Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
An engineer is migrating users from MAB to 802.1X on the network. This must be done during normal business hours with minimal impact to users. Which CoA method should be used?

A. Port Bounce
B. Port Shutdown
C. Session Termination
D. Session Reauthentication

Answer: D

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

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

Answer: A

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

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

Answer: B

NEW QUESTION 4
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: A

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

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

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

Answer: A

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

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

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

Answer: B

NEW QUESTION 7
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 authorization list
B. cts role-based enforcement
C. cts cache enable
D. cts role-based policy priority-static

Answer: B

NEW QUESTION 8
An administrator is configuring the Native Supplicant Profile to be used with the Cisco ISE posture agents and needs to test the connection using wired devices to determine which profile settings are available. Which two configuration settings should be used to accomplish this task? (Choose two.)

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

Answer: CE

NEW QUESTION 9
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 10
Which term refers to an endpoint agent that tries to join an 802 1X-enabled network?

A. EAP server
B. supplicant
C. client
D. authenticator

Answer: B

Explanation:
https://www.oreilly.com/library/view/cisco-ise-for/9780133103632/ch16.html#:~:text=What%20is%20a%
&text=The%20802.1X%20transactions%20are,Identity%20Services%20Engine%20(ISE).

NEW QUESTION 10
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 15
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 19
During a 802 1X deployment, an engineer must identify failed authentications without causing problems for the connected endpoint. Which command will successfully achieve this''

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

Answer: C

NEW QUESTION 23
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 25
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 27
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 32
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
What are two differences of TACACS+ compared to RADIUS? (Choose two.)

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

Answer: BD

NEW QUESTION 38
An organization wants to split their Cisco ISE deployment to separate the device administration functionalities from the mam deployment. For this to work, the administrator must deregister any nodes that will become a part of the new deployment, but the button for this option is grayed out Which configuration is causing this behavior?

A. One of the nodes is an active PSN.
B. One of the nodes is the Primary PAN
C. All of the nodes participate in the PAN auto failover.
D. All of the nodes are actively being synched.

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide/b_ISE_admin_27_

NEW QUESTION 40
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 44
What are two components of the posture requirement when configuring Cisco ISE posture? (Choose two)

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

Answer: BD

NEW QUESTION 48
Which two ports must be open between Cisco ISE and the client when you configure posture on Cisco ISE? (Choose two).

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

Answer: AE

NEW QUESTION 51
Which Cisco ISE deployment model is recommended for an enterprise that has over 50,000 concurrent active endpoints?

A. large deployment with fully distributed nodes running all personas
B. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with shared PSNs
C. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with dedicated PSNs
D. small deployment with one primary and one secondary node running all personas

Answer: C

NEW QUESTION 56
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 57
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 61
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 62
An administrator is configuring sponsored guest access using Cisco ISE Access must be restricted to the sponsor portal to ensure that only necessary employees can issue sponsored accounts and employees must be classified to do so What must be done to accomplish this task?

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

Answer: C

NEW QUESTION 65
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 68
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
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 75
An ISE administrator must change the inactivity timer for MAB endpoints to terminate the authentication session whenever a switch port that is connected to an IP phone does not detect packets from the device for 30 minutes. Which action must be taken to accomplish this task?

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

Answer: B

NEW QUESTION 80
A network engineer must enforce access control using special tags, without re-engineering the network design. Which feature should be configured to achieve this in a scalable manner?

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

Answer: A

NEW QUESTION 81
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 most

be issued for this to work?

A. copy certificate Ise
B. application configure Ise
C. certificate configure Ise
D. Import certificate Ise

Answer: B

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

NEW QUESTION 86
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 89
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 93
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 97
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 102
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 104
An engineer tests Cisco ISE posture services on the network and must configure the compliance module to automatically download and install on endpoints Which action accomplishes this task for VPN users?

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

Answer: A

NEW QUESTION 106
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 110
An administrator made changes in Cisco ISE and needs to apply new permissions for endpoints that have already been authenticated by sending a CoA packet to the network devices. Which IOS command must be configured on the devices to accomplish this goal?

A. aaa server radius dynamic-author
B. authentication command bounce-port
C. authentication command disable-port
D. aaa nas port extended

Answer: A

NEW QUESTION 112
An administrator needs to allow guest devices to connect to a private network without requiring usernames and passwords. Which two features must be configured to allow for this? (Choose two.)

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

Answer: AB

NEW QUESTION 113
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 117
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 119
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 124
Drag and drop the configuration steps from the left into the sequence on the right to install two Cisco ISE nodes in a distributed deployment.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 128
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
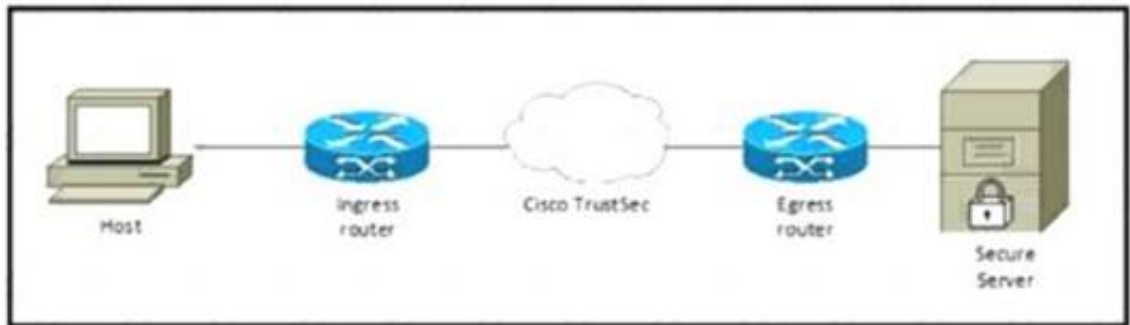D. Client Guest

Answer: C

NEW QUESTION 130
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 132
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 137
Which two actions must be verified to confirm that the internet is accessible via guest access when configuring a guest portal? (Choose two.)

