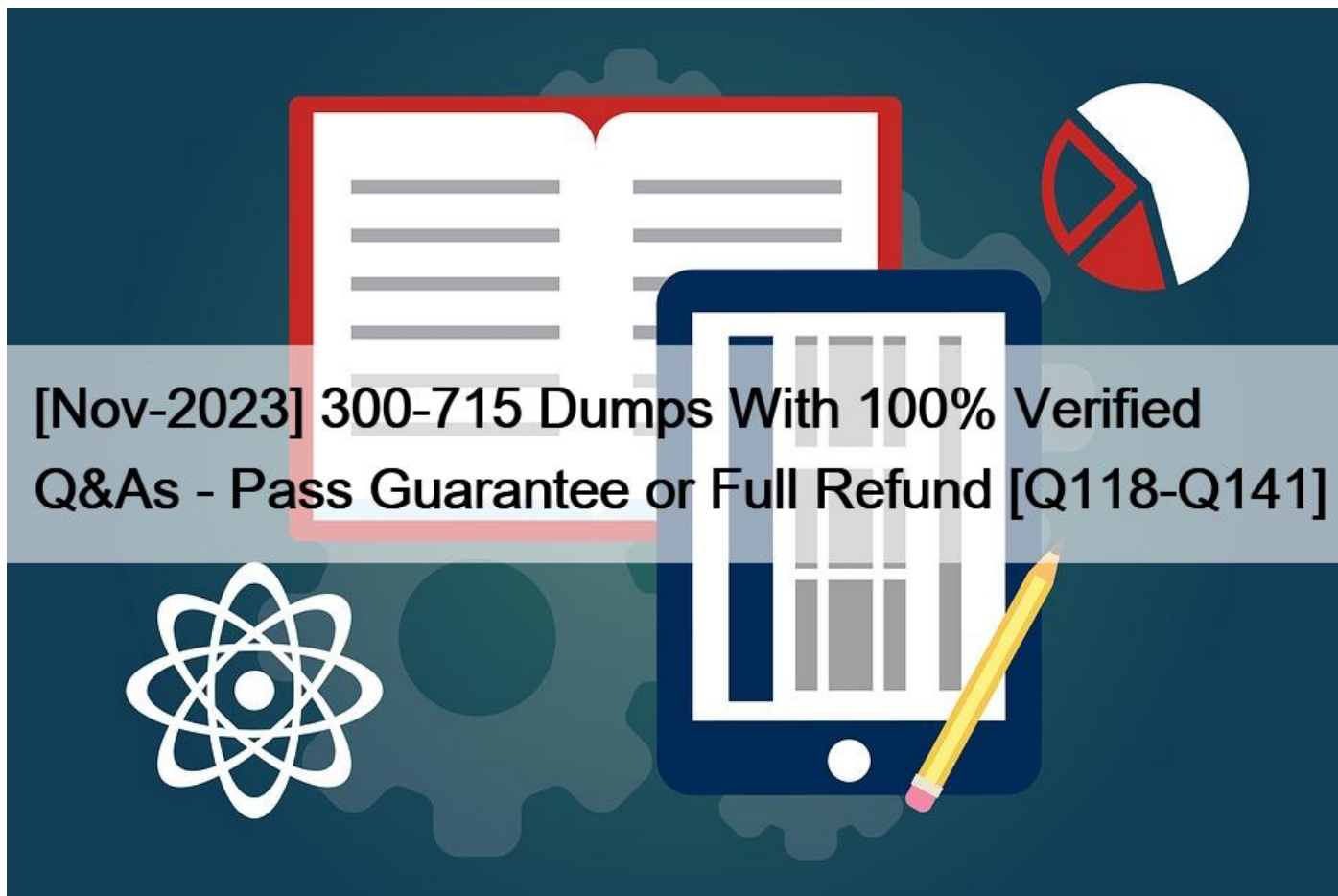


## [Nov-2023 300-715 Dumps With 100% Verified Q&As - Pass Guarantee or Full Refund [Q118-Q141]



[Nov-2023] 300-715 Dumps With 100% Verified Q&As - Pass Guarantee or Full Refund  
Pass Cisco 300-715 Exam With Practice Test Questions Dumps Bundle

Cisco 300-715 is a qualifying and concentration test for the CCNP Security certificate. The applicants must pass it along with the core exam to earn this professional-level certification. At the same time, the specialists who ace this test will also obtain the Cisco Certified Specialist ? Security Identity Management Implementation certificate. This exam is designed to evaluate the individuals' knowledge of Cisco Identity Service Engine. The area of coverage includes deployment & architecture, web auth and guest services, profiler, policy enforcement, network access for device administration, BYOD, and endpoint compliance, among others.

