300-715 Q&As

Implementing and Configuring Cisco Identity Services Engine (SISE)

Pass Cisco 300-715 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/300-715.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which interface-level command is needed to turn on 802 1X authentication?

A. Dot1x pae authenticator

B. dot1x system-auth-control

C. authentication host-mode single-host

D. aaa server radius dynamic-author

Correct Answer: A

QUESTION 2

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

Correct Answer: BE

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+ ProfileTACACS+ 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:

1.

Common tasks

2.

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:

1.

Shell

2.

WLC

3.

Nexus

4.

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.

QUESTION 3

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. Allow authentication for expired certificates within the EAP-TLS section under the allowed protocols.

C. Add a certificate issue from the CA server, revoke the expired certificate, and add the new certificate in system.

D. Authenticate the user\\'s system to the secondary Cisco ISE node and move this user to the primary with the renewed certificate.

Correct Answer: D

QUESTION 4

What sends the redirect ACL that is configured in the authorization profile back to the Cisco WLC?

A. Cisco-av-pair

B. Class attribute

C. Event

D. State attribute

Correct Answer: A

QUESTION 5

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

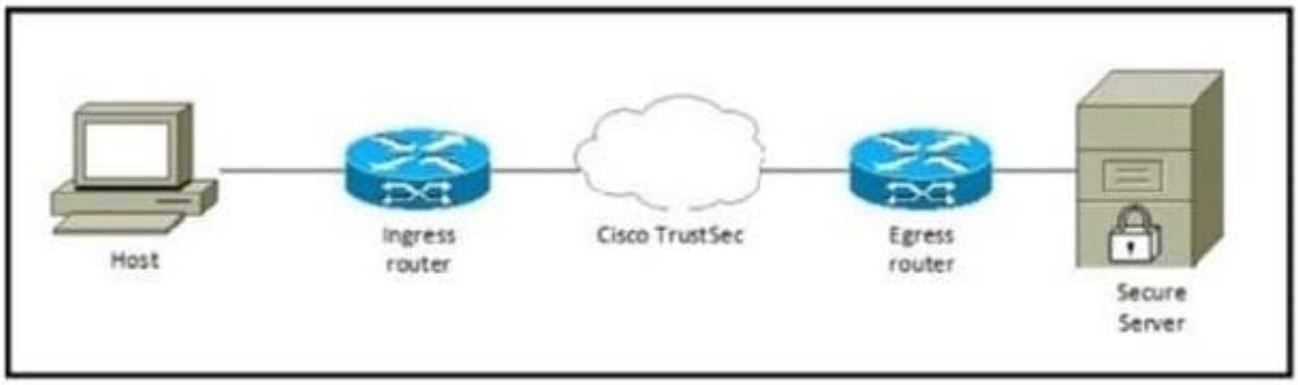
Correct Answer: D

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.

QUESTION 6

Refer to the exhibit.



Which component must be configured to apply the SGACL?

A. egress router

B. host

C. secure server

D. ingress router

Correct Answer: A

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

QUESTION 7

Which port does Cisco ISE use for native supplicant provisioning of a Windows laptop?

A. TCP 8909

B. TCP 8905

C. CUDP 1812

D. TCP 443

Correct Answer: B

QUESTION 8

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

A. The switch port is configured with authentication event server dead action authorize vlan.

B. The authorization results for the endpoints include a dACL allowing access.

C. The authorization results for the endpoints include the Trusted security group tag.

D. The switch port is configured with authentication open.

Correct Answer: D

QUESTION 9

Which of these is not a method to obtain Cisco ISE profiling data?

A. RADIUS

B. HTTP

C. SNMP query

D. active scans

E. Netflow

F. DNS

Correct Answer: D

QUESTION 10

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.

Correct Answer: D

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.)

QUESTION 11

Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. endpoint marked as lost in My Devices Portal

B. addition of endpoint to My Devices Portal

C. endpoint profile transition from Apple-Device to Apple-iPhone

D. endpoint profile transition from Unknown to Windows 10-Workstation

E. updating of endpoint dACL.

Correct Answer: CD

QUESTION 12

Which default endpoint identity group does an endpoint that does not match any profile in Cisco ISE become a member of?

A. Endpoint

B. unknown

C. blacklist

D. white list

E. profiled

Correct Answer: B

If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_identities.html

QUESTION 13

By default, which traffic does an 802.IX-enabled switch allow before authentication?

A. all traffic

B. no traffic

C. traffic permitted in the port dACL on Cisco ISE

D. traffic permitted in the default ACL on the switch

Correct Answer: D

QUESTION 14

An administrator adds a new network device to the Cisco ISE configuration to authenticate endpoints to the network. The RADIUS test fails after the administrator configures all of the settings in Cisco ISE and adds the proper configurations to the switch.

What is the issue?

A. The endpoint profile is showing as \\'\\'unknown"

B. The endpoint does not have the appropriate credentials for network access

C. The certificate on the switch is self-signed, not a CA-provided certificate

D. The shared secret is incorrect on the switch or on Cisco ISE

Correct Answer: B

QUESTION 15

What are the three default behaviors of Cisco ISE with respect to authentication, when a user connects to a switch that is configured for 802.1X, MAB, and WebAuth? (Choose three)

A. MAB traffic uses internal endpoints for retrieving identity.

B. Dot1X traffic uses a user-defined identity store for retrieving identity.

C. Unmatched traffic is allowed on the network.

D. Unmatched traffic is dropped because of the Reject/Reject/Drop action that is configured under Options.

E. Dot1 traffic uses internal users for retrieving identity.

Correct Answer: ADE