5822F1

NEW QUESTION: 8

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 IP address in the correct Endpoint Identity Group.

B. Enter the MAC address in the correct Endpoint Identity Group.

C. Enter the MAC address in the correct Logical Profile.

D. Enter the IP address in the correct Logical Profile.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

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. TCP port 514

B. UDP port 79

C. UDP port 16666

D. UDP port 1812 RADIUS

E. TCP port 161

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 10

What is a function of client provisioning?

A. Client provisioning ensures that endpoints receive the appropriate posture agents.

B. Client provisioning checks a dictionary attribute with a value.

C. Client provisioning ensures an application process is running on the endpoint.

D. Client provisioning checks the existence, date, and versions of the file on a client.

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html#:~:text=After%20Cisco%20ISE%20classifies%20a,packages%20and%20profiles%2C%20if%20necessary.

NEW QUESTION: 11

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

A. In closed mode, profiling does not work unless CDP is enabled.

B. The default profiler configuration is set to No CoA for the reauthentication setting

C. The profiler feed is not downloading new information so the profiler is inactive

D. The profiling probes are not able to collect enough information to change the device profile

Answer: B (LEAVE A REPLY)

NEW QUESTION: 12

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. Ensure that the NAT address is properly configured

B. Provide domain administrator access to Active Directory.

C. Enable IPC access over port 80.

D. Configure a secure LDAP connection.

E. Establish access to one Global Catalog server.

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 13

In which two ways can users and endpoints be classified for TrustSec?

(Choose Two.)

A. QoS

B. SXP

C. VLAN

D. dynamic

E. SGACL

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 14

Which profiling probe collects the user-agent string?

A. HTTP

B. DHCP

C. AD

D. NMAP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

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

A. Device Admin Service

B. Device Administration License

C. Command Sets
D. External TACACS Servers
E. Server Sequence
Answer: (SHOW ANSWER)

NEW QUESTION: 16
A network administrator notices that after a company-wide shut down, many users cannot connect their laptops to the corporate SSID. What must be done to permit access in a timely manner?
A. Connect this system as a guest user and then redirect the web auth protocol to log in to the network.
B. Authenticate the user's system to the secondary Cisco ISE node and move this user to the primary with the renewed certificate.
C. Add a certificate issue from the CA server, revoke the expired certificate, and add the new certificate in system.
D. Allow authentication for expired certificates within the EAP-TLS section under the allowed protocols.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gam 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: (SHOW ANSWER)
https://www.sciencedirect.com/topics/computer-science/remediation-action

NEW QUESTION: 18
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: (SHOW ANSWER)
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: 19
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 (LEAVE A REPLY)
Ref:https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html

NEW QUESTION: 20
Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)
A. endpoint profile transition from Unknown to Windows 10-Workstation
B. endpoint marked as lost in My Devices Portal
C. endpoint profile transition from Apple-Device to Apple-iPhone
D. updating of endpoint dACL.
E. addition of endpoint to My Devices Portal
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 21
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. administration
C. authentication
D. policy service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
An administrator is trying to collect metadata information about the traffic going across the network to gam added visibility into the hosts. This Information will be used to create profiling policies for devices us mg Cisco ISE so that network access policies can be used What must be done to accomplish this task?
A. Configure the RADIUS profiling probe within Cisco ISE
B. Configure the DHCP probe within Cisco ISE
C. Configure NetFlow to be sent to me Cisco ISE appliance.
D. Configure SNMP to be used with the Cisco ISE appliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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. Identify the non 802.1 * supported device types and create custom profiles for them to profile into.

