

Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)



NEW QUESTION 1

Refer to the exhibit.

```
Switch(config)# gigabitEthernet 1/0/2
Switch(config)# authentication port-control auto
Switch(config)# authentication host-mode multi-auth
```

In which scenario does this switch configuration apply?

- A. when allowing a hub with multiple clients connected
- B. when passing IP phone authentication
- C. when allowing multiple IP phones to be connected
- D. when preventing users with hypervisor

Answer: A

Explanation:

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

NEW QUESTION 2

Which protocol must be allowed for a BYOD device to access the BYOD portal?

- A. HTTP
- B. SMTP
- C. HTTPS
- D. SSH

Answer: C

NEW QUESTION 3

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 4

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 DHCP probe for Cisco ISE is not working as expected.
- B. The 802.1 X timeout period is too long.
- C. The endpoint is using the wrong protocol to authenticate with Cisco ISE.
- D. An AC I on the port is blocking HTTP traffic

Answer: B

NEW QUESTION 5

An administrator needs to give the same level of access to the network devices when users are logging into them using TACACS+. However, the administrator must restrict certain commands based on one of three user roles that require different commands. How is this accomplished without creating too many objects using Cisco ISE?

- A. Create one shell profile and multiple command sets.
- B. Create multiple shell profiles and multiple command sets.
- C. Create one shell profile and one command set.
- D. Create multiple shell profiles and one command set

Answer: A

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](https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide.html)
https://www.youtube.com/watch?v=llZwB71Szog&ab_channel=JasonMaynard

NEW QUESTION 6

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 7

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 8

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

Explanation:

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 9

An engineer needs to configure a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes. Which option must be selected in the Subject Alternative Name field?

- A. Common Name and GUID
- B. MAC Address and GUID
- C. Distinguished Name
- D. Common Name

Answer: B

Explanation:

The engineer needs to select the option of MAC Address and GUID in the Subject Alternative Name field when configuring a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes.

NEW QUESTION 10

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 11

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

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

Answer: DE

NEW QUESTION 12

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 rewall condition to check for any vendor rewall application.
- D. Enable the default application condition to identify the applications installed and valide the rewall app.

Answer: C

Explanation:

https://www.youtube.com/watch?v=6Kj8P8Hn7dY&t=109s&ab_channel=CiscoISE-IdentityServicesEngine

NEW QUESTION 13

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 14

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 15

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

Explanation:

https://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs/policy_defined_segmentation_with_tr (slide 25)

NEW QUESTION 16

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 17

An engineer is using the low-impact mode for a phased deployment of Cisco ISE and is trying to connect to the network prior to authentication. Which access will be denied in this?

- A. HTTP
- B. DNS
- C. EAP
- D. DHCP

Answer: A

NEW QUESTION 18

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 19

A Cisco ISE server sends a CoA to a NAD after a user logs in successfully using CWA Which action does the CoA perform?

- A. It terminates the client session
- B. It applies the downloadable ACL provided in the CoA
- C. It applies new permissions provided in the CoA to the client session.
- D. It triggers the NAD to reauthenticate the client

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/113362-config-web-auth-ise-00.ht>

NEW QUESTION 20

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

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

Answer: A

NEW QUESTION 21

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

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

Answer: C

NEW QUESTION 22

Which two features are available when the primary admin node is down and the secondary admin node has not been promoted? (Choose two.)

- A. hotspot
- B. new AD user 802 1X authentication
- C. posture
- D. BYOD
- E. guest AUP

Answer: BC

NEW QUESTION 23

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. Authenticate the user's system to the secondary Cisco ISE node and move this user to the primary with the renewed certificate.
- B. Connect this system as a guest user and then redirect the web auth protocol to log in to the network.
- 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: A

NEW QUESTION 24

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

- A. LDAP
- B. 802 1X
- C. Certificate-based
- D. LOCAL
- E. MAC based

Answer: DE

NEW QUESTION 25

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

300-715 Practice Exam Features:

- * 300-715 Questions and Answers Updated Frequently
- * 300-715 Practice Questions Verified by Expert Senior Certified Staff
- * 300-715 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 300-715 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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