Individuals who pass 300-715 exam display a strong understanding of core ISE concepts, such as user authentication, authorization, and accounting (AAA). They can configure and manage policies for wired and wireless endpoints, guest access, and posture services, including endpoint compliance checks. Candidates can also integrate ISE with other security solutions like Cisco Firepower and AnyConnect to enhance the security posture of their organization.

### QUESTION 118

Refer to the exhibit.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A network engineers configuring the switch to accept downloadable ACLs from a Cisco ISE server Which two commands should be run to complete the configuration? (Choose two)

- \* aaa authorization auth-proxy default group radius
- \* radius server vsa sand authentication
- \* radius-server attribute 8 include-in-access-req
- \* ip device tracking
- \* dot1x system-auth-control

#### QUESTION 119

What is the condition that a Cisco ISE authorization policy cannot match?

- \* company contact
- \* custom
- \* time
- \* device type
- \* posture

#### QUESTION 120

Which statement about configuring certificates for BYOD is true?

- \* The SAN field is populated with the end user name.
- \* The CN field is populated with the endpoint host name.
- \* An endpoint certificate is mandatory for the Cisco ISE BYOD.
- \* An Android endpoint uses EST, whereas other operating systems use SCEP for enrollment.

Section: BYOD

#### QUESTION 121

An engineer is configuring web authentication and needs to allow specific protocols to permit DNS traffic.

Which type of access list should be used for this configuration?

- \* extended ACL
- \* reflexive ACL
- \* numbered ACL
- \* standard ACL

Section: Web Auth and Guest Services

#### QUESTION 122

The default Cisco ISE node configuration has which role or roles enabled by default?

- \* Administration only
- \* Inline Posture only
- \* Administration and Pokey Service
- \* Policy Service Monitoring, and Administration

### QUESTION 123

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

- \* Endpoint
- \* unknown
- \* blacklist
- \* white list
- \* profiled

Explanation

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

### QUESTION 124

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

- \* Device Administration License
- \* Server Sequence
- \* Command Sets
- \* Device Admin Service
- \* External TACACS Servers

### QUESTION 125

What allows an endpoint to obtain a digital certificate from Cisco ISE during a BYOD flow?

- \* Application Visibility and Control
- \* Supplicant Provisioning Wizard
- \* My Devices Portal
- \* Network Access Control

Section: BYOD

### QUESTION 126

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

- \* addition of endpoint to My Devices Portal
- \* endpoint marked as lost in My Devices Portal
- \* updating of endpoint dACL
- \* endpoint profile transition from Apple-device to Apple-iPhone
- \* endpoint profile transition from Unknown to Windows10-Workstation

Section: Profiler

### QUESTION 127

Which statement is not correct about the Cisco ISE Monitoring node?

- \* The local collector agent collects logs locally from itself and from any NAD that is configured to send logs to the Policy Service node.
- \* Cisco ISE supports distributed log collection across all nodes to optimize local data collection, aggregation, and centralized correlation and storage.
- \* The local collector agent process runs only the Inline Posture node.
- \* The local collector buffers transport the collected data to designated Cisco ISE Monitoring nodes as syslog; once Monitoring nodes are globally defined via Administration, ISE nodes automatically send logs to one or both of the configured Monitoring nodes.

### QUESTION 128

An administrator is configuring RADIUS on a Cisco switch with a key set to Cisc403012128 but is receiving the error `Authentication failed: 22040 Wrong password or invalid shared secret.` what must be done to address this issue?

- \* Add the network device as a NAD inside Cisco ISE using the existing key.
- \* Configure the key on the Cisco ISE instead of the Cisco switch.
- \* Use a key that is between eight and ten characters.
- \* Validate that the key is correct on both the Cisco switch as well as Cisco ISE.

### QUESTION 129

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

- \* the minimum number that a predefined condition provides
- \* the maximum number that a predefined condition provides
- \* the minimum number that a device certainty factor must reach to become a member of the profile
- \* the maximum number that a device certainty factor must reach to become a member of the profile

### QUESTION 130

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?

- \* one primary admin and one secondary admin node in the deployment
- \* one policy services node and one secondary admin node
- \* one policy services node and one monitoring and troubleshooting node
- \* one primary admin node and one monitoring and troubleshooting node

### QUESTION 131

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)



C)



D)



- \* Option A
- \* Option B
- \* Option C
- \* Option D

### QUESTION 132

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

- \* hotspot
- \* new AD user 802 1X authentication
- \* posture

- \* BYOD
- \* guest AUP

### QUESTION 133

What is a requirement for Feed Service to work?