B. Manually add the MAC addresses of the devices to endpoint ID groups in the context visibility database.
C. Add an identity policy to dynamically add the IP address of the devices to their endpoint identity groups.
D. Create an AuthZ policy to identify Unknown devices and provide partial network access prior to profiling.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
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. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning
D. Scanning must be initiated from the MnT node to centrally gather the information
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
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 MnT node to centrally gather the information
B. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning
C. Scanning must be initiated from the PSN that last authenticated the endpoint
D. Cisco ISE must learn the IP-MAC binding of unknown endpoints via DHCP profiling, not via scanning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
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: B (LEAVE A REPLY)

NEW QUESTION: 27
What does a fully distributed Cisco ISE deployment include?
A. PAN and PSN on the same node while MnTs are on their own dedicated nodes.
B. PAN and MnT on the same node while PSNs are on their own dedicated nodes.
C. All Cisco ISE personas on their own dedicated nodes.
D. All Cisco ISE personas are sharing the same node.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html

NEW QUESTION: 28
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html 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: 29
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. aaa group server radius proxy
B. aaa group server radius
C. ip http port <port number>
D. permit tcp any any eq <port number>
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
A company is attempting to improve their BYOD policies and restrict access based on certain criteri a. The company's subnets are organized by building. Which attribute should be used in order to gain access based on location?
A. static group assignment

B. IP address
C. device registration status
D. MAC address
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html#ID1353

NEW QUESTION: 31
Which supplicant(s) and server(s) are capable of supporting EAP-CHAINING?
A. Cisco AnyConnect NAM and Cisco Identity Service Engine
B. Cisco Secure Services Client and Cisco Access Control Server
C. Cisco AnyConnect NAM and Cisco Access Control Server
D. Windows Native Supplicant and Cisco Identity Service Engine
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
An administrator connects an HP printer to a dot1x enable port, but the printer in not accessible Which feature must the administrator enable to access the printer?
A. MAC authentication bypass
B. change of authorization
C. TACACS authentication
D. RADIUS authentication
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/network-access-control/ise-for-printer-security/m-p/3933216

NEW QUESTION: 33
Which two values are compared by the binary comparison (unction in authentication that is based on Active Directory?
A. subject alternative name and the common name
B. MS-CHAPv2 provided machine credentials and credentials stored in Active Directory
C. user-presented password hash and a hash stored in Active Directory
D. user-presented certificate and a certificate stored in Active Directory
Answer: A (LEAVE A REPLY)
Basic certificate checking does not require an identity source. If you want binary comparison checking for the certificates, you must select an identity source. If you select Active Directory as an identity source, subject and common name and subject alternative name (all values) can be used to look up a user.
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/ b_ise_admin_guide_sample_chapter_01110.html

NEW QUESTION: 34

An administrator is troubleshooting an endpoint that is supposed to bypass 802 1X and use MAB. The endpoint is bypassing 802.1X and successfully getting network access using MAB. however the endpoint cannot communicate because it cannot obtain an IP address. What is the problem?

A. The 802.1 X timeout period is too long.

B. An AC I on the port is blocking HTTP traffic

C. The DHCP probe for Cisco ISE is not working as expected.

D. The endpoint is using the wrong protocol to authenticate with Cisco ISE.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 35

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: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/admin_guide/b_ise_admin_guide_23/b_ise_admin_guide_23_chapter_010111.html

NEW QUESTION: 36

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

A. Create a Cisco ISE machine account in the domain if the machine account does not already exist

B. Remove the Cisco ISE machine account from the domain.

C. Set attributes on the Cisco ISE machine account

D. Search Active Directory to see if a Cisco ISE machine account already ex.sts.

Answer: D (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html

NEW QUESTION: 37

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 node and one monitoring and troubleshooting node

B. one policy services node and one monitoring and troubleshooting node

C. one policy services node and one secondary admin node

D. one primary admin and one secondary admin node in the deployment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 38

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

A. Create a service posture condition using a non-OPSWAT API version.

B. Create a registry posture condition using a non-OPSWAT API version.

C. Create a compound posture condition using a OPSWAT API version.
D. Create an application posture condition using a OPSWAT API version.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
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 (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_admin_accesspolicy_settings.html#reference_0E24B8FBFAB248219E1194435670347F

NEW QUESTION: 40
Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)
A. The device queries the Cisco ISE authorization server
B. The device queries the external identity store
C. The Cisco ISE server queries the internal identity store
D. The Cisco ISE server queries the external identity store.
E. The device queries the internal identity store
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 41
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. authentication open
B. authentication port-control auto
C. dotlx pae authenticator
D. dotlxsystem-auth-control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Which interface-level command is needed to turn on 802 1X authentication?
A. Dofl1x pae authenticator
B. authentication host-mode single-host
C. dot1x system-auth-control
D. aaa server radius dynamic-author
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
Which three default endpoint identity groups does cisco ISE create? (Choose three)