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

Answer: BE

NEW QUESTION 142
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 146
Refer to the exhibit.
Which two configurations are needed on a catalyst switch for it to be added as a network access device in a Cisco ISE that is being used for 802 1X authentications? (Choose two)

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

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

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

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

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

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

Answer: AC

NEW QUESTION 150
A customer wants to set up the Sponsor portal and delegate the authentication flow to a third party for added security while using Kerberos Which database should be used to accomplish this goal?

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

Answer: B

Explanation:

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

NEW QUESTION 155
What must be configured on the Cisco ISE authentication policy for unknown MAC addresses/identities for successful authentication?

A. pass
B. reject
C. drop
D. continue

Answer: D

Explanation:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_id_stores.html

NEW QUESTION 159
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 162
Which three default endpoint identity groups does cisco ISE create? (Choose three)

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

Answer: ADE

Explanation:
Default Endpoint Identity Groups Created for Endpoints
Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide

NEW QUESTION 167
An administrator is attempting to replace the built-in self-signed certificates on a Cisco ISE appliance. The CA is requesting some information about the appliance in order to sign the new certificate. What must be done in order to provide the CA this information?

A. Install the Root CA and intermediate CA.
B. Generate the CSR.
C. Download the intermediate server certificate.
D. Download the CA server certificate.

Answer: B

NEW QUESTION 168
A network administrator is configuring authorization policies on Cisco ISE There is a requirement to use AD group assignments to control access to network resources After a recent power failure and Cisco ISE rebooting itself, the AD group assignments no longer work What is the cause of this issue?

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

Answer: A

Explanation:

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

NEW QUESTION 173

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.

	PEAP-MSCHAPv2
uses username and password for authentication	
uses certificates for authentication	
changes credentials through the admin portal	
supports fragmentation after the tunnel is established	PEAP-EAP-TLS
uses the X.509 format	
supports auto-enrollment for obtaining credentials	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

PEAP-MSCHAPv2
- uses username and password for authentication
- changes credentials through the admin portal
- supports fragmentation after the tunnel is established

PEAP-EAP-TLS
- uses certificates for authentication
- uses the X.509 format
- supports auto-enrollment for obtaining credentials

NEW QUESTION 175
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.

	TACACS+
combines authentication and authorization	
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 180
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 185
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 186
An engineer is unable to use SSH to connect to a switch after adding the required CLI commands to the device to enable TACACS+. The device administration license has been added to Cisco ISE, and the required policies have been created. Which action is needed to enable access to the switch?

A. The ip ssh source-interface command needs to be set on the switch
B. 802.1X authentication needs to be configured on the switch.
C. The RSA keypair used for SSH must be regenerated after enabling TACACS+.
D. The switch needs to be added as a network device in Cisco ISE and set to use TACACS+.

Answer: D

NEW QUESTION 187
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 188
An administrator has added a new Cisco ISE PSN to their distributed deployment. Which two features must the administrator enable to accept authentication requests and profile the endpoints correctly, and add them to their respective endpoint identity groups? (Choose two)

A. Session Services
B. Endpoint Attribute Filter
C. Posture Services
D. Profiling Services
E. Radius Service

Answer: DE

NEW QUESTION 190
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 191
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 192
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 ot 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 197
What are the minimum requirements for deploying the Automatic Failover feature on Administration nodes in a distributed Cisco ISE deployment?

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

Answer: D

NEW QUESTION 202
An organization is adding nodes to their Cisco ISE deployment and has two nodes designated as primary and secondary PAN and MnT nodes. The organization also has four PSNs An administrator is adding two more PSNs to this deployment but is having problems adding one of them What is the problem?

A. The new nodes must be set to primary prior to being added to the deployment
B. The current PAN is only able to track a max of four nodes
C. Only five PSNs are allowed to be in the Cisco ISE cube if configured this way.
D. One of the new nodes must be designated as a pxGrid node

Answer: C

NEW QUESTION 203
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 205
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 206
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 211
In which two ways can users and endpoints be classified for TrustSec? (Choose Two.)

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

Answer: AE

NEW QUESTION 215
Which two task types are included in the Cisco ISE common tasks support for TACACS+ profiles? (Choose two.)

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

Answer: BE

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

NEW QUESTION 217
An administrator is configuring posture with Cisco ISE and wants to check that specific services are present on the workstations that are attempting to access the network. What must be configured to accomplish this goal?

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

Answer: D

NEW QUESTION 222
......

Relate Links

100% Pass Your 300-715 Exam with Exambible Prep Materials

https://www.exambible.com/300-715-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/