- \* TCP port 3080 must be opened between Cisco ISE and the feed server
- \* Cisco ISE has a base license.
- \* Cisco ISE has access to an internal server to download feed update
- \* Cisco ISE has Internet access to download feed update

### QUESTION 134

An organization is migrating its current guest network to Cisco ISE and has 1000 guest users in the current database. There are no resources to enter this information into the Cisco ISE database manually. What must be done to accomplish this task efficiently?

- \* Use a CSV file to import the guest accounts
- \* Use SQL to link the existing database to Cisco ISE
- \* Use a JSON file to automate the migration of guest accounts
- \* Use an XML file to change the existing format to match that of Cisco ISE

[https://www.youtube.com/watch?v=DNYaFI-8zWk&ab\\_channel=CiscoISE-IdentityServicesEngine](https://www.youtube.com/watch?v=DNYaFI-8zWk&ab_channel=CiscoISE-IdentityServicesEngine)

### QUESTION 135

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?

- \* Client Provisioning
- \* Guest
- \* BYOD
- \* Blacklist

Explanation

[https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless\\_Networks/Unified\\_Access/BYOD\\_Design/The\\_Blacklist\\_identity\\_group\\_is\\_system\\_generated\\_and\\_maintained\\_by\\_ISE\\_to\\_prevent\\_access\\_to\\_lost\\_or\\_stolen\\_devices.html](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design/The_Blacklist_identity_group_is_system_generated_and_maintained_by_ISE_to_prevent_access_to_lost_or_stolen_devices.html) 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

### QUESTION 136

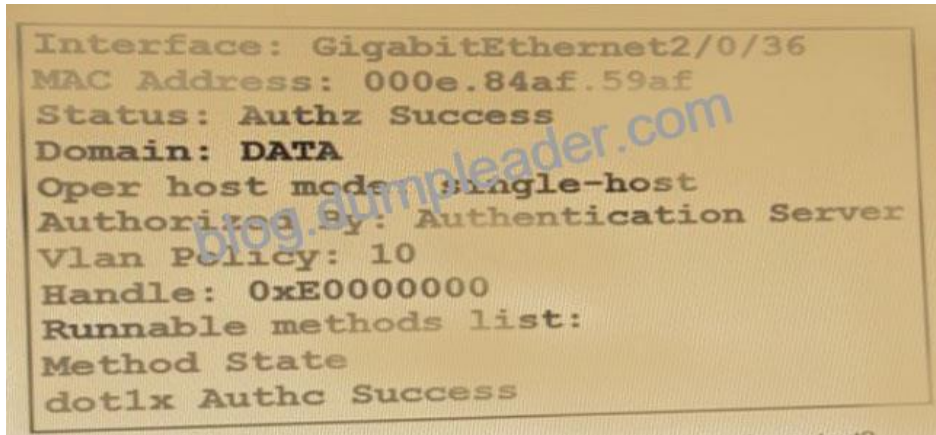
A user changes the status of a device to stolen in the My Devices Portal of Cisco ISE. The device was originally onboarded in the BYOD wireless Portal without a certificate. The device is found later, but the user cannot re-onboard the device because Cisco ISE assigned the device to the Blacklist endpoint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

- \* Manually remove the device from the Blacklist endpoint identity group.
- \* Change the device state from Stolen to Not Registered.
- \* Change the BYOD registration attribute of the device to None.
- \* Delete the device, and then re-add the device.

### QUESTION 137



Refer to the exhibit:



Which command is typed within the CU of a switch to view the troubleshooting output?

- \* show authentication sessions mac 000e.84af.59af details
- \* show authentication registrations
- \* show authentication interface gigabitethemet2/0/36
- \* show authentication sessions method

### QUESTION 138

Select and Place

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



### QUESTION 139

An engineer is enabling a newly configured wireless SSID for tablets and needs visibility into which other types of devices are connecting to it. What must be done on the Cisco WLC to provide this information to Cisco ISE9

- \* enable IP Device Tracking
- \* enable MAC filtering
- \* enable Fast Transition
- \* enable mDNS snooping

### QUESTION 140

Client provisioning resources can be added into the Cisco ISE Administration node from which three of these? (Choose three.)

- \* FTP
- \* TFTP
- \* www-cisco.com
- \* local disk
- \* Posture Agent Profile

### QUESTION 141

Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)

- \* The device queries the internal identity store
- \* The Cisco ISE server queries the internal identity store
- \* The device queries the external identity store
- \* The Cisco ISE server queries the external identity store.
- \* The device queries the Cisco ISE authorization server

**2023 Valid 300-715 test answers & Cisco Exam PDF:** [https://www.dumpleader.com/300-715\\_exam.html](https://www.dumpleader.com/300-715_exam.html)