A. Unknown
B. whitelist
C. end point
D. profiled
E. blacklist
Answer: (SHOW ANSWER)
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_24_new_chapter_010101.html#ID1678

NEW QUESTION: 44
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. pxGrid
C. monitoring
D. primary policy administrator
Answer: (SHOW ANSWER)

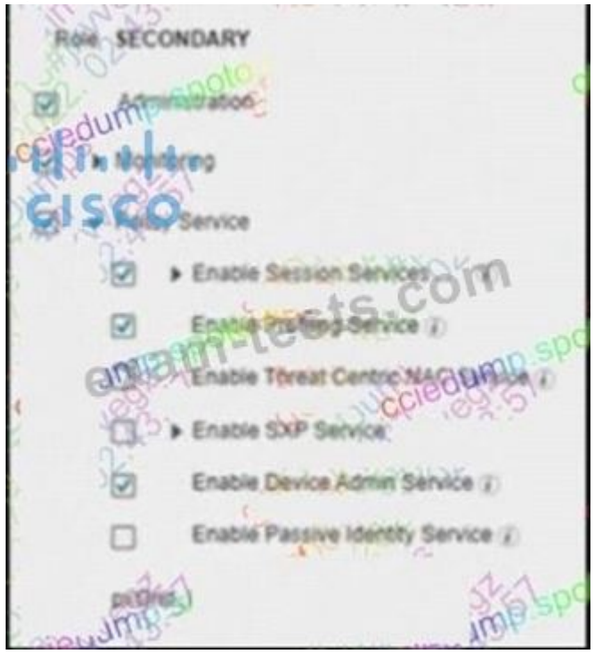
NEW QUESTION: 45
Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after togging into the device with this command set authorization
Which configuration is causing this issue?
A. The command set is allowing all commands that are not in the command list
B. The command set is working like an ACL and denying every command.
C. Question marks are not allowed as wildcards for command sets.
D. The wildcard command listed is in the wrong format
Answer: (SHOW ANSWER)

NEW QUESTION: 46
What is a method for transporting security group tags throughout the network?
A. by enabling 802.1AE on every network device
B. by embedding the security group tag in the IP header
C. by embedding the security group tag in the 802.1Q header
D. by the Security Group Tag Exchange Protocol
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47

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

A)



B)


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

C)


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

D)

A. Option A
B. Option D
C. Option C
D. Option B
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
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 uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.
C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.
D. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
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 (LEAVE A REPLY)
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: 50

An administrator is trying to collect metadata information about the traffic going across the network to gam added visibility into the hosts. This Information will be used to create profiling policies for devices us mg Cisco ISE so that network access policies can be used What must be done to accomplish this task?

A. Configure the DHCP probe within Cisco ISE

B. Configure the RADIUS profiling probe within Cisco ISE

C. Configure SNMP to be used with the Cisco ISE appliance

D. Configure NetFlow to be sent to me Cisco ISE appliance.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 51

Which statement about configuring certificates for BYOD is true?

A. The CN field is populated with the endpoint host name

B. An endpoint certificate is mandatory for the Cisco ISE BYOD

C. An Android endpoint uses EST, whereas other operating systems use SCEP for enrollment

D. The SAN field is populated with the end user name.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 52

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 Cisco ISE and add it to the Cisco ISE Policy

B. Create the redirect ACL on the WLC and add it to the Cisco ISE policy.

C. Create the redirect ACL on the WLC and add it to the WLC policy

D. Create the redirect ACL on Cisco ISE and add it to the WLC policy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

What is a valid guest portal type?

