



**Free Questions for 350-401 by certsinside**

**Shared by Riddle on 29-01-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

Question Type: MultipleChoice

---

Refer to the Exhibit.

```
Script

import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', password='test123!',
    allow_agent=False) as m:
    print(m.get_config('running').data_xml)

Output

$ python get_config.py
Traceback (most recent call last):
  File "get_config.py", line 3, in <module>
    with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
AttributeError: 'module' object has no attribute 'manager'
```

Refer to the Exhibit. Running the script causes the output in the exhibit. What should be the first line of the script?

**Options:**

---

**A-** from ncclient import manager

B- import manager

C- from ncclient import \*

D- ncclient manager import

**Answer:**

---

C

## Question 2

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

```
aaa new-model
aaa authentication login default group tacacs+ local
!
tacacs server prod
address ipv4 10.10.10.23
key cisco123
!
ip tacacs source-interface Gig 0/0
```

Which configuration must be applied for the TACACS+ server to grant access-level rights to remote users?

**Options:**

---

- A- R1(config)# aaa authentication login enable
- B- R1(config)# aaa authorization exec default local if-authenticated
- C- R1(config)# aaa authorization exec default group tacacs+
- D- R1(config)# aaa accounting commands 15 default start-stop group tacacs+

**Answer:**

---

C

**Explanation:**

---

The `aaa authorization exec default group tacacs+` command enables TACACS+ exec authorization, which allows the TACACS+ server to grant access-level rights to remote users. Exec authorization determines whether the user can access the privileged EXEC mode or remain in user EXEC mode after authentication. The TACACS+ server can also assign a privilege level to the user based on the configuration of the server. The default keyword specifies that this is the default method list for exec authorization. The `group tacacs+` keyword specifies that the TACACS+ server group defined by the `tacacs server` command is used for authorization.

## Question 3

---

### Question Type: MultipleChoice

---

An engineer must construct an access list for a Cisco Catalyst 9800 Series WLC that will redirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The Cisco ISE servers are hosted at 10.9.11.141 and 10.1.11.141. Which access list meets the requirements?

A)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
70 permit ip any host 10.9.11.141
80 permit ip any host 10.1.11.141
500 permit tcp any any eq www
600 permit tcp any any eq 443
700 permit tcp any any eq 8443
800 deny udp any any eq domain
```

B)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
70 permit ip any host 10.9.11.141
80 permit ip any host 10.1.11.141
500 deny tcp any any eq www
600 deny tcp any any eq 443
700 deny tcp any any eq 8443
800 deny udp any any eq domain
901 deny ip any any
```

C)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
70 deny ip any host 10.9.11.141
80 deny ip any host 10.1.11.141
500 permit tcp any any eq www
600 permit tcp any any eq 443
700 permit tcp any any eq 8443
800 deny udp any any eq domain
```

D)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
50 deny ip host 10.9.11.141 any
60 deny ip any host 10.9.11.141
70 deny ip host 10.1.11.141 any
80 deny ip any host 10.1.11.141
500 permit tcp any any eq www
600 permit tcp any any eq 443
700 permit tcp any any eq 80
```

**Options:**

---

- A- Option
- B- Option
- C- Option
- D- Option

**Answer:**

---

D

**Explanation:**

---

Option D is the correct access list to redirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The configuration steps are as follows<sup>12</sup>:

Define an extended access list that permits TCP traffic from any source to the Cisco ISE servers on port 80 (HTTP) and port 443 (HTTPS). In this case, the access list is named `ACL_WEBAUTH_REDIRECT` and it allows any host to connect to the IP addresses 10.9.11.141 and 10.1.11.141 on port 80 and port 443: `ip access-list extended ACL_WEBAUTH_REDIRECT` and `permit tcp any host 10.9.11.141 eq 80`, `permit tcp any host 10.9.11.141 eq 443`, `permit tcp any host 10.1.11.141 eq 80`, `permit tcp any host 10.1.11.141 eq 443`.

Apply the access list to the guest WLAN using the `ip access-group` command. This command filters the traffic on the interface based on the access list. In this case, the access list `ACL_WEBAUTH_REDIRECT` is applied to the guest WLAN interface in the inbound direction, which means that only the traffic that matches the access list can enter the interface: `interface wlan-guest` and `ip access-group ACL_WEBAUTH_REDIRECT in`.

Option A is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 80, which is required for HTTP redirection. Without this, the guest users will not be able to see the splash page on their web browsers<sup>12</sup>.

Option B is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 443, which is required for HTTPS redirection. Without this, the guest users will not be able to see the splash page on their web browsers if they use HTTPS<sup>12</sup>.

Option C is incorrect because it permits TCP traffic from any source to any destination on port 80 and port 443, which is too broad and may allow unwanted traffic to enter the guest WLAN interface. This may compromise the security and performance of the guest network<sup>12</sup>. Reference: 1: Configuring Web Authentication, 2: ISE and Catalyst 9800 Series Integration Guide

## Question 4

---



**Question Type: MultipleChoice**

---

Which Cisco DNA Center application is responsible for group-based access control permissions?

**Options:**

---

- A- Provision
- B- Design
- C- Policy
- D- Assurance

**Answer:**

---

C

## Question 5

---

**Question Type: MultipleChoice**

---

In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

**Options:**

---

A- EIRP

B- RSSI

C- SNR

D- bBi

**Answer:**

---

A

## Question 6

---

**Question Type: MultipleChoice**

---

A script contains the statement "while loop != 999:" Which value terminates the loop?

**Options:**

---

- A- A value equal to 999.
- B- A value less than or equal to 999.
- C- A value not equal to 999.
- D- A value greater than or equal to 999.

**Answer:**

---

A

## Question 7

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.



A client requests a new SSID that will use web-based authentication and external RADIUS servers. Which Layer 2 security mode must be selected?

**Options:**

---

- A- WPA + WPA2
- B- WPA2 + WPA3
- C- Static WEP
- D- None

**Answer:**

---

A

## Question 8

---

**Question Type: DragDrop**

---

An engineer plans to use Python to convert text files that contain device information to JSON. Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.

Answer:

```
import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']
```

```
l = 1
for line in text:
    description = list(line.strip().split(None, 4))
    print(description)
    Device_Number = 'Device' + str(l)
    i = 0
    dictionary_2 = {}
    while i < len(fields):
        dictionary_2[fields[i]] = description[i]
        i = i + 1
    dictionary_1[Device_Number] = dictionary_2
    l = l + 1
```

```
json.dump(dictionary_1, out_file, indent=4)
```

### Output of Python Code

```
switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3
```

### raw-data.txt

```
{
  "Device1": {
    "Device_type": "switch",
    "IOS_type": "ios",
    "IP_Address": "10.1.1.1",
    "Username": "user1",
    "Password": "pass1"
  },
  "Device2": {
    "Device_type": "router",
    "IOS_type": "ios-xr",
    "IP_Address": "10.1.1.2",
    "Username": "user2",
    "Password": "pass2"
  },
  "Device3": {
    "Device_type": "nexus-9k",
    "IOS_type": "nx-os",
    "IP_Address": "10.1.1.3",
    "Username": "user3",
    "Password": "pass3"
  }
}
```

```
out_file.close() out.json", "w")
```

```
with open(input_file) as text:
```

```
out_file = open ("Json-Output.json", "w")
```

```
with open(input_file) as text:
```

**To Get Premium Files for 350-401 Visit**

**<https://www.p2pexams.com/products/350-401>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/cisco/pdf/350-401>**