A. Sponsor

B. My Devices

C. Captive-Guest

D. Sponsored-Guest

Answer: D (LEAVE A REPLY)

NEW QUESTION: 54

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

A. Firepower

B. WLC

C. IOS

D. ASA

E. Shell

Answer: B,E (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100010.html TACACS+ Profile TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:
Common tasks
Custom attributes
There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)-Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.
The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:
Shell
WLC
Nexus
Generic
The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using a equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

NEW QUESTION: 55
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: (SHOW ANSWER)
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-policies

NEW QUESTION: 56
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. Add VLAN 310 in the common tasks of the authorization profile
C. Ensure that the endpoint is using The correct policy set
D. Ensure that the security group is not preventing the endpoint from being in VLAN 310
Answer: (SHOW ANSWER)

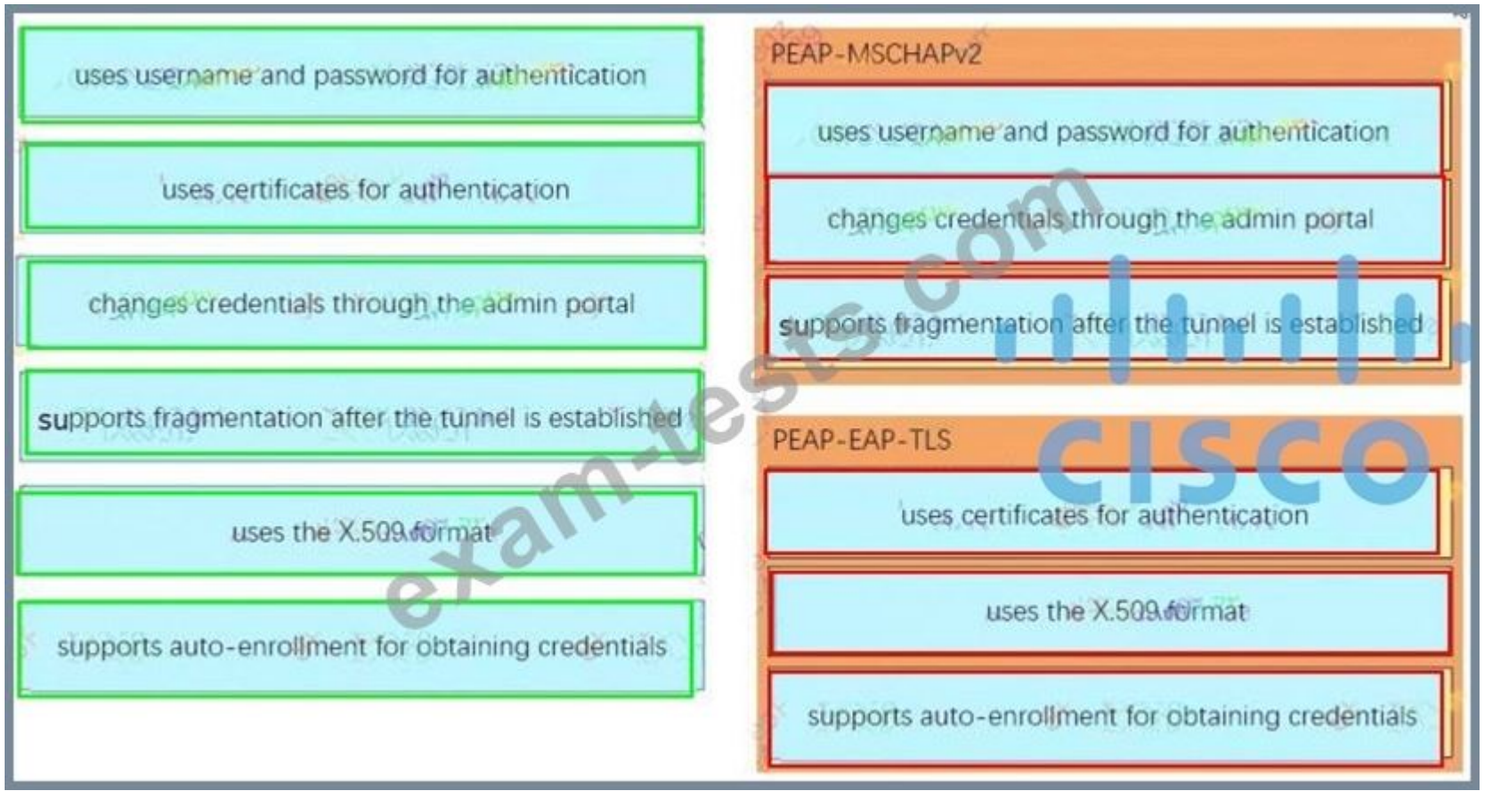
NEW QUESTION: 57
A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for one day When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the 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 (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_01101.html#:~:text=Cisco%20ISE%2C%20by%20default%2C%20deletes,5000%20endpoints%20every%20three%20minutes.

NEW QUESTION: 58
Which two ports must be open between Cisco ISE and the client when you configure posture on Cisco ISE? (Choose two).
A. TCP 443
B. TCP 80
C. TCP 8905
D. TCP 8906
E. TCP 8443
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 59
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 fails.
B. Authentication is redirected to the internal identity source.
C. Authentication is granted.
D. Authentication is redirected to the external identity source.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
Select and Place

Answer:



NEW QUESTION: 61

While configuring Cisco TrustSec on Cisco IOS devices the engineer must set the CTS device ID and password in order for the devices to authenticate with each other. However after this is complete the devices are not able to property authenticate What issue would cause this to happen even if the device ID and passwords are correct?

A. The devices are missing the configuration cts credentials trustsec verify 1

B. The 5GT mappings have not been defined

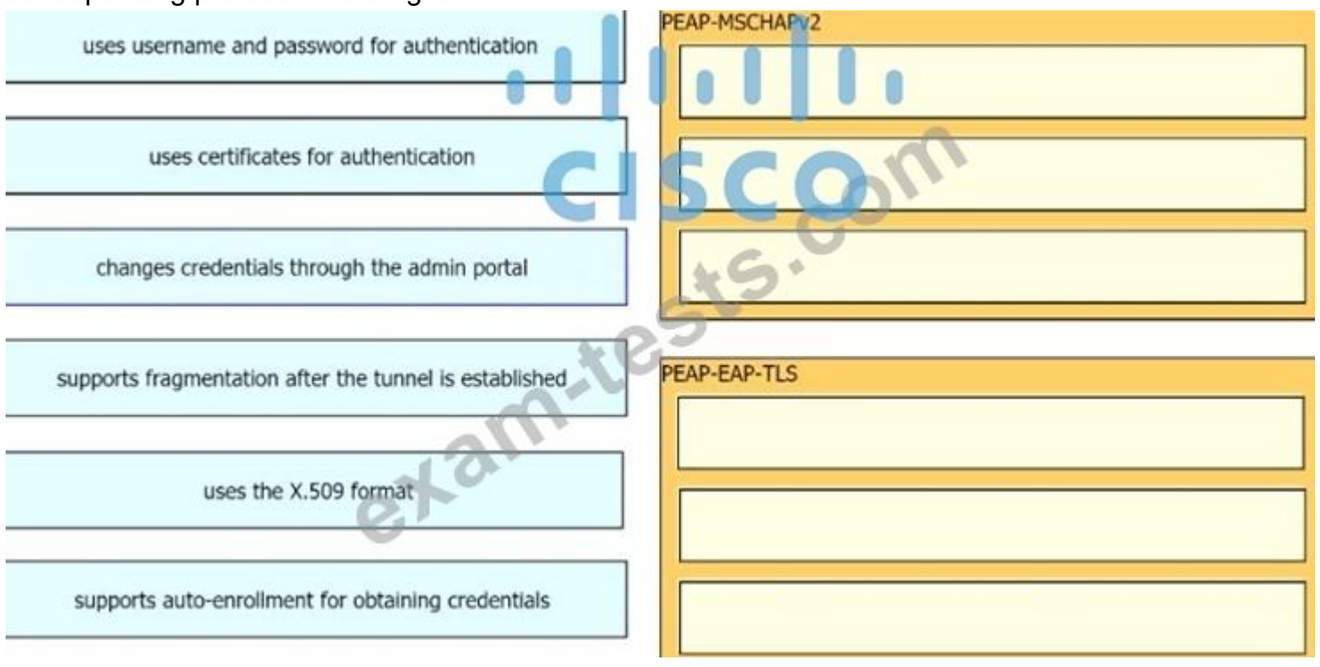
C. The device aliases are not matching

D. EAP-FAST is not enabled

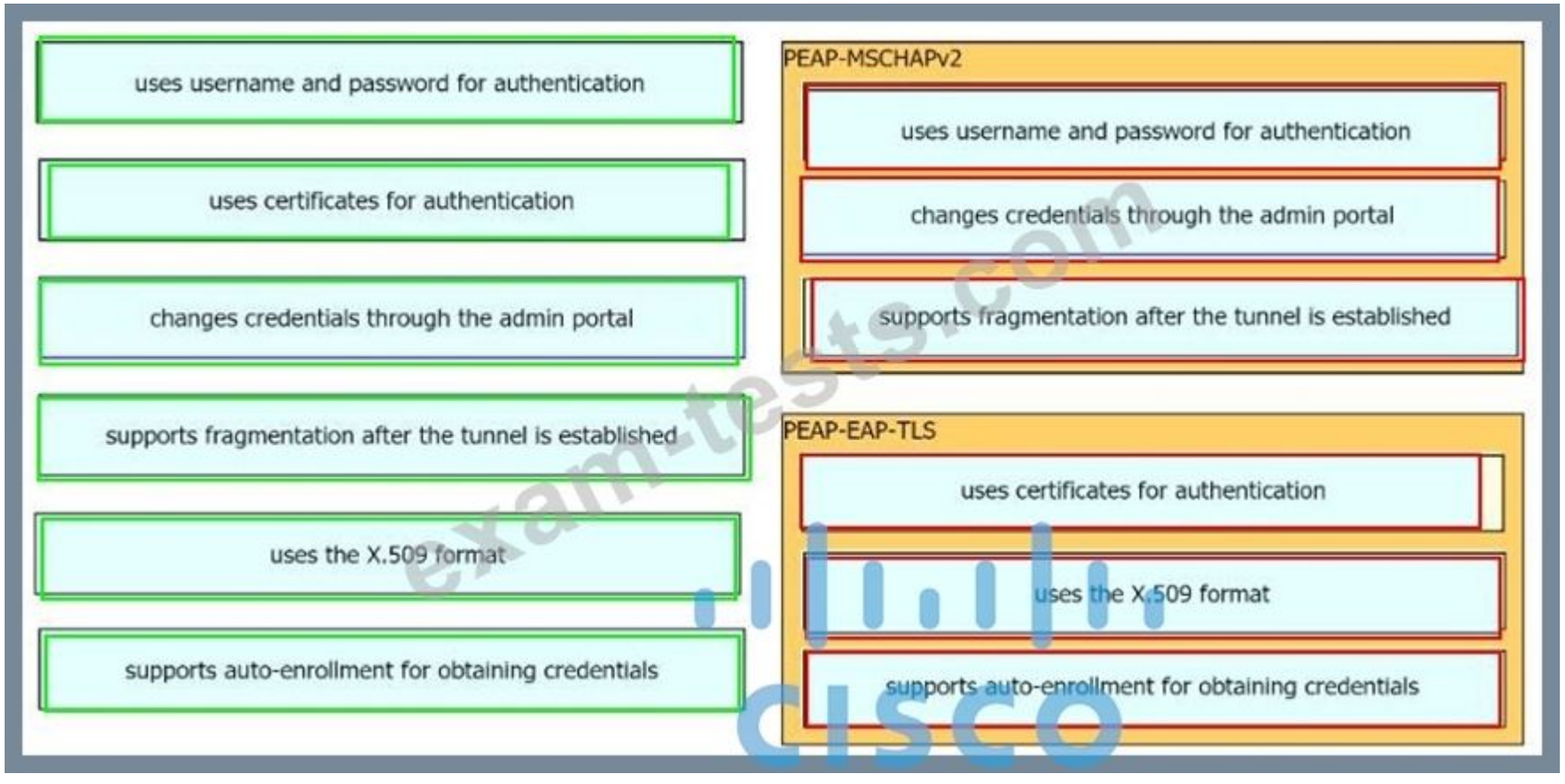
Answer: (SHOW ANSWER)

NEW QUESTION: 62

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.



Answer:



NEW QUESTION: 63
An organization is implementing Cisco ISE posture services and must ensure that a host-based firewall is in place on every Windows and Mac computer that attempts to access the network They have multiple vendors' firewall applications for their devices, so the engineers creating the policies are unable to use a specific application check in order to validate the posture for this What should be done to enable this type of posture check?
A. Use the file registry condition to ensure that the firewal is installed and running appropriately.
B. Use a compound condition to look for the Windows or Mac native firewall applications.
C. Enable the default firewall condition to check for any vendor firewall application.
D. Enable the default application condition to identify the applications installed and validade the firewall app.
Answer: (SHOW ANSWER)
https://www.youtube.com/watch?v=6Kj8P8Hn7dY&t=109s&ab_channel=CiscoISE-IdentityServicesEngine

NEW QUESTION: 64
Which two features must be used on Cisco ISE to enable the TACACS. feature? (Choose two)
A. Enable Device Admin Service
B. Command Sets
C. Device Administration License
D. Server Sequence
E. External TACACS Servers
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 65

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 (LEAVE A REPLY)

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html

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

NEW QUESTION: 66

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 (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/dot1x.html

NEW QUESTION: 67

An engineer deploys Cisco ISE and must configure Active Directory to then use information from Active Directory in an authorization policy. Which two components must be configured, in addition to Active Directory groups, to achieve this goat? (Choose two)

A. Active Directory External Identity Sources

B. Library Condition for External Identity. External Groups

C. Identity Source Sequences

D. LDAP External Identity Sources

Answer: A,B (LEAVE A REPLY)

E Library Condition for Identity Group: User Identity Group

NEW QUESTION: 68

Refer to the exhibit.

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 Portal and Guest Access policy lines are in the wrong order

B. The Guest Flow condition is not in the line that gives access to the quest portal

C. The Network_Access_Authentication_Passed condition will not work with guest services for portal access.

D. The Permit Access result is not set to restricted access in its policy line

Answer: A (LEAVE A REPLY)

NEW QUESTION: 69

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

A. Client Provisioning
B. Client Endpoint
C. Client Profiling
D. Client Guest
Answer: (SHOW ANSWER)

NEW QUESTION: 70
A network engineer is configuring a network device that needs to filter traffic based on security group tags using a security policy on a routed into this task?
A. cts role-based policy priority-static
B. cts role-based enforcement
C. cts cache enable
D. cts authorization list
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
What is needed to configure wireless guest access on the network?
A. valid user account in Active Directory
B. Captive Portal Bypass turned on
C. WEBAUTH ACL for redirection
D. endpoint already profiled in ISE
Answer: (SHOW ANSWER)

NEW QUESTION: 72
An engineer is designing a BYOD environment utilizing Cisco ISE for devices that do not support native supplicants Which portal must the security engineer configure to accomplish this task?
A. MDM
B. Client provisioning
C. My devices
D. BYOD
Answer: C (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01111.html

NEW QUESTION: 73
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 (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.html#90273 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: 74
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 (LEAVE A REPLY)
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: 75
Which two fields are available when creating an endpoint on the context visibility page of Cisco IS? (Choose two)
A. Security Group Tag
B. IP Address
C. Policy Assignment
D. Endpoint Family
E. Identity Group Assignment
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 76
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+ encrypts the entire payload being sent while RADIUS only encrypts the password.
B. TACACS+ uses secure EAP-TLS while RADIUS does not.
C. TACACS+ is FIPS compliant while RADIUS is not
D. TACACS+ is designed for network access control while RADIUS is designed for role-based access.
E. TACACS+ provides the ability to authorize specific commands while RADIUS does not
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 77
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 (LEAVE A REPLY)
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: 78
What are two components of the posture requirement when configuring Cisco ISE posture? (Choose two)
A. updates
B. access policy
C. conditions
D. Client Provisioning portal
E. remediation actions
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 79
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010110.html 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: 80
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. Configure a simple condition for each AD group and use it in the posture policy for each use case
B. identify The users groups needed for different policies and create service conditions to map each one to its posture requirement
C. Change the posture requirements to use an AD group lor each use case then use those requirements in the posture policy

D. Use the authorization policy within the policy set to group each AD group with their respective posture policy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 81

Refer to the exhibit:

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

Refer to the exhibit 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 (LEAVE A REPLY)

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